THE FINTECH EDITION 2018

FinTecHub

Queen Mary University of London
Centre for Commercial Law Studies

Simmons & Simmons

Contents

The FinTech Edition

2018

Published by
FinTecHub
London, 2018

Editor-in-Chief
Professor, Dr George A Walker

Assistant Editors
LLB, LLM Jin Enyi
BA, JD Jean René Santiago Cruz

FinTecHub@outlook.com

Issue 1, 2018

Published in London

Preface
Abstracts 1 & 2
Simmons & Simmons
Abstracts 3 & 4
Hyperfinance
Abstracts 5 & 6
Elsa
Abstracts 7 & 8
Queen Mary University of London
Simmons & Simmons Graduate Law Opportunities
Selected Papers

SMART CONTRACTS UNDER SWISS LAW
Dr Christian Schönfeld LLB, MA in Law and Economics, LLM (Lon)

BLOCKCHAIN IMPLICATIONS FOR LAND REFORM IN UKRAINE – LESSONS FOR INTERNATIONAL BUSINESS
LLB, MBA, LLM (Lon) Anastasia Demchuk

THE LEGAL NATURE OF BITCOIN AND ALTCOINS
LLM (Glas), Khalid Almlegi

BLOCKCHAIN-BASED DIGITAL COMMERCIAL BILLS: ADVANTAGES AND LEGAL CHALLENGES
LLB, LLM (Lon), Amelie Shuhui Ruan

THE SHIFT TO A DERIVATIVES MARKETS IN FINTECH
LLB, LLM (Lon), MSc(Auth), Eleni Samara

Preface

Professor
George A Walker
Editor-in-Chief

We would like to welcome you to the inaugural copy of The FinTech Edition. The FinTech Edition is a dedicated online academic and professional research journal focusing on the latest developments in the Law of Financial Technology (FinTech) and associated Regulatory Technology (RegTech).

This is an exciting and powerful area of change and development. FinTech is predicted to have a fundamental impact on the structure and operation of all types of financial markets. The full extent of actual disruption that may follow remains unclear at this time. Although, it has to be expected that this will result in fundamental change to many traditional aspects of banking and financial services markets structure and product and service delivery.

New Digital Economies and Digital Societies are being created across the world, which are essentially based on integrated forms of digital information and data management and exchange. This will impact many areas, including artificial intelligence (AI), virtual reality (VR), Big Data analytics, robotic (and bot) technology, biotechnology, and nanotechnology.

Big Tech companies will come together with traditional banking, securities and insurance firms, and now new FinTech start-ups and platforms in this highly competitive arena. New digital ecosystems are being created based on distributed ledger and blockchain technology, decentralisation and distribution, automation and smart function, and with the digitalisation, disintermediation, dematerialisation, mobilisation and personalisation of financial operations and facilities.

All of this has created substantial new questions and challenges in terms of legal definition, application and treatment. A whole area of new digital financial law is emerging to fill this gap as lawyers in all fields are forced to deal with the new issues created. It is hoped that the research undertaken and results produced with The FinTech Edition will assist with this process.

The articles included in the inaugural edition are selected from the best of the research papers written by exceptionally bright young Master of Law (LLM) degree students during 2016-2017. A large number of students elected to work in the areas of FinTech and RegTech with a substantial field of highly original and high-quality pieces of work being produced. All of the candidates concerned are to be congratulated on the quality of the work undertaken and their academic and professional endeavour and output.

The specific subjects covered in this edition are expected to be just that first with a large number of other follow-up pieces expected.

We thank all of the candidates involved and their supervisors for this first edition. We are also very grateful to all of the partners and senior associates from Simmons & Simmons who assisted candidates as part of our ground-breaking Student Support Programme. We must also thank the members of our dedicated internal team, including specifically Jin Enyi.

We can finally only welcome you, the reader, again to these pages and hope that the journal provides you with some insight and inspiration in relation to the changes unfolding in this highly exciting new area of legal and technological development and advance. The future is in these pages.

Abstracts

1

THE LEGAL NATURE OF BITCOIN AND ALTCOINS

LLM (Glas), Khalid Almelegi

For the full paper, please contact:
Khalidmelegi@gmail.com

There are currently over 1400 cryptocurrencies in circulation. The most infamous of these is Bitcoin. Since its creation in 2008, Bitcoin has attracted investors around the globe. The novel feature of cryptocurrencies is its underlying blockchain technology. Blockchains have the potential to change how financial systems and markets function.

Applications such as 'smart contracts' on the Ethereum platform benefit from blockchains. Smart contracts are contracts that self-execute without intermediaries. Furthermore, these platforms can run Decentralised Autonomous Organisations (DAOs), business organisations that operate entirely through smart contracts. Blockchains may also ease payments across different networks or ledgers, with inter-ledger protocols offering greater system connectivity.

Although FinTech offers many advantages, it also has disadvantages owing to its unprecedented nature. Specifically, legal ambiguity, cybersecurity risks, monetary policy risk, and systemic risk pose a significant challenge to FinTech's development. Greater technology dependence naturally means greater technology risk.

2

DEVELOPING FINTECH REGULATORY SANDBOX – A BALANCE BETWEEN INNOVATION AND DISRUPTION IN FINANCIAL MARKETS

LLB, LLM (Lon), Le Dan Yen Ngoc

For the full paper, please contact:
yen.ngoc.ld@gmail.com

The growth of technology applications in financial services (FinTech), coupled with technical concepts such as blockchain, distributed ledgers, and cryptocurrencies, has urged the development of 'regulatory sandboxes'.

Regulatory sandboxes are pilot schemes that allow the testing of innovative FinTech products and services under regulatory supervision with an aim to minimise detrimental impact on consumers and financial instability. In 2016, the United Kingdom launched the world's first regulatory sandbox, sparking change within the global FinTech industry.

This paper explores the key attributes of regulatory sandboxes, and it analyses the benefits and the current challenges they face. Finally, the paper conducts a comparative analysis of the regulatory sandbox models that different jurisdictions have adopted. Thereafter, it presents constructive policy prescriptions to develop more comprehensive regulatory sandbox models, in order to ensure that regulatory schemes protect societal stakeholders without stifling the development of FinTech.

Simmons & Simmons

From our offices in major business and financial centres throughout Europe, the Middle East and Asia, we view the world through the lens of our key sectors: Financial Institutions, Asset Management and Investment Funds and TMT and Life Sciences.

Since its emergence into the mainstream over the last few years, the FinTech sector has captured the interest and imagination of entrepreneurs, investors, governments and regulators, not to mention incumbent financial institutions and asset managers. The disruptive technologies and business models that lie at the heart of the FinTech revolution often raise a range of novel legal and regulatory issues.

The FinTech sector sits at the confluence of three of the four industry sectors on which Simmons & Simmons focuses, allowing us to combine our industry experience with our specialist legal expertise, to create a market leading FinTech team. We advise clients operating across the sector, from start-ups to some of the biggest names in the industry. We also advise businesses partnering with or investing in FinTech firms as well as financial institutions and asset managers developing their own FinTech products and services.

Our team is ranked in Band 1 in Legal 500 UK and was also awarded Islamic Finance News' 2017 IFN Law Award for FinTech.

The Simmons & Simmons FinTech Fund

As a result of our experience of working with businesses across the industry, we understand how difficult it can be for early-stage FinTech businesses to obtain expert legal advice. We also understand how crucially important receiving the right kind of advice can be to the long-term prospects of those businesses. This led to us launching a dedicated £100,000 fund in May 2016 to help promising FinTech start-ups solve the challenging legal or regulatory problems that could otherwise slow down their development or, in some cases, prevent them from getting off the ground altogether. This was the first fund of its kind offered in the legal industry in the UK.

More information our FinTech team is available at www.simmons-simmons.com/fintech.

Key contacts

Angus McLean
Partner
T +44 20 7825 4142
E angus.mclean@simmons-simmons.com

Penny Miller
Financial Services Regulatory Partner
T +44 207 825 4827
E penny.miller@simmons-simmons.com

simmons-simmons.com
elexica.com
@SimmonsLLP

Abstracts

3

FINTECH IN THE SERVICE OF LOANS IN THE UK

LLB (Auth), LLM (Lon), Filippos Papas

For the full paper, please contact:
papas5607@gmail.com

Following the Great Recession of 2008, the ensuing distress on the world's financial sector resulted in a liquidity crunch, which meant that banks were less able and willing to extend loans to individuals. As more and more people found themselves excluded from traditional sources of financing, financial technology (FinTech) emerged as a new avenue for credit, which also touted more agile and effective services. This paper tracks the history of FinTech's rise from the ashes of the Great Recession, describes its potential for transforming the financial sector, analyses the particular challenges it presents to regulators, and presents recommendations for relevant stakeholders to ensure the burgeoning industry's longevity.

Firstly, the paper describes the financial crisis of 2008, and how the resulting public outrage towards the banks, and consequent liquidity crunch from the banks' weak finances, spurred the evolution of FinTech. Thereafter, we will describe how Fintech is used for the facilitation and improvement of financial activities, focusing on the peer to peer lending industry. In Chapter 3, the paper describes the Financial Conduct Authority's balancing act to ensure stability in the financial markets and avoid stagnating the alternative market for finance at the same time. The paper concludes by considering rules to be implemented in 2017 and 2018, which promise to be transformative years for the financial industry.

4

LEGAL IMPLICATIONS OF FINANCIAL TECHNOLOGY – BLOCKCHAIN AND SMART CONTRACTS

LLB, LLM, LLM (Glas), Niels von Ahn

For the full paper, please contact:
nvonahn@t-online.de

Innovative financial technology (FinTech) can potentially enhance competition, create new business opportunities and reshape global markets. The paper analyses two of the fundamental instruments thereof: blockchain technology and smart contracts.

Although smart contracts are covered under contract law, it is clear that the far-reaching impacts of FinTech are insufficiently addressed by the existing legal framework. A new doctrine of constructive possession may be necessary to provide legal certainty and protection for virtual property. International private law issues are also a concern, due to blockchains' decentralised nature. Consequently, the 'lex rei sitae'-rule may need reform. This to establish the controlling property law as that of the place where the issuer or holder of the asset-controlling cryptographic key is based. In international transactions, parties should increasingly consider choosing the applicable law, but the current practice of connecting a contract to the location where the service is provided or directed is sufficient.

Finally, smart contract code is currently incapable of replacing law, with social consensus and conventional dispute mechanisms still relevant. Although, a clear tendency towards opting for alternative dispute resolution exists. That tendency, combined with the rise of FinTech, may eventually give rise to widespread use of digital dispute mechanisms.

Simmons & Simmons

HYPERFINANCE

ACCELERATING DIGITAL INNOVATION IN FINANCIAL SERVICES

Innovation is disrupting almost every link in the financial services value chain: from the emergence of automated investment services in wealth management, to the advent of new digitally-enabled business models such as crowdfunding, and increasingly intelligent regulatory software.

'Hyperfinance' is a flagship research programme from Simmons & Simmons which explores the barriers that inhibit banks and asset managers from embracing technology to improve their operational efficiency and customer service, and how the industry's leaders are adapting their innovation strategies to reach hyperspeed.

Are you ready for Hyperfinance?
Read the full findings of our research at hyper-finance.com

#hyperfinance

Abstracts

5

FINTECH AS A CORPORATE CHOICE FOR CORPORA-TIONS, INSPIRED BY LENDING MODELS AND THE UK/EU REGULATORY FRAMEWORK: CHALLENGES AND RISKS

LLB, LLM (Lon), Romina Fernández Flores

For the full paper, please contact:
rom_fdz@hotmail.com

Crowdfunding and peer-to-peer lending (P2P) platforms have enabled quicker, simpler, and — crucially — cheaper access to funding than that offered by traditional lending sources. Market actors are increasingly investing or financing business endeavours through these models.

This paper will review the market background, development and evolution of Fintech, and intro-duces the innovations that financial technology (FinTech) brings to the lending sector. Thereafter, the paper discusses the current regulatory frameworks for crowdfunding and P2P lending in the United Kingdom (UK) and the European Union (EU), and undertakes a comparative analysis of those regulations.

Precisely because of the aggressive growth and continual change of the online alternative finance market, it experiences significant risks. To wit, the paper identifies potential problems with crowdfunding and P2P lending, such as over lending, lack of due diligence, poor credit assessment, and unassessed systemic risk. Finally, it proposes practical recommendations at the national and international levels to prevent a future crisis in this burgeoning industry.

6

THE SHIFT TO A DERIVATIVES MARKETS IN FINTECH

LLB, LLM (Lon), MSc (Auth), Eleni Samara

For the full paper, please contact:
eselenisamara@gmail.com

In the period leading up to the global financial crisis in 2007, the derivatives markets reached USD700trn trillions. In the aftermath of the crisis, the markets were severely criticised for aggravating or causing of the crisis. This was largely due to the markets' complexity, the lack of transparency, and the interconnectedness of market participants. The paper analyses the main characteristics and core obligations of post-crisis regulation such as the Dodd-Frank Act and European Market Infrastructure Regulation (EMIR), the impact of financial technology (FinTech), especially distributed ledger technol-ogy (DLT), and Brexit can have on derivatives markets. The paper concludes that DLT offers a real prospect for the absolute unification and globalisation of derivatives markets. However, cooperation between market players and regulators is indispensable. The United Kingdom's 'regulatory sandbox' example should lead the way globally. It is envisioned that DLT will be an integral part of derivatives markets, as Brexit – given London's significance as global derivatives trade hub - dictate the need for the immediate deployment of a purely global technology.

The European Law Students' Association

QUEEN MARY, UNIVERSITY OF LONDON

The European Law Students' Association (ELSA) is an international, independent, non-political and non-profit making organisation run by and for students and recent graduates, interested in achieving academic and personal excellence in addition to their legal or law-related studies.

ELSA Queen Mary University of London and 300 other local ELSA groups span across 375 European law faculties, consisting of 50,000 members. ELSA QMUL is very active at our university, organising seminars, conferences, lectures, international study visits, as well as organising socials for our members.

Specific ELSA activities include:

Summer Law Schools of one week's duration with 40 hours of academic programme, followed by a social programme. There are 42 different summer law schools covering numerous topics of law such as medical law, business law, IP law, etc. Find out more at: https://lawschools.elsa.org/

Student Trainee Exchange Programme (STEP) gives students the opportunity to obtain international legal work experience. Depending on preference, the schemes last anywhere between 2 weeks to 2 months. The schemes are usually paid or the accommodation for the trainee is provided. Find out more at: https://step.elsa.org/

Moot Court Competitions consisting of EMC2, is a simulated hearing of a WTO dispute settlement and European Human Rights Moot Court Competitions (EHRMCC), pleaded before judges at the European Court of Human Rights. Find out more at: https://emc2.elsa.org/

Delegations are unique opportunities where ELSA delegates are sent to international institutions such as the UN and WTO. The delegates gain insight to the daily work of recognised international organisations and experience drafting of international legal documents first-hand. Find out more: https://delegations.elsa.org/

For more information, please visit www.elsa.org

ELSA QMUL contact
E-mail: elsaqmul@gmail.com
Facebook: fb.com/elsaqmul
Twitter: twitter.com/elsa_qm

Abstracts

7

IS THE CURRENT REGULATORY FRAMEWORK FOR P2P LENDING IN THE UK ADEQUATE?

LLB, LLM (Lon), Krishantini Palaraja

For the full paper, please contact:
krisha.87@gmail.com

Over the past few decades, technological innovations have radically transformed the financial services sector, from the advent of the Automated Teller Machine ("ATM"), electronic payment systems such as credit cards and debit cards, and online banking. The present day is no different, and currently financial technology (FinTech) is spurring a revolution in retail and wholesale payments, investment management, and lending.

Peer-to-peer lending (P2PL), a hybrid of shadow banking and FinTech, is a means of loan origination via internet-based platforms. The rapid growth of the P2PL sector has caught the attention of global financial regulators, who have responded differently to the particular challenges that this new model presents. In the UK, the Financial Conduct Authority (FCA) has devised an entirely new regime for regulating internet loan-based and investment-based crowdfunding platforms.

This paper examines the effectiveness of the UK's current regulatory framework for P2PL in dealing with the risks associated with the sector. In assessing the effectiveness of the regime, we will give increased focus to the risks affecting the investors of P2PL platforms. In doing so, we will analyze the P2PL regulations in the context of the FCA's operational objectives and the FCA's own review of its P2PL regime.

8

BLOCKCHAIN-BASED DIGITAL COMMERCIAL BILLS: ADVANTAGES AND LEGAL CHALLENGES

LLB, LLM (Lon), Amelie Shuhui Ruan

For the full paper, please contact:
shuhui.ruan@yahoo.com

Distributed ledger technology (DLT) initially came to public attention through Bitcoin, the first decentralized cryptocurrency. The rapid development of private cryptocurrencies since then has pushed states to acknowledge digital currency as a regulatory challenge and a competitor to state-issued fiat currency, with many reviewing the viability of central bank issued digital currencies. However, beyond cryptocurrencies, distributed ledgers and the smart contracts it can enable have the potential to improve the efficiency and reliability of financial services, and are thus likely to gradually replace the existing financial infrastructure. China has integrated these two trends towards digital currency and DLT-based financial infrastructure in its pilot project of a digital commercial bill exchange.

This dissertation will thus focus on the legal considerations around blockchain-enabled digital commercial bills. Although the concept has international implications, the paper will focus on the People's Bank of China's pilot project. In Section I, an explanation of China's context and rationale for the implementation of such a pilot project, especially the problems surrounding China's existing commercial bill market will be made. The project itself will be explained in Section II. Subsequently, Section III will examine the potential legal challenges raised by the new transactional paradigm of digital bills. Finally, Section IV will offer suggestions to establish an effective legal and regulatory framework governing the digital commercial bill exchange system that maximizes benefits and minimizes risks.

Queen Mary
University of London

Centre for Commercial Law Studies

Queen Mary University of London, School of Law's World Class Leadership

Member of the Russel Group of leading UK Universities;

Ranked the 37th best university in the world to study law
by the Times Higher Education subject ranking 2018;

Ranked 3rd in the UK and 1st in London in the Guardian University Guide 2018
subject league tables;

and

Scored 91 percent student satisfaction in the
National Student Survey (NSS) 2016.

Queen Mary, University of London
Centre for Commercial Studies (CCLS)
School of Law – Postgraduate Law Centre
Lincoln Inn's Field Campus
67-69 Lincoln's Inn Fields
London WC2A 3JB
United Kingdom

More information at
www.ccls.qmul.ac.uk/
T +44 (0)20 7882 8100
F +44 (0)20 7882 8101

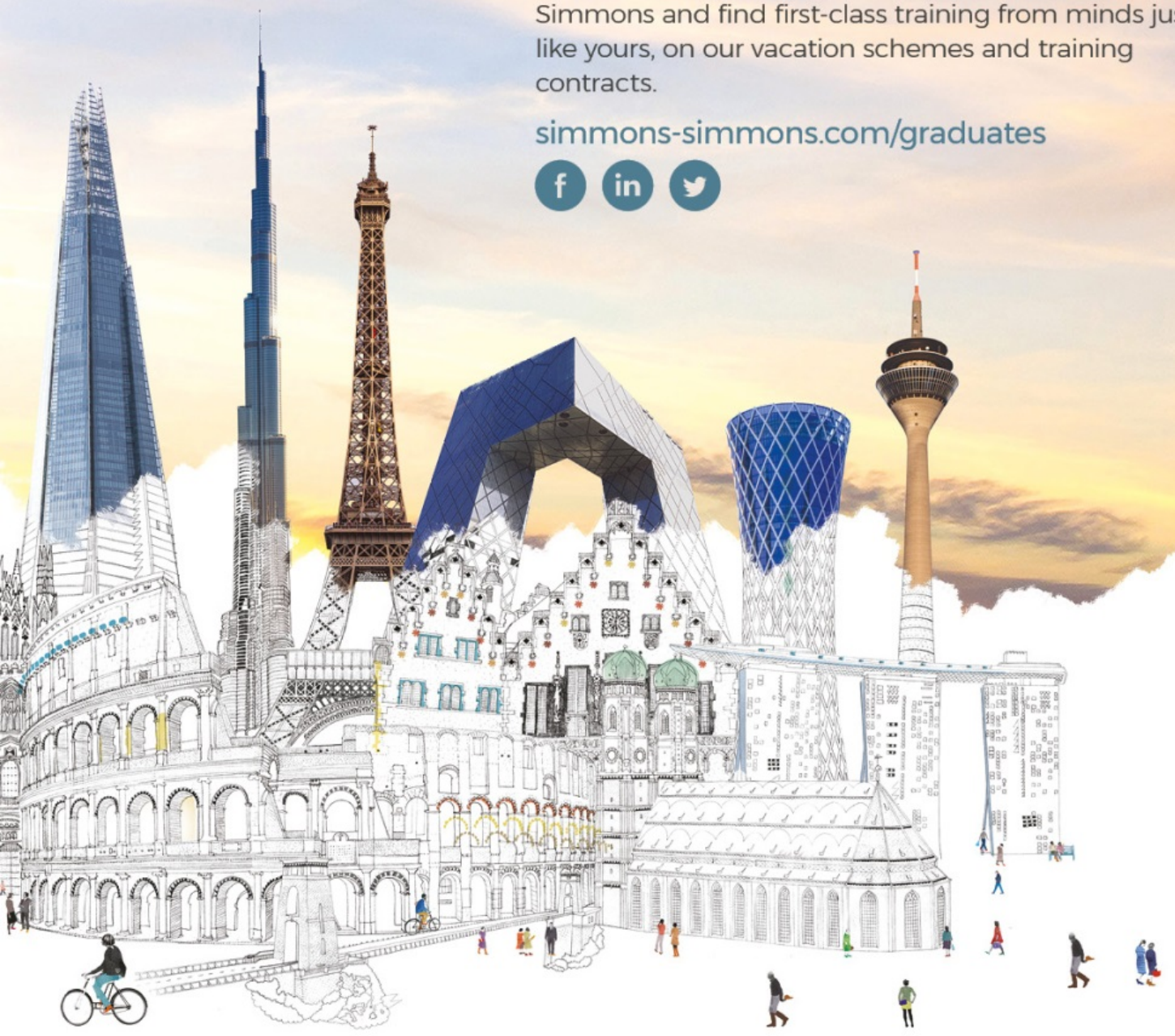
Simmons & Simmons

Graduate Law Opportunities

Uncover the world of law

The world is shaped by legal detail. The patenting in our phones. The copyright in our box-set streaming. The real estate in a city skyline. You've got the curious mind to see it, so now be part of it. Join Simmons & Simmons and find first-class training from minds just like yours, on our vacation schemes and training contracts.

simmons-simmons.com/graduates



Abstracts

9

BLOCKCHAIN IMPLICATIONS FOR LAND REFORM IN UKRAINE – LESSONS FOR INTERNATIONAL BUSINESS

LLB, MBA, LLM (Lon) Anastasia Demchuk

For the full paper, please contact:
Anastasia.demchuk@gmail.com

The paper deals with the severe and pervasive deficiencies of the property rights regime in Ukraine, and issues related thereto. Its principal aim is to examine why the issue of land reform has been so problematic for Ukraine since its independence, and to provide an explanation as to why it remains a significant challenge in the twenty-first century. Legal and administrative obstacles to securing property rights are presented through specific case studies. Furthermore, a historical overview charts the causes and effects of mismanagement and corruption in Ukraine, and how these factors have affected the evolution of the country's legal framework.

Against the aforementioned backdrop, this paper argues that blockchain can deliver a transparent and potentially tamper-proof technology that can potentially restore trust in Ukraine's legal system, if properly implemented. Finally, the paper explores how international business practices can be disrupted through the application of distributed ledger technology to private sector activities.

10

SMART CONTRACTS UNDER SWISS LAW

Dr Christian Schönfeld
LLB, MA in Law and Economics, LLM (Lon)

For the full paper, please contact:
christian.schoenfeld@ggaweb.ch

This dissertation examines what the legal qualification of Smart Contracts under Swiss law is and gives an over-view over how Smart Contracts may interact with the fundamental rules of contract law. Furthermore, on the basis of this examination the need for legislative action with respect to Smart Contracts will be assessed. All these questions will be examined under Swiss law. The examination will focus on the general questions of Swiss contract law as Smart Contracts still remain a largely theoretical construct. More specific assessment will become possible once more specific applications of Smart Contracts have been developed.

It is inter alia concluded that the potential applications of Smart Contracts on the blockchain are vast and sound very promising. If applied in a sensible way this technology indubitably will lead to gains in efficiency of contract execution and lower transaction costs.

However, Smart Contracts will not prevent contractual disputes from arising. Consequently, parties will still resort to court actions. In these cases, Smart Contracts may tend to make things more complicated because while they may not eliminate the need for courts they limit the accessibility of courts for their parties via their self-enforcing nature.

Furthermore, while Smart Contracts may attempt to substitute law by code that does not mean that they will be able to render the law useless. There will still be need for mandatory law for various purposes, including, but not limited, to protect the parties from adverse consequences which the Smart Contract technology itself may produce. No legislator, it can be assumed, will be willing to give up its legislative power and submit to a "tyranny of the code".

Selected Papers

Smart Contracts under Swiss Law

Dr Christian Schönfeld
LLB, MA in Law and Economics, LLM (Lon)

Smart Contracts under Swiss law

Table of contents

I. Introduction 2

1. Research question 2
2. Structure 2

II. General definitions 3

1. FinTech 3
2. Blockchain/distributed ledger 3
   a. Characteristics of blockchains/distributed ledgers 4
   b. Transactions on the blockchain 5
3. Autonomous agents 6
4. Digital assets and mirror assets 6

III. Smart Contracts 7

1. Definition 7
2. Characteristics of Smart Contracts 8
3. Advantages and disadvantages of Smart Contracts 8
4. Potential applications for Smart Contracts 10

IV. Legal analysis of Smart Contracts under Swiss law 11

1. Are Smart Contracts valid contracts under Swiss law? 12
2. What assets can be transferred via Smart Contracts? 15
3. What happens to mandatory provisions of Swiss law? 16
   a. Freedom of contract and its limits under Swiss law 16
   b. Consequences of parties exceeding the limits of freedom of contract 18
   c. Smart Contracts and the limits to freedom of contract 19
4. Enforcement 20
   a. Jurisdiction and applicable law 20
   b. Application of contractual remedies as provided by the law 20
   c. Enforcement of court decisions 21
   d. Alternative solutions 22

V. Is there a need for legislative action with regard to Smart Contracts? 23

VI. Conclusion 26

I. Introduction

In the recent past, 'FinTech' has claimed an increased public attention, becoming a buzzword for the promise of technological progress. Commentators expect that developments from the FinTech area will have a disruptive effect and change many businesses within a short period of time.[1] One significant technological concept that has emerged is the blockchain technology with its underlying idea of distributed ledgers. While Bitcoin, the most prominent of the cryptocurrencies, is the specific application of these technologies which has caught most public attention so far, potential applications reach beyond the area of cryptocurrencies.

One of the most promising ideas in this regard is the concept of 'Smart Contracts'. Simply put, Smart Contracts are programs used to execute and perform pre-defined output variables when pre-defined input variables are met. Their potential application is vast,[2] and the excitement about Smart Contracts has seen 2017 dubbed "the Year of Smart Contracts".[3]

This increased attention warrants a closer examination of what Smart Contracts are and how they fit into current contract law. Even more so as, irrespective of what their name may suggest, the legal qualification of Smart Contracts remains unclear at best. In addition, some underlying concepts, that a blockchain's reliability is attributed to the absence of any single party's control over it, may pose previously unknown challenges to contract law.

1. Research question

This dissertation examines what the legal qualification of Smart Contracts under Swiss law is and gives an overview over how Smart Contracts may interact with the fundamental rules of contract law. Furthermore, on the basis of this examination the need for legislative action with respect to Smart Contracts will be assessed. All these questions will be examined under Swiss law. The examination will focus on the general questions of Swiss contract law as Smart Contracts still remain a largely theoretical construct. More specific assessment will become possible once more specific applications of Smart Contracts have been developed.

2. Structure

This paper is structured as follows. Firstly, the terms which will be relevant in the subsequent analysis are defined and, in particular, the concept of Smart Contracts is examined. Then, based on these findings, the legal qualification of Smart Contracts under Swiss law, their interaction with the existing body of Swiss Contract law and problems arising in connection therewith will be examined. Finally, on the basis of the examination under Swiss law an attempt will be made to assess the need for action by the Swiss legislator with respect to Smart Contracts.

---

1 GEORGE A WALKER, 'Financial Technology Law' (draft, forthcoming, currently unavailable) ch 10.

2 Even though their use in practice remains limited.

3 Rob Marvin, 'Blockchain in 2017: The Year of Smart Contracts' (2016) <http://uk.pcmag.com/feature/86618/blockchain-in-2017-the-year-of-smart-contracts> accessed 13 August 2016.

II. General definitions

To enable an exact legal analysis of Smart Contracts under Swiss law, first a few important fundamental terms need to be defined and explained as their understanding will be relevant in the latter analysis. These are the following:

1. FinTech

One of the biggest buzzwords of the recent years in the financial industry and beyond has been 'FinTech'. FinTech simply is an abbreviation for financial technology.[4] This refers to the application of new technological solutions and methods in the financial sector.[5]

FinTech solutions have managed to capture the public's attention in a short time and already such solutions are being employed by large, established players within the financial sector but also within a multitude of start-ups. The potential of many of these solutions to fundamentally change the industry is immense[6] and, moreover, they are not limited to the financial sector. Instead, ideas are being developed to employ them in all forms of businesses outside of the financial sector, and thereto also, for example, within state administrations. Perhaps, one of the best examples for this is the plethora of (potential) applications for one of the core technologies to emerge from the FinTech sector, certainly the technology that caught the most public attention: the blockchain.

2. Blockchain/distributed ledger

Much has been said and written about the blockchain technology. It is the fundament of the first cryptocurrency which has risen to prominence, Bitcoin.[7] The blockchain's importance lies in the fact that it prevents Bitcoin – or any other data stored on the blockchain – from being counterfeited or – eg in the case of valuable assets – from being double spent. This is what enabled Bitcoin to become successful in the first place.[8]

But what is a blockchain or – more generally – a distributed ledger?[9] Basically, it is a database or a ledger with certain special characteristics. For instance, in the case of a cryptocurrency it lists all units of this currency and their owner and tracks transactions as changes in the database.[10] A more sophisticated definition is suggested by SAVELYEV according to whom a blockchain can be defined as:

> "a decentralized distributed database of all verified transactions that take place across the P2P-network system operating on cryptographic algorithms. Its value can be characterized by the following two core enablers: 1) it allows to transfer digital asset[s] (or virtual representation[s] of physical offline asset[s]) in a way that 2) facilitates disintermediation of the economy by allowing to maintain truthful records about the asset owners without involvement of a trusted

---

4 JEFF REED, 'FinTech Financial Technology and Modern Finance in the 21st Century' in J Reed, *Financial Technology* (2016) 5.

5 WALKER (n 1) ch 1.(1).

6 REED (n 4) 73.

7 The Bitcoin system was conceived in 2008 by an author who called himself SATOSHI NAKAMOTO, presumably an alias (SATHOSHI NAKAMOTO, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008)) <https://bitcoin.org/bitcoin.pdf> accessed 13 August.

8 ADAM ROTHSTEIN, *The End of Money The story of bitcoin, cryptocurrencies and the blockchain revolution* (John Murray Learning, 2017) 35. See also ALEXANDER SAVELYEV, 'Contract Law 2.0: «Smart» Contracts as the Beginning of the End of Classic Contract Law'(2016) Basic Research Program Working Papers Series Law at the National Research University Higher School of Economics (HSE), 5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241> accessed 13 August 2017.

9 KEVIN D WERBACH/NICOLAS CORNELL, 'Contracts *Ex Machina*' (draft March 2017) 67 Duke Law Journal (forthcoming) 11 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2936294> accessed 14 August 2017.

10 ROTHSTEIN (n 8) 36.

intermediary (registrar, financial institution, notary, etc.). Blockchain ensures equal access to transparent and trustworthy information."[11]

a. Characteristics of blockchains/distributed ledgers

A blockchain is *distributed*.[12] This means that it lacks a centralized database. Instead, it is run on and by each and every computer which forms a part of the blockchain network.[13]

A blockchain is (to some extent) *public*.[14] Everyone in this distributed network can have a look at it.

Even though this is relativized to some extent by the fact that the data which the blockchain contains is encrypted[15], it potentially creates a lack of privacy and/or confidentiality when it comes to the information contained on the blockchain. It has been pointed out with respect to Bitcoin as the prototypical application on the blockchain that it is not anonymous even though no names have to be used but account numbers which – theoretically – could be clearly designated to a specific user (however hard this may be). This makes the blockchain pseudonymous rather than anonymous.[16]

The information on a blockchain is *encrypted*: this is achieved with a public/private-key-encryption and shall preserve the security of the data and prevent its manipulation.[17]

The blockchain technology enables the users to maintain a distributed database to which changes and amendments are made constantly without the need for a central authority which implements these changes and controls the database. By achieving this, the blockchain technology *does not depend on a trusted intermediary* but gains its trustworthiness from the mathematical processes the system is based on.[18]

---

[11] SAVELYEV (n 8) 6 et seq.

[12] DON TAPSCOTT/ALEX TAPSCOTT, *Blockchain Revolution How the Technology behind Bitcoin is Changing Money, Business and the World* (Portfolio Penguin, 2016) 6. Sometimes instead of *distributed* the term *decentralized* is used (eg JOHN M NEWMAN, 'Innovation Policy for Cloud-Computing Contracts' (draft December 2014) F X Olleros/M Zhegu (eds), *Handbook of Research on Digital Transformations* (2016) (forthcoming) 23 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2534597> accessed 13 August 2017; SAVELYEV (n 8) 4; also HENNING DIEDRICH, *ethereum – blockchains, digital assets, smart contracts, decentralized autonomous organisations* (Wildfire Publishing, 2016) 160, who points out that a mutual understanding as to the terminology has not yet developed). However, this may cause some confusion as, strictly speaking, a decentralized system is not identical to a distributed system (for an explanation of the differences see BRIAN KELLY, *The Bitcoin Big Bang How Alternative Currencies Are About to Change the World* (Wiley, 2015) 64).

[13] TAPSCOTT/TAPSCOTT (n 12) 6.

[14] ibid (n 12) 6; SAVELYEV (n 8) 4.

[15] See below 9.

[16] STEPHEN MCJOHN/IAN MCJOHN, The Commercial Law of Bitcoin and Blockchain Transactions' (draft November 2016) Suffolk University Law School Legal Studies Research Paper Series Research Paper 16-13 (forthcoming), 6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874463> accessed 13 July 2016; SAVELYEV (n 8) 4; PEDRO FRANCO, *Understanding Bitcoin Cryptography, engineering, and economics* (Wiley, 2015) 9, who points out that this can be an advantage, for instance, where transparency may be desired. Therefore, the creator of a blockchain may decide to keep it "private" in that he may not open it for everyone to become a validator or even not open for everyone to make transactions on it. This may mitigate the issue of unwanted public accessibility of the blockchain data but comes with the price of relativizing the extent of disintermediation by reintroducing some extent of control over the blockchain (DIEDRICH (n 12) 194 et seq). For instance, a private blockchain may be used within a group of companies (JEFF REED, 'Blockchain The Essential Guide to understanding the Blockchain Revolution' in J Reed, *Financial Technology* (2016) 27 et seq).

[17] TAPSCOTT/TAPSCOTT (n 12) 6; SAVELYEV (n 8) 4 et seq. For an illustration of how the encryption mechanism works see MCJOHN/MCJOHN (n 16) 3.

[18] DIEDRICH (n 12) 122 et seq; SAVELYEV (n 8) 4 et seq; WERBACH/CORNELL (n 9) 11 and 13 et seq.

The blockchain technology *makes digital assets stored thereon unique*, that is they cannot be copied in the sense that double-spending is prevented.[19] This is what enables cryptocurrencies to become valuable because it prevents counterfeits[20], but the same would hold true for all assets, eg for music or movies stored on the blockchain.

A blockchain's use is not limited to cryptocurrency but *it can record everything* which can be expressed in code.[21] TAPSCOTT/TAPSCOTT list as examples "birth and death certificates, marriage licenses, deeds and titles of ownership, educational degrees, financial accounts, medical procedures, insurance claims, votes, [or] provenance of food.[22]

The combination of the above characteristics makes it possible to *use* the blockchain technology *to transfer rights* by changing the entries on the database.[23]

Finally, and most importantly in the context of this paper, the blockchain technology provides the technological foundation for Smart Contracts.[24]

b. Transactions on the blockchain

The game changing aspect of the blockchain technology lies in the way of how it effects and records transactions, ie how changes to the database are made.

In a traditional database maintained by a central authority whoever made a transaction would send the information relating to the transaction to the central authority to enable it to amend the database. But in a blockchain there is not central authority. Therefore, the information relating to the transaction (eg the transfer of a bitcoin from A to B) is sent to everyone in the network instead. Relying on the public/private-key-encryption every recipient can verify that the transaction is genuine.

If the database were to be amended to include the transaction at this point, this would create the danger of double-spending: with the right timing, A could transfer the bitcoin he already transferred to B again to C because not everyone in the blockchain system has received and verified the information regarding the first transaction yet. To prevent this, a transaction can only be added onto the blockchain by a 'miner' who has solved a mathematical inequality (essentially, correctly guessing a very complex number). This miner, then, sends the updated ledger to everyone in the network who can easily validate that the block he added is correct and, consequently, will accept this updated version of the database as correct. Only now is the first transaction incorporated on the blockchain database and an attempt at double-spending would be fruitless because it is incompatible with the new version of the database.[25] This method is called proof-of-work.

While the proof-of-work method makes it difficult to falsify information on the blockchain[26] the downside of its (required) complexity is that it also comes with high costs.[27]

---

19 SAVELYEV (n 8) 5.

20 ROTHSTEIN (n 8) 35; DIEDRICH (n 12) 6. Thereby, "digital scarcity" is achieved (DIEDRICH (n 12) 7).

21 TAPSCOTT/TAPSCOTT (n 12) 7.

22 ibid (n 12) 7. See for further examples MCJOHN/MCJOHN (n 16) 6 et seq; WERBACH/CORNELL (n 9) 11 et seq; ROTHSTEIN (n 8) 170 et seq; FRANCO (n 16) 39; DIEDRICH (n 12) 29 and 64 et seq; REED (n 16) 62 et seq.

23 MARIA LETIZIA PERUGINI/PAOLO DAL CHECCO, 'Smart Contracts, a preliminary evaluation' 2015) 1 <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2729548> accessed 7 June 2017; WERBACH/CORNELL (n 9) 14.

24 See below ch III.

25 For a more detailed description see MCJOHN/MCJOHN (n 16) 3 et seq; for an explanation of the proof-of-work method see ROTHSTEIN (n 8) 44 et seq.

26 ROTHSTEIN (n 8) 47.

27 Eg in processing capacity, time or power. See MCJOHN/MCJOHN (n 16) 5.

Therefore, the alternative mechanism of proof-of-stake is being developed and tested which, rather than rewarding the validators on the blockchain for their work, aims at incentivizing them by rewarding their honesty.[28]

3. Autonomous agents

There is no generally accepted definition of the term 'autonomous agent'.[29] One possible definition describes them as "agents that are run without human assistance. They follow a computer program and have an existence of their own. These agents can enter into contracts, receive and spend funds, or even enlist the help of humans to perform certain tasks for them."[30]

TAPSCOTT/TAPSCOTT mention that an autonomous agent performs its task on behalf of its creator, ie their programmer.[31]

The most famous early example of an autonomous agent in practice is the Decentralized Autonomous Organization (The DAO) created by Christoph Jentzch. It was conceived as an autonomous corporation which served as a vehicle for crowdfunding. The potential funders would purchase shares in the DAO which allowed them to vote on how to use the accumulated capital for various projects suggested to be funded by the DAO.[32]

The DAO's actions were still guided by the decisions of its shareholders as a whole. However, given their autonomy and their presumed ability to learn and to adapt to changed circumstances[33] it seems feasible that at some point autonomous agents may develop. At such point, it will be arguable whether or not they still perform their tasks on behalf of their creator. At the least, they are not "just computer programs".[34]

Whether autonomous agents constitute agents in the legal sense of an agency relationship between a principal and an agent shall be examined as part of the legal assessment of Smart Contracts under Swiss law.[35]

4. Digital assets and mirror assets

It has been stated that (virtually) everything can be recorded on the blockchain and, consequently, becomes transferable on the blockchain.[36]

While this is true on a technological level, a further distinction has to be made between digital assets and mirror assets:

Digital asset refers to an asset "whose ownership is recorded digitally and which is directly controlled by its owner."[37] An example for a digital asset is a Bitcoin. But this could also include shares of a company issued on the blockchain.[38]

---

[28] See ROTHSTEIN (n 8) 167 et seq for the example of coin age. Also, DIEDRICH (n 12) 152 et seq.

[29] TAPSCOTT/TAPSCOTT (n 12) 122 with further references; SAVELYEV (n 8) 9, with particular regard to the Decentralized Autonomous Organisation (DAO). Other terms used for autonomous agents include decentralized autonomous corporations (sometimes also called *distributed* autonomous organization: WERBACH/CORNELL (n 9) 29), organizations or corporations or, more generally, decentralized applications (FRANCO (n 16) 187).

[30] FRANCO (n 16) 187.

[31] TAPSCOTT/TAPSCOTT (n 12) 122.

[32] ROTHSTEIN (n 8) 192 et seq; WERBACH/CORNELL (n 9) 29; for the DAO in general also see TAPSCOTT/TAPSCOTT (n 12) 126 et seq.

[33] TAPSCOTT/TAPSCOTT (n 12) 122.

[34] ibid.

[35] See below 29.

[36] See above 10.

[37] FRANCO (n 16) 183.

[38] ibid 185.

Mirror asset, as a subgroup of digital assets, refers to "a digital asset that represents ownership of a real-world asset".[39] In this sense, mirror assets are comparable to certificates eg in gold with the only difference that the mirror asset is stored on a blockchain.[40] For a legal analysis of mirror assets under Swiss law see below ch IV.2.

III. Smart Contracts

This leads over to the concept which shall be examined in more depth: Smart Contracts.

1. Definition

The notion of Smart Contracts becoming possible has been met with excitement by the FinTech community. But the term and the general concept are far from new. They were coined by former law professor and computer specialist NICK SZABO in 1997.[41] He used it to describe his vision of a contract which could execute automatically.

The reason why Szabo's concept has received increased attention recently lies in the fact that its implementation became realistic with the advent of the blockchain technology and its way of enabling trustless transactions.[42]

A plethora of definitions for the term have been thrown around[43], however, a generally agreed upon definition has not yet emerged.[44] Moreover, many of the existing definitions aim to make the theoretical idea palpable but often lack the exactness required to enable a legal assessment of the concept.[45] An attempt at a more elaborate definition has been made by SAVELYEV. According to this author:

> "it is possible to define [a] Smart contract as a piece of software code, implemented on [a] Blockchain platform, which ensures self-enforcing and autonomous nature of its terms triggered by conditions defined in advance and applied to Blockchain-titled assets."[46]

---

[39] DIEDRICH (n 12) 140.

[40] ibid 141.

[41] NICK SZABO, 'The Idea of Smart Contracts' (1997) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html> accessed 13 August 2017; ROTHSTEIN (n 8) 189; KELLY (n 12) 40 and 153; WERBACH/CORNELL (n 9) 5 and 9; DIEDRICH (n 12) 166.

[42] SAVELYEV (n 8) 9, goes so far as to call it a "paradigm-shifter".

[43] ANIL AWASTHI, "'Revolutionary' Smart Contracts Automate Trust' (2016) American Banker Bank Technology vol 1 no 175, 1 <https://www.americanbanker.com/opinion/revolutionary-smart-contracts-automate-trust> accessed 14 August 2017. According to SAVELYEV (n 8) 7, the simplest definition is that a "Smart contract is an agreement whose execution is automated." However, for the purposes of this paper this definition proves to be insufficiently specified. It is noteworthy that MAX RASKIN, 'The Law and Legality of Smart Contracts' (2017) 1 Geo. L. Tech. Rev. 305, 310 <https://poseidon01.ssrn.com/delivery.php?ID=141119082090096123064119075028065007050013055041044089022119079091085029072104022096036063025103104037062107011079126082123079015075086034086116064093079097003031007008001002103077091107126123087081119123081084021024104017075093086025031093084112066071&EXT=pdf> accessed 13 August 2017, further distinguishes between *strong* Smart Contracts where the costs of change or revocation of the contract are prohibitive and *weak* Smart Contracts where this is not the case. This dissertation will focus on strong Smart Contracts.

[44] SAVELYEV (n 8) 7. The author attributes this to the fact that Smart Contracts are a relatively new and technologically complex concept. However, the term was first coined in 1997 by NICK SZABO.

[45] See the discussion of SAVELYEV (n 8) 7 et seq; DIEDRICH (n 12) 166.

[46] SAVELYEV (n 8) 15.

2. Characteristics of Smart Contracts

From the above definition of the term "Smart Contract" its main characteristics can be derived. These are:

Smart Contracts exclusively exist in an *electronic* form but not in any other be it oral or written.[47]

Smart Contracts are *software-implemented*.[48] This may also increase their certainty due to the higher precision of programing language. Interpretative discretion as we are used to encounter in traditional contracts is basically eliminated.[49] In fact, everything outside of the code is merely explanatory but has no influence on the Smart Contract.[50]

Smart Contracts are implemented *on a blockchain*. This characteristic could not have been part of the original concept as envisioned by NICK SZABO and is, therefore, not part of his early definition. However, it seems sensible to include it as it is the blockchain technology which makes self-enforcing, automated Smart Contracts independent from the parties and decentralised, ie it replaces a central authority.[51]

Smart Contracts are *conditional* in nature.[52] They only execute once the conditions are met.

But they *will* execute because Smart Contracts are *self-enforcing*.[53] Once it is concluded, it will execute itself independently from the parties when the conditions are fulfilled.[54] Everything will be done on an automated level. It is, therefore "technically binding for all the parties to it, they are no longer dependent on [a] human intermediary, which is subject to errors and subjective discretion".[55] It is the self-enforcement which, in effect, distinguishes Smart Contracts from traditional contracts.[56]

Smart Contracts are *self-sufficient*, ie they have no need of any legal institutions, be it authorities or legal rules.[57] Moreover, as shall be examined at a later point[58], recourse to these legal institutions is not only unnecessary but actually impossible. Basically, the code is the law.[59]

It concerns *assets on the blockchain*, that is digital assets including mirror assets.[60]

3. Advantages and disadvantages of Smart Contracts

From the above it becomes clear that Smart Contracts may have some *advantages* when compared to traditional contracts:

---

47 ibid 12. This in itself is nothing spectacularly new (WERBACH/CORNELL (n 9) 6 et seq). However, it has been argued that the "smart part" of a contract could also be limited to particular clauses of a contract with the remaining provisions being in the traditional form (PERUGINI/DAL CHECCO (n 23) 10).

48 SAVELYEV (n 8) 12 et seq; REED (n 16) 39.

49 SAVELYEV (n 8) 13. Similarly, DIEDRICH (n 12) 167; JEFF REED, 'Smart Contracts The Essential Guide to using Blockchain Smart Contracts for Cryptocurrency Exchange' in J Reed, Financial Technology (2016) 10 et seq.

50 WERBACH/CORNELL (n 9) 29.

51 SAVELYEV (n 8) 9. Similarly, KELLY (n 12) 17; AWASTHI (n 43) 1; WERBACH/CORNELL (n 9) 5 and 16; DIEDRICH (n 12) 167 et seq; REED (n 16) 11 and 39.

52 SAVELYEV (n 8) 14; DIEDRICH (n 12) 167 et seq; REED (n 16) 8 et seq and 39.

53 SAVELYEV (n 8) 15.

54 In fact, they will not be able to interfere with its execution (DIEDRICH (n 12) 167 et seq; REED (n 49) 8 et seq; SAVELYEV (n 8) 18).

55 SAVELYEV (n 8) 15; WERBACH/CORNELL (n 9) 9.

56 WERBACH/CORNELL (n 9) 9; DIEDRICH (n 12) 5 and 22 et seq.

57 SAVELYEV (n 8) 15; DIEDRICH (n 12) 167.

58 See below ch IV.3.

59 REED (n 16) 41.

60 DIEDRICH (n 12) 169 et seq.

The main advantage that may result from employing Smart Contracts in sensible way lies in the reduction of transaction costs as compared to traditional contracts.[61] Cost savings may be possible at every stage of the Smart Contract's lifecycle.[62]

Drafting of the Smart Contract may become cheaper if reusing the original code. This effect will have the greatest impact with regard to standardized transactions. The processing and the execution are simplified which may lead to cost reductions.[63] To some extent, even an automatization of the drafting of Smart Contracts may seem possible. Finally, a reduction in transaction costs may also occur due to the possibility to get rid of a costly intermediary, for instance a bank.[64]

If transaction costs are lower, the application of a Smart Contract becomes cheaper. This has two consequences:

Firstly, it becomes efficient to apply Smart Contracts in areas where contractual agreements used to be too expensive to be applied efficiently.[65] This may enable transactions which were not commercially viable before.

Secondly, the cheaper Smart Contracts become, the more affordable they become for parties who could not make use of contractual agreements before. Where contractual agreements in a particular area used to be only available for big companies or high net-worth individuals they may become available for smaller businesses or individuals with moderate financial means at their disposal. For instance, escrow agreements may become affordable in cases where, currently, the costs of the escrow agent render them too expensive.

However, Smart Contracts may also come with some *disadvantages*:

The self-enforcing automated nature of Smart Contracts also leads to them being relatively inflexible when compared to traditional contracts. Where the parties to a traditional contract can (and quite often do) amend a contract during its lifetime due to unforeseen or changed circumstances the same proves to be harder, if not impossible, when Smart Contracts are concerned. In this sense, it is not possible to react to unforeseen events. Furthermore, somewhat subjective criteria in traditional contracts such as reasonableness or unspecified materiality requirements which may provide the parties some desired flexibility are not feasible in code-based Smart Contracts.[66] This may, ultimately, lead to the execution of the Smart Contract actually having adverse unintended consequences, especially the more complex the contract is.[67]

Some hope (and some fear) that the advent of Smart Contracts may limit the need for lawyers substantially if not render them completely obsolete. This seems questionable at best. Irrespective of their self-sufficient nature and their guaranteed execution, Smart Contracts do not stand outside of the law. They, and the parties to them, still exist within the legal system and have to adhere to its boundaries. Furthermore, Smart Contracts for all their potential will not eliminate disputes, albeit that they may change them.[68] It is in all these cases that lawyers will still be needed to advise their clients on the sensible course of action even more so as we only just began to grasp the challenges and implications of Smart Contracts under the existing body of statutes and case law.

---

61 FRANCO (n 16) 10.

62 WERBACH/CORNELL (n 9) 17.

63 REED (n 16) 19 et seq and 40. For an example, see KELLY (n 12) 155.

64 KELLY (n 12) 154.

65 WERBACH/CORNELL (n 9) 17.

66 REED (n 16) 41 et seq; WERBACH/CORNELL (n 9) 43 et seq.

67 However, there are already projects which try to make Smart Contracts also usable for more complex contractual relationships (AKBER DATOO, 'FinTech Solutions in Complex Contracts Optimization' in Susanne Chishti/Janos Barberis (eds.), *TheFINTECHBook The Financial Technology Handbook for Investors, Enterpreneurs and Visionaries* (Wiley, 2016) 107 et seq).

68 Similarly, WERBACH/CORNELL (n 9) 45. For the potential effects of Smart Contracts on enforcement see below ch IV.4.

Also, it can be questioned whether the drafting of Smart Contracts really is easier for anyone except for skilled software programmers. They have to be drafted in a language and based on a deterministic logic which, currently, is still strange to most people. Hence, a skill gap persists and to overcome this gap will take time. Until then, even if parties may be able to rely less on lawyers they will have to put increased trust in the programmers' abilities. It goes without saying, that even the most skilled programmer is prone to human error.[69]

It is reasonable to assume that future developments in Smart Contracts will address these disadvantages and mitigate the risks connected therewith. However, it is unlikely that this will happen in the short run.[70]

Because of all these potential disadvantages, parties which are not as affected by the potential reduction in transaction costs because they can afford to rely on traditional contracts may be reluctant to sacrifice this degree of flexibility and control for a moderate cost reduction. Consequently, they may be reluctant to use Smart Contracts.

4. Potential applications for Smart Contracts

With Smart Contracts being a complex and highly technical concept it seems sensible to provide some illustrative examples of potential real-world applications to make the idea more palpable. This list does not intend to be exhaustive but to give a feel for what Smart Contracts may be capable of. Among others, the following ideas have been put forth:

A straightforward idea is to use Smart Contracts for *escrow* agreements without an escrow agent.[71] Instead of relying on the independent and trusted escrow agent, the assets to change hands could simply be blocked on the blockchain with the Smart Contract transferring them from one party to the other once the required conditions have been met.

They could be employed in *financial instruments* and, for instance, enable the exercise financial derivatives such as options.[72] Also, a 'smart bond' could be used to affect the agreed payments over the lifetime of the debt instrument.[73]

Further examples include the use of Smart Contracts for peer-to-peer *remittance services and automated payment transfers*[74], eg the monthly rent payment to the landlord without need of a bank as an intermediary.

Within *crowdfunding* systems, Smart Contracts could be used to control the flow of funds, that is to the project in case the required threshold is met or back to the funders if not.[75] In a similar way, they could be employed in *insurance* in order to, on the one hand, pool the incoming funds and, on the other hand, distribute payments to policyholders if the insured risk realizes.[76]

---

69 WERBACH/CORNELL (n 9) 42 et seq.

70 Similarly, ibid 44.

71 KELLY (n 12) 17; WERBACH/CORNELL (n 9) 25 et seq; CHRIS DEROSE, 'Smart Contracts: Blockchain's Solution for the Underserved' (2016) American Banker Consumer Finance vol 1 no 61, 1 <https://www.americanbanker.com/opinion/smart-contracts-blockchains-solution-for-the-underserved> accessed 14 August 2017; DIEDRICH (n 12) 173.

72 PERUGINI/DAL CHECCO (n 23) 24.

73 FABIO MASSACCI/CHAN NAM NGO/JULIAN WILLIAMS, 'Decentralized Transaction Clearing Beyond Blockchains' (2016) 19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2794913> accessed 13 August 2017. A real-world application of this is the Smart Bond developed by UBS (CLAUDIO LISCO, 'Cutting through the blockchain hype' (2016) <https://www.ubs.com/magazines/innovation/en/our-approach/2016/path-finding.html> accessed 13 August 2017).

74 DEROSE (n 71) 1 et seq; DIEDRICH (n 12) 65.

75 WERBACH/CORNELL (n 9) 18; SAVELYEV (n 8) 9 et seq.

76 SAVELYEV (n 8) 9 et seq. One application which is currently being developed concerns smart flight delay insurance (PERUGINI/DAL CHECCO (n 23) 22). See also WALKER (n 1) ch 4.(5).

Generally speaking, Smart Contracts could be of use in "transactions that involve changes in electronic records of many stripes" *across different industries*.[77] This includes clearing and settlement of on and off-exchange trading activity, processing of health and property information, licensing of creative content such as music, films or books including royalty payments.[78] Another possible application lies within an *intragroup* context, eg in that a group of companies automatizes their cash pooling by using a Smart Contract solution.

But Smart Contracts could also be used for *more complex transactions*, for instance the automated execution of the will of a deceased person.[79]

Furthermore, on a more general level it has been suggested that the Smart Contract does not have to cover the entire contract but it may be limited to specific aspects of it or in a set of contracts only some may be Smart Contracts[80]. Specific provisions could entail the automatic execution of *penalty clauses* or provisions which are conditional upon a *deadline* being or not being met.[81]

This shows that the potential applications for Smart Contracts are vast and manifold. It remains to be seen which applications will develop in practice. However, the sheer potential makes the question of how Smart Contracts are to be treated in legal practice and which problems may arise in this context more pressing.

IV. Legal analysis of Smart Contracts under Swiss law

After having defined the relevant terminology and having explained how Smart Contracts and their underlying technologies function we are able to examine the legal implications of Smart Contracts under Swiss law.

The aim of the following analysis is to examine how Smart Contracts are to be treated under Swiss law and what problems may arise in connection with Smart Contracts. This is important because the understanding of how Smart Contracts work (or what deficiencies may surface) in a legal sense will be critical for their successful use.[82]

Covering all the specific problems which may arise in this regard would go beyond the scope of this paper. Furthermore, an exhaustive analysis will not be feasible until specific applications of Smart Contracts have started to occur in practice. Therefore, in the following assessment the emphasis will be put on the basic overarching questions which the application of Smart Contracts is likely to raise as a first analysis under Swiss law.[83] While examples deriving from specific areas of contract law (eg the sale of immovable property) may be given for illustrative purposes, more detailed analyses of different contract types seem unfeasible before specific real-world implementations of Smart Contracts have been further developed.

The questions to be examined hereafter will be whether Smart Contracts qualify as contracts under Swiss law, what types of assets can be transferred via Smart Contracts, how Smart Contracts interact with mandatory law and how the law can be enforced against Smart Contracts deviating from it. Although this structure has been adapted in view of the peculiarities of Swiss law it has been inspired by the structure of few examinations which have been conducted with respect to other jurisdictions.[84]

---

77 MCJOHN/MCJOHN (n 16) 10; REED (n 49) 15 et seq.

78 MCJOHN/MCJOHN (n 16) 10 et seq; also, REED (n 49) 16 et seq.

79 WERBACH/CORNELL (n 9) 18

80 MCJOHN/MCJOHN (n 16) 11.

81 PERUGINI/DAL CHECCO (n 23) 22 et seq.

82 AWASTHI (n 43) 1.

83 So far, the discussion of Smart Contracts under Swiss law has remained limited. A reference to Smart Contracts can be found in ROLF H WEBER/SIMONE BAUMANN, 'FinTech – Schweizer Finanzmarktregulierung im Lichte disruptiver Technologien' (2015) Jusletter <http://jusletter.weblaw.ch/juslissues/2015/816.htmlprint> accessed 13 August 2017; a limited examination of the general implications of Smart Contracts in JANA ESSEBIER/DOMINIC A WYSS, 'Von der Blockchain zu Smart Contacts' (2017) Jusletter <http://jusletter.weblaw.ch/juslissues/2017/889.html> accessed 4 June 2017.

84 Namely, WERBACH/CORNELL (n 9); SAVELYEV (n 8); and MCJOHN/MCJOHN (n 16).

1. Are Smart Contracts valid contracts under Swiss law?

The term 'Smart Contract' includes 'contract' which raises the fundamental question whether Smart Contracts constitute contracts not only in a colloquial sense but also in a legal sense. This is a controversial question among proponents of Smart Contracts.[85] At least this is not self-evident and warrants further examination.[86] In any case, the result of this examination may differ depending on the relevant jurisdiction. So far, this examination has only been conducted for a few jurisdictions.[87]

The main aspects of Swiss private law are codified in the CC and the CO.[88] The former contains, among else, the law of property while the latter contains general rules for all types of contracts (eg with regard to form requirements, statute of limitation, powers of the agent or set-off) and specific rules for a variety of contract types (eg sale, lease or employment contract).[89]

However, the CO does not contain a statutory definition of the term 'contract'. Furthermore, some inconsistencies persist in that contract may refer to different things depending on the context.[90]

Pursuant to BUCHER a contract refers to the mutual express of an intent which is aimed to create legal consequences by (at least) two parties.[91] Entering into a contract is one of several ways under Swiss law which leads to the creation of an obligation.[92] An obligation in this sense creates the creditor's right to request from the debtor a performance which, generally speaking, may include the debtor performing an action, abstain from performing an action or tolerating something.[93] In other words, it entails a promise by the debtor to the creditor.

Because of this definition of an obligation the question has been raised whether the self-executing nature of a Smart Contract prevents them from qualifying as a legal contract. The argument is that since the parties cannot exert any influence over the performance of their 'obligations' once they have entered into the Smart Contract they

---

85 SAVELYEV (n 8) 10.

86 This is irrespective of the fact that the term "Smart Contract" was originally coined by NICK SZABO, a former law professor (see above 14).

87 Under US law WERBACH/CORNELL (n 9) 19 et seq, conclude that Smart Contracts qualify as contracts in a legal sense. For an assessment under Russian law which reaches the same conclusion see SAVELYEV (n 8) 10 et seq.

88 Swiss Civil Code of 10 December 1907 (CC), SR 210; Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of 30 March 1911 (CO), SR 220.

89 In addition to contract law, the CO also contains rules on partnerships and various forms of companies as well as securities law.

90 Eg either the *process of entering into a contract* or the *resulting contractual relationship*, see EUGEN BUCHER, *Schweizerisches Obligationenrecht Allgemeiner Teil ohne Deliktsrecht* (2nd edn Schulthess Polygraphischer Verlag Zürich, 1988) 40 <http://www.eugenbucher.ch/obligationenrecht/or-allgemeiner-teil-2-auflage-1988/> accessed 6 August 2017.

91 BUCHER (n 90) 40: "Der Vertrag ist konstituiert durch die von zwei Parteien ausgehende, übereinstimmende und auf Herbeiführung eines rechtlichen Erfolgs gerichtete Willenserklärung ... . An einem Vertrag können auch mehr als zwei Parteien beteiligt sein."

92 Other reasons which lead to the creation of an obligation include, for instance, obligations resulting from tort (arts 41 et seq CO) or from unjust enrichment (arts 62 et seq CO). See also HANS MERZ, *Sechster Band Obligationenrecht Allgemeiner Teil Erster Teilband Einleitung §§1-3 Entstehung, allgemeine Charakterisierung Die Obligation §§ 4-20*, in Christoph von Greyerz/Max Gutzwiller/Hans Hinderling/Arthur Meier-Hayoz/Hans Merz/Paul Piotet/Roger Secrétan/Werner von Steiger/Frank Vischer (eds), Schweizerisches Privatrecht vol VI/1 (Helbing & Lichtenhahn Verlag AG, 1984) 50 et seq. However, it is also possible to enter into a contract in order to *change* an obligation (eg assignment) or to *cancel* an obligation (ANDREAS VON TUHR/HANS PETER, *Allgemeiner Teil des Schweizerischen Obligationenrechts vol I* (3rd edn) (Schulthess Polygraphischer Verlag AG, 1979) 148).

93 MERZ (n 92) 119 and 123 et seq.

do not really exchange promises to perform their obligations. Consequently, Smart Contracts would not really create obligations.[94]

However, under Swiss law this argument seems to be of limited validity. On the one hand, it could be argued that putting the Smart Contract on the blockchain can already be regarded as part of the obligation. Furthermore, (i) an obligation may also entail simply tolerating that something happens, eg that the Smart Contract executes itself[95], and (ii) the decisive factor whether a contract has been formed is the mutual intention of the parties to enter into an obligation.[96]

It can be concluded, therefore, that *on a general level* Smart Contracts can qualify as contracts in the sense of the CO.[97]

As just mentioned pursuant to art 1 para 1 CO the only thing required for the conclusion of a contract is the *mutual expression of intent by the parties*. On a general level, this requirement poses little problem for Smart Contracts.

The fact that the parties enter into a Smart Contract by electronic means (instead of, for instance, in writing) has no relevance for its qualification as a contract.[98] While the form of a contract may concern its validity it says nothing about the meeting of the minds of the parties.[99] Consequently, simply putting a Smart Contract onto the blockchain can be regarded as an expression of intent.[100]

WERBACH/CORNELL further address the problem that a Smart Contract being code on a blockchain is only entered onto the blockchain by one party giving it a unilateral appearance. While the authors shortly discuss other possible ways of putting a Smart Contract onto the blockchain involving both parties they seem to conclude that the standard approach, at least, puts in question whether a mutual expression to enter into a contract and to its shared understanding actually exists.[101] Under Swiss law this seems to be less of a problem as the intent can be implied.[102] This namely includes the case where one party shows its intent by performing its contractual duties[103] or when the transaction is entirely favourable for one party such as a gift.

---

94 WERBACH/CORNELL (n 9) 21. SAVELYEV (n 8) 17, states in this regard "[i]f nothing depends on the will of the debtor then he is under no obligation to the creditor, since there can be no liability for breach of such an 'obligation', it is discharged on force majeure basis."

95 It appears SAVELYEV (n 8) 17, argues similarly when he states: "[I]t would be more correct to state that the main consequence of conclusion of Smart contract is not an appearance of 'obligations' but the resulting self-limitation of certain rights by technical means."

96 See SAVELYEV (n 8) 11 for a discussion of the parties will to enter into a legally binding obligation.

97 See also WERBACH/CORNELL (n 9) 44, who reach the same conclusion with respect to US law.

98 Digital contracts which are not in writing in the sense of art 13 CO are nothing new but already exist eg in online shopping (WERBACH/CORNELL (n 9) 7). Similarly, for Russian law: SAVELYEV (n 8) 11 et seq and WERBACH/CORNELL (n 9) 23. However, the form of the contract may be of relevance when it comes to statutory form requirements (see below 36).

99 WERBACH/CORNELL (n 9) 23.

100 Similarly, WERBACH/CORNELL (n 9) 46, who argue that the "very fact that parties submit their cryptographic private keys to commit resources to a smart contract is proof of such a commitment".

101 ibid 23 et seq.

102 Art 1 para 2 CO for the expression of intent in general and art 6 CO with respect to the implied acceptance of an offer.

103 So-called '*Realakzept*'; see BRUNO SCHMIDLIN, *Obligationenrecht Allgemeine Bestimmungen Art. 1-18 OR Kommentar zu Art. 3-10 OR*, in Berner Kommentar Kommentar zum schweizerischen Privatrecht vol VI 1. Abteilung 1. Teilband Lieferung 2 (Stämpfli & Cie AG, 1985) art 3 nos 58 et seq and art 6 nos 72 et seq and also ERNST A KRAMER, *Obligationenrecht Allgemeine Bestimmungen Allgemeine Einleitung in das schweizerische Obligationenrecht und Kommentar zu Art. 1 und 2 OR*, in Berner Kommentar Kommentar zum schweizerischen Privatrecht vol VI 1. Abteilung 1. Teilband Lieferung 1 (Stämpfli & Cie AG, 1980) art 1 no 20. See the example of SAVELYEV (n 8) 11, who reaches a similar conclusion under Russian law.

Thus, in a legal sense Smart Contracts show the meeting of the minds required by art 1 CO and, therefore, create legally binding obligations. However, this is not to say that Smart Contracts in any way prevent any party from suffering from a defect in consent be it by misstating their intent or by not forming their intent correctly.[104]

The above discussion implicitly assumed that the parties to the Smart Contract were either individuals or legal persons, ie legal subjects with the capacity to enter into a contract.[105] However, a problem may arise when it comes to autonomous agents[106] entering into a Smart Contract.

As long as an autonomous agent is still guided by the intent of its creator or its creators (as it was, for instance, the case with The DAO or with a fridge which automatically orders food whenever needed because it has been programmed to do so by its owner), this should not be too problematic to reconcile with Swiss contract law. It seems reasonable to argue that the use of the autonomous agent merely constitutes the way in which the person or persons behind it express their intent to enter into the Smart Contract. From that point of view, autonomous agent are not agents in the legal sense but rather means of communication.

This perspective would start to break down, however, once autonomous agents achieve true autonomy in the sense that they no longer strictly adhere to the will of their user or programmer.[107] Entering into a binding contract requires the legal capacity and the capacity to act otherwise the contract is void ab initio.[108]

In the case of 'true' autonomous agents entering into a contract it becomes hard to argue that they express the intent of an individual with the capacity to enter into a Smart Contract. One might try to solve this problem by applying the rules of agency.[109] However, the more autonomous the agent becomes the more this seems like a stretch.

Arts 32 et seq CO contain rules regarding agency stating that "[t]he rights and obligations arising from a contract made by an agent in the name of another person [ie the principal] accrue to the person represented, and not the agent."[110] The same effect arises, inter alia, if the counterparty was not aware of the agent acting as an agent but did not care with whom the contract was made.[111]

One of the problems in treating an autonomous agent as an agent of its creator lies in the fact that Swiss law requires that an agent is capable of judgement.[112] If the agent is incapable of judgement, the contract he entered into is void.[113] However, Swiss law does not recognize computer programs as legal subjects, hence, assigning them the capability of judgement and, consequently, the ability to act as a true agent is not possible de lege lata.

An alternative solution would be to attribute all obligations which arise because of the actions of the autonomous agent to its creator because of him being the agent's creator or user. For the aim of attributing liability this seems feasible de lege lata. However, where 'truly' autonomous agents are concerned this solution is at odds with what the participants in the blockchain environment actually intended. After all, the idea behind an autonomous agent ultimately seems to be to create a truly independent participant on the blockchain.

---

[104] WERBACH/CORNELL (n 9) 46 et seq.

[105] Art 11 et seq CC for individuals and art 11 et seq in connection with art 53 CC for legal persons.

[106] For an explanation of the term see above ch II.3.

[107] See for this possibility above ch II.3.

[108] BUCHER (n 90) 114 et seq.

[109] Art 32 et seq CO.

[110] Art 32 para 1 CO.

[111] Art 32 para 2 CO.

[112] ROGER ZÄCH/ADRIAN KÜNZLER, *Obligationenrecht Stellvertretung Art. 32-40 OR* (2nd edn), in Heinz Hausheer/Hans Peter Walter (eds.), Berner Kommentar Kommentar zum schweizerischen Privatrecht (Stämpfli Verlag, 2014) art 32 no 130 with reference to art 18 CC.

[113] ibid art 32 no 129.

Consequently, while the current legal rules may prove sufficient for now, the legislator may have to create a statutory solution when it becomes visible that the autonomous agent's technology has advanced far enough. In other words, the question will be whether the legislator wants to allow for autonomous agents to become bound by Smart Contracts themselves.

2. What assets can be transferred via Smart Contracts?

Enthusiasts predict that at some point virtually everything can be put onto and traded via the blockchain.[114] Many of the Smart Contract applications proposed in the literature are concerned with the transfer of digital or real-world assets such as, for instance, commodities or securities. As tempting as these ideas sound, several legal obstacles will have to be overcome before this will really be possible under Swiss law:

Reality proves that real digital assets only existing on the blockchain can be traded and transferred. Nonetheless, the legal qualification of such purely digital assets under Swiss law remains unclear. As far as can be seen, this question has not yet been examined.[115] While this would go beyond the scope of this paper, the basic problem is as follows:

Generally speaking, Swiss law distinguishes between ownership (absolute and limited rights in rem, ie physical objects[116]) and claims (*Forderungsrechte*).[117] Purely digital assets have no physical quality but exist only on the database which is the blockchain. Claims, on the other hand, are targeted against a debtor obliged to perform or refrain from performing an action or to tolerate an action being taken. Purely digital assets, eg a Bitcoin, cannot be said to constitute a claim against someone else. They are merely an entry on the Blockchain without providing any form of recourse to someone else. Hence, purely digital assets stand outside of the Swiss system of rights in rem or claims.[118] Currently, this does not seem to pose too many problems but at some point, it may become desirable for the legislator to provide legal certainty, eg when market participants start to give charges over purely digital assets.

The next obstacle arises with respect to transactions in real-world assets (eg commodities such as oil) done via the blockchain. This has to be achieved by using mirror assets since the real-world assets themselves cannot reside on the blockchain.[119]

There, the problem lies in the fact that Swiss law, currently, does not recognize digital mirror assets on a general level and, consequently, it would be dubitable at best whether their use would have the desired consequences (ie transfer of ownership of the real-world asset as a consequence of the "transfer" of the mirror

---

[114] See above 10. TAPSCOTT/TAPSCOTT (n 12) 7.

[115] A first attempt has been made, however, for UK law: see WALKER (n 1) ch 9 (3).

[116] THOMAS SUTTER-SOMM, *Fünfter Band Sachenrecht* (2nd edn), in Christine Chappuis/Daniel Girsberger/Sybille Hofer/Ernst A Kramer/Peter V Kunz/Thomas Sutter-Somm/Wolfgang Wiegand/Stefan Wolf (eds.), Schweizerisches Privatrecht vol V/1 (Helbing Lichtenhahn Verlag AG, 2014) nos 16 et seq.

[117] BUCHER (n 90) 5. However, exceptions to this duality exist, eg intermediated securities pursuant to the Federal Act on Intermediated Securities (ISA) which are assets sui generis (BGE 138 III 139 (consid 5.2.1); Swiss Federal Council, 'Botschaft zum Bucheffektengesetz sowie zum Haager Wertpapierübereinkommen' of 15 November 2006, Federal Gazette (2006) 9315, 9339; Harald Bärtschi, 'Die rechtliche Umsetzung des Bucheffektengesetzes', (2009) AJP 1071, 1071).

[118] This may lead to counterintuitive results. For example, under a sales contract pursuant to art 186 CO either the property to a right in rem will be transferred or a claim will be assigned from the seller to the purchaser. This is not possible for a purely digital asset. Instead, it seems the contractual obligation would be that the 'purchaser' pays the specified amount of money to the "seller" for the latter to amend the entry on the blockchain accordingly. In other words, the 'seller' has to render a service in favour of the 'purchaser' which would hint to this transaction being some form of a service contract.

[119] See for the definition of "mirror assets" above ch II.4.

asset).[120] Ultimately, to create the legal certainty required should parties become used to using mirror assets, this situation will have to be mitigated by the legislator on a statutory basis.

However, in creating the statutory basis for mirror assets he could, to some extent, rely on remedies to similar problems which have been in use for a long time and can already be found in Swiss law. In this regard, documents of title to goods[121] come to mind. Documents of title to goods are negotiable securities under Swiss law and refer to moveable objects which can be the object of freight transport and whose value rests in their substance.[122] It has to be noted that the carrier or warehouse keeper must not be the sole owner of the good in question.[123] A duly constituted document of title to goods can be pledged which creates a pledge over the underlying goods as well.[124] Furthermore, it serves as a surrogate for tradition, that is the transfer of the ownership of the document of title to goods also leads to the transfer of ownership in the underlying goods.[125] Hence, documents of title to goods under Swiss law can be said to constitute a form of mirror assets on a written instead of digital basis. Nonetheless, documents of title to goods under Swiss law are still largely paperbound. While the commercial practice attempts to mitigate the downsides of switching from paper-based, fully enforceable documents of title to digital, perhaps unenforceable, documents of title by employing means like insurance, problems still prevail when it comes to disputes.[126] At some point, legislative action in this respect might become necessary. This chance could be used to legislate digital mirror assets as well.

3. What happens to mandatory provisions of Swiss law?

a. Freedom of contract and its limits under Swiss law

As a general principle of Swiss contract law the parties enjoy freedom of contract.[127] This includes, among other things, the freedom to determine the terms of the contract or the freedom to impose or refrain from any form requirements.[128]

However, this freedom is subject to the limits set by the law.[129] Art 19 para 2 CO specifies in that respect that "[c]lauses that deviate from those prescribed by law are admissible only where the law does not prescribe mandatory forms of wording or where deviation from the legally prescribed terms would contravene public policy, morality or rights of personal privacy." Hence, freedom of contract under Swiss law is limited by the following:

Mandatory private or public law[130]: This covers contractual provisions which are in conflict with mandatory provisions of federal or cantonal, private or public Swiss law.[131] That a rule is deemed mandatory can be stated

---

120 Arguably, one limited exception to this are intermediated securities pursuant to the ISA.

121 Arts 1153 et seq CO.

122 ANDREAS FURRER, 'Auf dem Weg zu elektronischen Warenpapieren Stand der Entwicklung in den einzelnen Transportmodalitäten' in Lukas Gschwend/Peter Hettich/Markus Müller-Chen/Benjamin Schindler/Isabelle Wildhaber (eds.), *Recht im digitalen Zeitalter Festgabe Schweizerischer Juristentag 2015 in St. Gallen* (Dike Verlag AG, 2015) 340 with further references.

123 ibid.

124 Art 1154 CO for the modalities and FURRER (n 122) 342.

125 Art 925 CC; FURRER (n 122) 342; SUTTER-SOMM (n 116) nos 1286 et seq.

126 FURRER (n 122) 372.

127 Art 18 para 1 CO.

128 ERNST A KRAMER, *Das Obligationenrecht Band VI, 1. Abteilung Allgemeine Bestimmungen 2. Teilband, Unterteilband 1a Inhalt des Vertrages Kommentar zu Art. 19-22 OR*, in Arthur Meier-Hayoz (ed), Berner Kommentar Kommentar zum schweizerischen Privatrecht vol VI Das Obligationenrecht (Verlag Stämpfli & Cie AG, 1991) arts 19-20 nos 42 and 43 et seq in detail.

129 See the second half of art 18 para 1 CO. Also, KRAMER (n 128) arts 19-20 no 48.

130 ibid arts 19-20 nos 132 et seq and, namely, nos 146 et seq and 148.

131 ibid arts 19-20 no 132.

explicitly in the statutory text but it may also result from the interpretation of the statute.[132] Examples of mandatory provisions include:

- in private law[133]: art 404 CO pursuant to which an agency contract may be revoked or terminated by either party at any time without cause[134]; arts 361 and 362 CO which list the provisions of employment law from which either no derogation at all is permissible to the detriment of the employer or the employee or from which no derogation is permissible to the detriment of the employee[135]; or arts 659 et seq CO which impose restrictions on the acquisition of own shares by holding companies or their subsidiaries. Another example would be form requirements eg that a sale of immovable property must be done as a public deed.[136]
- in public law[137]: the prohibition of pacta de quota litis for lawyers[138]; prohibitions on the sale of munitions and war material[139]; sale and purchase of illegal drugs[140].

Public policy ('ordre public')[141]: This refers to fundamental and general value principles of Swiss law which are not explicitly laid out in statutes or have not been specified enough.[142] An example would include an arbitration clause which was held to have breached fundamental standards of the legal system by, among else, giving one party the sole control over whether arbitration should be used instead of state courts and giving this party the sole right to appoint the arbitrators.[143]

Morality[144]: This namely includes contracts which are in conflict with socioethical values, professional ethics or which interfere with contractual rights of third parties in a qualified way or contractual obligations which are in a severe imbalance to the value of their consideration.[145]

The rights of personal privacy[146] prevents contracts which affect the freedom and personal integrity of a party or which lead to excessive restrictions on the side of one party.[147]

These limitations to the freedom of contract serve different purposes which have to be determined for every relevant provision separately. While some rules, for instance prohibitions of criminal law, mainly aim to fight crime[148], other rules are aimed at protecting the parties. Form requirements often aim to prevent the parties from taking a hasty decision without due regard to its consequences or to facilitate the provision of proof in case a

---

132 ibid arts 19-20 no 146.

133 ibid arts 19-20 no 146.

134 BGE 98 II 305 (308 et seq); BGE 104 II 108 (consid 4); BGE 106 II 157 (consid 2).

135 KRAMER (n 128) arts 19-20 no 147.

136 Art 216 para 1 CO.

137 KRAMER (n 128) arts 19-20 no 149.

138 BGE 41 II 474 (consid 1).

139 BGE 82 II 129.

140 BGE 106 IV 295 (297).

141 KRAMER (n 128) arts 19-20 nos 151 et seq.

142 ibid arts 19-20 no 155.

143 ibid arts 19-20 no 157 with reference to a German case law.

144 ibid arts 19-20 nos 168 et seq.

145 ibid arts 19-20 nos 193 et seq.

146 ibid arts 19-20 nos 208 et seq. This namely includes protection of personal integrity pursuant to arts 27 et seq CC.

147 ibid arts 19-20 nos 212 et seq; see also arts 27 et seq CC.

148 Swiss Federal Council, 'Botschaft des Bundesrates an die Bundesversammlung zu einem Gesetzesentwurf enthaltend das schweizerische Strafgesetzbuch' of 23 July 1918, Federal Gazette (1918) vol IV 1, 5.

dispute arises.[149] Consumer protection rules protect the weaker party to the contract from the negative consequences due to the imbalance of bargaining power or sophistication.[150]

b. Consequences of parties exceeding the limits of freedom of contract

A contract which is unlawful or immoral in the sense described above is void.[151] Where the unlawfulness or the immorality only concerns certain terms of the contract, only those terms are void if it can be assumed that the parties had entered into the contract without these terms.[152] As a default rule, that means that the contract or the specific provisions are void ab initio.[153]

It has to be noted that this consequence may also apply where contractual provisions may seem to stay within the freedom of contract but really are only aimed at circumventing or bypassing mandatory law.[154]

In certain cases, it is possible that an invalid provision is replaced by a valid provision (eg an excessive interest rate is lowered to a legally permissible interest rate).[155]

Furthermore, parties exceeding the space of their contractual freedom may face other adverse consequences in addition to the contract being void.[156]

A breach of public law often results in sanctions such as fines or imprisonment. This applies not only to breaches of core criminal provisions but is also the case in other areas of public (and sometimes even private) law.[157] Furthermore, civil liability may arise with respect to damages caused.[158]

The underlying contract being void prevents any obligations from ever arising for the parties. Performance of these inexistent obligations, therefore, lacks a legal causa. Consequently, prior to performance, the parties can refuse to perform their obligation under the contract.[159] Thereafter, the parties have claims against each other for restitution based on unjust enrichment[160] or vindication[161].[162]

---

149 VON TUHR/PETER (n 92) 235.

150 MARLIS KOLLER-TUMMLER, '1. Teil: Einführung in die Grundlagen des privatrechtlichen Konsumentenschutzes' in Ernst A Kramer (ed), *Zehnter Band Konsumentenschutz im Privatrecht* (2008) in Roland von Büren/Christine Chappuis/Daniel Girsberger/Ernst A Kramer/Thomas Sutter-Somm/Pierre Tercier/Wolfgang Wiegand, Schweizerisches Privatrecht vol X (Helbing Lichtenhahn Verlag) 12.

151 Art 20 para 1 CO.

152 Art 20 para 2 CO.

153 KRAMER (n 128) arts 19-20 no 308.

154 ibid arts 19-20 nos 262 et seq.

155 VON TUHR/PETER (n 92) 227 et seq.

156 KRAMER (n 128) arts 19-20 no 369.

157 ibid arts 19-20 nos 369 et seq.

158 ibid arts 19-20 no 404.

159 VON TUHR/PETER (n 92) 225.

160 Arts 62 et seq CO. Pursuant to art 66 CO an exception from this rule applies only "in respect of anything given with a view to producing an unlawful or immoral outcome." Pursuant to Swiss case law and academic commentaries this provision is to be understood restrictively in that restitution is excluded with respect to anything given in order to *incite or reward* an unlawful or immoral outcome (BGE 134 III 438 (consid 3); Yves Rüedi, *Obligationenrecht Allgemeine Bestimmungen Die Entstehung aus ungerechtfertigter Bereicherung, Art. 62-67 OR Ausschluss der Rückforderung, Art. 66 OR*, in Berner Kommentar Kommentar zum schweizerischen Privatrecht vol VI 1. Abteilung 3. Teilband 2. Unterteilband (Stämpfli Verlag AG, 2011) art 66 nos 297 et seq). For the meaning of unlawfulness and immorality in this context see Rüedi ibid nos 351 et seq.

161 Art 641 para 2 CC.

162 KRAMER (n 128) arts 19-20 nos 399 et seq.

c. Smart Contracts and the limits to freedom of contract

How do the abovementioned principles, the limits to the parties' freedom of contract, work when it comes to Smart Contracts?

It has been established that two of the defining characteristics of Smart Contracts are (i) that the "code is the law" and (ii) that they are automatically executed without any party being able to interfere with the execution.[163] In other words, the parties can write anything which is technically possible into the Smart Contract and this content will be executed without the parties having any possibility of preventing that (unless that is written into the Smart Contract as well[164]) and without taking mandatory law into consideration. Under the logic of a Smart Contract, preventing its execution because of anything not within its code (for instance, mandatory law) would amount to a breach of the Smart Contract which is impossible.[165]

Of course, the parties to a Smart Contract are free to draft a Smart Contract in a way which is in line with the limits of freedom of contract. However, the described characteristics of Smart Contracts raise the risk of Smart Contracts being used to circumvent mandatory law. In its most extreme form, Smart Contracts could be used to enforce illegal agreements such as drug deals, that is contracts which are unenforceable under Swiss law, on a factual level.[166] Where one of the advantages of the Smart Contract technology is that the parties *need not* invoke the court system to get their deserved remedies[167] the disadvantage lies in the fact that the parties *cannot* invoke the court system for the same purpose. The state, on the other hand, may only aim to deanonymize and pursue the culprits of such a transaction after the fact.[168] The rule of the code may turn into the "tyranny of the code".[169]

If the colourful term 'tyranny' is cast aside the question remains how much of a problem this effect of Smart Contracts turns out to be. This cannot be predicted on a general level but will have to be assessed with regard to specific applications of Smart Contracts once they begin to develop. However, some general statements seem possible based on the what rationale lies at the core of the different limitations to the freedom of contract:

It goes without saying that a circumvention of criminal law or provisions which protect the public order cannot be tolerated. Breach of this provisions, for instance the use of Smart Contracts to launder money, will be a problem in any case.

Furthermore, the same may at first sight hold true when it comes to provisions which aim to protect the weaker party to a contract, eg in the case of consumer or employee protection. Here, one party is awarded statutory protection because the legislator assumes it will need it. However, future applications of Smart Contracts may also be able to mitigate some problems arising from an imbalance of bargaining power.[170] If this is the case, then it may be sensible to re-evaluate the need to apply such provisions with respect to Smart Contracts.

Finally, it may be argued that parties who elect to enter into Smart Contracts instead of traditional contracts make the conscious decision to give up some of the protection of traditional contract law in favour of the benefits that Smart Contracts offer. This may be the case for parties which have the necessary technological and commercial sophistication to assess the consequences of their choice and where a relative balance of bargaining

---

[163] See above ch III.2.

[164] SAVELYEV (n 8) 18 et seq.

[165] ibid 18.

[166] ibid 20 et seq; WERBACH/CORNELL (n 9) 49 et seq.

[167] NEWMAN (n 12) 26.

[168] SAVELYEV (n 8) 21.

[169] NEWMAN (n 12) 27.

[170] See, for example, SAVELYEV (n 8) 20, who, on the one hand, emphasizes the egalitarian nature of Smart Contracts, that is their inability to protect weak parties such as consumers, but also mentions that Smart Contracts may – instead of protecting them – raise their bargaining power, rendering (some) need for protection obsolete.

power exists. This may warrant to extend the freedom of contract for such parties to some extent. Again however, the argument seems less convincing where less experienced parties are concerned. Bearing in mind that Smart Contracts potentially lower transaction costs and, consequently, open up contractual agreements to less experienced parties[171] their need for legal protection may even increase.

Consequently, the need for a re-evaluation of the limits of freedom of contract may arise eventually potentially leading to an extension of freedom of contract in some areas and to further limitations in others. For that, however, one has to wait and see how Smart Contracts will develop.

4. Enforcement

Regardless of the reassessment of mandatory law just discussed, there is no doubt that some limitations to the freedom of contract will prevail in the future. Also, the mere fact that a contractual obligation is being performed with the use of a Smart Contract does not guarantee that all parties will be happy with the outcome. Furthermore, some parties will not be happy with having entered into the Smart Contract in the first place. Disputes will still arise.[172] How to deal with such disputes concerns the question of how to enforce the law with respect to Smart Contracts.

It appears that the area of enforcement is the biggest question mark in considering the transition from traditional contracts to Smart Contracts. Several problems arise:

a. Jurisdiction and applicable law

Before it can give a judgement, a court has to establish that it has jurisdiction in the matter first. Furthermore, to be able to decide in the case it also has to determine the applicable law.

The rules with regard to these questions in an international case can be found in the PILA.[173] On a general level, it seems safe to assume that many of the questions arising can be solved by applying these rules: Jurisdiction in contract disputes lies either with the court at the domicile of the defendant or at the place of performance of the contract.[174] When it comes to contracts, arts 116 et seq PILA leave the parties the option to choose the applicable law and provides that in case no choice of law has been made the law of the state with the closest connection to the contract shall be applicable. Further, more detailed rules follow.

However, the need may arise to revise these rules, namely, with respect to jurisdiction considering how the application of Smart Contracts may influence who will be claimant and who will be defendant in court proceedings.[175]

b. Application of contractual remedies as provided by the law

The fundamental change that Smart Contracts bring, the fact that they are intended to eliminate the need for enforcement in the first place[176] by being self-executing, arguably also causes the biggest challenge for their implementation in the existing legal system.

Under traditional contract law, whenever disputes arise one of the parties will seek for help from the judges[177] which are entrusted with the authority to adjudicate on the dispute and, then, "the whole power of the state will be

---

171 See above III.3.

172 WERBACH/CORNELL (n 9) 52.

173 Art 1 para 1 of the Federal Act on the Private International Law of 18 December 1987 (PILA), SR 291.

174 Art 112 et seq PILA.

175 See just below ch IV.3.b.

176 WERBACH/CORNELL (n 9) 20.

put forth, if necessary, to carry out their judgments and decrees."[178] It seems fair to argue that the remedies of current contract law actually are built bearing in mind that one party will always have the possibility to have their day in court. The system is fine-tuned with regard to the possibility of ex post judication by a judge.[179] For instance, a party whose consent was deficient when entering into the contract can refuse performance[180] leaving its counterparty only the option to go to the court and ask for a judgement ordering performance.

Smart Contracts, on the other hand, intend to render the role of the court as an enforcer obsolete as they are self-enforcing and cannot be stopped by the parties.[181] But this also prevents the party with the deficient consent from refusing performance. Instead of becoming the defendant in a procedure when its counterparty asks for performance, its only option now is to go to court itself as claimant and ask for restitution and rescission of the contract. Litigation will "be shifted from claims of breach to claims of restitution."[182] While this new situation does not necessarily change the claims of the party with the deficient consent, it does change its situation quite drastically. Being the claimant instead of the defendant has procedural consequences such as a possible change in jurisdiction of the court[183], having to make advance payments for the costs of the proceedings and posting security for the same and/or the presumable costs of the defendant and it may also move the burden of proof at least on a factual level if not on a legal level.[184] This also changes the chances of success, the risks involved in a transaction and the relative power of the parties between each other in a way which could not have been foreseen by the legislator when he enacted the currently applicable remedial system.[185]

c. Enforcement of court decisions

Assuming a party has overcome all the obstacles mentioned before and has succeeded in obtaining a court order in his or her favour the final question which remains is how to enforce this court order.

The enforcement of court orders (*Realvollstreckung*) goes according to the provisions of title 10 of the CPC[186] unless the decision to be enforced relates to the payment of money or the provision of collateral, in which case it is enforced pursuant to the provisions of the DEBA[187]. The rules for the enforcement of foreign court orders are found in the PILA.[188] To enforce an order to act, refrain from acting or to tolerate an action being performed the court can resort to measures like threatening a fine or punishment (indirect force) or direct force or substitute performance.[189] Enforcement abroad works pursuant to the law of the relevant foreign jurisdiction.

---

177 An alternative to the state judiciary would be to enter into arbitration. The issues raised here with respect to state courts apply mutatis mutandis when it comes to arbitration.

178 As it was so famously put by OLIVER WENDELL HOLMES Jr, 'The Path of the Law' (1896-97) 10 Harvard Law Review 457, 457 <http://www.constitution.org/lrev/owh/path_law.htm> accessed 14 August 2017.

179 WERBACH/CORNELL (n 9) 31.

180 Arts 23 et seq CO.

181 WERBACH/CORNELL (n 9) 31.

182 ibid 52.

183 Pursuant to the general rule in art 2 PILA the court at the domicile of the defendant shall have jurisdiction (see also art 112 PILA for contractual disputes).

184 See also WERBACH/CORNELL (n 9) 52 et seq.

185 Similarly, ibid 53.

186 Swiss Civil Procedure Code of 19 December 2008 (CPC), SR 272.

187 Federal Act on Debt Enforcement and Bankruptcy of 11 April 1889 (DEBA), SR 281.1.

188 Art 335 CPC. Swiss Federal Council, 'Botschaft zur Schweizerischen Zivilprozessordnung (ZPO)' of 28 June 2006, Federal Gazette (2006) 7221, 7382.

189 Art 343 CPC; Swiss Federal Council (n 188) 7385.

While the courts and other enforcement authorities have been employing these traditional methods of enforcement for a while and have gathered substantial experience with the obstacles that lie on the way to enforcement the enforcement of court orders relating to Smart Contract transactions might pose additional difficulties.

The preeminent problem in this respect arises when the authorities are unable to 'convince' the losing party (not even by exerting direct force) to obey to the court's order and, instead, would have to resort to substitute performance. It is not inconceivable that this situation might arise since the highly encrypted nature of all blockchain technologies make it relatively easy for any losing party to effectively obstruct the enforcement by simply refusing to obey the court order.

Due to the distributed nature of the blockchain on which the Smart Contract runs and its verification mechanism[190], there is no central intermediary which the authorities could address to enforce the court order. Furthermore, entries on the blockchain are permanent, that is irreversible.[191] "There is no technical means, short of undermining the integrity of the entire system, to unwind a transfer."[192]

Instead, the only way to enforce the court order against the will of the losing party would be to convince the required majority of blockchain validators in the network to implement a counter transaction to give effect to the court order which, presumably, would be quite costly and time consuming and could render enforcement economically inefficient or even useless, eg when a depreciating asset is concerned.[193] The decentralised nature of the blockchain technology effectively pre-empts outside control or corrective intervention.

Therefore, while Smart Contracts were intended to render a cumbersome and slow enforcement of contracts obsolete[194], they may in some cases even prevent the desirable enforcement of court orders.

d. Alternative solutions

Several approaches to mitigate obstacles that lie in the way of enforcement of court orders on a blockchain system have been discussed. However, none of them seems to be fully satisfying:

- *Introduction of a superuser with the right to modify the blockchain*[195]: This effectively eliminates the central premise behind the blockchain technology by re-introducing a central, controlling authority and, thereby, undermines the entire appeal of the blockchain solution.[196]
- *Enforcement outside of the blockchain*[197]: Instead of implementing changes on the blockchain themselves, the authorities could only try to force the losing party to obey the court order by effecting the necessary changes on the blockchain. Alternatively, damage claims could be enforced against its "offline" assets. As discussed, this is not only complex and time-consuming but it can also prove to be fruitless if the losing party has no 'offline' assets that can be confiscated.[198]

---

190 See above ch II.2.

191 AWASTHI (n 43) 1. WERBACH/CORNELL (n 9) 17, use instead the term "irrevocable".

192 WERBACH/CORNELL (n 9) 17. The possible consequences of such an intervention can be seen in the case of the DAO where it resulted in a hard fork effectively splitting the DAO blockchain into two incompatible blockchains, one of which still contains the original transactions while they have been retracted on the other (WERBACH/CORNELL (n 9) 31).

193 The complexity of this task also depends on the specific nature of the concerned blockchain. Enforcement would be simpler in the case of a private blockchain as compared to a public one.

194 WERBACH/CORNELL (n 9) 13 et seq.

195 SAVELYEV (n 8) 22.

196 ibid 22.

197 SAVELYEV (n 8) 22; NEWMAN (n 12) 28.

198 ibid.

- *Incentivising enforcement by imposing reputation costs based on a blockchain-voting system*[199]: This proposition seems to be mainly aimed at preventing future problems by incentivizing parties to adopt proper behaviour by rating their behaviour and, thereby, influencing their reputation.[200] It seems worth to consider applying such a mechanism also when it comes to the refusal to adhere to a court order. However, this does not directly overcome the problem of enforceability of an existing court order.
- *Waiver of judicial enforcement and reliance on developing commercial and technological remedies*[201]: Due to the described obstacles to traditional enforcement parties to Smart Contracts could overcome not to resort to traditional judicial enforcement and rather rely on the fact that commercial practices and technological solutions will develop to mitigate these problems over time.[202] It is fair to assume that such practices and solutions will develop over time.[203] While this seems to be an interesting approach it appears questionable whether this could lead to satisfying results for all parties. On the one hand, this might work for sophisticated market participants. On the other hand, less sophisticated parties with a higher need for protection (eg consumers) might have a hard time in forgoing state judicial support.

V. Is there a need for legislative action with regard to Smart Contracts?

The preceding examination has shown potential applications of Smart Contracts and potential advantages and disadvantages of this new concept. The subsequent legal analysis has identified areas of Swiss law where problems may arise in connection with Smart Contracts. Therefore, the question which remains is whether there is a need for legislative action in view of Smart Contracts.

It is submitted here, that the answer is no, that there is no current need for legislative action. At the moment, Smart Contracts are still a mostly theoretical concept and specific applications remain limited. Rather, it seems sensible to monitor how the technology develops and assess the need for legislative action when more specific recommendations for change are possible.[204]

This cautious approach will enable the legislator to limit its intervention to the required minimum and avoid excessive legislative action.

At first, the commercial practitioners will develop their own practical solutions to the extent possible which are tailor-made to solve the problems as they arise as they have done time and time again in similar situations in the past.

The experience in applying Smart Contracts will grow over time and the users will start to understand their advantages and disadvantages. They will find ways to mitigate risks associated with the disadvantages as far as possible. Examples may include:

- the use of private blockchains instead of public blockchains to strike a balance between the advantages of full decentralisation and some amount of control by an intermediary authority;
- alternative solutions which achieve to have a similar effect as mirror assets would have[205];

---

[199] NEWMAN (n 12) 27.

[200] ibid 27 et seq.

[201] MCJOHN/MCJOHN (n 16) 15 et seq.

[202] ibid.

[203] SAVELYEV (n 8) 22. See also TAPSCOTT/TAPSCOTT (n 12) 219 et seq who discuss the idea of a "blockchain jury".

[204] This corresponds with the conclusion the Swiss Federal Council drew after assessing the impact of virtual (or crypto-)currencies (Swiss Federal Council, 'Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070)' of 25 June 2014 <http://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf> accessed 14 August 2017) 3.

[205] See above ch IV.2.

- tools which simplify the drafting and application of Smart Contracts including some level of standardisation in contract templates and the development of Smart Contract toolboxes[206]; or
- the development of dispute resolution mechanisms to circumvent the obstacles which may prevent the traditional enforcement of court orders in connection with Smart Contracts.[207]

This productive creativity of the market practitioners will be supported by the fact that Swiss contract law can be considered to be very flexible and easily adaptable to new developments. It can be expected that the overwhelming majority of the questions which may arise can be solved in a satisfying way simply by resorting to the existing body of contract law. Swiss contract law is completely open to entirely new types of contracts developing and the law leaves the courts substantive room for the development of new solutions to new problems.[208] Existing statutory and case law can be used by analogy and the courts can develop the law by filling gaps.

An additional argument that legislative intervention at this time would come to early is because it seems fair to assume that regulation of Smart Contracts (and the blockchain technology as well) would need to be coordinated on an international level to some extent to be able to be effective. Due to the decentralization of the blockchain technology the effect of regulation on a national level might remain very limited. In effect, it might be even questionable at times which national law is applicable considering the decentralised nature of the technology. However, it seems that it is too early for an internationally coordinated effort as everyone is only beginning to grasp the implications of these new technologies.

Nonetheless, it seems reasonable to assume that some form of legislative action will be required once the use of Smart Contracts has spread more widely. General statements about what this will entail are hard to make since this will depend on the specific applications of Smart Contracts yet to be developed. However, the above analysis allows for some predictions.

Firstly, it seems crucial to point out that not the technology (ie the blockchain and Smart Contract) should be regulated but their use. Simply put, the use of Smart Contracts to sell illegal drugs should be prohibited but not Smart Contracts as such.[209]

Secondly, a problem which may call for a decision of the legislator in the future is the question of capacity of autonomous agents.[210] Current law may be sufficient to attribute the actions of autonomous agents to their programmer or user, for instance with respect to liability. However, once these programs achieve a certain level of autonomy it will have to be evaluated whether the current law leads to a satisfying outcome in view of this changed circumstances.

Thirdly, the existing contract law was created with traditional contracts' ex post adjudication as the main means of enforcement in mind. The fact that Smart Contracts execute automatically and cannot be stopped even by the parties may change this on a fundamental level.[211] On the one hand, the automatic enforcement of Smart

---

[206] See eg CHRISTOPHER D CLACK/VIKRAM A BAKSHI/LEE BRAINE, 'Smart Contract Templates: foundations, design landscape and research directions' (2016, revised 2017) <https://arxiv.org/pdf/1608.00771.pdf> accessed 14 August 2017.

[207] See the examples above ch IV.4.d.

[208] Art 1 CC states in this respect: "[1] The law applies according to its wording or interpretation to all legal questions for which it contains a provision. [2] In the absence of a provision, the court shall decide in accordance with customary law and, in the absence of customary law, in accordance with the rule that it would make as legislator. [3] In doing so, the court shall follow established doctrine and case law."

[209] Similarly, MCJOHN/MCJOHN (n 16) 17, according to which rules should not be formulated technology-specific.

[210] See ch IV.1.

[211] See also WERBACH/CORNELL (n 9) 45 et seq.

Contract can render other remedies obsolete. On the other hand, this may be problematic because the law limits the parties' choice of remedies, for example when it comes to contractual penalty clauses.[212] The need for such clauses can be circumvented by employing a Smart Contract (or they could be written on the Smart Contract and – illegally – enforced).[213] Therefore, at some point the legislator may have to decide whether, for instance, a relaxation of existing prohibitions may be beneficial. In this respect, it may be sensible to distinguish between sophisticated and less sophisticated parties. While relaxation may be desirable for the former an increased protection of the latter (eg consumer protection rules) may be sensible. Protection of weaker parties is likely to remain a problem which warrants statutory intervention as Smart Contracts are not able to handle it.[214]

Fourthly, the legislator will have to find a way to satisfy the need for digital mirror assets.[215] This is perhaps the most urgent problem as it has already arisen outside of the Smart Contracts context. Practitioners can only mitigate the limits of the existing law to some extent. At the same time, this provides the legislator with the opportunity to find a more general solution which is not only limited to the blockchain and Smart Contract technologies.

Fifthly, the decentralized nature of the blockchain technology and its lack of any central authority challenges the traditional ex post enforcement of contract and other mandatory law.[216] Not only is the enforcement of rules from outside of the blockchain/Smart Contract difficult, but the idea of changing entries on the blockchain by 'force' threatens the whole concept and the functionality of the technology on a fundamental level. Therefore, this is, perhaps, the most complex problem to overcome and it seems reasonable to say that it is unclear how this will be achieved. Several proposals are already being discussed and developed.[217] In view of the undisputed benefits that the technology has, the legislator will face a trade-off and will have to strike a balance between enabling parties to use the technology and maintaining the rule of law. For instance, the benefits resulting from the fact that Smart Contracts will be executed as agreed under all circumstances, may lead to the evaluation whether some of the mandatory rules, eg contractual remedies such as rescission of the contract, need to be limited in order not to interfere with the integrity of the blockchain.

Finally, one must not forget that the blockchain and Smart Contract technologies are relatively new and were originally developed by a community of technologically interested people with a very particular mind-set and, among else, with the specific goal in mind to get rid of a central authority.[218] The reaction to the correctional intervention to save The DAO may serve as an example. After the participants of The DAO suffered substantial losses when programmers were able to exploit a vulnerability of its code, the original creators opted to revert The DAO blockchain to its previous state. From a legal point of view, this course of action seems self-evident. However, it was met with substantial opposition by the community when

> "someone claiming to be the attacker published a blog post in which they criticized the founders of the DAO for their backpedalling. The DAO, the attacker claimed, was created to

---

[212] Art 163 para 2 CO; ANDREAS VON TUHR/ARNOLD ESCHER, *Allgemeiner Teil des Schweizerischen Obligationenrechts vol II* (3rd edn) (Schulthess Polygraphischer Verlag AG, 1974) 285.

[213] NEWMAN (n 12) 26 et seq.

[214] SAVELYEV (n 8) 20, calls this the egalitarian nature of Smart Contracts.

[215] See above ch IV.2.

[216] See above IV.4.

[217] See IV.4.d. SAVELYEV (n 8) 22.

[218] NAKAMOTO (n 7) 1.

replace law with code, warts and all. The attacker hadn't stolen anything, in their own view. They had merely found a legal loophole."[219]

Ultimately, this led to a hard fork in the blockchain effectively splitting it into two coexisting blockchains, one with and one without the disputed transactions.[220] As the technology makes its transition into the world of commerce this mind-set may change and with it the willingness to accept correcting interventions by the legislator.

VI. Conclusion

The potential applications of Smart Contracts on the blockchain are vast and sound very promising. If applied in a sensible way this technology indubitably will lead to gains in efficiency of contract execution and lower transaction costs.

But insofar as Smart Contract proponents expect Smart Contracts to render legal practitioners, courts and maybe even the law useless they are mistaken[221]:

Smart Contracts will not prevent contractual disputes from arising. Consequently, parties will still resort to court actions. In these cases, Smart Contracts may tend to make things more complicated because while they may not eliminate the need for courts they limit the accessibility of courts for their parties via their self-enforcing nature.

Furthermore, while Smart Contracts may attempt to substitute law by code that does not mean that they will be able to render the law useless. There will still be need for mandatory law for various purposes, including, but not limited, to protect the parties from adverse consequences which the Smart Contract technology itself may produce. No legislator, it can be assumed, will be willing to give up its legislative power and submit to a "tyranny of the code".

The results from the previous analysis of Smart Contracts under Swiss law serve as an example of the obstacles which the law and commercial practice will have to overcome to be able to efficiently apply Smart Contracts. While Smart Contracts qualify as contracts in the legal sense problems may arise with respect to questions such as the capacity to enter into contracts, what assets can be transferred via Smart Contracts, the adherence to mandatory law and enforcement.

All this is not to say that Smart Contracts are a negative development but that they will be but one of several available forms to enter into and perform agreements. They will add to the existing contract law rather than substitute it.

What the balance, which eventually will be found, will look like remains to be seen. But it appears to be a sensible advice to closely and continually monitor the progress of the Smart Contract technology in order to be able to mitigate undesired consequences and not to end up like the sorcerer's apprentice in GOETHE's poem only able to exclaim:

"Wrong I was in calling
Spirits, I avow,
For I find them galling,
Cannot rule them now."[222]

---

[219] ROTHSTEIN (n 8) 196.

[220] See also WERBACH/CORNELL (n 9) 31.

[221] See SAVELYEV (n 8) 21 and WERBACH/CORNELL (n 9) 3, with reference to the former.

[222] JOHANN WOLFGANG VON GOETHE, 'The Sorcerer's Apprentice' (English translation of ‚Der Zauberlehrling' (1827)) <http://germanstories.vcu.edu/goethe/zauber_e4.html> accessed 13 August 2017.

Blockchain Implications for Land Reform in Ukraine – Lessons for International Business

LLB, MBA, LLM (Lon)
Anastasia Demchuk

Blockchain Implications for Land Reform in Ukraine – Lessons for International Business

TABLE OF CONTENTS:

INTRODUCTION

1 Historical and Current Problems of Property Rights Protection

2 Development and Challenges of Land Tenure in Ukraine

2.1 Acceleration of the Land Reform

2.2 Assessment of the Current Legal Framework

2.3 Governmental Corruption and Its Impact on the Land Reform

2.4 Imperfections of Current Property Rights Protection System

3 Blockchain as a Possible Solution for Property Rights Protection

3.1 How Blockchain Works Technically

3.2 Blockchain as a Possible Solution for Recordkeeping of Property Rights

ANALYSIS

4 Blockchain for Land Registration. Analysis of Developed and Developing Countries' Experience

4.1 Applying Blockchain to the Specific Problems for Land Reform in Ukraine

FINDINGS

5 Alternative Advantages of Blockchain in International Business

CONCLUSION

BIBLIORGRAPHY

INTRODUCTION

The current rapid pace of technological change, and its frequently novel and unpredictable interactions with and impact on society, poses a challenge to legislators and regulators globally. The potentially most disruptive of these is the Distributed Ledger Technology ('DLT'). The most notable application of this technology, commonly referred to as *blockchain*, thus far is in the creation of the cryptocurrency unit Bitcoin. Bitcoin has been the subject of much analysis, hyperbolic commentary and wild speculation. However, until recently the media focus on Bitcoin obscured the potentially far more significant deployment of blockchain technology by the commercial sector and by state institutions, with both the negative and positive connotations its use by such actors necessarily imparts. Blockchain is now employed by a number of financial institutions and commercial entities worldwide in a host of transactions, and has recently been trialed by a number of governments keen to apply it to solve a range of administrative and legislative problems. Despite the exponential increase in the use or proposed use of blockchain, regulators and lawmakers still struggle to establish suitable guidance or legislation to assist in the integration of the technology into existing legal frameworks.

The purpose of this paper is to critically analyze the phenomenon of blockchain technology in the specific context of its application to land reform in Ukraine. This is part of a drive by the Ukrainian state to ensure the protection of property rights and, consequently, to instill a greater degree of confidence in overseas companies investing in the Ukraine. The importance of demonstrating a robust and impartial legal framework within which property transactions can be securely conducted is self-evident. This particularly so in Ukraine's case, being heavily dependent on Foreign Direct Investment. This paper also contains an empirical comparative analysis of the issues faced by other jurisdictions in relation to property rights protection (land tenure).

Ukraine was chosen as a suitable subject for study in part because of the author's Ukranian nationality and consequent familiarity with the Ukrainian legal system, but principally because of the particular challenges the country faces, and the proposed use of blockchain technology to address some of these issues. The International Monetary Fund's involvement in this process is encouraging the country to adopt more radical solutions to the endemic problem of corruption, which the current system of land transfer facilitates. Processes and procedures for evidencing transactions, ascertaining title, proving ownership and other fundamental areas of land law have been identified as being inherently flawed in Ukraine, but – as this paper will argue – they are also well-suited, in theory, to the inclusion of blockchain technology. While the benefits of the successful deployment of blockchain technology will be assessed, the potential pitfalls and obstacles of and to introducing DLT will also be examined. This particularly during the transition period. Possible points of friction include, *inter alia*, resistance and potential fraudulent activities from vested interests, inaccurate data on current registers and inadequate regulatory and legal oversight of the transfer process.

The relative paucity of material relating to the legal issues surrounding the use of blockchain technology and the sparse empirical evidence available on the success, or otherwise, of its application in commercial and public sectors limit the scope of a literature review. Nevertheless, this paper will argue that the use of blockchain in public and commercial sector activities is not only feasible, but highly desirable in the context of current technological advancements.

1 Historical and Current Problems of Property Rights Protection

The evolution of property rights into the form extant in nearly all contemporary free market economies has been a protracted and complex process. The fundamental importance of the establishment of enforceable real property rights in stimulating economic development is well attested. Thereto, the law can provide certainty, which facilitates investment and provides a secure basis for conducting transactions.[1] The parties to the purchase, sale, rental or other forms of transfer or rental of property entered into contractual relations in the knowledge that the inherent risks in such activity would hopefully be ameliorated by recourse, if necessary, to a court of law or a similarly disinterested institution or individual endowed with the authority to settle disputes following clearly established rules.

In Eastern Europe, development and spread of enforceable property rights has been a slow and uneven process. However, following the collapse of the Soviet-system, nearly all sovereign states now have a firmly established and sophisticated legal nexus, which (in theory) guarantees state protection for property rights. An obvious corollary of the efficacy of such legislation is the existence of a judicial and political framework which assures their continued, universal application. The right to exploit, sell, lease, exchange, or freely engage in any other profit (or otherwise) generating activity within the boundaries set out by relevant legislation is fundamental.[2]

Eggertsson identifies three basic categories of property rights: Firstly, there are owners' rights which determine what an individual can legitimately do on his property. Second, there is the right to generate an income from an asset and to engage in contractual relations with other parties for this purpose. Finally, he notes the critical importance of the right to alienate or sell ownership rights over an asset to others. The equitable and just application and dispensation of relevant legislation, and adherence to the rule of law, are as in all other areas

[1] Timothy Besley & Ghatak Maitreesh, 'Property Rights and Economic Development' (2009). CEPR Discussion Paper No. DP7243. Available from: <https://ssrn.com/abstract=1372563> [Accessed: 5 May 2017]

[2] Adam Przeworski, Fernando Limongi & Salvador Giner, 'Political Regimes and Economic Growth' (1993) Journal of Economic Perspectives (1993), vol. 7, no. 3 <https://link.springer.com/chapter/10.1007/978-1-349-24076-0_1> [Accessed: 18 May 2017]

of the law, paramount to its relevance and effectiveness. As author underlines, property rights underpin or are directly connected to many other rights deemed desirable in a stable and fair society.[3]

The number of states with a developed, well-established legal system, an independent and potent judiciary and effective means of enforcing judgment and – arguably – a democratic mandate have increased steadily over the course of the 19th and 20th centuries.[4] However, many sovereign states possess executive, legislative and judicial structures in which the balance of power is unevenly distributed, partially as a result of the imperfect creation or application of laws, the dominance of interest groups, and the prevalence of corruption.[5] The arbitrary appropriation of land by the state or private institutions or individuals, non-recognition of title, weakness of state institutions, poor administration, inaccurate and/or incomplete records and cost and complication involved in the enforcement of rights are all common features of many developing countries. As a result, lawful title holders may be deprived of their rights, as would individuals who are unable to provide proof of title, despite having 'owned' the land for generations. Expropriation of their land or extortion are a near-inevitable consequence.[6]

According to a report by the Independent Evaluation Group of the World Bank, *70 percent* of the world's population still lacks access to proper land titling or demarcation.[7] As Don Tapscott noted, "a significant proportion of the world's population subsequently believe they own land or property, whilst being unable to convincingly substantiate their right."[8]

The economic consequences of a lack of appropriate legal safeguards for property rights was summed up by Hernando De Soto, who noted "When something is not legally on record as being owned, it can therefore not be used as collateral to get credit, as a credential that you can be able to transfer part of your property to invite investment in. Things are owned, but when they are not adequately recorded, therefore cannot fill the functions of creating capital and credit."[9] In noting this intertwined relationship between the economic health of a community or state, De Soto expands on this thesis by pointing out that a lack of legal title can stem the flow of capital and thus freeze investment, as an asset is incapable of being used as adequate security for a loan. The asset in question "cannot be used to obtain surplus value through multiple transactions because [its] improperly fixed nature … leaves too much room for misunderstanding, faulty recollection and reversal of agreements. In short it is dead capital".[10]

Indeed, the ineffectualness or rudimentary operation of 'land administration' – e.g. the registration of title, record keeping, conflict resolution and land management – in turn reduces the convertibility of land into liquid assets. Procedural impotence or gridlock, particularly when coupled with other political issues, can consequently have a dampening effect on investor confidence, as evidenced in Ukraine in recent years

[3] Thrftinn Eggertsson. *Economic Behavior and Institutions.* (Cambridge University Press, 1990)

[4] Daniel Kaufmann, Simon Johnson & Pablo Zoido-Lobatón, 'Regulatory Discretion and the Unofficial Economy' Vol 88 (2) The American Economic Review. Available from: <http://www.jstor.org/stable/116953> [Accessed: 18 May 2017]

[5] David Stanfield, *Creation of Land Markets in Transition Countries: Implications for the Institutions of Land Administration.* International Conference on Land Tenure and Administration (Orlando, November 1996)

[6] Council on Hemispheric Affairs*, 'Human Rights Violations in Honduras: Land Seizures, Peasants' Repression, and the Struggle for Democracy on the Ground'*. Available from: <http://www.coha.org/human-rights-violations-in-honduras-land-grabs-peasants-repression-and-big-companies/> [Accessed: 3 May 2017]

[7] April Connelly & Caroline Heider, 'Why Land Administration Matters for Development', World Bank Group, (2016). Available from: <https://ieg.worldbankgroup.org/blog/why-land-administration-matters-development> [Accessed: 3 May 2017]

[8] Alex Tapscott & Don Tapscott, *Blockchain Revolution* (Portfolio Penguin Group, 2016)

[9] Hernando De Soto, *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else* (Black Swan, 2000)

[10] ibid

according to recent report.[11] To reiterate; the economic prosperity of a country is heavily contingent upon the formalization and adequate recording of property rights, with the systemic failure of the politico-administrative apparatus to provide security for the latter potentially having a profound effect on a nation state's development. A study reaffirmed the critical importance of the maintenance of such rights, which in theory serve to preclude the exercise of arbitrary power, in concluding that the reliability of institutions guaranteeing property rights was of far greater import in sustaining economic development than that of contracting institutions.[12] It is almost unnecessary to add that this is particularly valid in cases where the country in question is heavily dependent on FDI, and 'plugged in' to the global economy.

2 Development and Challenges of Land Tenure in Ukraine

Those countries of Eastern and Central Europe which, after WWII, fell under the Soviet Union's direct or indirect control or sphere of influence, initiated in 1946 the process of transitioning from pre-war capitalist, market-oriented economies (based on private ownership of the means of production with state support and some ownership of productive assets) to centralized economies structured on a socialist blueprint laid down by the Soviet Union (based on public ownership of the means of production with some private ownership and use). This process was not applied uniformly, but rather varied in extremity and design depending on the degree of influence exerted by the Soviet Union. Regardless, however, of the difference between these states, the general trend was the same: The curtailment or elimination of existing private property rights and the creation of state property rights over new investments in land.[13]

The swift decline of Soviet power in the late 1980's witnessed a near-complete reversal of this process - a transformation back to a capitalist, free market system in all of the post WWII socialist 'transition' countries, bar Belarus.[14] The unexpectedly rapid collapse of the Soviet edifice rendered the process particularly disruptive, and economically painful, for the countries which had formerly been completely integrated (and indeed, either never been independent states or which had only a very limited experience of nationhood) into the USSR.[15]

One of the principal defining features of this transition has been the privatization of publicly owned land and physical assets attached to the land, that is, the recreation of private rights to land. In many states, these reforms were either imposed as part of agreements for the provision of financial assistance by external parties such as the IMF and the United States, and/or the result of advice dispensed by think tanks, consultancies and other third parties who were commissioned to 'modernize' the ex-socialist economies.[16]

---

[11] Dragon Capital, 'Corruption and lack of trust in the judiciary in Ukraine are the largest obstacles for foreign investors. Dragon Capital and the European Business Association survey results' (*Dragon Capital*, 14 September 2016). Available from: <http://www.dragon-capital.com/en/about/media/press_releases/corruption_and_lack_of_trust_in_the_judiciary_in_ukraine_are_the_largest_obstacles_for_foreign_investors.html> [Accessed: 20 June 2017]

[12] Acemoglu Daron, James Robinson & Simon Johnson, "Institutions as a fundamental cause of long-run growth." *Handbook of economic growth* (2005)

[13] Csaba Csáki & Zvi Lerman, *Land Reform in Ukraine: The First Five Years,* (World Bank Publications, 1997). Available from: <http://documents.worldbank.org/curated/en/936661468319489762/Land-reform-in-Ukraine-the-first-five-years> [Accessed: 3 May 2017]

[14] ibid

[15] Andrzej Rapaczynski & Roman Frydman, 'Institutional Reform in Eastern Europe: Evolution or Design' 1992, BYU Law Review. Available from: <http://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1736&context=lawreview> [Accessed: 15 July 2017]

[16] Rawi Abdelal, *National Purpose in the World Economy: Post-Soviet States in Comparative Perspective* (Cornell University Press, 2001)

These private rights include private ownership, which encompasses the right to hold and transfer rights to land, as well as leasehold or other subsidiary tenure forms where the state continues to be the owner of the land. The institutional definition of property rights to land has been at the core of both transitions, and indeed enshrined in the constitutional documents for many of them.[17] As mentioned above, the road traversed by these states to fully functioning free market economies was frequently far from smooth, with endemic problems of corruption, cronyism and the capture of major parts of the economy by a small number of individuals (the so-called oligarchs) being notable features of countries such as Russia and Ukraine.[18] While the turbulence experienced by those countries which later acceded to the European Union has largely subsided (although recent developments could undermine the progress made in Poland and Hungary), Ukraine succumbed to a succession of political convulsions which have seen ever-growing economic divergence from its neighbors.[19] While in part attributable to its lack of mineral resources, Ukraine also suffers from its unenviable geopolitical situation and the persistent, related problem of national identity: the vexatious issue of whether Ukraine is 'European' or 'Russian' is one which continues to exercise passions, not least with regard to Russia's annexation of Crimea and the simmering civil conflict in the Donbas region in the east of the country. The country witnessed a steady decline in FDI inflows between 2012 and 2014, as the country's tensions with Russia and external concerns about the pace and efficacy of reforms shook investor confidence.[20]

Since independence in 1991, Ukraine has struggled to establish a stable, functioning democracy subject to the rule of law. Established ('Western') European legal norms, such as notions of personal and public freedom, protection of human/civil rights, protection against - and redress for - arbitrary breaches of the law by the state have been introduced, but the lack of rigor in their enforcement has been inconsistent, with the most egregious excesses perhaps most notably committed by former, deposed, president Viktor Yanukovych and his associates.[21] The challenge of developing an effective regulatory framework, and the administrative and governmental institutions capable of overseeing it, has until now proven to be beyond the Ukrainian state's capabilities.

Even prior to Ukraine's independence, the Supreme Soviet attempted to enact land reforms which would pave the way for a shift to a capitalist economy. The first resolution, entitled "On Land Reform", was passed in December 1990. It subsequently came into effect after Ukraine became fully independent on the 15th of March 1991. Since then, a series of laws, regulations and decrees have followed, incrementally establishing a comprehensive legal framework for land reform in Ukraine.[22]

---

[17] Adam Przeworski, *Democracy and the Market: Political and Economic Reforms in Eastern Europe and Latin America,* (Cambridge University Press, 1991)

[18] Allina Pisano, 'Sub Rosa Resistance and the Politics of Economic Reform: Land Redistribution in Post-Soviet Ukraine' (2004). World Politics, Cambridge Press, Volume 56, , July 2004. Available from: https://www.cambridge.org/core/journals/world-politics/article/sub-rosa-resistance-and-the-politics-of-economic-reform-land-redistribution-in-post-soviet-ukraine/78325D8788FA3330677336AAFDB099E2 [Accessed: 2 June 2017]

[19] Simon Tilford, 'Poland and Ukraine : A tale of two economies', Centre for European Reform Bulletin Issue 95/2014. Available from: <http://www.cer.eu/sites/default/files/publications/attachments/pdf/2014/bulletin_95_st_article1-8624.pdf> [Accessed: 10 July 2017]

[20] Trading Economics, Ukraine Foreign Direct Investment – Net Inflows Statistical Data 1998-2017. Available from: <https://tradingeconomics.com/ukraine/foreign-direct-investment> [Accessed: 10 June 2017]

[21] OECD, 'Anti-Corruption Reforms in Ukraine' (2015), Round 3 Monitoring of the Istanbul Anti-Corruption Action Plan. Available from: <https://www.oecd.org/corruption/acn/Ukraine-Round-3-Monitoring-Report-ENG.pdf> [Accessed: 2 June 2017]

[22] Resolution of Supreme Soviet of Ukraine "On Land Reform" (December 18, 1990; amended May 5, 1993), Law on Forms of Land Ownership (January 30, 1992), Law on Collective Agricultural Enterprise (May 4, 1993) Resolution of Supreme Soviet of Ukraine "On Acceleration of Land Reform and Privatization of Land" (7 March, 1992), Land Code (March 13, 1992), Law on Peasant Farms (June 22, 1993), Government Decree "On Privatization of Land Plots" (December 26, 1992), Resolution of Supreme Soviet of Ukraine "On the Social – Economic Situation in Ukraine and Measures for Its Stabilization" (January 27,

The monopoly held by the state over the ownership of land, a defining feature of the Soviet state since 1917, has been whittled away post-independence with the reform of land ownership being seen by successive governments as a necessary prerequisite for both securing foreign investment, and for creating an economic system predicated on free market principles.[23] The dearth of state bodies capable of providing support and guidance to facilitate this process resulted in advice being solicited, as previously mentioned, from developed countries with perceived expertise in the issues at stake. The selfsame countries were also used as templates upon which to model the Ukrainian system, built as it was entirely from scratch.[24]

The resultant reforms implemented by the Ukrainian state in 1992 established the principal forms of land tenure permissible under law, alongside legislation dealing with state ownership, and collective and private land tenure. One of the pillars of these reforms was the wholesale transfer of previously state-owned land to private hands, a measure designed to boost the productivity of the agricultural sector. The second strand of the reforms involved the drawing up of regulations conveying land to members of agricultural enterprises who were, at the time, using these enterprises.[25] At that time, collective farming was prevalent in Ukraine. Privatization, therefore, had as one of its main objectives the transfer of land to private landowners, but this aim failed to be fully realized in the initial stages of the reform program as many previously state-run agricultural concerns managed to maintain near-total legal control over their land and assets. The poorly thought-out and drafted legislation was open to circumvention and abuse. The lacunae resulted in the enacting of further, remedial, law by Ukraine's president on the 10th of November 1994 in the form of a decree: "On Urgent Measures to Accelerate Land Reform in the Field of Agricultural Production".

The central concern of this legislation was to expedite the process governing the transfer of land from collective ownership in state-run agricultural enterprises to private ownership through a fair, carefully regulated redistributive system. The new right of title was to be evinced through the possession of a share certificate, with the owners of the certificates being entitled to the right of disposal of an allotted parcel of land (pai), through private exploitation, sale or lease. Almost 6.7 million citizens, who were members of about 11,000 collective agricultural enterprises, were theoretically entitled to receive certificates. However, serious flaws in the distribution process resulted in many cases of certificates for land parcels not being issued at all, or never being delivered to the legitimate owner.[26] With the adoption of a newly amended constitution in June 1996,

---

1993), Law on Amendments and Additions to Some Laws of Ukraine (May 5, 1993), Government Resolution "On Priority of Measures for implementation of Land Reform" (No. 334 May 7, 1993), President Decree "On Immediate Measures for Acceleration of Land Reform in the Sphere of Agriculture Production" (No. 666, November 10, 1994), Government Resolution 'Procedure for Monetary Valuation of Agricultural Land and Land of Settlement" (213, March 23, 1995), President Decree "On Leasing of Plots of Non-Agricultural Land for Entrepreneurial Activity" *(*June 12, 1995), President Decree "Regulations for Division of Land Shares, Transition to Collective Ownership of Agricultural Enterprises and Organizations" (No. 720, August 8, 1995)

[23] Avi Lerman, 'Agricultural Transition in Post-Soviet Europe and Central Asia after 25 Years' (2015), The Center for Agricultural Economic Research and The Hebrew University of Jerusalem, Volume 79. Available from: <https://www.iamo.de/fileadmin/documents/sr_vol79.pdf> [Accessed: 2 July 2017]

[24] Adam Przeworski, *Democracy and the Market: Political and Economic Reforms in Eastern Europe and Latin America,* (Cambridge University Press, 1991)

[25] Csaba Csáki & Şevl Lerman, 'Land reform in Ukraine : the first five years' (1997) World Bank discussion paper, 371, International Bank for Reconstruction and Development, http://documents.worldbank.org/curated/en/936661468319489762/pdf/multi-page.pdf

[26] The World Bank, Organization for Economic Co-operation and Development, *Publication Achieving Ukraine's Agricultural Potential Stimulating Agricultural Growth and Improving Rural Life (2004)*. Available from: https://www.oecd.org/tad/agricultural-policies/34031855.pdf [Accessed: 6 June 2017]

Ukraine's state-owned collective agricultural enterprises as distinct legal entities were, theoretically, stripped of their rights. In practice, however, the situation in respect of land rights remained largely unchanged.[27]

1997 witnessed a further legislative attempt to affect a new strategy for the development of land reform. The law in question again envisaged the transformation of extant collective agricultural entities into enterprises subject to free market forces, an aim which was to be achieved through the creation of 'land shares'. Members of soon-to-be-dissolved collectives were issued these legal instruments, each of which entitled the shareholder exclusive rights over a plot of land.[28] On the 21st of April 1998, Decree No. 332/98 'On Protection of the Rights of Owners of Land Parcels (shares)' was passed.[29] This provided further clarity on the matter of how the newly-created private owners of land plots would be protected in law, by stipulating that contractual agreements covering the sale, lease and transfer of rights to land parcels (shares) were, after notarization, subject to registration by the district state administration at the location of the collective agricultural enterprise or agricultural cooperative. Any relevant changes to the records were to be securely logged in the register of certificates for the right to a land parcel (share). All records were drawn up manually and stored as hardcopies, in a paper-based form.

2.1 Acceleration of the Land Reform

Against a backdrop of seemingly unending economic instability and political turbulence, successive Ukrainian governments enacted a series of land law reforms over the 25-year period after independence. These also oversaw the establishment of a number of property rights institutions. The point of Avi Lerman proclaims that the frequent – sometimes violent – changes of government has resulted in a great degree of inconsistency and uncertainty regarding both the law itself, and its enforcement by weak state institutions. Systemic problems persist, including the inaccurate recording of land ownership in the register, corruption, an illicit (but thriving) rental market, and the widespread issue of unregistered rights.[30] Perhaps most significantly to state, from the perspective of foreign investors, is the fact that there is still no functioning, legal market for agricultural land, despite nearly two decades having elapsed since the ratification of Decree No. 332/98.

The enactment in 2013 of a law entitled 'On the Registration of Property Rights' and a related piece of legislation - 'On State Land Cadastre' – was designed, like preceding statutes, to tackle the inherent inequities in the Ukrainian system, chiefly through the expedient of digitalizing land records. The dual system of electronic land registration, which affected the administrative separation of land plots and property rights attached to them, has been controversial according to senior associate at Ukraine's leading law firm, Vasil Kisil & Partners.[31] The remit of the newly established State Service of Ukraine for Geodesy, Cartography and Cadastre (StateGeoCadastre) was to be restricted to the registration of land plots, whereas the State Registration Service assumed responsibility for the registration of property ownership which included plots of land.

The efficacy of these reforms has been, to put it mildly, questionable: A system designed to streamline the process of determining the ownership of, and alienating, property has only partially succeeded. While 1.6

[27] OECD, Privatisation in the 21st Century: Recent Experiences of OECD Countries, Report on Good Practices January 2009 https://www.oecd.org/daf/ca/corporategovernanceofstate-ownedenterprises/48476423.pdf

[28] The World Bank (n 26)

[29] President Decree No. 332/98 was passed, 'On Protection of the Rights of Owners of Land Parcels, http://zakon2.rada.gov.ua/laws/show/332/98

[30] Lerman (n 23)

[31] Anna Sisetska, 'State Registration of Land Lease Rights' (2014) Ukrainian Journal of Business Law. Available from: <http://www.vkp.ua/content/files/sisetska_ujbl_page23-24.pdf> [Accessed: 8 June 2017]

million hectares of state farmland is recorded in the state register, a staggering 8.9 million hectares of state farmland has not yet been entered.[32]

Other issues have arisen with regard to the process of reconfirmation of ownership, a requirement which has revealed itself to be particularly vulnerable to abuse and/or error. The procedure was necessitated by the fact that a significant amount of land had never been previously registered with any state institution. A related difficulty surrounded the introduction of a new format of title documentation of land ownership concludes Dr Fateeva in her research.[33] The State Land Agency was no longer permitted to grant certified entitlement to land, a reform which has led to a number of landowners who have lost their certificates being trapped in the vicious circle of being unable to reregister their rights with the newly created State Registration Service. The lengthy and expensive process of having to petition the court for official recognition of their legal rights over land is an inequity which has yet to be adequately addressed.[34]

The transfer of information from paper to the electronic system has also thrown up a further issue. While the e-register promised free access to an online database of registered land plots, neither the State Land Agency nor State Registration Service provided any additional information about ownership or – crucially - encumbrances on the plot. These lacunae, errors and systemic failures have attracted considerable criticism, with many experts noting that the new register actually serves to perpetuate corrupt practice rather than provide adequate remedies to the longstanding problems detailed above. Reforms aside, the status of agricultural land remains highly contentious.[35] One of Ukraine's greatest natural assets, historically, has been its abundant and fertile farmland, a feature of the country which successive post-independence governments have sought to protect by the imposition of strict restrictions on its transfer. Around 71% of Ukrainian land (42.7 million hectares) falls under the agricultural category, but the state's designation of this land as a strategic asset has had unfortunate economic consequences, with decades of underinvestment and under-exploitation. Over 10 million hectares of this land is owned by the state, which amounts to around 25% of the total amount of agricultural land in Ukraine, and approximately 23 million private landowners and land-users.[36]

Part 1 Article 14 of the Constitution of Ukraine states that land resources are to be considered a 'strategic national asset', guaranteeing its absolute protection by the state when are where necessary.[37] This constitutional clause has exacerbated the difficulty of ensuring that liberalizing legislation - such as Article 90 of the Land Code of Ukraine[38] – is actually rendered effective. Starting in 2001, successive governments of all stripes have stymied reform of ownership and legal alienation of agricultural land, for a variety of reasons.

In that year the Ukrainian Parliament (Verkhovna Rada) voted through a ban on the alienation of agricultural land, and a further bar on the ability to alter its usage (i.e. a moratorium on the conversion of farmland to

[32] Heinz-Wilhelm Strubenhoff, 'Unleashing the potential of agriculture in Ukraine' Future Development Brookings. Available from: <https://www.brookings.edu/blog/future-development/2016/03/03/unleashing-the-potential-of-agriculture-in-ukraine> [Accessed: 6 July 2017]

[33] Inna Spasibo-Fateeva, *Problems of state registration of rights and transactions* (National Law Academy of Ukraine Yaroslav Mudry Research, 2015). Available from: https://www.yurradnik.com.ua/.../2004_3_007_problemi_gosudarstvennoj_regi> [Accessed: 6 July 2017]

[34] Alexander Borodkin, 'Specifics Of Purchasing And Formalising The Rights To The Land Plots In Light Of Reforming The Procedure For Registration Of Property Rights To Real Estate' (2013) *Pravovy Tyzhden*. Available from: <http://www.vkp.ua/content/files/borodkin_pravovy_tyzhden_osoblyvosti_prydbannya_ukr.pdf> [Accessed: 3 May 2017]

[35] Lerman (n 23)

[36] The World Bank (n 26)

[37] The Constitution of Ukraine of June 28, 1996. The Supreme Council of Ukraine record, 1996, no. 30 [in Ukrainian]. http://ufpp.gov.ua/content/PDF/zakonodavstvo/konstitychiya.pdf

[38] The Land Code of Ukraine. <http://land.gov.ua/za-typamy-normatyvno-pravovoho-aktu/zemelnyi-kodeks.html>

industrial, residential or other purposes). Ostensibly, the ban was intended to frustrate the ability of mal-administered local authorities to engage in 'shadow activity', in other words, to abuse the extant system. Although the original moratorium was only intended to last until January 2005, it was repeatedly extended and in November 2016 the Ukrainian parliament voted to do so again, until the outset of 2018. [39] The tight restrictions on land alienation have helped to fuel a more widespread lack of confidence in the Ukrainian economy, both domestically and abroad, as has the inconsistent and somewhat arbitrary use of Article 14 by the State. In 2015, for example, further limitations were imposed on the right to lease agricultural land, in part due to the government's uneasiness at possible foreign (read: Russian) interference in Ukraine's political and economic affairs.[40]

As at July 2017, extant legislation only permits landowners to lease their land plots, exchange them for another land plot, or to bequeath them to their direct descendants. The designated purpose of the land cannot be altered, nor can the land be used as collateral or rights assigned to it. While these limitations remain on the statute books, in practice landowners have adopted a range of approaches in order to obviate and circumvent them. Informal leases, grossly unequal land 'swaps' which are, in fact, thinly disguised sales, and outright corruption are all widespread according to expert group review.[41]

Political machinations at a national as well as local level have compounded this problem, as numerous parliamentarians have vested interests in maintaining the status quo. [42]With the issue of agricultural land law reform being repeatedly kicked into the long grass by the majority of its lawmakers, it has only been since the IMF's insistence that the country tackle some of its more deep-rooted structural problems – a prerequisite for financial assistance – that the first tentative signs of progress are becoming visible. Two recent legislative amendments, 'On the Registration of Property Rights' and 'On State Land Cadastre' have been cited as evidence of a hardening of the Ukrainian government's determination to deal with some of the problems outlined above, though arguably the changes still lack clarity.[43] However, the contentious, critical issue of the agricultural land moratorium shows little sign of resolution.

The International Monetary Fund's position merits attention at this point, in part because of the importance to Ukraine's economy of the loans advanced by the organization, and because the IMF's 'stamp of approval' – i.e. recognition that the country is implementing those reforms necessary to bring it into line with the legislative framework governing other developed economies. In March 2015, the IMF opened a four-year credit program with Ukraine for $17.5US billion. A loan was offered, and accepted, which was structured to be delivered in four tranches. IMF drew up a memorandum of cooperation with Ukraine, a document which strongly iterates the need for the latter signatory to accelerate the pace of land reform, and to lift the moratorium on the alienation of agricultural land. The creation of a transparent land market is central to the IMF's position: It sees this as

---

[39] The World Bank, *Issues and Options for Improved Land Sector Governance in Ukraine Application of the Land Governance Assessment Framework in Ukraine,* (2014). Available from: <http://siteresources.worldbank.org/INTLGA/Resources/Ukraine_Synthesis_Report.pdf> [Accessed: 6 July 2017]

[40] Alan Bjerga, Volodymyr Verbyany,' That Boom You Hear Is Ukraine's Agriculture' *Bloomberg* (14 October 2016). Available from: <https://www.bloomberg.com/news/articles/2016-10-14/that-boom-you-hear-is-ukraine-s-agriculture> [Accessed: 2 May 2017]

[41] Denys Monastyrskyi ,Igar Tyshkevich , Olga Khomenko, Olexiy Pavlenko Mykola Skyba, Nadiya Koval, Tetiana Yuschenko, Vladimir Shulmeister Yana Lavryk, Yaroslav Pylypchuk, 'Moratorium on land: the extent of losses for the Ukrainian economy' (*Ukrainian Institute for the Future,* 18 May 2017). Available from: <https://uifuture.org/en/post/moratorium-on-land-the-extent-of-losses-for-the-ukrainian-economy_251> [Accessed: 15 July 2017]

[42] Taras Zinchuk, 'Agricultural Policy in the context of EU integration: realities and prospects for Ukraine'. (2006), *Ekonomika Ukraine.* Available from: <http://ir.znau.edu.ua/handle/123456789/4038> [Accessed: 6 July 2017]

[43] Sisetska (n 31)

fundamental to combating corruption in the country and in bringing the burgeoning shadow market for agricultural land under the purview of the state. [44] This, in the IMF's view, will help to re-instill investor confidence in Ukraine's ability to provide those legal safeguard imperative to securing their investments.[45] The desperate financial straits in which the country has floundered for the past few years, most seriously during the period following Russia's annexation of Crimea and the eruption of internal conflict in eastern Ukraine, has resulted in the Verkhovna Rada appearing to conclude that the only realistic option is compliance with the IMF's terms.

The country is thus caught in a bind: reforms are not just desirable, but crucial to securing continuing financial support from western institutions and companies. [46]On the other hand, corruption and administrative and technological shortcomings and failings render any such reforms a highly complex and potentially exorbitantly expensive prospect. Taking into account the overall situation, it could be noted that the reform process is thus not simply a matter of enacting relevant legislation, but establishing a suitably robust system in which the newly liberalized market can transact with confidence. In the context of land – particularly of the agricultural variety – this means an overhaul of the entire system of registering title, with a focus on ensuring to the maximum possible degree that the online registration system is secure and that amendments and alterations can only be made with the consent and knowledge of all relevant parties.

The current incompleteness of the land cadastre and the widespread existence of errors in cadastral records has the potential to seriously complicate land transactions and cause additional risks for property rights holders, or those prospective investors wishing to purchase land. The possibility of data being manipulated with relative ease by dishonest parties is not hypothetical, as cases detailed in following sections will illustrate, but alarmingly frequent. Legal action initiated as a result of injustices arising from fraudulent practices is often unsuccessful, with the costs of litigating high and the registry system an unreliable and indeed not uncommonly useless evidential source. In such situations, the courts may be powerless to redress an obviously iniquitous state of affairs.[47]

The question therefore arises, in light of the above, of whether repealing the moratorium might actually worsen the situation, opening the floodgates to document falsification, illegal appropriation of agricultural land and injustices being perpetrated on a massive scale. A premature, poorly thought-out liberalization drive therefore presents considerable risks to Ukraine's economic health.[48]

It is argued, that, without a complex solution able to provide adequate data security and transparency, the results could be nothing short of catastrophic: an environment in which first registration of newly created rights over land, and secondary transfer of those rights, is essential, as is a mechanism which permits for parties to

---

[44] Interfax Ukraine, 'IMF requirement for land reform in Ukraine remains in force' (*Interfax - Ukraine News Agency,* 14 July 2014). Available from: <http://en.interfax.com.ua/news/economic/436243.html> [Accessed: 18 July 2018]

[45] International Monetary Fund. European Dept., 'Country Report No. 17/83' (2017). Available from: http://www.imf.org/en/Publications/CR/Issues/2017/04/04/Ukraine-2016-Article-IV-Consultation-and-third-review-under-the-Extended-Arrangement-44798 [Accessed: 15 June 2017]

[46] Rostyslav Averchuk, 'Foreign Direct Investment in Ukraine: War and Peace' (*Vox Ukraine*, 2 February 2017). Available from: <https://voxukraine.org/2017/02/02/investments-in-ukraine-en/> [Accessed: 5 August 2017]

[47] Respective cases are discussed in the following part

[48] E. Segura & O. Ustenko, 'Assessment of the Consequences of Lifting the Land Moratorium in Ukraine', (The Bleyzer Foundation, 2016). Available from: http://www.usubc.org/files/Lifting%20of%20Land%20Moratorium%20final.pdf [Accessed: 15 July 2017]

transact with minimal interference from the state, due to lack of trust by society K. Yarmolenko underlines[49]. The latter is important, not from a libertarian, ideological standpoint, but simply because the current byzantine nexus of rules and regulations governing the alienation of land lends itself to abuse. In a country in which the average monthly salary is currently roughly $300, the temptation for graft by underpaid state employees is easily understood.[50] The issues to be tackled before repealing the moratorium discussed in further detail in the next paragraphs.

2.1 Assessment of the Current Legal Framework

Before the moratorium on the alienation of agricultural land is lifted, it is crucial that current Ukrainian land legislation is adjusted to regulate the market conditions which will exist following implementation of the reforms.

State registration of rights over land is thus of particular importance. As mentioned earlier in this research, the piece of legislation passed on the 7th of July 2011 – 'On the State Land Cadaster' – created a dual system; a Cadaster and a Register of Rights. The latter includes information on the land itself, a database of land plots which includes relevant data derived from – *inter alia* - land surveys. The Register records legal rights over the land and is maintained by the Ministry of Justice. All records are to be converted to or created in electronic format. As many legal scholars have noted, however, the system remains mired in red tape.

One issue arising from the transfer of data from 'hard' to 'soft' formats relates to the reliability of the state cadastre record system and the process of registering property rights. Ukraine's cabinet adopted 'On Approval of the Procedure for the State Land Cadaster' (Law No 1051) on the 17th of October 2012, a piece of legislation which sets out the procedure for assigning cadastral numbers to land plots, as well as the mechanism for their registration. Until 2002, paper-based certificates were issued for the land by the state, which were recorded in the central register: Cadastral information was not collected in electronic form and there was no requirement for a cadastral number. Not until mid-2003 was a requirement introduced for the logging and registration of the coordinates of a plot of land, and it is estimated by the Ukrainian cadastral administration that five million land ownership certificates are still unrecorded in the database, notwithstanding the 2003 Act and the further requirement in 2013 for all property rights to be registered. Whilst the Cadaster should theoretically provide a blueprint for a future register for information on agricultural land, the flawed operation of the system perhaps indicates instead the difficulties the reform program will face argues A. Borodkin.[51] Moreover, the discrepancies which have become apparent in recent years, partially as a result of fraud, have led some experts on the matter to conclude that identifying property rights correctly will be a task beyond the current capabilities of the Ukrainian state.[52]

Of course, the lack of an effectively functioning land cadastral system significantly impacts on the state's ability to adequately protect land ownership. Adding to these concerns is the legal obligation of the state to collect all relevant information on plots of land, including ownership thereof and transfer of ownership rights, and store this information in the cadaster and the State Register of Real Property Rights.

---

[49] ForkLog, Interview with Konstantin Yarmolenko, advisor for the head of Ukraine Agency for E-Governance, (24 April 2017). Available from: <http://forklog.net/ukraines-real-estate-title-registration-to-start-using-blockchain-in-2018/> [Accessed: 2 June 2017]

[50] Trading Economics, 'Ukraine average Monthly Wages 1996-2017. Data. Chart. Calendar'. Available from: <https://tradingeconomics.com/ukraine/wages> [Accessed: 10 June 2017]

[51] Alexander Borodkin, 'Specifics Of Purchasing And Formalising The Rights To The Land Plots In Light Of Reforming The Procedure For Registration Of Property Rights To Real Estate', (2013) Pravovy Tyzhden. Available from: <http://www.vkp.ua/content/files/borodkin_pravovy_tyzhden_osoblyvosti_prydbannya_ukr.pdf> [Accessed: 3 May 2017]

[52] ForkLog (n 49)

It should be noted that according to the Final and Transitional Provisions of the Law of Ukraine 'On the State Land Cadastre', ownership of a piece of land in situations in which the rights arose prior to 2004 is regarded as legally formed, regardless of whether a cadastral number was assigned. However, the land cannot be disposed of until a cadastral number is received, as the information about such a plot is not included in the State Register of Land. Art. 111 of Ukraine's Land Code also stipulates that any restrictions placed on the use of land are subject to state registration, which of course means that any such non-registered constraints are in fact unenforceable.

The hope harbored by the instigators and proponents of the agricultural reform program is that the abolition of the moratorium will provide a stimulus to landowners to register their right, thus expanding the land cadaster, rendering it more accurate and complete. Anyone wishing to dispose of their land will be forced to register both it and any property rights attached to it.[53]

The second major concern relates to the security of the state registers. As mentioned, the adoption of the 'Land Cadaster' legislation provided the legal grounding for the creation of an electronic cadastral system in Ukraine, with all required information about land plots in the country to be stored electronically in a single format. The simple, guiding premise behind these changes is that an electronic record system would decrease the instances of loss of archives, shadow sales, unlawful change of boundaries firmly believes S. Tymchenko (Head of the State Agency of Land Resources of Ukraine).[54] Indeed, the law simplifies procedures for requesting and obtaining information from the cadaster, primarily through providing online access to it.

While the objective is laudable, the collation and centralization of such a vast quantity of sensitive information naturally raises the question of its potential vulnerability to cyber-attack, particularly given the parlous state of relations with Russia and the cost of defending such a large and tempting target from hackers. [55] In fact, repeated and sustained attacks on the database of property rights registrations have emerged over the past few years, with many hacks seemingly directed at erasing or altering entries – particularly of encumbrances discussed below. Of course, such security concerns are virtually universal, but Ukraine's persistent difficulties with corruption make ensuring the sanctity of the system a challenge, as efforts to protect it from outside interference must take account of the very real possibility of such attacks being facilitated by internal actors.

2.2. Governmental Corruption and Its Impact on the Land Reform

The problem of corruption referenced in the preceding section is significant, dogged and according to some sources, growing. Transparency International, an NGO whose mission is to assess corruption at a variety of levels, currently places Ukraine at a lowly 131st place in its global index, out of 176 countries surveyed. This compares very unfavorably with, for example, neighboring post-Communist Poland, which ranked 29 on the same scale.[56]

---

[53] A Potikha, 'Moratorium on the sale of land: pros and cons' (*Social Communications Research Centre*, 2017). Available from: <http://www.nbuviap.gov.ua/index.php?option=com_content&view=article&id=2879:chi-buti-rinku-zemli-v-ukrajini&catid=8&Itemid=350> [Accessed: 10 June 2017]

[54] Sergij Tymchenko, 'The public land cadastre is not beneficial to corrupt individuals' *Dzerkalo Tyzhnia* (1 February 2013). Available from: <https://dt.ua/privatizatsiia/publichniy-zemelniy-kadastr-ne-vigidniy-lishe-korupcioneram.html> [Accessed: 22 July 2017]

[55] Pavel Polityuk, 'Ukraine points finger at Russian security services in recent cyber attack' *Reuters* (1 July 2017). Available from: <http://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19M39P> [Accessed: 5 August 2017]

[56] Transparency International, 'Corruption Perception Index 2016. Survey'. Available from: <https://www.transparency.org/news/feature/corruption_perceptions_index_2016> [Accessed: 10 June 2017]

New registration procedures, which took effect from the 1st of January 2016, were touted as major steps towards introducing a far greater level of transparency into the Ukrainian economic system.[57] Decentralization broadened the list of bodies authorized by the Ministry of Justice to perform state property registration, and there was an overall move to simplify existing procedures. Under the changes, registration of various types of personal property, including land, can now be executed not only by the state, but also by notaries, accredited banks, centers of administrative services of local councils and even Ukrainian National Post offices.

The introduction of the principle of extraterritoriality perhaps created an effective form of providing citizens and businesses with easier access to administrative services. Nevertheless, a number of well-informed commentators have raised concerns that the new, simplified system potentially increases the risk of document falsification. Registration entities are not required to verify the authenticity of documents and signatures, as this is not within their remit. There is consequently significant potential for the presentation of falsified documents and/or fake signatures to be used in transactions. The abolition of paper certificates and their replacement with entry on the electronic register has, as mentioned above, engendered a heightened risk of remote infiltration, and while the Ukrainian Ministry of Justice has repeatedly asserted the integrity of its security measures no such claim can be made for many of the systems of – for example – notaries holding passwords and access keys to the system. [58] This in turn enables attackers to create falsified records on the system, employing the login details of a particular notary. As touched on above, the straightforward, more prosaic, but very real risk of the notary being susceptible to bribery is also present. To appreciate this hazard, one has only to reference the difficulties that arose following the introduction in 2016 of new commercial registers: Raids on the integrity of the register occurred almost immediately upon its launch, in many instances facilitated or even instigated by the registrars and notaries themselves.[59]

2.4 Imperfections of Current Property Rights Protection System

To illustrate imperfections of current legal and administrative systems, two cases of commercial and non-commercial disputes on the ground of illicit property right grabbing facilitated by unlawful registrar's actions illustrated below.

Case 1:

One of the most notorious, egregious examples of this form of attack took place in 2015-2016, and concerned attempts to illegally seize ownership the Horizon Business Park Center. In October 2015, based on a falsified court document, the registration service of Kyiv abolished registration of Unicredit's (Italy's largest bank by Tier 1 capital) ownership rights to the Horizon business center and re-registered them with an LLC called 'Project-A'. The bank was able to successfully defend its rights as an examination of the purported documents of ownership confirmed them to be forgeries, but a further attack was instigated against Unicredit in February 2016, despite restrictions on registration actions being in place. A private notary in the Obuhovsky notary

[57] Laws "On Amendments to the Law of Ukraine" On State Registration of Legal Entities and Individual Entrepreneurs "and some other legislative acts of Ukraine on the decentralization of powers on state registration of legal entities, individuals - entrepreneurs and public entities" and "On Amending the Law of Ukraine "On State Registration of Real Property Rights and their Encumbrances" and some other legislative acts of Ukraine on With respect to the decentralization of powers for the state registration of real property rights and their encumbrances"

[58] Ministry of Justice of Ukraine "CETAM" and State Databases of The Ministry of Justice Have a Decent Protection Level against Cyber-attacks' (*Ministry of Justiceof Ukraine,* 30 June 2017). Available from: <https://minjust.gov.ua/news/ministry/setam-ta-reestri-ministerstva-yustitsii-mayut-dostatniy-riven-zahistu-abi-protistoyati-kiberatakam---minyust> [Accessed: 15 July 2017]

[59] Ministry of Justice of Ukraine, 'Ministry of Justice of Ukraine together with business and society continues combating raiders" (*Ministry of Justice of Ukraine,* 07 February 2017). Available from: <https://minjust.gov.ua/news/ministry/minyust-razom-z-biznesom-ta-gromadskistyu-prodovjue-borotisya-z-reyderami> [Accessed: 15 July 2017]

district canceled the bank's proprietary rights of the bank and again registered them with 'Project-A'. It was only after a direct appeal to the Ministry of Justice by the bank that the registration actions of the notary were annulled, with the District Administrative Court of Kyiv once more prohibiting any registration actions against the business center. Incredibly, the same notary tried the same tactic again upon the reinstatement of his rights on July the 2nd, 2016. The cost to the bank, in both time and money, of these legal assaults was of course of some significance, but much more important from Ukraine's perspective was the damage the case, and others like it, wrought on the reputation of the country's political and legal system.[60] If even Unicredit, a major international bank with access to vast funds, could repeatedly be attacked by a local notary entering false information on the register with apparent impunity, then the prospects for smaller commercial entities wishing to securely deal in Ukrainian land and property are not promising. One problem experienced by Unicredit during the fiasco was the almost Kafkaesque qualities of the Ukrainian justice system, which tied the company up in lengthy court procedure and administrative processes even after the initial ruling in their favor.[61] The main drawback was the inability of the court to effectively block any further registration actions, which gave the notary and his backers the possibility of alienating the property. It should be noted, that the rights over the property are able to be sold and resold multiple times, making restoration of ownership to the lawful rights-holders exceptionally difficult.

Case 2: A oft-repeated concern by Ukrainian legal practitioners is that the property rights that have not yet been included in the electronic database since 2011 remain extremely vulnerable. This category, as has been pointed out, is actually currently far larger than that of registered rights. The following case study provides a succinct example of this problem.

In 2016, it was reported that about one hundred and fifty land plots in the Kirovograd region had been leased to a company called Agri Invest Ukraine without the consent of the landowners. The situation came to light after suspicions were aroused about land transactions being conducted on behalf of deceased individuals and of people residing in the secessionist and annexed territories in Eastern Ukraine (Donbass or Crimea). In this instance, the country's Ministry of Justice reacted with uncharacteristic swiftness to restore the properties to their legitimate owners. [62] This was a particularly high-profile case and it would not be cynical to suggest that this was the primary reason for the Ministry of Justice rapid response; the number of similarly fraudulent activities concerning far smaller parcels of land is a matter of speculation, but given the limited resources of the state and the ubiquity of corruption, it would not be unreasonable to suppose that the problem is both widespread and of significant concern.

Unicredit bank regional director Tamara Savoshenko, perhaps provided the most public and pointed critique of the state's general approach to the problem, stating that; "Fraud should be addressed not only by intervention of the Ministry of Justice on a case-by-case basis, but systemically".[63] The rights that Unicredit believed it possessed over the property transpired to be of no utility whatsoever without an adequate legal framework through which to enforce them. The Ukrainian justice system's failure to effectively deal with the issues at

---

[60] Unicredit Bank, 'Unicredit Bank Reacts To Illegal Actions By "Project A" Around The "Horizon Park" Business Centre' (Unicredit Bank 9 April 2016). Available from: <https://En.Ukrsotsbank.Com/News/View/1250/> [Accessed: 18 July 2017]

[61] Unicredit Bank, 'One Of The Biggest Unscrupulous Debtors Blocks The Work Of Unicredit Bank In Ukraine' (*Unicredit Bank* 12 August 2015). Available from: <Https://En.Ukrsotsbank.Com/News/View/1096/> [Accessed: 18 July 2017]

[62] Ministry of Justice of Ukraine, 'Committee of Ministry of Justice of Ukraine Restored 150 land Plots From Raydership' (*Ministry of Justice of Ukraine,* 09 February 2017). Available from: <https://minjust.gov.ua/news/ministry/komisiya-minyustu-vryatuvala-vid-reyderskogo-zahoplennya-vlasnikiv-150-zemelnih-dilyanok> [Accessed: 15 July 2017]

[63] Fin Balance, 'Unicredit Bank Applies About The Return Project-A Attention To The Business Center "Gorizont Park"' (*FinBalance*, 22 July 2016). Available from: <http://finbalance.com.ua/news/UniCredit-Bank-zayaviv-pro-povtornu-sprobu-zakhoplennya-yoho-biznes-tsentru-Horizont-Park> [Accessed: 2 June 2017]

hand were compounded by the administrative confusion, alluded to a number of times in this dissertation, which exists in Ukraine, with various limbs of the state possessing overlapping or conflicting powers and little communication between government departments. The Unicredit case neatly illustrates the uphill struggle faced by reformers in Ukrainian politics, with justice often being the preserve of the wealthy and well-connected. Trust in the system from both local and foreign parties is understandably low, and has a dampening effect on FDI and internal investment.[64]

In summary, although Ukraine's system is being actively reformed with the aim of protecting ownership rights and strengthening the rule of law, some very significant problems persist which continue to undermine confidence in the state. The technical solutions which are the subject of this dissertation could serve to strengthen the reform process: The provision of a secure system of property transaction using blockchain would arguably bring clarity, transparency and integrity to a system sorely deficient in all three areas. The next paragraphs discuss the qualitative characteristics and prospective application of technology.

3 2. How Blockchain Works Technically

One of the most intensely scrutinized and widely discussed technologies of the past two years has been that of Digital Ledger Technology, commonly referred to as Blockchain. The heightened international interest in blockchain was reflected in the World Economic Forum's decision to name blockchain technology third in their list of top ten emerging technologies in 2016.[65] The degree of excitement generated by a relatively unglamorous and, until recently, obscure technology is arguably analogous only to that created during the first years following the creation of the internet itself. Since the late 2000's, the most prominent example of the application of the technology was the cryptocurrency Bitcoin, an endeavor which continues to invite commentary, controversy and speculation, both in the financial sense and in terms of the underlying technology's potential application to other spheres of activity.[66]

The salient feature of Bitcoin, and indeed of distributed ledger technology generally, is its elimination of the need for intermediaries. Until now, many forms of business transaction have required third party involvement in order to guarantee the rights of the transacting parties, such as lawyers, notaries and other similarly qualified professionals. The issuing of currency, too, has long been the exclusive preserve of the nation state, both a cause and result of the increase in the power of ruling political entities, a centrifugal trend which has endowed authorities in developed countries (and many developing nations) with an extraordinary degree of influence over the everyday lives of their citizenry. [67] The blockchain technology upon which Bitcoin and other cryptocurrencies are based theoretically obviates the need for an intermediary, either private or public, to be party to a transaction to ensure its legitimate execution. Blockchain allows parties to transact directly with each

---

[64] Gershon Feder, Klaus Deininger, 'Land Registration, Governance, and Development: Evidence and Implications for Policy' (2009) Volume 24, Issue 2, 1, The World Bank Research Observer. Available from: <https://academic.oup.com/wbro/article/24/2/233/1684787/Land-Registration-Governance-and-Develoment> [Accessed 12 June 2017]

[65] World Economic Forum's Meta-Council on Emerging Technologies, 'Top 10 Emerging Technologies of 2016' (World Economic Forum 2016). Available from: <http://www3.weforum.org/docs/GAC16_Top10_Emerging_Technologies_2016_report.pdf> [Accessed: 13 May 2017]

[66] Marcus O'Dair, 'Blockchain Revolution review – Satoshi Nakamoto's world-changing innovation' (2016) The Guardian. Available from: <https://www.theguardian.com/books/2016/jul/06/blockchain-revolution-how-technology-behind-bitcoin-changing-money-business-don-alex-tapscott-review> [Accessed: 5 May 2017]

[67] Milton Friedman, 'Lerner on the Economics of Control' (1947) Vol. LV, No. 5, Journal of Political Economy. Available from: <http://www.journals.uchicago.edu/doi/abs/10.1086/256579?journalCode=jpe> [Accessed: 5 June 2017]

other, secure in the knowledge that the agreed terms cannot be manipulated or repudiated without the express authorization of both parties.[68]

As Levin notes, this security is achieved through blockchain's creation of "cryptographic signatures and public keys chain-linked to form an unforgeable record of transactions for, say, digital cash or any ledger record. Crypto proof replaces the notary" [69] In a recent blog post, Cassie Findlay of the Recordkeeping Roundtable writes: "A decentralized archive utilizing the Blockchain…could offer an uncontested space from which records could be accessed. Documents and other sets of data can be validated by the Blockchain (as it provides) decentralized proof which cannot be erased or modified by anyone. The technology potentially offers a means for society…to keep their own records with some assurance about inviolability and longevity that was not possible before".[70]

In short, blockchain technology offers the possibility of instantly recording any data and instantly perform verification of a transaction, and in such a way as to render such a record virtually inviolable – in principle - without the consent of all relevant parties.

European Parliamentary Research Service developed a clear explanation of the principles blockchain works. Each record in a blockchain is entered onto a shared distributed ledger ('SDL') and time-stamped, providing a clear chronological map of what was altered and when. A digital record is stored in a data block, and each subsequent record is added to it creating a chain; complex algorithms are employed to achieve both this and the cryptography which ensures that the records are secure, an encryption process known as 'hashing' which is executed via a large number of powerful computers ('nodes') on the same network. After this has been carried out, a digital fingerprint or 'hash' is placed at the end of the sequence. It is this time-stamp which is critical to the blockchain process, creating as it does a chronological record which is essentially unalterable as the information is copied to all computers in the network simultaneously. Regular synchronization is executed by these computers, ensuring that all of them have the same shared data. Any subsequent changes to a record can only be logged through the creation of an entirely new 'block' and access to the information is only permissible via an electronic key.[71]

Melanie Swan in her book argues, that Blockchain's attraction lies in this combination of transparency (for the transacting parties) and data security, with decentralization of records and highly sophisticated cryptography providing protection from problems both longstanding and relatively novel (*inter alia* hacking, deliberate or accidental damage to or destruction of records, and theft). [72]

2.1 Blockchain as a possible solution for recordkeeping of property rights

A number of commentators on Annual World Bank Conference on Land and Poverty 2017 have raised the possibility of employing novel technologies of data management to property rights recordkeeping, in particular

---

[68] David Parkins, 'The great chain of being sure about things' (2015) The Economist. Available from: <https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable> [Accessed: 16 May 2017]

[69] Jonathan Levin, 'I love the Blockchain, just not bitcoin' (2014) CoinDesk. Available from: <www.coindesk. com/love-blockchain-just-bitcoin> [Accessed: 1 May 2017]

[70] Cassie Findlay, 'Decentralised and inviolate: the blockchain and its uses for digital archives', Recordkeeping Roundtable. Available from: <http://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/> [Accessed: 1 August 2017]

[71] Philip Boucher, 'How blockchain technology could change our lives', (2017). Analysis, EPRS European Parliamentary Research Service, PE 581.948

[72] Melanie Swan, *Blockchain: Blueprint For A New Economy* (2015)

land tenure. In theory, the level of certainty and accuracy attainable through the technology lends itself to automation uncovers the other potential advantage of employing blockchain in the registration of records and transactions. If the registry contains a legally valid record and full details of the land, including any attached encumbrances, then the mechanism for alienating this right could in theory become relatively straightforward.[73] Blockchain based land registry databases would enable transacting parties to gain access to the relevant database with a valid, encrypted digital key, and of course would be constrained from making alterations to the document without the explicit approval of the other participating party/parties. The asset attached to the blockchain record in a form of "token" once validated could be transmitted to a new right holder in seconds, unveils Lantmäteriet (Swedish Land Registration Authority) in its report.[74]

4 Blockchain for Land Registration. Analysis of Developed and Developing Countries' Experience

To recap; decentralization of state-mediated transactions through the application of blockchain is, arguably, in the interests of all legitimate involved parties with an interest in seeing the equitable dispensation of justice, particularly in the context of developing countries heavily reliant on foreign investment for economic growth.[75] The guarantee of property rights through the creation and retention of accurate transactional records is essential, therefore, in Ukraine's case for the reasons outlined above. The age-old problem in countries in which the rule of law is inconsistently applied - of centralized records being falsified and illegally adjusted - could be effectively addressed through the adoption of blockchain.

The prospective advantages of blockchain technology are not limited to developing economies, however. A number of developed, wealthy, states are currently exploring the possibility of applying blockchain to their record-keeping procedures. Whilst in the former countries the technology is viewed in part as a means of restoring faith in their administrative and adjudicative processes, in the latter blockchain is seen primarily as a means of expediting transactions and reducing occasional systemic errors and fraudulent activity. In streamlining registration procedure ('cutting out the middleman'), it has the added appeal of reducing expenditure.

Two countries have thus far begun to integrate blockchain into their land registry systems: Sweden and Georgia. Conveniently, from an empirical perspective, the two states each has a very distinct economic profile, and is at a different stage of development. Georgia, for example, had a GDP per capita of only 3,853 USD in 2016, compared to Sweden's 51,599 USD in the same period.[76] Whereas Sweden and Georgia fall neatly into definitions of 'developed' and 'developing', respectively, it represents a particularly interesting example to study the influence of blockchain implementation on current legal and administrative systems. Taking into account pilot project in Sweden is rather more advanced than Georgian, thus the analysis on implementation is scrutinized further.

In Sweden, the Lantmäteriet (Swedish Mapping, Cadastre and Land Registration Authority), Landshypotek Bank, have launched a pilot land registration scheme based on distributed ledger technology in collaboration with Telia, ChromaWay and Kairos Futures (all tech companies) each is responsible to supplement the project.

---

[73] Mats Snäll, 'Blockchain and the Land Register – a new "trust machine"?' (Annual World Bank Conference on Land and Poverty, Washington, 20-24 March 2017). Available from: <https://www.conftool.com/landandpoverty2017/index.php?page=browseSessions&print=head&form_session=547> [Accessed: 8 July 2017]

[74] Lantmäteriet, 'The Land Registry in the blockchain', (2016). Available from: <http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf> [Accessed: 27 July]

[75] North Douglass, *Institutions, Institutional Change and Economic Performance* (Cambridge: Cambridge University Press 1990)

[76] Central Intelligence Agency, 'Country Comparison :: Gdp - Per Capita'. Available from: <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2004rank.html> [Accessed: 3 August 2017]

Telia's role in the project is to program secure identity verification technology, while ChromaWay is providing a blockchain-based smart contract system as a framework for 'smart' transacting.[77] The involvement of the private sector in the creation and implementation of blockchain-based transactions is vital, not simply because most states lack the expertise and resources to design and implement such a complex technology, but also because land alienation is chiefly an activity carried out in the open market by non-state actors.

Since the trust in authorities is quite high, in Sweden's case, time and cost savings for transacting parties and the state would be accompanied by the benefit of permitting banks, brokers, sellers and purchasers to track the progress of the transaction at all stages. To add, blockchain technology does not wholly remove the participation of the intermediary in contract formation, however, as the registry on which the records are logged needs to be a trusted third party.[78] Therefore, the imposition of strict regulations and guidelines for the operator of any such registry would go far to address concerns about fraud, data loss and breaches of trust in general, as would making the registry's complete catalogue accessible and transparent.

According to a recent report by the Lantmäteriet, registration of land ownership or pending ownership confirmation can take up to four months to settle under the current system, which would be substantially reduced once a blockchain-based system is in place. Registration and approval processes are, at this moment, required to be completed by hand and dispatched by regular post, adding additional layers of time-consuming bureaucracy. Blockchain would not just accelerate and simplify this procedure, but also - once the registry is verified by the Lantmäteriet and other involved parties – eliminate the requirement for verification of proof of ownership in future sale or purchase transactions, as this would have already been established and secured by digital key. The Swedish authorities have also indicated that this type of registry would theoretically allow for a loosening of current, strict due diligence requirements when selling land or accessing the mortgage and credit market, as the data would be transparent and easily accessible.[79]

The Swedish government envisages enacting changes to current legislation which recognizes only handwritten and signed contracts in a format specified by law (1915: 218) on agreements and other legal acts in the field of property law[80]. The broadening or amendment of the law to fully encompass electronic documents is highly likely upon successful blockchain registry application. The current pilot scheme aims to move contracts for the sale and purchase of land to smart contracts, based on electronic keys to verify the transaction. As mentioned above, a blockchain-based smart contract, needs only to be signed by each party using a cryptographic key that only the party has access to.

In 2014 the EU drew up a Regulation on The Electronic Identification and Trust Services (910/2014/EC), which brought the validity of contracts certified by electronic signature within its ambit. The Regulation established a legal framework for Member States to apply, covering electronic identification, signatures, seals and documents and is intended to introduce a greater degree of uniformity and certainty into the area of electronic signatures and identities. The overarching aim of the EU legislation is to promote the adoption and spread of document exchange via electronic means through the provision of a stable and reliable legal basis for conducting such transactions by 2018. At the heart of the Regulation is the issue of proof – establishing whether a transacting party is who he, she or it claims to be.[81] Article 25 of the Regulation sets out the principle that all electronic signatures and verification services, such as electronic signatures, seals, time stamps, and certificates for

[77] Lantmäteriet (n 74)

[78] Boucher (n 71)

[79] Lantmäteriet (n 74)

[80] Lag (1915:218) Om Avtal Och Andra Rättshandlingar På Förmögenhetsrättens Område (SE)

[81] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/Ec Oj L 257/73

website authentication shall be admissible as evidence in legal proceedings. Smart contracts signed through an encrypted key system should in theory demonstrate the valid existence of a contractual-relationship, carrying the same legal weight as hand-signed or electronic legally-binding contracts. Some ambiguity persists, however, in relation to whether the electronic key generated in blockchain constitutes an electronic signature as defined under Article 25 of Regulation 910/2014/EC.

This seemingly arcane debate is actually of considerable import, as a failure to unambiguously establish the legal status of a blockchain contract could have serious ramifications in terms of its enforceability and whether it is binding on either or both parties. [82] The lively discourse on this subject in the United States is indicative of the confusion and controversy which still plagues blockchain. While Vermont for example, has recently enacted legislation making blockchain evidence self-authenticating, but only after considerable debate and repeated failure to get the bill in question through the State legislature. Similarly, Arizona has just passed legislation recognizing 'smart' contracts, as has Nevada but it is apparent that the recognition process has been slow and, as yet, sporadic.[83] This can be attributed to a hitherto widespread unfamiliarity with the new technology and a lack of understanding of the way in which it works; the high demand for blockchain coders is indicative of its novelty.[84]

However, these shortcomings, while serious, are also open to relatively straightforward solutions, assuming that the political will and the legislative apparatus is adequate to implement them. Since current land registration systems are ultimately overly reliant on manual interaction, with records having to be entered, updated and amended, and/or deleted if necessary. The system they are stored on may be vulnerable to attack or natural disaster, or indeed technological failure. Ensuring the sanctity and security of a registration system from this multitude of potential weak points is, naturally, a costly enterprise. In theory, blockchain has the potential to affect a significant risk reduction, resulting in a corresponding lowering in maintenance costs and supplement efficiency while conducting "smart transactions".

4.1 Applying Blockchain to the Specific Problems for Land Reform in Ukraine

As discussed, Ukraine is rapidly approaching the point at which the longstanding moratorium on the alienation of agricultural lands will be lifted. For this reason, it is arguably ideally suited to applying blockchain to its land registration procedures, a state such as Ukraine in which the legislative and judicial apparatus has been compromised through endemic problems of graft, cronyism and maladministration. Considering the technology limits the scope of the "middleman" interference, it could be seen as promising a tool to help reducing corrupt activities reported nowadays in Ukraine.

---

[82] Aaron Wright, Primavera De Filippi, 'Decentralized blockchain technology and the rise of *lex cryptographia'* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664>

[83] Arizona State, US. Arizona House Bill 2417, On Signatures; electronic transactions; blockchain technology (US). Available from: <http://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf> [Accessed: 27 July 2017]

Nevada State, US. Senate Bill No. 398, Establishes various provisions relating to the use of blockchain technology. (BDR 59-158). Available from: <https://www.leg.state.nv.us/Session/79th2017/Bills/SB/SB398_R1.pdf> [Accessed: 27 July 2017]

Vermont State, US. General Assembly of the State of Vermont, An act relating to miscellaneous economic development provisions No. 157. Sec. I.1. 12 V.S.A. § 1913

<http://legislature.vermont.gov/assets/Documents/2016/Docs/ACTS/ACT157/ACT157%20As%20Enacted.pdf>

Craig A. de Ridder, Mercedes K. Tunstall, Nathalie Prescott, 'Recognition of Smart Contracts' (*Pillsburylaw*, January 2017). Available from: <https://www.pillsburylaw.com/en/news-and-insights/recognition-of-smart-contracts.html> [Accessed: 5 May 2017]

[84] Martin Arnold, 'Universities add blockchain to course list' *Financial Times*, (18 June 2017). Available from: <https://www.ft.com/content/f736b04e-3708-11e7-99bd-13beb0903fa3?mhq5j=e1> [Accessed: 19 July 2017]

It has already been established that Ukraine's future economic prosperity is inextricably bound up with the efficacy of a system of legally formalized, safeguarded and enforceable property rights, stored in an adequately secure format and location, however Ukraine still falls significantly short of attaining that goal. The desirability of agricultural land as an asset has therefore raised legitimate concerns amongst current owners of Ukrainian land that the liberalizing reforms may lead to further fraud, and have a negative impact on their rights.[85] A cumbersome or byzantine registration system and lack of transparency could feasibly have this undesired result, and the Ukrainian government has consequently openly expressed an eagerness to find technological means to avoid these possible pitfalls – including blockchain. It should be added that this interest is not restricted to technology to facilitate land registration, but rather as part of a wholesale solution to a host of administrative and legal difficulties affecting the country. With a view to rolling out the technology to other state services should the land registry experience be successful.

From the vantage point of any potential investor, the agricultural land reforms need to be accompanied by a system of reliable, accessible record keeping and the ability to prove beyond doubt, with ease, the time and date of any record or transaction and the exact terms of an agreement. Without these, the land's value would be significantly reduced on the open market, as would the willingness of an owner to invest in its development based on unpredictable legal environment.[86] Assuming that a future transaction would be carried out under the auspices of the two existing state bodies tasked with overseeing the alienation and registration of land, then blockchain would eliminate the delay created by information being exchanged, cross-checked and validated between them creating an additional layer of trust to transacting parties. This would help to access the record of particular record or transaction by the regulator in real time.

Ukrainian legislation currently in force covering electronic transactions is worth examining in detail at this juncture, as it appears – *prima facie* – to hold the possibility of being extended to cover smart contracts taking an example of the particular US states. Law No. 675-VIII, 'On Electronic Commerce'[87] enacted on the 3rd of September 2015 (hereafter referred to as the e-commerce Act). The objective of this piece of legislation was to codify basic legal principles in e-commerce transactions, an aim it largely succeeded in achieving. However, despite, the clarity the e-commerce Act brought to a number of previously contentious areas of electronic transactions (such as establishing the form of an electronic contract), a number of problems remain unresolved.[88]

In a nutshell, the Act stipulates that contracts concluded in electronic form have legal equal weight to those concluded in written form. Permissible methods of signing an e-contract are also set out in the same Act and at first glance it appears to provide an exhaustive list of these methods. A certain degree of confusion surrounds the Act's ambit, however, as certain issues relating to the electronic signature are regulated by other laws, specifically the Civil Code of Ukraine, a previous piece of legislation entitled "On Electronic Documents and Electronic Document Management" of May 22nd, 2003 No. 851-IV (EDM), and another law passed at the same time; "On Electronic Digital Signatures " May 22nd, 2003 No. 852-IV (EDS).[89]

---

[85] Ukraine Crisis Media Centre, 'Expert discussion: Moratorium on land sales – risks and benefits' (*Ukraine Crisis Media Centre,* 18 May 2017). Available from: <http://uacrisis.org/56351-moratorij-na-prodazh-zemli> [Accessed: 6 July 2017]

[86] Kenneth Rapoza , 'Corruption Is Killing Ukraine's Economy' Forbes. Available from: <https://www.forbes.com/sites/kenrapoza/2016/10/14/how-corruption-corrodes-ukraines-economy/#54d001eb124e> [Accessed: 5 August 2017]

[87] Law No. 675-VIII, 'On Electronic Commerce' (UA)

[88] Vlada Karpova, 'E-commerce: legal aspects' Accountant and Law, Vol. 45. Available from: <http://bz.ligazakon.ua/magazine_article/BZ009513> [Accessed: 3 May 2017]

[89] Law 'On Electronic Documents and Electronic Document Management' No. 851-IV (UA), Law 'On Electronic Digital Signatures' No. 852-IV (UA)

According to the e-commerce Act, an electronic contract can be signed by electronic signature, electronic digital signature (hereinafter - EDS), electronic signature by one-time identifier or analogue of a handwritten signature (facsimile reproduction of a signature by means of mechanical or other copying of an analogue of a handwritten signature). Unfortunately, this Law does not contain any instructions regarding the signing procedure itself. Accordingly, in order to determine the requirements that must be observed when using an electronic signature, the provisions of the legislation governing electronic signature issues should be consulted. The use of an electronic signature brings with it a host of potential problems.[90] According to the EDM Act, the integrity and authenticity of an original electronic document should be capable of being verified. However, the selfsame law also adds that the integrity of an electronic document can only be proved by checking an EDS. Since it is impossible to confirm the integrity of a document signed with the help of an electronic signature, it cannot be asserted that such a document is valid. This position has also been adopted by the State Fiscal Service of Ukraine[91]. The consequence of this confusion is that, based on the current provisions of Ukrainian legislation, electronic signatures for the conclusion of contracts cannot legitimately be used as proof of a document's authenticity as O. Nimko notes.[92]

Whilst the e-commerce Act in theory equated electronic contracts to their written counterparts, it is important to reiterate the point made above, that current Ukrainian legislation remains insufficiently standardized, and that the status of key certification authorities is, to put it charitably, not always clear. The provisions of the e-commerce Act are consequently unable to work effectively, with the lack of proper regulatory oversight of the use of electronic signatures carries potential substantive risks for parties transacting online.

Considering the flaws in the various pieces of legislation in force, any large-scale introduction of blockchain as a mechanism for contracting would have to be accompanied by corresponding amendments made to the laws governing contractual relations. As already mentioned in the context of the US, such changes would not necessarily be easy to enact, as it is highly probable that the Ukrainian legislature would have to be convinced of the security and utility of the technology before approving any new law. Given the complexity of the tapestry of laws and regulations which currently govern electronic transactions, and the gaps in the legislation detailed above, teething problems with the application of the novel technology are inevitable.

The author is also convinced that blockchain technology would help to bolster the rule of law through the introduction of transparency into hitherto opaque processes, casting much-needed light into the dim recesses of the Ukrainian judicial-administrative process. Fundamental to the success of this endeavor is, ultimately, the will of the government to see through a reform program which will undoubtedly cause displeasure and unease among those who have for many years benefited from the general flaccidity of the Ukrainian state in uniformly applying elementary principles of the rule of law.

---

[90] Vlada Karpova, 'E-commerce: legal aspects' Accountant and Law, Vol. 45. Available from: <http://bz.ligazakon.ua/magazine_article/BZ009513> [Accessed: 3 May 2017]

[91] C. V. Bilan, 'The letter of the State Fiscal Service of Ukraine No. 23705/6 / 99-99-22-04-02-15' (*The State Fiscal Service of Ukraine,* 12 November 2015). Available from: <http://sfs.gov.ua/baneryi/podatkovi-konsultatsii/konsultatsii-dlya-yuridichnih-osib/64917.html> [Accessed: 26 April 2017]

C. V. Bilan, 'The letter of the State Fiscal Service of Ukraine No. 9985/6 / 99- 95-42-01-16-01' (*The State Fiscal Service of Ukraine,* 06 May 2016). Available from: <http://sfs.gov.ua/baneryi/podatkovi-konsultatsii/konsultatsii-dlya-yuridichnih-osib/67999.html> [Accessed: 26 April 2017]

[92] Olga Nimko, 'Legal regulation of e-commerce in Ukraine' (Państwo i Prawo. Badania podstawowe i stosowane: wyzwania i wyniki: zbir artykuw naukowych konferencji Miedzynarodowej naukowo-praktycznej Conference, Zakopane, August 2016). Available from: <http://ir.znau.edu.ua/bitstream/123456789/5965/1/EMGP_2016_27-31.pdf> [Accessed: 1 July 2017]

Encouragingly, an example of *Prozorro* (transparent: ukr) blockchain-based state E-auction activity already exists developed with a help of Transparency International Ukraine, the Ministry of Economic Development and Trade of Ukraine and implemented with support by the EBRD with a promotion of anti-corruption initiative led by bank.[93] A state procurement system has been in active operation for almost two years, giving a fillip to those who believe that the state is not just paying lip service to reforming its weak institutions.

In theory, Ukraine's independence from the strictures of EU law gives an advantage of enacting amendments to existing domestic legislation with relative ease, assuming parliamentary support therefore. These changes would ensure that elements necessary for the unimpaired operation of blockchain - such as ownership verification and smart transacting - would all be adequately legally protected. The successful application of DLT in securing land rights in Ukraine could inspire other states suffering from similar structural ailments to adopt a blockchain-based solution. The possibility of effecting a reduction in corruption is such that a number of countries with comparable problems are also beginning to tentatively explore the possibility of using blockchain – Honduras and Georgia, to name two recent examples.[94] Indeed "blockchain is the opportunity to help government to be less corrupt, to have the rule of law, and to have something else that sits alongside the rule of law, which is not just a set of rules but a sense of trust in the institutions. People could not have their property rights taken away by a despot who changes the record because ownership is not controlled by a central government register." David Cameron believes.[95] Transferring property records held by the state to blockchain could also lead to further deployments of the technology to other areas of government and international business activities. In an ideal situation, this would lead to a virtuous circle of increased trust, investment, and state activities becoming steadily more transparent.

FINDINGS

5 Alternative Advantages of Blockchain in International Business

With the advent of blockchain technology the approach to the storage and processing of large information flows has shifted. Existing database technology is rapidly becoming outdated as a result of the considerable security advantages afforded by distributed ledger technology, with any piece of information entered into the system being indelibly recorded and, if the system is open, completely transparent and immutable. The information is also far better protected from computer failure, as its distribution across the network renders it more secure.[96]All of these features could also be applied in any number of private sector activities, simplifying and streamlining the administrative workload of large corporations and providing a degree of trust vital to conducting global business. The current buzz of excitement surrounding DLT may, IBM estimated in a recent report, translate into widespread disruption for any international business relying on transactions or managing data within five to seven years.[97]

---

[93] European Bank for Reconstruction and Development, 'Are you ready for eProcurement? Guide to Electronic Procurement Reform' (*EBRD,* 2015). Available from: <www.ebrd.com/documents/legal-reform/guide-to-eprocurement-reform.pdf> [Accessed: 2 August 2017]

[94] Laura Shin, 'The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project' *Forbes* (7 February 2017). Available from: <https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/> [Accessed: 17 May 2017]

[95] Oscar Williams-Grut, 'David Cameron wants to use blockchain technology to fight government corruption' (*Business Insider,* 28 February 2017). Available from: <http://uk.businessinsider.com/david-cameron-on-blockchain-fintech-and-fighting-corruption-2017-2> [Accessed: 8 May 2017]

[96] Boucher (n 71)

[97] IBM, 'Making blockchain ready for business' (*IBM*, 2016). Available from: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12353USEN&> [Accessed: 1 May 2017]

Having looked at blockchain's salient features, it is clear that not only could the technology potentially have a profoundly transformative effect on the Ukrainian land registration system, but might also be harnessed to improve other functions of government. As mentioned, DLT is already being used by the Ukrainian government in procurement, an area traditionally offering considerable scope for corrupt activity, particularly in instances where adequate oversight mechanisms are lacking.

Taking a broader view, blockchain holds the possibility of fundamentally altering the way in which a wide range of private sector activities are conducted. From asset exchange, creating financial records and forging contractual relations to data management and even validating the ownership of intellectual property, also in sectors as dissimilar as insurance and retail, DLT could provide an additional layer of security and expedite and simplify transactions believes Sir Walport.[98]

These possibilities are easy to see when DLT, for all its complexity, is stripped down to its fundamentals: "The blockchain is a simple digital platform for recording and verifying transactions so that other people can't erase them later - and anyone can see them."[99] – essentially the holy grail in business transactions. All this is in addition, of course, to the most well-known deployment of technology, namely in Bitcoin and its digital currency progeny. Smart contracts – discussed earlier - for the exchange of assets (property rights) could serve as a benchmark or standard of best practice for international businesses heavily reliant on asset exchange, such as supply chain and financial transactions. The IBM report on DLT referenced above predicts that blockchain will result in considerable time and cost savings for companies (and consumers), and the elimination of many human errors. DLT would permit real-time monitoring of cash flow and status updates for, say, purchasing parties in manufacturing contracts.

On a macro level, the establishment of blockchain to carry out transactions both in the public and private sector could strengthen economic relations between states themselves. The reinforcement of trust at every level would conceivably have a positive effect on the relationship between individuals, companies, regions and countries. One major obstacle as highlighted, standing in the way of this idealistic vision is, however, the uneven diffusion of any new technology in a given society.[100]

It should also be added that support for the new technology has not been unequivocal. The US 'think tank' the RAND Corporation issued a report early in 2017 which adopted a fairly negative stance toward cryptocurrencies and to DLT technology in general. Underlying this is a fear, particularly by those who believe in the centralization of political power, that DLT will actually serve to threaten the ability of the state to effectively police its citizenry. The argument is a nuanced and complex one and need not trouble us here, suffice to say that blockchain may encounter resistance from unexpected quarters, not all of which can be discounted as the result of neo-luddite scaremongering.[101]

---

[98] Mark Walport, *Distributed Ledger Technology; Beyond Blockchain. A Report by Chief Scientic Adviser* (The UK Government Office for Science 2016). Available from: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs -16-1-distributed-ledger-technology.pdf> [Accessed: 1 May 2017]

[99] Kate Knibbs, 'What's the Blockchain, and Why Does Bitcoin Depend On It? (Gizmondo, 15 April 2015). Available from: <https://gizmodo.com/tag/whats-the-blockchain-and-why-does-bitcoin-depend-on-it-1698025216> [Accessed: 1 May 2017]

[100] Alexander Ponomarev et al, 'Untrusted Business Process Monitoring and Execution Using Blockchain' (BPM 2016 | Rio de Janeiro, September 2016)

[101] Advait Deshpande et al, 'Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and the Prospects for Standards' (2017) The British Standards Institution (BSI). Available from: <https://www.bsigroup.com/en-GB/Innovation/dlt/> [Accessed: 1 July 2017]

In the financial world, non-FinTech companies were initially generally slow to recognize the possibilities afforded by DLT, but are now among its most vocal supporters. Currently more than forty of the largest banking entities, including Goldman Sachs, Barclays, The Bank of America and JP Morgan, have joined the R3 consortium to jointly explore the new technology.[102] Credit organizations are acutely aware of the threat to their existence that rapid technological change may portent, and are consequently attempting to collectively harness the technology to stave off the threat of upstart rivals providing superior services at a lower cost. Enhanced accessibility, certainty and speed are the principal attractions offered by DLT, in part due to the elimination of the need for intermediaries, whether the state or privately contracted: The costs incurred through the provision of legal services in particular, such as those of lawyers and notaries, are expected to be dramatically reduced.

Some of the larger financial institutions have accordingly expressed an interest in establishing a consolidated database of all transactions, the professed aim being to cut out agencies such as SWIFT whose services are critical for the operation of most financial institutions with a global footprint. Recent breaches of SWIFT's security protocols have also illustrated the problem of relying on 'traditional' e-services, whose own systems and software may be vulnerable to infiltration.[103] Of course, distributing information also carries the risk identified by the RAND Corporation, namely that any illegal activity (such as breaches of international sanctions or transfer of narcotics revenue) may be very difficult to identify, let alone halt. Like any technological innovation, DLT's integrity is in this respect only as ethical as the institutions or individuals who employ it. Consequently, while the advantages of harnessing blockchain for the purposes of financial transactions are manifold, it nevertheless should be acknowledged, and appreciated, that such a system may also be used in other, less desirable contexts. However, if these challenges, and those listed below, can be overcome, then the hopes harbored by proponents of the technology may come to fruition. A recent suggested use of DLT neatly encapsulates the straightforward (conceptually speaking) benefits offered by blockchain: The heads of a number of nuclear power plants (NPPs) in the UK have suggested that employing DLT to secure the operating systems and information critical to running their facilities would be extremely desirable, particularly as the weaponized Stuxnet virus demonstrated the vulnerability of NPPs in Iran.[104]

CONCLUSION

At this moment in time, Distributed Ledger Technology is at a formative stage of development, and although excitement surrounds the breadth of its potential application it remains largely untested in many spheres. Literature on the subject remains relatively sparse and much of the current theory is exactly that – highly theoretical. However, a large-scale experiment being carried out in Sweden may contain useful indicators of the advantages and drawbacks of blockchain's usage. The country's proposed employment of blockchain to record property data and facilitate 'smart' transactions could demonstrate that much of the hype surrounding DLT is justified. Improvements in reliability, transparency and speed are all expected. It should be noted that Sweden has a highly digitized land registration system, and scores very highly in terms of the strength of its judicial and administrative processes.

---

[102] Kadhim Shubber, 'Blockchain initiative pulls in another 13 banks' (2015) Financial Times. Available from: <https://www.ft.com/content/72ffd222-66be-11e5-97d0-1456a776a4f5> [Accessed: 17 May 2017]

[103] Jim Finkle & Tom Bergin, 'Swift Confirms New Cyber Thefts, Hacking Tactics' *Reuters* (London/Boston, 12 December 2016). Available from: <https://www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT> [Accessed: 5 May 2017]

[104] Deloitte, 'Bitcoin, Blockchain and Distributed ledgers. Caughts between promise and reality', (*Deloitte*, 2016). Available from: <https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf> [Accessed: 22 June 2017]

In countries with less stable economies and which are exposed to sovereign risk, such as Ukraine, blockchain's introduction would undoubtedly be both complex and challenging. However, as argued in this dissertation, DLT also represents one of the most promising potential solutions to the deep-rooted problems which almost thirty years of independence have singularly failed to dislodge.

Securing land property rights in Ukraine is an objective of almost existential importance for the country, as it is desperately in need of investment following years of political upheaval, an economy notable for its oligarchical characteristics, and the loss of territory in Crimea (most likely permanently) and the Donbass region. The near-audible ticking of the clock as it approaches the moment at which the agricultural land moratorium will be lifted has added a sense of extreme urgency to the question of land rights. If a secure system of land registration is not in place at 'zero hour', there is a real possibility of corruption, fraud and misappropriation of property on a massive scale. The current unreliable electronic system, excessive involvement and intrusion of third parties or the authorities when performing any action relating to the alienation of property, and widespread dearth of confidence among the population in the state's ability to protect property rights are all major obstacles. As discussed, the byzantine legal framework enmeshing property disputes is also extremely problematic and requires a determined initiative from the government to bring the system into line with that, for example, of the EU.

Removing the involvement of the 'middleman' through distributed ledger technology would arguably go some way to mitigating the risk of data fraud, a result of blockchain's essential immutability. This in turn could restore some degree of trust in the security of land title, reinvigorating the country's stagnant mortgage market encouraging foreign businesses to invest. However, a number of unresolved questions remain, not least of which is how cash-strapped governments such as that of Ukraine can afford or be willing to pay for the extremely high initial costs of setting up a blockchain network, the expenditure involved in recruiting DLT experts and inevitable private sector advisors, and the price of the hardware necessary to keep the whole system up and running.

Ultimately, the theoretical benefits of blockchain to the nation state and to the private sector appear indisputable, with long-term improvements in the speed and certainty of transactions flowing from blockchain's inherent features touched on above - tamper proof records invulnerable to cyber-attacks, and the efficiency and security provided by so-called 'smart contracts' to international business. However, the challenge of persuading legislatures of the need to provide the requisite legal armature and legal enforcement may also prove difficult, at least until further and more convincing empirical evidence of distributed ledger technology viability has been provided. Further academic research and continuing examination and scrutiny of the efficacy of the technology would assist in this respect, providing compelling and irrefutable evidence of blockchain's feasibility and utility to both the public and private sectors.

The Legal Nature of Bitcoin and Altcoins

LLM (Glas),
Khalid Almelegi

Contents

Introduction 1
1.0 What is Bitcoin? 4
1.1 How Bitcoins Work 5
1.2 The Blockchain Ledger 7
1.3 How Bitcoins Are Obtained 9
1.3.1 Mining Bitcoin 9
1.3.2 BTMs and Bitcoin Exchanges 10
1.4 Bitcoin Cash 11
1.4.1 Why Bitcoin Cash 12
1.5 Altcoins Based on Bitcoin 12
2.0 Ethereum 14
2.1 How Ethereum Works 15
2.2 What are Smart Contracts? 17
2.3 Decentralised Applications 19
2.4 Decentralised Organisations 19
2.5 Decentralised Autonomous Organisations 21
2.6 Dispute Resolution via Smart Contracts 21
2.7 Technological uses for DLT and SCs 22
2.8 Other Blockchain 2.0 Projects 25
3.0 Interledger 26
3.1 Payments Through the Interledger System 27
3.2 Hyperledger 28
3.3 Why Hyperledger Fabric is Different from Other Blockchains 29
3.3.1 Shared Ledger 31
3.3.2 Smart Contracts 31
3.3.3 Consensus 31
4.0 FinTech Disadvantages 32
4.1 Legal Issues 32
4.1.1 Contract Law 32
4.1.2 Evidentiary, Enforcement, and Jurisdictional Issues 33
4.1.3 Criminal Activity 34
4.2 Potential Technology Failures 34
4.2.1 Anonymity Failure 34
4.2.2 Theft 35
4.2.3 Denial of Service 35
4.2.4 Blockchain Security 35
4.3 Monetary Policy 36
4.4 Financial Stability and Consumer Protection 37
4.5 Financial Crimes Enforcement Challenges 37
4.6 Systemic Risk and Blockchain 37
4.6.1 Centralisation, Blockchains, and Systemic Risk 38
4.6.2 Decentralisation, Blockchains, and Systemic Risk 39
Conclusion 44

Introduction

> I'm sure that in 20 years there will either be very large transaction volume or no volume. -Satoshi Nakamoto[1]

Throughout most of history, cash was king. In the early 1970s, people used cash in almost all their purchases. Personal cheques were often used for the purchase of luxury items. While credit cards were starting to become a thing, not many retailers accepted them. They were accepted in countries like the US and the UK, but other nations were still cash focused. Countries such as the Soviet Union allowed neither credit cards nor checking accounts for their citizens. Cash was the dominant used payment method. In the 1980s and 1990s, this changed. Credit cards started being used as an alternative to cash in many countries.[2]

Then, in the 1980s, cryptographers like David Chaum and others began working on developing ways how e-commerce would sustain the advantages of cash in an economy.[3] In 1982, Chaum wrote a proposal about digital currency.[4] A pioneer in his field, Chaum talked about how the issue of double spending could be addressed by creating a central server.[5] Chaum did not find much support; nevertheless, Chaum proceeded with the creation of DigiCash in 1994.[6] Unfortunately, DigiCash went bankrupt four years later.[7]

Two years after DigiCash, e-gold was introduced in 1996. With over one million accounts in 2003, many of e-gold's accounts were suspected of illegal activities.[8] This led to the shutdown of e-gold by the U.S. government in 2007.[9] However, before the crackdown by the authorities, many users of

---

[1] Satoshi Nakamoto Re: What's with this odd generation? See 'What's With This Odd Generation?' (*Bitcointalk.org*, 2010) <https://bitcointalk.org/index.php?topic=48.msg329#msg329> accessed 29 June 2017

[2] C Neal Koblitz and Alfred J. Menezes, 'Cryptocash, Cryptocurrencies, And Cryptocontracts' (2016) 78 Designs, Codes and Cryptography 87, 88

[3] ibid 88

[4] David Chaum, *Blind Signatures For Untraceable Payments* (1982)

[5] ibid 202

[6] Seth Litwack, 'Bitcoin: Currency Or Fool's Gold? A Comparative Analysis Of The Legal Classification Of Bitcoin' (2015) 29 Temple International and Comparative Law Journal 312; Hanna Halaburda and Miklos Sarvary, *Beyond Bitcoin: The Economics Of Digital Currencies* (1st edn, Palgrave Macmillan 2016) 113

[7] 'How Digicash Blew Everything' [1999] *Next Magazine*

[8] This was due to e-gold's nature in being an online service that did not require the identity of the account holder in order to be used and permitted its users to transact in its currency that users, later on, could convert to real money. See also Raj Samani, François Paget and Matthew Hart, 'Digital Laundry: An Analysis Of Online Currencies, And Their Use In Cybercrime' (2013) 8 https://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf accessed 29 June 2017

[9] Litwack (n 6) 312

e-gold had migrated to another digital currency, WebMoney.[10] The latter was created due to the outcome of the collapse of the Russian banking sector in 1998.[11] Anonymously established in 1998, WebMoney had a database of over seven million users at its peak in 2009.[12] Aside from e-gold and WebMoney, Liberty Reserve was also involved in illicit activities. Launched in 2001, Liberty Reserve saw a massive influx of users. It had a database of over one million customers, of which 200,000 were based in the United States as of May 2013. Before being shut down by the authorities in 2013, Liberty Reserve is estimated to have aided in laundering over six billion USD.[13]

Wei Dai, a member of a group known as "Cypherphunk", published a paper[14] in which he described the anonymity of virtual currency.[15] In his paper, Wei Dai discusses how, if a virtual currency were to exist, governments would not be able to intervene, and that such intervention would "not temporarily destroyed but permanently forbidden and permanently unnecessary".[16] Cypherpunk's mailing list is believed to have aided in the development of what is called Bitcoin today, which will be discussed later on.[17]

The above was somehow a glimpse of how some individuals tried to establish a digital currency before Bitcoin. Such ideas influenced Bitcoin. Nevertheless, most of them were unsuccessful.

This paper will aim to discuss and explain cryptocurrencies and smart contracts (SC), and explain their underlying blockchain technology, whether in its public or private form. Furthermore, although this technology offers numerous advantages, the disadvantages can be catastrophic if left unaddressed by the regulators.

Chapter one will discuss what Bitcoin is and who created Bitcoin; furthermore, this part will also describe the underpinning technology of Bitcoin, the "Blockchain". Chapter one will go on to explain how Bitcoin works. This part will conclude with other coins that are based on Bitcoin's technology.

---

[10] ibid
[11] Mark Herpel, '2011 Observations On The Digital Currency Industry' [2011] SSRN Electronic Journal
[12] Samani, Paget and Hart (n 8) 3
[13] ibid 8
[14] See also Wei Dai, 'B-Money, An Anonymous, Distributed Electronic Cash System' (*Weidai.com*, 1998) <http://www.weidai.com/bmoney.txt> accessed 17 August 2017. (proposing a monetary protocol without the need for government or government-sponsored entities)
[15] Nikolei M. Kaplanov, 'Nerdy Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation' 25 Loyola Consumer Law Review 115; Alan Cunningham, 'Decentralisation, Distrust & Fear Of The Body – The Worrying Rise Of Crypto-Law' (2016) 13 SCRIPTed 239
[16] Dai (n 14)
[17] Reuben Grinberg, 'Today Techies, Tomorrow The World? Bitcoin' (The Milken Institute Review 2012) 22

The second chapter will discuss Ethereum and SCs. Ethereum is often considered to be a vital part of blockchain 2.0, which corresponds to the platform allowing applications such as SCs to function on the blockchain. Chapter three will talk about Interledger and Hyperledger, and how the latter offers to enable cross-border payments and make them much easier. Hyperledger Fabric is a private blockchain that is currently being tested by companies. Chapter four will aim to discuss the disadvantages of such technologies if they are to be used by the financial sectors. Also, it will address their legal and technological issues, including their impact on monetary policy, financial crimes, and financial stability.

1.0 What is Bitcoin?

Bitcoin is often known as a cryptocurrency, digital or virtual currency.[18] Bitcoin is a cryptocurrency that is digital, open source, largely decentralised, and not backed by any government,[19] unlike fiat money which is regulated and supported by its issuing government.[20]

Bitcoin is not the only digital currency that exists. In fact, there is a similarity between Bitcoin and other digital currencies.[21] Although they may share similarities, Bitcoin is different. Bitcoin is not subject to any regulations by financial authorities, which makes it difficult to regulate.[22] Moreover, it cannot be issued by any central authority, nor can holders of Bitcoins be defrauded of the currency.[23]

As a digital currency and transfer system, Bitcoin was created by an unknown person or group under the alias of Satoshi Nakamoto.[24] It is often believed that Wei Dai's proposal influenced Satoshi Nakamoto.[25] Bitcoin was first created in 2008 and was later launched on January 3, 2009.[26] In total, 21 million Bitcoins will be generated according to the Bitcoin algorithm. The last Bitcoin to be produced is estimated to be issued between 2110 and 2140.[27] One of the main features of Bitcoin is that it offers anonymity, as it is decentralised, hard to track and monitor, and is thus often resorted to by individuals who seek to evade the authorities unless they associate themselves with their public key.[28] However, although Bitcoin may be seen as anonymous, the transactions on the platform are transparent.[29] Bitcoin records every transaction that ever happened in detail on the network's

[18] 'What Is Bitcoin?' (*CoinDesk*, 2015) <https://www.coindesk.com/information/what-is-bitcoin/> accessed 17 August 2017
[19] Mark Edwin Burge, 'Apple Pay, Bitcoin, And Consumers: The ABCs Of Future Public Payments Law' (2016) 67 Hastings Law Journal 1527
[20] Trevor I. Kiviat, 'Beyond Bitcoin: Issues In Regulating Blockchain Transactions' (2015) 65 Duke Law Journal 576
[21] Other digital currencies such as Pecunix or GoldMoney; See also Reuben Grinberg, 'Bitcoin: An Innovative Alternative Digital Currency' (2012) 4 Hastings Science & Technology Law Journal 174
[22] Octav Negurita, 'Bitcoin - Between Legal And Financial Performance' (2014) 6 Contemporary Readings in Law and Social Justice 247
[23] Grinberg (n 21) 174
[24] The notion of Bitcoin first appeared in 2008 in a paper published by Satoshi Nakamoto. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin.org (October 2008), https://bitcoin.org/bitcoin.pdf
[25] Kaplanov (n 15) 115
[26] Ralph E. Jr. McKinney and others, 'The Evolution Of Financial Instruments And The Legal Protection Against Counterfeiting: A Look At Coin, Paper, And Virtual Currencies' (2015) 2015 University of Illinois Journal of Law, Technology Policy 294
[27] Adam Chodorow, 'Bitcoin And The Definition Of Foreign Currency' (2016) 19 Florida Tax Review 373
[28] Larissa Lee, 'New Kids On The Blockchain: How Bitcoin's Technology Could Reinvent The Stock Market' 12 Hastings Business Law Journal 84
[29] 'How Do Bitcoin Transactions Work?' (*CoinDesk*, 2015) <https://www.coindesk.com/information/how-do-bitcoin-transactions-work/> accessed 17 August 2017

general ledger, which is known as a blockchain.[30] Not to be confused with Bitcoins and blockchains, blockchains are the underpinning technology of Bitcoin,[31] and will be discussed later on in detail.

1.1 How Bitcoins Work

Bitcoins are like cash; they can be lost. However, how Bitcoins are lost, is quite different. They can also be destroyed just like computer files since they are, in essence, computer files.[32] Bitcoins are flexible, as they can either be stored on a personal computer wallet, mobile wallet, online wallet, on a hardware wallet, or even on a paper wallet. Their usage is as simple as sending an e-mail.[33]

The way in which how Bitcoin transactions work is that they "are sent from and to electronic bitcoin wallets, and are digitally signed for security."[34] Bitcoin transactions use a scripting system which is stack-based.[35] These transactions use the Bitcoin protocol. Such transactions are programmable, meaning they can be automated.[36] Transactions are viewable by anyone on the network, and if one wanted to view a specific transaction, one could go back to the point in which Bitcoins were created. One of the main features of Bitcoins is that they do not exist; not even on a hard drive. This stands in contrast to fiat money, which is usually issued by the government and often held in a bank account in which the depositor that deposited the money knows it already exists.[37]

To ensure that the transactions are secure, Bitcoin uses a widely used technique when it comes to online transactions, the public-key encryption method. By doing so, this approach ensures that transactions are secure; whenever users decide to send bitcoins, they require two things, a bitcoin address and a private key. The payee owns the private key which acts as a password, while the other key is public. The public key is similar to the name of a bank in today's financial systems, or

[30] Pamela J. Martinson and Christopher P. Masterson, 'Bitcoin And The Secured Lender' (2014) 33 Banking & Financial Services Policy Report 14
[31] Matt Lucas, 'The Difference Between Bitcoin And Blockchain For Business - Blockchain Unleashed: IBM Blockchain Blog' (*Blockchain Unleashed: IBM Blockchain Blog*, 2017) <https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/> accessed 18 July 2017
[32] Kaplanov (n 15) 116
[33] 'How To Store Your Bitcoins' (*CoinDesk*, 2015) <https://www.coindesk.com/information/how-to-store-your-bitcoins/> accessed 11 August 2017
[34] ibid
[35] 'Script' (*En.bitcoin.it*) <https://en.bitcoin.it/wiki/Script> accessed 2 August 2017
[36] Jerry Brito, Houman Shadab and Andrea Castillo, 'Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, & Gambling' (2014) 16 Columbia Science and Technology Law Review 207
[37] Coindesk (n 29)

the payee's account. The payor then uses their private key in order to approve the payment that is to be made to the recipients' account. The public key is sometimes referred to as a Bitcoin address.[38]

This address is generated randomly and is made up of random letters and numbers. The private key is also made up of random letters and figures but, as previously mentioned, it is kept secret. Bitcoin users' address is visible on the network, and it informs how many Bitcoins a user possesses in their wallet. However, to unlock the wallet and take the bitcoins contained within it, a private key is required. This key is usually with the user of the wallet.[39] The transactions that occur when Bitcoins go in or out of the wallet are recorded on the blockchain, which can be observed in real time.[40]

Other advantages of the Bitcoin technology are that it is secure, efficient, and it does not require a third party presence. Third party presence has often been seen as a dilemma, whether the third party in question is a government, bank, payment network, or even a clearing house.[41] As for the matter of security, the security of the Bitcoin, as described by Nakamoto, is "cryptographic proof", since it eliminates the requirement of a third party that traditionally authorises transactions by enabling users to deal with one another directly.[42]

Not relying on a third party might be seen problematic due to issues such as double spending by the same user.[43] In order to resolve such an issue while ensuring that party privacy is protected, Bitcoin uses a public-key encryption and a "peer-to-peer distributed timestamp server" that is called the "blockchain", which ensures that the coins have not been spent before. This differs from traditional payment systems, which usually depend on a central authority that clears the transaction every time in order to ensure that no double spending occurs.[44]

[38] J. P., 'Bits And Bob' *The Economist* (2011) <http://www.economist.com/blogs/babbage/2011/06/virtual-currency> accessed 2 July 2017*;* See 'Getting Started - Bitcoin Wiki' (2015) <https://en.bitcoin.it/wiki/Help:Getting_started> accessed 2 July 2017
[39] Coindesk (n 29)
[40] See 'Bitcoin Block Explorer' (*Blockchain.info*, 2017) <https://blockchain.info/> accessed 17 August 2017 (shows all the transactions that goes in and out of the blockchain ledger)
[41] Kaplanov (n 15) 116
[42] Nakamoto (n 24)
[43] J.P. (n 38)
[44] Nakamoto (n 24)

1.2 The Blockchain Ledger

A Blockchain is a type of distributed ledger (DL). A Distributed Ledger Technology (DLT) is a type of database.[45] A DLT can either be permissionless or permissioned.[46] The difference is that permissionless DLT allows anyone to view, transact, and even participate in the validation process, as Bitcoin does.[47] This means that transaction verification goes through a distributed consensus in order to be confirmed.[48] However, permissioned DLTs are controlled by its selected participants. These participants are usually pre-selected; however, they can also be selected at a later stage. Usually, permissioned blockchains are managed by an organisation and are fully private.[49]

The Bitcoin blockchain, which is a public ledger, contains all the Bitcoin transactions that have been transacted.[50] This ledger is self-regulated.[51] Due to the ledger being decentralised, it operates on a network of thousands of computers, similar to the peer-to-peer music sharing network.[52] Throughout the blockchain, each block confirms the validity of the previous block, all the way to the first block, which is referred to as the "genesis block". Thus, previous blocks cannot be overwritten.[53]

Blockchains can be simply seen as a full history of banking transactions, and each block of the blockchain is like an individual bank statement.[54] A built-in mechanism exists in the blockchain in order to prevent double spending or the tampering of the master record of the transactions.[55] Furthermore, the blockchain database is shared on the Bitcoin protocol by all the participating nodes[56] across the network, which have the task of validating and relaying the ongoing

[45] Deloitte and the Monetary Authority of Singapore, 'The Future Is Here Project Ubin: SGD On Distributed Ledger' (2017) 8
[46] Financial Conduct Authority, 'Discussion Paper On Distributed Ledger Technology' (2017) 10; Permissioned blockchains such as Eris, Hyperledger, Ripple and others
[47] International Monetary Fund, 'Fintech And Financial Services: Initial Considerations' (2017) 11
[48] Gibson C. Todd and Kirk Tyler, 'Blockchain 101 For Asset Managers' (2016) 23 The Investment Lawyer 7
[49] International Monetary Fund (n 47) 11
[50] Catherine Martin Christopher, 'The Bridging Model: Exploring The Roles Of Trust And Enforcement In Banking, Bitcoin, And The Blockchain' (2016) 17 Nevada Law Journal 144
[51] Shahla Hazratjee, 'Bitcoin: The Trade Of Digital Signatures' (2015) 41 Thurgood Marshall Law Review 59
[52] More Sheridan, 'Bitcoins: Currency Of The Geeks' (*Bloomberg.com*, 2011) https://www.bloomberg.com/news/articles/2011-06-16/bitcoins-currency-of-the-geeks accessed 2 July 2017
[53] David Lee Kuo Chuen, *Handbook Of Digital Currency: Bitcoin, Innovation, Financial Instruments, And Big Data* (Elsevier 2015) 49
[54] Ryan Surujnath, 'Off The Chain: A Guide To Blockchain Derivatives Markets And The Implications On Systemic Risk' (2017) 22 Fordham Journal of Corporate and Financial Law 262, 263
[55] Hazratjee (n 51) 59
[56] A node is every computer that is connected to the Bitcoin network that uses software in order to validate and relay transactions. See also Melanie Swan, *Blockchain: Blueprint For A New Economy* (1st edn, O'Reilly 2015) x

transactions.[57] In other words, every computer connected to the Bitcoin network has a copy of the entire blockchain.[58] Thus, by doing so, the blockchain provides a complete history of the transactions performed by a particular address in the past.[59]

Within the blockchain, there many ever changing encrypted puzzles that are dependent on CPU power to be solved. The CPU power helps the system solve the puzzle, which thus validates the transaction by breaking the encryptions. After the encryption has been successfully broken, Bitcoins are awarded. This process is known as "mining".[60]

One important factor of blockchains is cryptography, which provides security. Blockchains depend on cryptography, because cryptography is the method through which communications can take place within the blockchain network; participants communicate through coded messages by applying cryptographic algorithms.[61] This is done to ensure secrecy. Cryptography is used to allow all the connected nodes on the blockchain network to be connected without the need to have a server or even a central authority.[62] Thus, by doing so, no single owner owns the blockchain; this is why a blockchain system is often referred to as decentralised.

Furthermore, Nakamoto claimed that if attacks on the blockchain were successful, and if the attackers were somehow able to outweigh the number of users on the network, this would lead to the whole Bitcoin system becoming useless, and would result in its destruction. Hence, this would not be in the attackers' best interests, as this will render the system useless by causing a lack of interest by the market participants towards the coins. This would imply that, if the attackers succeed, the coins they retrieved would become valueless.[63] This would necessarily be so because the value of the Bitcoins is derived from supply and demand.[64]

Finally, the blockchain offers numerous advantages. The fact that it is being shared among various users makes it hard to hack or even shutdown.[65] Moreover, the more famous Bitcoin becomes, the

[57] Alexander Savelyev, 'Contract Law 2.0: 'Smart' Contracts As The Beginning Of The End Of Classic Contract Law' (2017) 26 Information & Communications Technology Law 118
[58] Chuen (n 53) 48
[59] Joshua A.T. Fairfield, 'Bitproperty' (2015) 88 Southern California Law Review 821
[60] Hazratjee (n 51) 59
[61] Chris Dannen, *Introducing Ethereum And Solidity* (Apress 2017) 1
[62] ibid
[63] Hazratjee (n 51) 60
[64] Kaplanov (n 15) 116
[65] Kadhim Shubber, 'Banks Find Blockchain Hard To Put Into Practice' (*Ft.com*, 2016) <https://www.ft.com/content/0288caea-7382-11e6-bf48-b372cdb1043a?mhq5j=e2> accessed 6 July 2017

harder it is going to be for attackers to destabilise the system due to the huge number of miners that participate in the Bitcoin system.[66] Besides, the transactions that have been completed cannot be reversed. Such transactions cannot be reversed, because this is how the system is designed to work.[67] Further technological advantages of using the blockchain shall be discussed in the next chapter.

1.3 How Bitcoins Are Obtained

There are various methods in which individuals wishing to obtain Bitcoins can get them. Bitcoins can be obtained through a specific software (mining),[68] exchanges that permit Bitcoin trading,[69] Bitcoin Automatic Teller Machines (BTMs),[70] or even through purchasing them from individuals that sell them directly by meeting them.[71]

1.3.1 Mining Bitcoin

Mining is the process in which a block is created that is referred to as a Bitcoin.[72] This means that Bitcoins are created through mining.[73] A miner is a node on the bitcoin network (blockchain) whose role is to validate new transactions.[74] After a miner validates a transaction, it is then placed in the new block which is afterwards broadcasted to other nodes on the network. This consensus system is known as "proof-of-work" (PoW) which is based on SHA-256.[75] After that, miners are awarded Bitcoins as an incentive. This incentive acts as a protection for the system by keeping attackers from

[66] Hazratjee (n 51) 61
[67] Martinson and Masterson (n 30) 15
[68] Kaplanov (n 15) 121
[69] 'Exchanges' (*CryptoCompare*, 2017) <https://www.cryptocompare.com/exchanges/#/overview> accessed 11 August 2017
[70] Halaburda and Sarvary (n 6) 147; Mark Abell, Simon Fielder and Mumuksha Singh, 'Bitcoin And International Franchising' (2014) 12 International Journal of Franchising Law 34
[71] ibid
[72] 'Mining - Bitcoin Wiki' (*En.bitcoin.it*, 2016) <https://en.bitcoin.it/wiki/Mining> accessed 4 July 2017; Pedro Franco, *Understanding Bitcoin: Cryptography, Engineering, And Economics* (Wiley 2015) 143
[73] Peter Kelly-Detwiler, 'Forbes' (*Forbes.com*, 2016) <https://www.forbes.com/sites/peterdetwiler/2016/07/21/mining-bitcoins-is-a-surprisingly-energy-intensive-endeavor/#6afe79815bbf> accessed 4 July 2017
[74] Tim Swanson, 'Consensus-As-A-Service: A Brief Report On The Emergence Of Permissioned, Distributed Ledger Systems' (2015) 4
[75] Surujnath (n 54) 270; Other cryptocurrencies that use PoW systems are B-money, RPOW, BitGold, ZeroCoin, Dogecoin, Dash, Primecoin, and Ethereum. See Fabio Massacci, Chan Nam Ngo and Julian Williams, 'Decentralized Transaction Clearing Beyond Blockchains' 3

assailing the system.[76] This was explained in Nakamoto's white paper, which stated that due to the miners who commit their time and energy in mining, the system is protected against any attacks.[77]

By mining, users can obtain Bitcoins instead of purchasing them.[78] Anyone can mine Bitcoins. Mining is usually done through the downloading of the Bitcoin program and running it. After the program is installed, the computer tries to validate the block by calculating it. This process is called a "hash".[79] A hash is what a miner's computer is required to solve which is a mathematical problem.[80] Afterwards, the system awards 25 Bitcoins to the miner that happens to validate the block.[81] The system used to award 50 Bitcoins in the past, but according to the Bitcoin protocol, the reward halves approximately every 210,000 blocks verified (approximately every four years).[82]

There are several different methods when it comes to mining Bitcoin. That is because "Bitcoin uses cryptographic algorithms including elliptic curve digital signature algorithm (ECDSA) and hash functions."[83] There are three ways in which Bitcoin mining can be done: solo mining, mining contracts, and mining pools.[84]

1.3.2 BTMs and Bitcoin Exchanges

The first BTM opened on October 29, 2013, in Vancouver, Canada. The BTM was located in a Coffee shop. A total number of 81 transactions were performed during the first week of the BTM introduction.[85] Such transactions were estimated to be worth more than $10,000.[86] In the beginning, BTMs only sold Bitcoins and did not permit users to obtain state-issued currencies in exchange for Bitcoins. However, currently, some BTMs that were introduced by the end of 2014 can purchase

[76] Hazratjee (n 51) 59
[77] Nakamoto (n 24) 4
[78] Kaplanov (n 15) 119
[79] Andy Greenberg, 'Crypto Currency' (*Forbes.com*, 2011) <https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html> accessed 3 July 2017
[80] 'Hash - Bitcoin Wiki' (*En.bitcoin.it*, 2015) <https://en.bitcoin.it/wiki/Hash> accessed 4 July 2017
[81] Greenberg (n 85)
[82] Chuen (n 53) 53
[83] ibid 46
[84] ibid 53
[85] Kurt Wagner, 'World's First Bitcoin ATM Opens In Vancouver, Canada' (*Mashable*, 2013) <http://mashable.com/2013/10/30/bitcoin-atm-2/#eN30qxDrlsq4> accessed 6 July 2017
[86] Jon M. Chang, 'Over $10K In Transactions For Bitcoin's First ATM' (*ABC News*, 2013) <http://abcnews.go.com/Technology/bitcoin-atm-conducts-10000-worth-transactions-day/story?id=20730762> accessed 6 July 2017

users Bitcoins in exchange for local currencies.[87] At the time of writing, there are 1329 BTMs located in 56 countries around the globe.[88]

An alternative method to purchase or sell Bitcoins is through an online cryptocurrency exchange. Individuals or even merchants can use online cryptocurrency exchanges. These exchanges allow the trading of Bitcoins in which their value is determined based on demand.[89] Online cryptocurrency exchanges are similar to traditional financial exchanges.[90]

1.4 Bitcoin Cash

On August 1st, 2017 a coordinated "hard fork" was initiated on the Bitcoin network which led to the creation of "Bitcoin Cash" (sometimes referred to as Bcash).[91] Whenever a change to the digital currency's software occurs, it is called a "hard fork". This change resulted in the creation of two separate versions of the blockchain of the digital currency that share the same history.[92] Thus, this led to the splitting of the Bitcoin network in which one supports normal Bitcoins and the other supports Bcash. They both coexist together and run along side by side.[93] After the fork, Bitcoin owners hold one unit of Bitcoin Cash for every unit of Bitcoin they owned pre-fork.[94]

Bcash is not worth the same as Bitcoin. As of this writing, on August the 3rd 2017, Bitcoin Cash is worth around $441.92 while Bitcoin is worth $2750.57 according to coinmarketcap.[95] However, what is impressive is that Bcash has managed to secure its place among the top 5 cryptocurrencies with approximately $7 Billion of the total market cap of cryptocurrencies.[96] On its third day of creation,

[87] Halaburda and Sarvary (n 6) 148
[88] 'Bitcoin ATM Map – Find Bitcoin ATM, Online Rates' (*Coinatmradar.com*, 2017) <https://coinatmradar.com/> accessed 6 July 2017
[89] Halaburda and Sarvary (n 6) 148
[90] ibid 147
[91] Jonathan Garber, 'Bitcoin Is Expected To 'Fork' Today, And Its Price Could Take A Dramatic Hit — Here's What That Means' (*Business Insider*, 2017) <http://uk.businessinsider.com/what-does-a-bitcoin-fork-mean-2017-7?r=US&IR=T> accessed 3 August 2017; Aaron van Wirdum, 'A Beginner'S Guide To Claiming Your "Bitcoin Cash" (And Selling It)' (*Bitcoin Magazine*, 2017) <https://bitcoinmagazine.com/articles/beginners-guide-claiming-your-bitcoin-cash-and-selling-it/> accessed 3 August 2017
[92] David Farmer, 'What Is A Bitcoin Fork?' (*The Coinbase Blog*, 2017) <https://blog.coinbase.com/what-is-a-bitcoin-fork-cba07fe73ef1> accessed 3 August 2017
[93] Timothy Lee, 'Bitcoin Vs. Bitcoin Cash: Why Bitcoin Just Split, And Why It Matters' (*Ars Technica UK*, 2017) <https://arstechnica.co.uk/tech-policy/2017/08/bitcoin-cash-network-split/> accessed 3 August 2017
[94] Eric Jhonsa, 'Why Bitcoin Cash Prices Are Likely To Dive Again' (*TheStreet*, 2017) <https://www.thestreet.com/story/14261684/1/here-s-why-bitcoin-cash-prices-are-likely-to-slump-again.html> accessed 9 August 2017
[95] Coinmarketcap is a website that lists the prices of all the digital currencies. See 'Cryptocurrency Market Capitalizations' (*Coinmarketcap.com*, 2017) <https://coinmarketcap.com/> accessed 3 August 2017
[96] ibid

Bcash managed to surpass the likes of Ripple and Litecoin in regarding market cap.[97] Likewise, Bcash can be obtained from a variety of exchanges and can also be stored on wallets.[98]

1.4.1 Why Bitcoin Cash

Bcash was created to solve some limitations of the Bitcoin network. Bcash is a fork of the Bitcoin blockchain ledger. It offers faster transactions speeds compared to Bitcoin.[99] The number of transactions per second that Bitcoin can withstand is three,[100] due to its limited block size which is capped to 1MB.[101] This was seen as a limitation for Bitcoin. Visa, for example, can handle thousands of transactions per second.[102] Thus, Bcash increased this limit to 8MB.[103]

1.5 Altcoins Based on Bitcoin

Bitcoin may be the first decentralised cryptocurrency to exist; however, it is not the only coin out there. Although as of writing this, Bitcoin has the largest market cap ($55,848,585,574 as of 08/08/2017),[104] there are other coins out there that have been created to address issues in the Bitcoin protocol such as privacy, robustness, and speed.[105]

First generation alternative coins are non-profit, and use a code similar to Bitcoin's, but altered. Introduced in October 2011, Litecoin is similar to Bitcoin, yet offers faster transaction confirmation times.[106] Another coin is Peercoin, which launched in August 2012 which uses a Proof of Stake (PoS) consensus which requires less computing power rather than a PoW, and is much faster due to its protocol. Another advantage that PoS offers over PoW is that participants are allowed to share rewards for mining without the need to join other mining pools or buy better hardware required to mine better. By doing this, Peercoin is less vulnerable to a 51% attack. On July 7, 2013, Primecoin

[97] Frank Chaparro, 'Bitcoin Cash Is Already The 3Rd-Largest Cryptocurrency' (*Business Insider*, 2017) <http://uk.businessinsider.com/bitcoin-cash-price-and-marketcap-2017-8?r=US&IR=T> accessed 3 August 2017
[98] 'Peer-To-Peer Electronic Cash' (*Bitcoin Cash*, 2017) <https://www.bitcoincash.org/> accessed 3 August 2017
[99] ibid
[100] '7 Transactions Per Second? Really?' (*Hashingit.com*, 2014) <http://hashingit.com/analysis/33-7-transactions-per-second> accessed 3 August 2017
[101] Peer-To-Peer Electronic Cash (n 98)
[102] Selena Larson, 'Bitcoin Split In Two, Here's What That Means' (*CNNtech*, 2017) <http://money.cnn.com/2017/08/01/technology/business/bitcoin-cash-new-currency/index.html> accessed 3 August 2017
[103] Peer-To-Peer Electronic Cash (n 98)
[104] See 'Cryptocurrency Market Capitalizations' (*Coinmarketcap.com*, 2017) <https://coinmarketcap.com/> accessed 8 August 2017
[105] Lawrence H. White, 'The Market For Cryptocurrencies' (2015) 35 The Cato Journal 388, 389
[106] A typical Litecoin transaction takes 2.5 minutes instead of 10

was launched by Peercoin's main developer.[107] However, unlike Peercoin which uses a PoS system, Primecoin uses a new PoW protocol (which focuses on finding prime numbers) that helps reduce confirmation times to 1 minute.[108]

A cryptocurrency faster than the above coins is Darkcoin (renamed to Dash), which launched in April 2014. Dash, a non-profit project, offers a payment confirmation system that takes seconds. Moreover, it offers more anonymity than Bitcoin. Dash's transactions are "obfuscated". BlackCoin, launched on February 24, 2014, uses a PoS system. It offers faster verification and is connected to a decentralised exchange, BlackHalo, which offers user anonymity.[109]

Ripple is a payment system and a cryptocurrency that shares similarities with other cryptocurrencies, but is markedly different in one aspect. Ripple also adopts the Bitcoin blockchain concept and utilises it. Furthermore, Ripple's blockchain is also a shared public ledger.[110] However, Ripple is not a non-profit.[111] Ripple is the 3rd largest cryptocurrency regarding market cap coming in after Bitcoin and Ethereum. Ripple first started trading in August 2013. Ripple Labs have created this cryptocurrency. Unlike other cryptocurrencies that rely on mining, Ripple does not, as all Ripples are already pre-mined by Ripple Labs. [112] Ripple excels as a payment network due to its consensus algorithm, which takes 5 seconds to verify transactions. This makes it ideal for competing with payment systems such as American Express, Mastercard and Visa. Ripple's coin is not the only thing that the company offers; it offers a wholesale remittance system that offers "real-time, cross-border payments"[113] that is currently being tested by several banks including the BoE.[114] What is more interesting is that this system is much cheaper and faster than the legacy Automated Clearing House system. Another project that rivals Ripple, but is non-profit in nature, is Stellar.[115]

[107] Jack Clark, 'Virtual Currency Speculators Shut Down Cloud: Digitalocean Forced To Halt New Signups After Cointard Flood' (*Theregister.co.uk*, 2013) <http://www.theregister.co.uk/2013/07/16/digitalocean_primecoin_cloud_problems/> accessed 8 August 2017
[108] White (n 105) 389
[109] ibid
[110] Ripple Labs Inc, 'The Ripple Protocol Consensus Algorithm' (2014) 2
[111] White (n 105) 390
[112] Adam Levine, 'The Ripple Problem: The Problem Of Ripple And The Liabilities Of Legitimacy' (*Let's Talk Bitcoin*, 2013) <https://letstalkbitcoin.com/the-ripple-problem> accessed 29 July 2017
[113] White (n 105) 390
[114] Stan Higgins, 'UK Central Bank Tests Ripple'S Interledger Protocol For Cross-Border Payments' (*CoinDesk*, 2017) <https://www.coindesk.com/uk-central-bank-tests-ripples-interledger-protocol-cross-border-payments/> accessed 8 August 2017
[115] White (n 105) 390

2.0 Ethereum

In the previous chapter, we discussed Bitcoin. In this chapter we will focus on Ethereum.

After the emergence of Bitcoin, developers who were impressed by the Bitcoin system started working on further developments of the Bitcoin system. Their goal was simple; to improve what a coin can do other than being a digital currency.[116] Then came Bitcoin Protocol: the Blockchain 2.0 (sometimes referred to as Bitcoin 2.0 or Cryptography 2.0), which is known for its decentralised applications.[117]

One example of the Blockchain 2.0 projects which is now in effect, is the Ethereum protocol.[118] Ethereum may sometimes be seen as a better version of Bitcoin. Hence, this is why it is sometimes referred to as Bitcoin 2.0.[119] Ethereum has succeeded in creating a system of its own: its own blockchain.[120] Ethereum has also managed to attract a broad range of corporations such as Microsoft,[121] Barclays and UBS,[122] IBM, and Samsung.[123]

Ethereum was created by Vitalik Buterin and others.[124] Buterin, a Canadian national of Russian origins, came up with an idea when he was 19 years old in 2011.[125] Buterin's idea was that he could utilise the blockchain technology in order "to support a whole new programming language," that

[116] Hazratjee (n 51) 56
[117] 'What You Need To Know About Bitcoin 2.0 & Blockchain 2.0' (*NewsBtc*) <http://uk.newsbtc.com/blockchain-2-0/> accessed 19 July 2017
[118] 'Ethereum Project' (*Ethereum.org*, 2017) <https://www.ethereum.org/> accessed 12 July 2017
[119] Ian Allison, 'UBS and Barclays Are Front Runners with Bitcoin 2.0 Technology Ethereum' (*International Business Times UK*, 2015) <http://www.ibtimes.co.uk/ubs-barclays-bnp-paribas-are-front-runners-bitcoin-2-0-technology-ethereum-1514138> accessed 16 July 2017; Michael Nofer and others, 'Blockchain' (2017) 59 Business & Information Systems Engineering 185
[120] Franco (n 72) 199
[121] Giulio Prisco, 'Microsoft Partners with Ethereum Company, Offers Cloud-Based Blockchain Application Development Platform To Its Clients' (*Bitcoin Magazine*, 2015) <https://bitcoinmagazine.com/articles/microsoft-partners-with-ethereum-company-offers-cloud-based-blockchain-application-development-platform-to-its-clients-1446484607/> accessed 16 July 2017
[122] Allison (n 119)
[123] Stan Higgins, 'IBM Reveals Proof Of Concept For Blockchain-Powered Internet Of Things' (*CoinDesk*, 2015) <http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/> accessed 16 July 2017
[124] 'Who Created Ethereum?' (*CoinDesk*) <http://www.coindesk.com/information/who-created-ethereum/> accessed 12 July 2017
[125] Nick Vogel, 'The Great Decentralization: How Web 3.0 Will Weaken Copyrights' (2017) 15 John Marshall Review of Intellectual Property Law 140

allows the building and publishing of distributed applications.[126] Ethereum was officially launched on July 30, 2015.[127]

The Nakamoto plan involved three steps in which only two were implemented: The decentralised blockchain and the transaction system which permits the transfer of value between parties without an intermediary, which is done by the Bitcoin protocol. These two steps were successfully implemented in Bitcoin's blockchain. However, for Blockchain 2.0 to be successful where Bitcoin was not, the third phase needed to be Turing complete.[128] Turing complete[129] is a programing language[130] that allows the ability to run any coin, protocol, or blockchain,[131] which is the defining feature of Ethereum[132] and gives it its characteristic flexibility, unlike Bitcoin.[133]

2.1 How Ethereum Works

Ethereum is a platform that can run all blockchains and platforms. Decentralised applications can run on this platform.[134] It is also open-ended (open source) by design rather than being a closed-ended platform for a single purpose.[135] This stands in contrast to Bitcoin, which focuses solely on currency.[136] The platform allows the running of smart contracts.[137] The Ethereum platform's main purpose is to easily enable people to write decentralised applications using the underlying blockchain technology.[138] Ethereum uses Ethash, which is a planned PoW algorithm that permits decentralised

[126] Swan (n 56) 21
[127] Stephan Tual, 'Ethereum Launches - Ethereum Blog' (*Ethereum Blog*, 2015) <https://blog.ethereum.org/2015/07/30/ethereum-launches/> accessed 15 July 2017
[128] Swan (n 56) 21
[129] "Turing-complete language is a language that, by definition, can perform any computation. In other words, if there is an algorithm for something, it can express it." See Sebastián Peyrott, 'An Introduction To Ethereum And Smart Contracts: A Programmable Blockchain' (*Auth0*, 2017) <https://auth0.com/blog/an-introduction-to-ethereum-and-smart-contracts-part-2/> accessed 19 July 2017; Marie Duzi defines Turing as "A numerical function is effectively computable by an algorithmic routine if and only if it is computable by a Turing machine" Marie Duzi, *A Procedural Interpretation Of The Church-Turing Thesis.* (2013) 9; Paolo Tasca and others, *Banking Beyond Banks And Money: A Guide To Banking Services In The Twenty-First Century* (Springer 2016) 246
[130] Arthur B, 'Smart Contracts: Turing Completeness & Reality – Hacker Noon' (*Hacker Noon*, 2016) <https://hackernoon.com/smart-contracts-turing-completeness-reality-3eb897996621> accessed 17 July 2017
[131] Swan (n 56) 21
[132] Peyrott (n 129)
[133] Cunningham (n 14) 251
[134] Hazratjee (n 51) 85
[135] Vitalik Buterin, 'A Next-Generation Smart Contract And Decentralized Application Platform' (*GitHub*, 2017) <https://github.com/ethereum/wiki/wiki/White-Paper> accessed 19 July 2017
[136] Vogel (n 125) 140
[137] Ethereum Project (n 118)
[138] 'What Can You Do With It? | Ethereum Builder's Guide' (*Ethereumbuilders.gitbooks.io*, 2015) <https://ethereumbuilders.gitbooks.io/guide/content/en/what_is_ethereum.html> accessed 12 July 2017

mining by Ethereum clients, unlike Bitcoin which uses a centralised ASICs.[139] Miners are awarded 5 Ether for each block that they successfully mine.[140] The average block time in Ethereum takes 12-15 seconds, unlike Bitcoin which takes 10 minutes. Also, unlike Bitcoin where the majority of Bitcoins have already been mined, only half of the Ethereum coins are estimated to be mined by the year 2021.[141]

Ethereum is also an open source blockchain. Ethereum and Bitcoin both permit the creation of an economic system within the software itself that provides accounts that can be managed and also contains a local unit of exchange that can be transacted between the accounts on the network. Such units of exchange are usually referred to as coins, tokens, or sometimes cryptocurrencies. These units act as money within these systems.[142] In the case of Ethereum, this currency is known as the Ether (ETH).[143] This currency serves as the fuel in regards to all Ethereum transactions.[144] However, clients may also create their own currency.[145]

We have already discussed that Bitcoin was first to create the blockchain system. However, the platform that Ethereum offers has been seen more attractive due to it taking the blockchain technology one step further. Whether it is application developers that would likely build products and provide services on Ethereum, or whether it is non-programmers, such as individuals that represent financial services, consulting, insurance, law, or governments, all can benefit from the technology that the Ethereum blockchain offers.[146]

[139] 'Ethash' (*GitHub*) <https://github.com/ethereum/wiki/wiki/Ethash> accessed 27 July 2017
[140] 'Ether: The Crypto-Fuel For The Ethereum Network' (*Ethereum.org*) <https://www.ethereum.org/ether> accessed 27 July 2017
[141] 'History Of Ethereum: How It's Set To Overtake Bitcoin By 2018' (*mining.com*, 2017) <http://www.mining.com/web/history-ethereum-set-overtake-bitcoin-2018/> accessed 27 July 2017
[142] Dannen (n 61) 2
[143] Franco (n 72) 201
[144] Allen & Overy, 'Decentralized Autonomous Organizations' (2017) 2
[145] 'Create Your Own Crypto-Currency With Ethereum' (*Ethereum.org*) <https://www.ethereum.org/token> accessed 27 July 2017
[146] Vitalik Buterin, 'Visions, Part 1: The Value Of Blockchain Technology - Ethereum Blog' (*Ethereum Blog*, 2015) <https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/> accessed 14 July 2017

2.2 What are Smart Contracts?

One of the most developed areas of law is contract law. Contract law is constantly evolving as new ideas such as new business models emerge that require specifically tailored contracts that suit such needs.[147]

Blockchains are not just used for digital currencies; they can be used to create smart contracts (SCs) as well.[148] SCs could have an impact on how the law is practised. SCs utilise the concept of blockchain.[149] They are a revolutionary blockchain application that existed before Bitcoin.[150] While there is no universally agreed definition of what a SC is, it can be succinctly described as a contract that contains a computer code, which has been drafted with the purpose of being self-executing.[151] These SCs are similar to normal paper contracts which are drafted in natural human language; however, SCs are written through a process called, "coding", which is a language that computers understand.[152] The computer system that reads the SC also executes its terms.[153] In simple terms, a SC is a contract that is captured in code.[154] Hence, this is why it is referred to as "smart".

However, the term "smart contract" is not novel. It was first described by Nick Szabo,[155] a computer scientist who studied law. Szabo described it first in 1997.[156] Szabo also describes SCs as a computerised transaction algorithm that has the purpose of performing the terms of the contract.[157] According to Gideon Greenspan, a SC can also be defined as follows: "A smart contract is a piece of code which is stored on an (sic) Blockchain, triggered by Blockchain transactions, and which reads

---

[147] Savelyev (n 57) 120
[148] Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology And The Rise Of Lex Cryptographia' [2015] SSRN https://ssrn.com/abstract=2580664 15
[149] Riikka Koulu, 'Blockchains and Online Dispute Resolution: Smart Contracts As An Alternative To Enforcement,' (2016) 13 SCRIPTed: A Journal of Law, Technology and Society 53
[150] Cognizant, 'Blockchain In Banking: A Measured Approach' (2016) 5
[151] Andy Robinson and Tom Hingley, 'Smart Contracts: The Next Frontier?' (*Oxford Law Faculty*, 2016) <https://www.law.ox.ac.uk/business-law-blog/blog/2016/05/smart-contracts-next-frontier> accessed 15 July 2017; Samuel Bourque and Sara Fung Ling Tsui, *A Lawyer's Introduction To Smart Contracts* (Scientia Nobilitat - Platform for Exchange of Scientific Ideas 2014) 4; See also Shawn Bayern, 'Dynamic Common Law And Technological Change: The Classification Of Bitcoin' (2014) 71 Washington and Lee Law Review Online 38
[152] Tanel Kerikmäe and Addi Rull, *The Future Of Law And Etechnologies* (Springer 2016) 134
[153] Bourque and Tsui (n 151) 4
[154] Institute of International Finance, 'Getting Smart: Contracts On The Blockchain' (2016) 2
[155] Nick Szabo is the first person who described smart contracts in his paper on *Formalizing and Securing Relationships on Public Networks.* See Nick Szabo, 'Formalizing And Securing Relationships On Public Networks' (1997)
[156] Michael Gord, 'Smart Contracts Described By Nick Szabo 20 Years Ago Now Becoming Reality' (*Bitcoin Magazine*, 2016) <https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751/> accessed 15 July 2017
[157] Savelyev (n 57) 120

and writes data in that Blockchain's database".[158] Nevertheless, due to the arrival of Bitcoin and its sophisticated blockchain technology, the concept of SCs can be put to use in new ways.[159] Through its use of cryptography, blockchain technology offers the security and the accuracy required for a platform in order to fully utilise the concept of SCs.[160]

SCs are contracts that are designed to self-execute the terms of the prescribed agreement within them when the conditions of the agreement are met. The parties to a SC, or users, design the contract based on their needs, similar to drafting a paper contract, and once they agree to all the terms stipulated in the contract, they sign the contract "cryptographically" and upload it on the blockchain.[161] Afterwards, the SC is in charge of executing the terms within the contract by itself. Whenever a condition that has been written within the contract is met, the contract itself triggers the appropriate action in reaction to that condition. A brief example can be given to illustrate how such a SC would function. Party A sells Party B goods. After the merchandise have been transferred, the SC proceeds with paying Person A the funds of Person B as prescribed in the smart contract. If Party B decides to abstain from payment, then the SC would recover the merchandise of Part A in return for non-payment. Hence, this is one scenario where a SC can be used. If utilised properly, this notion can be used on a larger scale, such as in trading financial instruments, loan agreements, and much more. It will also result in the reduction of costs and will help speed transactions.[162]

These SCs are designed to live on the blockchain and not a server, as they are deployed on the distributed ledger. The SCs on the blockchain transactions will be executed by the Ethereum Virtual Machine (EVM).[163] These SCs do not exist physically, as they are made up of code. Finally, as previously stated, the concept of SCs is not a novel concept.[164] In fact, variations of them existed in

[158] Gideon Greenspan, 'Beware Of The Impossible Smart Contract' (*Blockchain News*, 2016) <http://www.the-blockchain.com/2016/04/12/beware-of-the-impossible-smart-contract> accessed 16 July 2017
[159] Reggie O'Shields, 'Smart Contracts: Legal Agreements For The Blockchain,' (2017) 21 North Carolina Banking Institute 179
[160] Institute of International Finance (n 154) 2
[161] ibid
[162] World Economic Forum, 'The Future Of Financial Infrastructure: An Ambitious Look At How Blockchain Can Reshape Financial Services' (World Economic Forum 2016) 39
[163] Franco (n 72) 199
[164] Bourque and Tsui (n 151) 5

the past, such as transaction processing systems (TPS), which have been used by banks for at least the last three decades.[165]

2.3 Decentralised Applications

A decentralised application (also known as Dapps or DA) is a software.[166] This program is designed to operate without the need of a middle man. Perhaps the most common one today is the decentralised virtual currency.[167] According to Johnston, a DA must possess three features: A Type I DA, such as Bitcoin, possesses its blockchain. Type II DAs, such as Omni Protocol, use the blockchain technology of Type I Das, but are "protocols and have tokens that are necessary for their function".[168] The final type is Type III DA. These applications use the protocol of a Type II DA, such as the SAFE Network that uses the Omni Protocol to issue "safecoins."[169] These applications can either be closed or open source. However, it would be hard to make closed-source applications more attractive than open-source applications.[170]

These applications are quite similar to SCs. However, DAs varies in two aspects. Firstly, a DA can have an unlimited number of participants on all sides of the market. Secondly, DAs are not bound to be created for a financial purpose. The concept of a DA itself is not novel. Examples of decentralised applications include BitMessage, BitTorrent, Gems, LaZooz, Maidsafe, OpenBazaar, Popcorn, Storj, Time, Tor, and Twister.[171]

2.4 Decentralised Organisations

A blockchain is not only limited to connecting nodes. "It also allows for the execution and interconnection of a variety of SCs that interact with one another in a decentralised and distributed

---

[165] Allan I. Mendelowitz and Willi Brammertz, 'Smart Contracts Were Around Long Before Cryptocurrency' (*American Banker*, 2016) <https://www.americanbanker.com/opinion/smart-contracts-were-around-long-before-cryptocurrency> accessed 13 August 2017

[166] Siraj Raval, *Decentralized Applications* (O'Reilly 2016)

[167] Carla L. Reyes, 'Moving Beyond Bitcoin To An Endogenous Theory Of Decentralized Ledger Technology Regulation: An Initial Proposal' (2016) 61 Villanova Law Review 199

[168] David Johnston, 'The General Theory Of Decentralized Applications, Dapps' (*GitHub*, 2015) <https://github.com/DavidJohnstonCEO/DecentralizedApplications> accessed 3 August 2017

[169] Angela Ruth, 'Why Build Decentralized Applications: Understanding Dapp - Due' (*Due*, 2016) <https://due.com/blog/why-build-decentralized-applications-understanding-dapp/> accessed 26 July 2017; SAFE Network is a decentralised data storage and communications network that uses peer-to-peer technology in order to store data. *See* 'SAFE Network' (*Safenetwork.org*) <https://safenetwork.org/> accessed 26 July 2017

[170] Raval (n 166)

[171] Vitalik Buterin, 'Daos, Dacs, Das And More: An Incomplete Terminology Guide - Ethereum Blog' (*Ethereum Blog*, 2014) <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/> accessed 17 July 2017

manner."[172] A decentralised organisation (DO) can be formed by multiple SCs, which permits it to operate according to specific rules and procedures that are stated within the SCs.[173] The pooling of multiple SCs together to form a DO proves the validity of the theory of Michael Jensen and William Meckling that firms are nothing more than a collection of contracts and relationships between various parties.[174]

DOs that are based on blockchain allow individuals and machines to come together through a set of SCs rather than needing to join traditional business entities and help with avoiding the bureaucratic process.[175] A typical corporation involves a specific structure that is under the control of certain individuals who interact in accordance with the company's charter and bylaws to keep the company running. In a DO, the protocol that is in the code specifies how these individuals interact by having a structure that is enforced on the blockchain.[176]

This will also help with the reduction of future operational costs as transactions will be recorded directly on the blockchain which will help with corporate governance while providing transparency and a history for future auditing. Furthermore, multi-signature technology may prove to be useful when it comes to corporate governance decision-making among parties.[177]

Creating a DO can help shareholders participate in the decision-making process instead of having to delegate the process to a chosen board of directors,[178] as the decision-making will be coded in the smart contract. When it comes to distributing duties within the corporation, shareholders will be able to vote through the decentralised voting system that is set out within their SCs. Thus, DOs take the idea of a traditional organisation and make it decentralised.[179]

[172] Wright and Filippi (n 148) 15
[173] ibid
[174] Michael C. Jensen and William H. Meckling, 'Theory Of The Firm: Managerial Behavior, Agency Costs And Ownership Structure' (1976) 3 Journal of Financial Economics 8, 9
[175] Wright and Filippi (n 148) 16
[176] Buterin (n 171)
[177] Wright and Filippi (n 148) 16
[178] Jeremy Epstein, 'Companies Of The Future: No CEO, No Boss, Managed By Blockchain' (*VentureBeat*, 2017) <https://venturebeat.com/2017/04/23/companies-of-the-future-no-ceo-no-boss-managed-by-blockchain/> accessed 20 July 2017
[179] Buterin (n 171)

2.5 Decentralised Autonomous Organisations

A decentralised autonomous organisation (DAO) "is an entity that lives on the internet and exists autonomously."[180] DAOs run according to rules that are encoded in a smart contract.[181] However, this entity depends on individuals whom it hires to perform certain tasks that it itself cannot do.[182] It runs on a peer-to-peer network. It also incorporates governance structures and decision-making rules like corporations.[183] Its rules and bylaws are written in its code.

However, it is important to explain what a DAO is not, and whatever is not a DAO can either be a DO or a DA. Firstly, a DAO possesses internal capital; Bitcoin and Ethereum are examples of DAOs. This differs from BitTorrent, which possesses no internal capital and is thus a DA.[184]

Secondly, if we compare a DO to a DAO, we see that the difference resides in wording; DAO contains the word "autonomous", unlike a DO in which the human shareholders are responsible for making the decisions as discussed above. The DAO, on the other hand, makes decisions on its own behalf.[185] The Ethereum platform permits the running of such applications, whether they be DAs, DOs, or DAOs.

2.6 Dispute Resolution via Smart Contracts

A method in which disputes between parties to a SC could be resolved is multisignature transactions. Multisignature transactions could aid in resolving potential disputes via SCs. A multisignature transaction can be applied to transactions by making it a 2-of-3 transaction. For this to work, coins are to be sent to a multisignature address where the future transaction is allocated to. The specified address contains a buyer, a seller, and a third party arbitrator or mediator that is selected by both parties. After the coins are sent to the address, neither party can move the coins from the joint address without the approval of two out of the three parties that share the same address. Hence, an example may be given to show how such a process would work in simple terms. In a scenario where both the buyer and seller are satisfied with the exchange, they both sign off on the transaction,

[180] ibid
[181] 'Decentralized Autonomous Organisations' (*BlockchainHub*) <https://blockchainhub.net/daos/> accessed 26 July 2017
[182] Buterin (n 171)
[183] Allen and Overy (n 144) 2
[184] Decentralized Autonomous Organisations (n 187)
[185] Buterin (n 171)

which will lead to the transferring of the coins from the joint address to the seller.[186] However, if either party is not satisfied, for example, in case the seller signed off but the buyer, unsatisfied, refused to sign off on the transfer, a dispute would arise. In such scenario, the third-party that was chosen to be an arbitrator can decide on who should receive the coins and would sign off on the transfer. Hence, the third party's signature fulfils the requirement that is required to complete the 2-of-3 transaction.[187]

The multisignature transaction can offer flexibility. The third-party, which is the arbitrator that is assigned to the multisignature address, can also be a specialist in a specific field. In a transaction that involves the sale of art, the assigned third party can be an expert that verifies and inspects the validity of the sold product.

Another third-party alternative to an arbitrator can be a program called an oracle.[188] An Oracle can act as an arbitrator in a SC and resolve certain disputes.[189] Oracles can be in charge of gathering information about the state of the world in some scenarios.[190]

2.7 Technological uses for DLT and SCs

DLT and SCs are very promising. These technologies may have an impact on improving global payments, insurance, syndicated loans, reduce counterparty risk and enable faster settlements in financial documents, and help with the issuance of CoCo bonds.[191] Furthermore, SCs could aid banks in monitoring the posted collateral that is being used in transactions and reduce counterparty risk.[192] They may also aid regulators in detecting illegal transactions. Some firms have already started exploring various ways on how to utilise SCs in order to try and integrate them "with various securities, including bonds, futures, and options."[193] An example of how SCs may change the insurance industry can be given. For instance, when the SC verifies the passing of the policyholder,

[186] James Gatto and Elsa S. Broeker, 'Bitcoin And Beyond: Current And Future Regulation Of Virtual Currencies' (2015) 9 Ohio State Entrepreneurial Business Law Journal 467
[187] Brito, Shadab and Castillo (n 36) 207
[188] Mike Hearn, 'Contract' (*En.bitcoin.it*) <https://en.bitcoin.it/w/index.php?title=Contract&redirect=no> accessed 20 July 2017
[189] Stefan Thomas and Evan Schwartz, 'Smart Oracles: A Simple, Powerful Approach To Smart Contracts' (*GitHub*, 2014) <https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts> accessed 20 July 2017
[190] Hearn (n 188)
[191] World Economic Forum (n 162) 39-44
[192] ibid
[193] Institute of International Finance (n 154) 3

the life insurance SC will automatically execute the transferring of funds of the policyholder to their chosen beneficiary. Another example in which SCs can be helpful is lender syndications. These syndications can be formed by a SC, which would be in charge of releasing the term loan once its requirements are fulfilled.

Aside from SCs, some central banks also have been studying the proposal of a central bank-issued digital currency by using blockchain technology.[194] The Bank of England, for example, is studying the implications of such a proposal.[195]

Barclays Bank is currently studying the usage of SCs.[196] Barclays sees that SCs may aid in derivatives documentations such as the ISDA master agreement, its credit support documentation, and confirmations. Incorporating the ISDA master agreement into a SC may aid in reducing risk and costs and increasing efficiency.[197] Barclays envisions that SCs would be provided to counterparties, which would then download and use it in correlation with the master agreements that would be stored on a centralised distributed ledger.[198] The use of SCs in this scenario would be seen as a safety net, which might help prevent human errors that may lead to a systemic risk, since derivatives are sophisticated financial instruments that involve significant counterparty risk.

As a result, the implementation of blockchain technology in the derivatives market will lead to the removal of requiring post-trade confirmation, and will reduce the process of central clearing. This is because all participants on the network will sign the same dataset in trade-related procedures. Therefore, the blockchain will reduce the possibility of an error occurring, reducing lags, speeding up the end-to-end process, and reduce disputes between counterparties, because the records of the

[194] Richard Milne, 'Sweden's Riksbank Eyes Digital Currency' (*Ft.com*, 2016) <https://www.ft.com/content/0e37795c-ab33-11e6-9cb3-bb8207902122?mhq5j=e3> accessed 16 July 2017.
[195] Bank of England, 'Staff Working Paper No. 605: The Macroeconomics Of Central Bank Issued Digital Currencies' (2016) 3
[196] Ian Allison, 'Barclays Gets Into The Nuts And Bolts Of Smart Contract Templates' (*International Business Times UK*, 2016) <http://www.ibtimes.co.uk/barclays-gets-into-nuts-bolts-smart-contract-templates-1596874> accessed 19 July 2017
[197] Pete Rizzo, 'How Barclays Used R3's Tech To Build A Smart Contracts Prototype' (*CoinDesk*, 2016) <http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/> accessed 16 July 2017; For example, digital currency based derivatives are being created by a startup named Hedgy. See Stan Higgins, 'Hedgy Raises $1.2 Million For Smart Contract-Powered Bitcoin Derivatives' (*CoinDesk*, 2015) <http://www.coindesk.com/hedgy-1-2-million-smart-contract-bitcoin-derivatives/> accessed 20 July 2017
[198] ibid

data stored will be on the blockchain.[199] Similarly, ISDA and the European Securities Market Authority have suggested that SCs may help aid the netting process, among other things.[200]

Furthermore, other banks, such as JP Morgan and Credit Suisse, have conducted equity swaps tests through a SC, which proved successful. These tests were months-long and were organised by Axoni to show the reliability of the software when it comes to handling complex post-trade services such as margin payments and corporate action processing.[201] Santander has also viewed several uses for SCs.[202] BNP Paribas is also exploring SCs.[203]

SCs would benefit not only large corporations but also consumers. SCs can be seen to be unbiased whenever it comes to the protection of consumer rights. Such contracts may grant consumers an equal bargaining power when they negotiate business terms with such corporations during online transactions. For example, individuals who wish to purchase online merchandise can assign robots to negotiate on their behalf that are pre-programmed based on their preferences.[204]

DLT and SCs offer benefits such as speeding the business process, lowering risk, increasing accuracy, less exposure to human error, eliminating third-party reliance, lowering unnecessary costs and much more. Operational risk of over-the-counter (OTC) trading would be eliminated if we were to decentralise the clearing process. The benefit in return by using SCs and blockchain technology would be immeasurable.[205] The Depository Trust & Clearing Company (DTCC) in 2016 processed more than $1.5 quadrillions worth of securities, which equate to more than 356 million settled transactions.[206] Financial institutions are expected to spend $1 billion on blockchain projects in 2017,

[199] Oliver Wyman and Euroclear, 'Blockchain In Capital Markets: The Prize And The Journey' (2016) <http://www.dltmarket.com/docs/BlockchainInCapitalMarkets-ThePrizeAndTheJourney.pdf> accessed 6 August 2017 7
[200] European Securities and Markets Authority, 'Reply Form For The Discussion Paper On The Distributed Ledger Technology Applied To Securities Markets' (2016) 11
[201] Michael del Castillo, 'JP Morgan, Credit Suisse Among 8 In Latest Bank Blockchain Test' (*CoinDesk*, 2016) <http://www.coindesk.com/jp-morgan-credit-suisse-among-8-in-latest-bank-blockchain-test/> accessed 19 July 2017
[202] 'Financial Institutions: Blockchain Activity Analysis' (*Lets Talk Payments*, 2015) <https://letstalkpayments.com/financial-institutions-blockchain-activity-analysis/> accessed 28 July 2017
[203] Bailey Reutzel, 'Blockchain Smart Contracts Startup Selected By BNP Paribas Accelerator' (*CoinDesk*, 2017) <http://www.coindesk.com/blockchain-smart-contracts-bnp-paribas/> accessed 19 July 2017
[204] Joshua A.T. Fairfield, 'Smart Contracts, Bitcoin Bots, And Consumer Protection' (2014) 71 Washington and Lee Law Review Online 41
[205] Madiha M. Zuberi, 'A Silver (‘Chain’) Lining: Can Blockchain Technology Succeed In Disrupting The Banking Industry?' (2017) 36 Banking & Financial Services Policy Report 3
[206] 'DTCC 2016 Annual Report' (*Dtcc.com*, 2017) <http://www.dtcc.com/annuals/2016/index.html#business> accessed 4 August 2017

which will make blockchain one of the fastest developing softwares on the market.[207] Financial institutions, such as investment banks, could save up to $12 billion a year by 2025.[208]

2.8 Other Blockchain 2.0 Projects

Ethereum is not the only project referred to as Blockchain 2.0. There are several blockchain technology projects that fall under the title of Blockchain 2.0. Some of these projects have been launched already, and some are still under development. Among these projects are Bitshares,[209] Colored Coins,[210] Counterparty,[211] Omni Layer (previously known as Mastercoin),[212] NXT,[213] Open Assets,[214] Open Transactions,[215] and Ripple.[216]

[207] Morgan Stanley, 'Blockchain In Banking: Disruptive Threat Or Tool?' (2016) <http://www.the-blockchain.com/docs/Morgan-Stanley-blockchain-report.pdf> accessed 19 July 2017 5
[208] Anna Irrera and Jemima Kelly, 'Blockchain Could Save Investment Banks Up To $12 Billion A Year: Accenture' (*Reuters*, 2017) <http://uk.reuters.com/article/us-banks-blockchain-accenture-idUKKBN1511OU> accessed 27 July 2017; See also The Goldman Sachs Group, Inc, 'Profiles In Innovation: Blockchain: Putting Theory Into Practice' (2016) <https://msenterprise.global.ssl.fastly.net/wordpress/2017/07/Goldman-Sachs-Blockchain-putting-theory-to-practice.pdf> accessed 6 August 2017 3
[209] 'Bitshares - Your Share In The Decentralized Exchange' (*Bitshares.org*, 2017) <https://bitshares.org/> accessed 3 August 2017
[210] 'Framework For Digital Currencies: An Open Source Banking Infrastructure For A Future Of Digital Money' (*Coloredcoins.org*, 2017) <http://coloredcoins.org/> accessed 3 August 2017
[211] 'Counterparty Extends Bitcoin In New And Powerful Ways.' (*Counterparty.io*, 2017) <https://counterparty.io/> accessed 3 August 2017
[212] 'Omni Layer: Open-Source, Fully-Decentralized Asset Platform On The Bitcoin Blockchain' (*Omnilayer.org*) <http://www.omnilayer.org/> accessed 26 July 2017
[213] 'Nxt' (*Nxt*, 2017) <https://nxt.org/> accessed 3 August 2017
[214] 'Openassets/Open-Assets-Protocol' (*GitHub*, 2016) <https://github.com/OpenAssets/open-assets-protocol> accessed 3 August 2017
[215] 'About The Open-Transactions Project' (*Opentransactions.org*, 2017) <http://opentransactions.org/wiki/index.php/About> accessed 3 August 2017
[216] 'Ripple' (*Ripple*, 2017) <https://ripple.com/> accessed 3 August 2017

3.0 Interledger

A payment protocol that creates one global network for all payments? It simply does not exist. However, a payment system that enables payments across payment platforms by individuals with accounts on the connected ledgers, i.e. an Interledger Protocol (ILP), is being developed by the W3C Interledger Community Group.[217]

Programmed on Web technologies, ILP is distinctive as it offers users the simplest and yet most efficient way to make payments. ILP is not only limited to users, it can also connect payment networks such as banks and cryptocurrencies. An upside to using the ILP is that it protects users' information by executing transactions without giving retailers the users' personal information.[218]

Although the internet today has given users around the globe free content and information, it has not been equally successful with regard to payments. This is where ILP succeeds. ILP allows the transfer of payments through the web. The purpose of ILP is for it to be used by all payment systems, retailers, web participants and others.[219] Besides facilitating transfers between users that are on the same ledger, ledgers are used to help track and record accounts and balances made by digital payment systems. However, in today's markets, the possibility of inter-ledger payments is expected. This is usually done by creating a new connection. However, any new connection must be trusted by both parties in order to safeguard the money.[220]

Payments that are sent on networks located in the same state are often straightforward. Likewise, if the payment is made internally within the same network or ledger. However, such payments were to be made to different ledgers, or different accounts in different countries, they would be cumbersome.[221]

[217] Adrian Hope-Bailie and Stefan Thomas, 'Interledger: Creating A Standard For Payments', *Proceedings of the 25th International Conference Companion on World Wide Web: International World Wide Web Conferences Steering Committee* (2016) 281
[218] ibid
[219] ibid
[220] Stefan Thomas and Evan Schwartz, *A Protocol For Interledger Payments* 1
[221] 'The Interledger Protocol (ILP)' (*Interledger.org*) <https://interledger.org/rfcs/0003-interledger-protocol/> accessed 28 July 2017

The IPL can be integrated into any ledger, although this requires enabling escrow transfers as this will permit funds to held in escrow before they are sent to the recipient. No other methods are required for the protocol to work. The protocol will then allow connectors to compete amongst each other by offering competitive rates and quicker ways for sending payments. Furthermore, the protocol is not finite, as it can handle any volume of payments regardless of their size.[222]

3.1 Payments Through the Interledger System

Ledgers may either be centralised or decentralised. There are numerous uses in which a ledger can be used to track value nowadays. Payments between accounts existing on the same system are book transfers. However, a connector is needed if the transfers need to be concluded between different systems. As the connecter facilitates interledger payments by managing book transfers between several ledgers, the connector must be trustworthy. Especially, because the connector can decide not to transfer the payment. To hedge against this, legal agreements are entered into with the connector, and emphasis is put on the respective connector's reputation. Thus, only a specific set of institutions can act as connectors which makes the entire process somehow limited and cumbersome.[223]

The interledger payment protocol enables payments between accounts on two ledgers by connecting them irrespective of the networks they are on.[224] The ledger does so by defining an escrow for ledgers to stage the transfer and abide by such transaction after the delivery of a "cryptographically signed proof that the pre-agreed condition has been met."[225] The sole purpose of this is to allow funds to pass safely through unsecured connectors.[226]

On the other hand, a ledger that offers escrow promises that it alleviate the cumbersome payment process. Escrow, in this case, acts as security. When the sender wishes to make a payment, the funds are escrowed first. Once the connector confirms that the money is in the escrow account, the connector goes forward with depositing the funds also in an escrow account. Afterwards, the transaction is concluded. The ledgers themselves provide escrow.

[222] Thomas and Schwartz (n 220) 1
[223] ibid 2
[224] ibid 1
[225] Hope-Bailie and Thomas (n 217) 281
[226] ibid

3.2 Hyperledger

To allow for multiple blockchain standards, the Linux Foundation created Hyperledger (previously Open Ledger Project)[227] in 2015.[228] Counting more than 120 members, and still increasing, the members of the Hyperledger project are technological companies, FinTech start-ups, world-leading financial organisations (stock-exchanges and financial intermediaries), the Bank of England and other banks, aeroplane and consumer electronics manufacturers, telecommunication providers and many others.[229]

To accelerate the development of blockchain technology, industry groups have been formed or consolidated.[230] One of these blockchain groups, the Ethereum Enterprise Alliance, consists of JPMorgan, Microsoft Corp, Intel Corp and others. Likewise, leading world banks have invested over $100 million in the R3CEV organisation which is building a promising ledger named "R3 Corda"[231], which is similar to Hyperledger in many ways.[232]

The Hyperledger project's goal is to utilise and develop blockchain technologies through a joint effort,[233] thereby creating an enterprise grade, open source distributed ledger framework and code base. The purpose of the project is to utilise the blockchain technology to change the way in which businesses transact globally.[234]

---

[227] Pete Rizzo, 'Linux Foundation-Led Blockchain Project Grows To 30 Members' (*CoinDesk*, 2016) <https://www.coindesk.com/linux-foundation-led-hyperledger-project-swells-to-30-members/> accessed 30 July 2017

[228] Linux Foundation, 'Hyperledger-Fabricdocs Documentation: Release Master' (2017) 16

[229] Marko Vukolic, *Rethinking Permissioned Blockchains* (2017) <https://vukolic.github.io/rethinking-permissioned-blockchains-BCC2017.pdf> accessed 30 July 2017

[230] Anna Irrera, 'Hyperledger Releases Its First Production Ready Blockchain' (*Business Insider*, 2017) <http://uk.businessinsider.com/hyperledger-releases-blockchain-code-strong-enough-for-corporations-2017-7> accessed 1 August 2017

[231] Richard Gendal Brown, 'Introducing R3 Corda™: A Distributed Ledger Designed For Financial Services' (*R3*, 2016) <http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services> accessed 2 August 2017

[232] Jonathan Shieber, 'Blockchain Consortium R3 Raises $107 Million' (*TechCrunch*, 2017) <https://techcrunch.com/2017/05/23/blockchain-consortium-r3-raises-107-million/> accessed 1 August 2017; 'Why The R3CEV Blockchain Consortium Is Splintering & What That Signals' (*Daily Fintech*, 2016) <https://dailyfintech.com/2016/11/28/why-the-r3cev-blockchain-consortium-is-splintering-what-that-signals/> accessed 2 August 2017

[233] Linux Foundation (n 227) 16

[234] Christian Cachin, 'Architecture Of The Hyperledger Blockchain Fabric' [2016] Workshop on Distributed Cryptocurrencies and Consensus Ledgers 1

Among the Hyperledger projects[235] is the Hyperledger Fabric version 1.0 which was released on July 11, 2017.[236] Even though it was recently released, some organisations were testing earlier versions of the Fabric.[237] About 29 organisations and more than 150 engineers have worked on the creation of the Hyperledger Fabric project.[238]

Hyperledger Fabric is a distributed ledger platform that permits the running of "SCs, leveraging familiar and proven technologies, with a modular architecture allowing pluggable implementations of various functions."[239] The protocol is run by its peers (nodes) of which there are two kinds: The first one is a validating peer. This node is in charge of running consensus, validating transactions, and maintaining the ledger. The second peer is non-validating. This node acts as a proxy to connect clients to the first type of peer. The second type of peer, although it cannot execute transactions, it can verify them.[240]

3.3 Why Hyperledger Fabric is Different from Other Blockchains

Being a private blockchain, Hyperledger Fabric uses a chaincode.[241] However, similar to Ethereum's blockchain, Hyperledger Fabric uses SCs and allows nodes within the system to transact freely amongst each other.[242] Moreover, the Accord Project is launching the first legal SC with Hyperledger.[243]

[235] ibid
[236] 'Release Notes' (*Hyperledger-fabric.readthedocs.io*, 2017) <http://hyperledger-fabric.readthedocs.io/en/latest/releases.html> accessed 1 August 2017
[237] Michael del Castillo, 'Fabric 1.0: Hyperledger Releases First Production-Ready Blockchain Software' (*CoinDesk*, 2017) <https://www.coindesk.com/fabric-1-0-hyperledger-releases-first-production-ready-blockchain-software/> accessed 1 August 2017
[238] Irrera (n 230)
[239] Alexandru Stanciu, 'Blockchain Based Distributed Control System For Edge Computing' [2017] 2017 21st International Conference on Control Systems and Computer Science (CSCS) 669
[240] ibid
[241] Nikola Bozic, Guy Pujolle and Stefano Secci, 'A Tutorial On Blockchain And Applications To Secure Network Control-Planes' [2016] 2016 3rd Smart Cloud Networks & Systems (SCNS)
[242] Linux Foundation (n 227) 16
[243] Roger Aitken, 'Accord Project's Consortium Launching First Legal 'Smart Contracts' With Hyperledger' (*Forbes.com*, 2017) <https://www.forbes.com/sites/rogeraitken/2017/07/26/accord-projects-consortium-launching-first-legal-smart-contracts-with-hyperledger/#5dfa9fb5472c> accessed 1 August 2017

However, unlike Bitcoin and Ethereum's blockchains which are public and permissionless,[244] Hyperledger Fabric is a private, decentralise[245] and open source permissioned blockchain system.[246] Also, Bitcoin and Ethereum does not verify the identity of their respective users. In contrast, since Hyperledger Fabric is private and permissioned, members within this network will have to obtain a Membership Service Provider (MSP) to use the network.[247]

By describing permissioned network here, we are addressing networks that encompass whitelisted organisations that run validating and non-validating nodes in which users transacting on such networks are granted an identity to run on these. The identities of the participants are known to the network's issuing authority service.[248]

Also, Hyperledger Fabric and other networks allows participants to create separate ledgers for specific transactions by establishing channels. This is vital on such network since users on the network may be competitors and want to keep trade secrets hidden from other participants. Privacy may be established between participants on the network when they create a channel that only authorised participants may join. As they will possess copies of the ledger to that specific channel.[249]

Another advantage of Hyperledger Fabric is its flexibility, as Hyperledger Fabric's modularity permits corporations to use their own identity. Therefore, these companies will not have to rebuild their identity on a new network again. Instead, they can reuse it by simply plugging it in.[250]

[244] Devon Allaby, 'The Trust Trade-Off: Permissioned Vs Permissionless Blockchains' (*Fjordnet.com*, 2016) <https://www.fjordnet.com/conversations/the-trust-trade-off-permissioned-vs-permissionless-blockchains/> accessed 30 July 2017
[245] Bozic, Pujolle and Secci (n 241)
[246] Hyperledger is not the only permissioned blockchain; Tendermint; Symviont Assembly; R3 Corda; Iroha; Kadena; Chain; Quorum; and MultiChain are other notable permissioned blockchains. See also Christian Cachin and Marko Vukolić, 'Blockchain Consensus Protocols In The Wild' 8; Linux Foundation (n 234) 16; Vukolic (n 229) 3
[247] Linux Foundation (n 227) 6
[248] ibid
[249] ibid 17
[250] Sharon Cocco and Gari Singh, 'Top 6 Technical Advantages Of Hyperledger Fabric V1.0 For Blockchain Networks' (*Ibm.com*, 2017) <https://www.ibm.com/developerworks/cloud/library/cl-top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/index.html> accessed 1 August 2017

3.3.1 Shared Ledger

Hyperledger is a shared ledger.[251] The Hyperledger Fabric contains a ledger subsystem that contains the 'world state' and a transaction log. Participants on the network have a copy of the ledger to.[252]

The current status of the ledger can be seen by accessing the world state at any time. It acts as the database of the ledger itself. The transaction log contains records of all the transactions that have occurred in accordance with the current value of the world state. Thus, the ledger itself consists of the world state database and the transaction log history.[253]

3.3.2 Smart Contracts

The Hyperledger Fabric enables the application of SCs. These contracts are inscribed within the chaincode.[254] Whenever an application that is external to the blockchain needs to interact with the ledger, such contracts are invoked. An interaction occurs between the world state and the chaincode and not the transaction log.[255]

3.3.3 Consensus

The transactions that take place on the network must be written down in order within the ledger even if they are to be among different participants that coexist on the same network. To ensure the success of transactions being recorded on the ledger, a method that rejects bad transactions must exist to help in dismissing errors or bad transactions. Also, Hyperledger Fabric does not use mining like Bitcoin.[256]

Unlike Bitcoin which relies on a PoW for mining that is based on SHA-256 to secure consensus, Hyperledger participants may choose between several consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT) SOLO, Kafka, and SBFT based on their needs.[257]

[251] 'Hyperledger Whitepaper' 3
[252] Linux Foundation (n 227) 17
[253] ibid
[254] 'Hyperledger Whitepaper (n 251) 2
[255] Linux Foundation (n 227) 17
[256] ibid
[257] ibid

4.0 FinTech Disadvantages

Bitcoins, DLT, Ethereum, Hyperledger Fabric, Interledger, and SCs all offers advantages, and they may revolutionise how things are done, especially in the financial sector. Nowadays, it is obvious that technology and regulation intersect. Technology changes how markets function, changes financial services, sectors and market structures. This is why it is necessary to regulate such changes to ensure market safety and efficacy. "Neither technology nor regulation is exogenous."[258] As the advantages to using FinTech is to cut costs, reduce risks, offer transparency and avoid mitigated risks such as human error and greed.

However, as much as there are advantages, technology also comes with a price. Although FinTech may be seen to encompass various advantages, its main advantage and disadvantages at the same time is security. Security can be regarded as the double-edged part of FinTech. If FinTech cannot guarantee security, then any technology applied will be rendered useless.

4.1 Legal Issues

4.1.1 Contract Law

SCs, like standard contracts, will require a substantial amount of work to sort their legal status. One challenge will be jurisdiction. That is, determining which law is applicable when seeking to determine the legality of the contract, to resolve any disputes in interpreting the contract, or which courts a SC dispute must be brought before. If a blockchain acts as a business record, can a litigant then submit it before a court?[259] Will SCs be seen as valid contracts?[260]

Another issue that will arise is the scarcity of lawyers that can code. Thus, computer programmers would be needed to help with the drafting of a smart contract. However, will computer programmers be liable for faulty algorithms or even ethical issues with regard to the practice of law by non-lawyers?[261]

[258] International Monetary Fund (n 47) 14
[259] Institute of International Finance (n 154) 9
[260] O'Shields (n 159) 185
[261] Institute of International Finance (n 154) 9

Although SCs are estimated to reduce legal costs, the costs will be transferred to the drafting process. As stated by Houman Shadab, "by requiring parties to strictly commit, at the outset, to decisions of a smart contract, the need for transactional attorneys and others to structure smart contractual relationships may increase. Parties would most likely want to specify a more detailed range of contingencies and outcomes ahead of time before committing themselves to abide by the decisions of a software-driven contract."[262]

Also, depending on whether the SC is on a public or permissionless system, it might face issues with consumer privacy laws, anti-money laundering (AML) and know your customer (KYC) procedures.[263]

4.1.2 Evidentiary, Enforcement, and Jurisdictional Issues

Evidentiary issues may arise whereby the way these contracts are written can become burdensome. Since such contracts are written in computer code, courts will face issues during adjudication when it comes to the interpretation hereof. This issue may be resolved by developing a copy of the SC in natural language once the contract is successfully signed. Moreover, experts in the fields of SC technology may be referred to when validating any SC technicalities during litigation.[264]

Enforcement issues may arise with SCs due to "evidentiary issues, enforceability of waivers of defences, and jurisdictional and choice-of-law questions."[265] One of the main advantages of SCs is that they self-execute and, based on that, they eliminate the requirement for human intervention. However, issues with regard to their enforcement may reduce their appealing nature. Thus, there will always be a requirement for human intervention whenever it comes to settling legal disputes.[266]

For a contract to be legally enforceable, the contract must adhere to the rules of its governing law. For example, some agreements may be oral, whereas others must be in written form. SCs would have to respond to these circumstances to be enforceable. It may be tricky for SCs to showcase "mutual assent" to a contract, as offer and acceptance complete mutual assent, and these can either be in writing or orally.[267]

[262] ibid
[263] ibid
[264] Bourque and Tsui (n 151) 11
[265] O'Shields (n 159) 185
[266] ibid
[267] ibid

Lastly, jurisdiction issues may arise since SCs are deployed on a blockchain, a type of DL.[268] For example, identifying the jurisdictional seat of the SC could be troublesome. Since SCs are applications deployed on a blockchain, which is itself located worldwide on a consensus network. Thus, this will raise issues when narrowing down the seat of the SC.[269] Hence, issues such as these would be complex, and leaving them unresolved after the contract has been signed would be unpropitious, especially in sophisticated transactions.

4.1.3 Criminal Activity

Ethereum's blockchain raises several potential risks with regard to SCs. Issues such as arson, terrorism, theft of cryptographic keys, and leakage of confidential information. This is related to the risks that come with the technology due to the connection of parties unknown to one another to conduct private dealings anonymously. Also, the automatic execution of the agreed terms might lead to the creation of new underground markets in which unknown individuals can hire assassins, hackers, or even terrorists to carry out tasks on their behalf while remaining anonymous. For instance, once the SC receives confirmation from the party that was hired to do the job, the SC can gather information from the outside world such as reputable news agency for reports of a terrorist attack in the designated area specified in the smart contract. After doing so, the contract would release the agreed upon funds.[270]

4.2 Potential Technology Failures

Technology is always subject to fail. That is one of the risks that come with the usage of technology. Transactions that are conducted with Bitcoins or other alt coins are nevertheless prone to such failures. The following examples will elaborate on such failures.

4.2.1 Anonymity Failure

Bitcoin, Ethereum and some alt coins' transactions are public. However, accounts that are involved in these transactions are anonymous. However, as unique public keys are used in transactions, the individuals behind the accounts used can be identified.[271]

[268] Bourque and Tsui (n 151) 13, 14
[269] ibid.
[270] Institute of International Finance (n 154) 9
[271] Grinberg (n 21) 179

4.2.2 Theft

Cryptocurrencies are similar to cash, of some sort. Both can be lost or stolen. Cryptocurrencies kept to significant sums is similar to keeping cash in a wallet. They can be lost if the wallet they are stored on are deleted. Furthermore, even if they were to be sent to online wallet services, such services have been hacked before.[272]

4.2.3 Denial of Service

Public permissionless currencies that are based on a PoW consensus system can be subject to Denial of Service attack (DoS). Since these networks depend on miners that maintain and keep up to date the ledger if a 51% network capacity were to be achieved such attack would cripple the network and cause loss of confidence.[273]

4.2.4 Blockchain Security

As always, technologies come with risk: hacking. Whenever there is a hack that is related to Bitcoin, Ethereum or blockchains, it cast doubt on the suitability of such technology in the financial industry. In early 2014, the world's largest Bitcoin trading platform of the time known as "Mt.Gox" based in Tokyo, Japan, was hacked. This hack resulted in the theft of Bitcoins worth approximately $460 million. Furthermore, $27.4 million went missing from the exchange's bank accounts.[274] This was the world's largest Bitcoin-related heist up to date. However, not the last. The second largest heist was Bitfinex. Bitfinex, a Bitcoin based exchange in Hong Kong, China, was hacked in early August 2016. The hack resulted in the loss of about $72 million worth of Bitcoins. However, Bitfinex claimed that the coins were stolen directly from the customers' wallets.[275]

---

[272] Richard Boase, 'Hackers Steal $1.2 Million Of Bitcoins From Inputs.Io, A Supposedly Secure Wallet Service' (*CoinDesk*, 2013) <https://www.coindesk.com/hackers-steal-bitcoins-inputs-io-wallet-service/> accessed 8 August 2017; See also Laura Shin, 'Hackers Have Stolen Millions Of Dollars In Bitcoin -- Using Only Phone Numbers' (*Forbes.com*, 2016) <https://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#5445648f38ba> accessed 8 August 2017; See also 'Parity Wallet Hacked With $32M In Ethereum Stolen' (*CryptoNinjas*, 2017) <https://www.cryptoninjas.net/2017/07/20/parity-wallet-hacked-32m-ethereum-stolen/> accessed 8 August 2017

[273] Grinberg (n 21) 180

[274] Robert McMillan, 'The Inside Story Of Mt. Gox, Bitcoin's $460 Million Disaster' (*WIRED*, 2014) <https://www.wired.com/2014/03/bitcoin-exchange/> accessed 9 August 2017

[275] Todd and Tyler (n 48) 12

Thus, these hacks show that cybersecurity remains a threat. Nevertheless, these hacks were Bitcoin related. Ethereum was also hacked, in a different way. Ethereum's hack will be discussed below.

Hence this is why financial institution have been sceptical towards implementing blockchain technology. Nevertheless, these issues have been found to be in public blockchains and not private ones.

4.3 Monetary Policy

In the UK, digital currencies pose a significant looming risk. They could affect the Monetary Policy Committee's (MPC) "influence aggregate demand as part of its remit to achieve 2% inflation in the consumer prices index".[276] As the MPC is responsible for influencing aggregate demand through the adjustment of Bank Rate. This affects the interest rate paid on reserves of commercial banks that are at the Bank of England (BoE). Monetary policies have several impacts on aggregate demand. However, a key one "is via the transmission of changes in Bank Rate to the interest rates offered by commercial banks to savers and borrowers."[277] As a result, the spending decisions of households and businesses have an impact on "the aggregate amount of economic activity and inflationary pressure in the economy."[278]

It is worth evaluating the risk that digital currencies may pose to monetary stability. Up until now, most payments in the UK are conducted by traditional Sterling-based payment systems. Thus, the MPC still can influence the aggregate demand throughout the state and achieve its monetary stability goals even if a relatively small amount were to be made by digital currencies. However, if a spike in usage of digital currencies were to happen, then that would cause fragmentation to the UK's economy. This would then result in the reduction of the BoE's ability to influence demand.[279]

Another possible threat to monetary stability is a general dependence on digital currencies. In this scenario, individuals within the economy would conduct their day-to-day transactions with an alternative currency other than the sterling and only use sterling when necessary such as interacting with the state (for example paying taxes). This would cause a stir, and impair the BoE's ability to

[276] Bank of England, 'The Economics Of Digital Currencies' (2014) <http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf> accessed 9 August 2017 9
[277] ibid
[278] ibid
[279] ibid

influence price-setting, as all payments would then be conducted in an alternative currency to sterling within the economy.[280]

Although this scenario is hypothetical, regulators must not undermine the predicament it may cause were it to happen. As when Bitcoin first appeared in 2009, it was not quite noticeable. However, today with over 843 digital currencies as of August 9, 2017, Bitcoin leads the digital currency market with a market cap that sits around $54 billion and rising. Digital currencies pose a grave threat to economies around the globe and should not be underestimated.

4.4 Financial Stability and Consumer Protection

According to the IMF, cryptocurrency may also pose a threat to financial stability and consumer protection. The IMF notes that if extensive use of SCs were to occur, it might affect financial stability simply by automatically executing terms of contracts that have an adverse effect on the system through a feedback loop (risks of automated high-speed trading for example). The IMF report then goes on to state that consumers may not understand what they agree on due to the compounded nature of SCs. As such, these developments may be difficult to courts and regulators to fathom.[281]

4.5 Financial Crimes Enforcement Challenges

Anti-terrorism laws and money laundering rules are an example of issues that may face SCs. As according to these statutes and regulations, they require that participants in such transactions know and verify the identity of the counterparties and to report any "suspicious activity" to the authorities. However, since self-execution is a part of SCs, parties to a SC agreement will need to comply with these regulations.[282]

4.6 Systemic Risk and Blockchain

As previously discussed in chapter three, some banks have been testing implementing derivative agreements into SCs through DLT. DLT technology offers significant innovation to financial markets if not revolutionise how modern business is conducted. Whether it is by incorporating blockchain technology between institutions or using SC to execute specific trades. However, a fork in the road

[280] ibid
[281] International Monetary Fund, 'Virtual Currencies And Beyond: Initial Considerations' (2016) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> accessed 8 August 2017 23
[282] O'Shields (n 159) 192

lies ahead of current regulations and regulators to address such matters. It may be too early to decide whether blockchain technology could replace quintessential core banking solutions.[283] The following part argues that the current derivatives regulation exists due to its risk of causing a systemic risk and that if blockchain technology were to be used, regulation must take into consideration the risk that comes with blockchain technology. Furthermore, this part will discuss how blockchain technology may also create systemic risk differently. Thus, regulators must consider the size of such risks and the legal hurdles that may face DLT.

4.6.1 Centralisation, Blockchains, and Systemic Risk

Derivatives are sophisticated financial instruments that have been known to enhance the risk of systemic financial risk if mismanaged properly.[284] Although there is no universal definition for systemic risk, it is often defined as bank runs, failures of interconnected firms, general distrust in financial systems, and payment crises.[285] Another way in which systemic risk is often defined is that it affects companies that are often labelled as "too big to fail, too interconnected to fail, or too leveraged to fail."[286] Hence, the introduction of the Dodd-Frank Act in the US,[287] which is often criticised for shifting risk to a central entity. Consequently, the act may either be viewed as significantly good or bad for avoiding systemic risk. The blockchain, on the other hand, offers to do what central counter parties (CCPs) do, but in a much more efficient manner.[288]

The blockchain offers decentralisation to CCPs functions. Often CCPs are attributed with mitigating systemic risk; however, they can also contribute to systemic risk. CCPs may be another too big to fail entity.[289] A trait of the blockchain is that it cannot fail in a specific part. A blockchain may decentralise key clearing functions and assign tasks to members of the network. SCs can then be used to automate the collateral management, default management, matching and affirmation and the settlement process.[290] As a result, CCPs role would be minimised if not replaced. In his article,

[283] Satya Swarup Das and Virtusa Polaris, 'Will Blockchain Replace Core?' (*M.bankingexchange.com*, 2017) <http://m.bankingexchange.com/news-feed/item/6736-will-blockchain-replace-core> accessed 6 August 2017
[284] Surujnath (n 54) 291, 292
[285] Raimonda Martinkutė-Kaulienė, 'Risk Factors In Derivatives Markets' (2014) 2 Entrepreneurial Business and Economics Review 77, 78, 80
[286] Surujnath (n 54) 292
[287] Dodd-Frank Wall Street Reform and Consumer Protection Act, (2010)
[288] Surujnath (n 54) 292
[289] Alan De Genaro, 'Systematic Multi-Period Stress Scenarios With An Application To CCP Risk Management' (2016) 67 Journal of Banking & Finance 120
[290] Surujnath (n 54) 294

Craig Pirrong states that there are specific core functions of CCPs that blockchains may not be able to fulfil, such as mutualising default risk and managing positions.[291] Even though blockchains currently do not offer the diverse duties of a CCP, we must not turn a blind eye to other advantages that it offers, including disintermediation.

4.6.2 Decentralisation, Blockchains, and Systemic Risk

As blockchain technology continues to develop, regulators must consider whether the current existing regulatory framework can be applied to such technology. As with any technology, regulators and market participants must take into considerations the impact that the technology may cause and that it could be harmful. This part will not aim to focus on the risk of over-centralisation and the associated risks as these have already been well addressed in legal literature. Instead, it will seek to address how disintermediation caused by blockchains may impact the settlement process and that decentralisation does not, contrary popular belief, prevent risks.[292]

Even though it may be too early to draft a new regulatory framework for such technology, some existing frameworks can be considered when it comes to regulating blockchain markets. One of the key goals of authorities is to focus on preventing systemic risk. Regulators must take into consideration that decentralised networks pose a different kind of risk. Regulators should address issues such as recourse, settlement finality and potential cyberattacks on the blockchain network. Also, regulators must be aware of behaviours that may raise red flags by unscrupulous market participants who might decide to take advantage of the blockchain's capability. Competent authorities should remain observant in requiring reporting by swap participants as blockchains may enhance this matter if regulations would be updated to permit reporting through a shared ledger.[293] Furthermore, another legal hurdle that regulators should be concerned with when it comes to blockchain is AML and KYC due to acts of money laundering and terrorist financing. As banks that are interested in using DLT must make sure that the information is in accordance with the KYC and AML reporting requirement.[294]

[291] Craig Pirrong, 'A Pitch Perfect Illustration Of Blockchain Hype' (*CoinDesk*, 2016) <https://www.coindesk.com/a-pitch-perfect-illustration-of-blockchain-hype/> accessed 7 August 2017
[292] Surujnath (n 54) 295
[293] ibid
[294] Zuberi (n 205) 4

There are crucial factors that must be satisfied for an agreement to become legally binding. Blockchain transactions lack such factors due to such transactions being visible and easily verifiable. For instance, in the Bitcoin protocol, transactions that take place are irrevocable by any single user once the transaction enters into the blockchain ledger. However, what if a legal dispute were to arise with regard to such transaction being a fraudulent transaction? A court may order compensation of damages to the affected party, but the transaction itself cannot be "undone".[295] As the system per se cannot resolve internal problems within the Bitcoin system.

Although transactions may not be irrevocable by one user, it is possible that transactions may be repeated if specific conditions are met. The Bitcoin protocol depends on a PoW process that verifies transactions that are going into the ledger that is done by the miners. It uses the PoW process to ensure that no double spending occurs. However, if a 51%-attack were to happen, such transactions could be undone.[296] This is considered a paramount flaw in the Bitcoin system. If a single entity reaches the 51% mining hash-rate, it can easily prevent and reverse transactions and even cripple the network. However, it will not be able to reverse transactions that has been logged in a long time ago. Moreover, it cannot create new coins or even steal coins from other users.[297] Thus, the damage it may cause is limited. However, such disturbance can render the system useless and cause people to lose trust in the system.

We have previously discussed in chapter one and two that Bitcoin and Ethereum are decentralised systems. However, these systems are not immune to attacks. On June 17, 2016, an attack on a DAO run on the Ethereum network was hacked.[298] Unlike Bitcoin 51%-attack, this attack was different. The hacker managed to exploit a fault in the programming language of the SC which led to the success of the hack.[299] Even though the main goal of creating a DAO is to eliminate the need for a third party, "humans, it turns out, are tough to take out of the equation."[300] Critics of Ethereum

[295] Surujnath (n 54) 295
[296] '51% Attack' (*Learncryptography.com*) <https://learncryptography.com/cryptocurrency/51-attack> accessed 5 August 2017; See also 'Weaknesses' (*En.bitcoin.it*) <https://en.bitcoin.it/wiki/Weaknesses> accessed 5 August 2017 (describes what a 51% attacker might do to the network)
[297] ibid
[298] Allen and Overy (n 144) 4
[299] David Siegel, 'Understanding The DAO Attack' (*CoinDesk*, 2016) <https://www.coindesk.com/understanding-dao-hack-journalists/> accessed 5 August 2017
[300] Klint Finley, 'A $50 Million Hack Just Showed That The DAO Was All Too Human' (*WIRED*, 2016) <https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/> accessed 5 August 2017

believe that the hack was due to the flexibility that Ethereum's platform offers to its users.[301] The attacker managed to steal $55 million worth of Ethers from the DAO.[302]

Nevertheless, Ethereum's founders proposed creating a soft fork to combat the hack. By offering a firmware update to its current user database and blacklisting the address that the Ethers were syphoned to.[303] Thus, by doing so, a separate blockchain would be created, and the hacker would not be able to use the stolen Ethers. However, since Ethereum uses a PoW consensus that depends on mining, the attacker promised the users that would refuse the fork incentives. Nevertheless, the soft fork was abandoned due to a fault in its code, and 85% approved a hard fork, and the Ethers stolen from the DAO were returned to a refund SC.[304]

Although the hard fork was successful, it could have also failed. The problem with the firmware update is that it is an update. Like any update, it is dependent on the users installing it, as Ethereum cannot oblige users to do so. All in all, this shows that in the future an attacker may be able to convince users to refuse the update. Consequently, this can be considered as a flaw in the decentralised system.[305]

From the things that can be learned from this attack is that blockchains are not immutable as they often claim. This question their notion of settlement finality that was stated by Ethereum's founder Vitalik Buterin with regard to decentralised systems. As financial firms find this notion essential especially when dealing with certain assets. Due to ownership considered vital element during their normal course of business.[306]

This brings us to the question of finality of a public blockchain. Moreover, as mentioned above, a 51%-attack on a blockchain that uses PoW consensus can undermine the security of the blockchain and result into the reverting of specific transactions. This as miners are in charge of updating the ledger in a public blockchain. This may be an issue in public blockchains that are permissionless,

[301] Siegel (n 299)
[302] Matthew Leising, 'The Ether Thief' (*Bloomberg.com*, 2017) <https://www.bloomberg.com/features/2017-the-ether-thief/> accessed 5 August 2017
[303] Siegel (n 299)
[304] 'The DAO, The Hack, The Soft Fork And The Hard Fork' (*Cryptocompare*, 2017) <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/> accessed 5 August 2017
[305] Surujnath (n 54) 298
[306] Vitalik Buterin, 'On Settlement Finality' (*Ethereum Blog*, 2016) <https://blog.ethereum.org/2016/05/09/on-settlement-finality/> accessed 6 August 2017

unlike private ones. Private consortium blockchains that are permissioned and do not use PoW consensus but use a different consensus system may be seen as an alternative to prevent such attack and ensure settlement finality. Nevertheless, these blockchains are also not attack proof.

We have discussed public blockchain that uses a PoW consensus. However, to avoid the problems that come with public blockchains, private ones that use a different system may be used to prevent such issues. Conversely, an administrator is in charge of maintaining a private blockchain, as an administrator grants users access to the private blockchain. Consortium ledgers such as Hyperledger Fabric and R3 Corda are secure networks for users, as users can only gain access to such networks if they are pre-approved by the system administrator.[307] However, what users decide to do in the blockchain, is up to them. As consortium blockchains cannot prevent its members from colluding,[308] participants within this blockchain may choose to collude similar to the collusion among financial firms that have been revealed recently in the case of the LIBOR rate scandal.[309]

This brings us to how decentralised systems may pose to cause system risk. This can be seen due to the problem with transaction finality. Although, eliminating third parties can be regarded as an advantage of using decentralised systems, such elimination means that systemic risk might impact markets.[310] This is because if a rise of disintermediation were it to occur, systemic risk would impact markets themselves and not its financial institutions.[311]

Therefore, if participants within a blockchain agreement were to suffer from insolvency, it would be difficult to determine liability since it would be hard to pinpoint a moment of finality.[312] This will lead to a lack of liquidity that may be faced by participants if they are unable to transfer the settlement asset for another claim. This call for the finality of transactions is stated in the Core Principles for Systemically Important Payment Systems that has been noted in the report of the Bank for International Settlements.[313]

---

[307] Linux Foundation (n 227) 6
[308] Phil Gomes, 'A Morning Exploration Of Blockchain Technology In Financial Services' (*Edelman*, 2016) <http://www.edelman.com/post/exploration-blockchain-technology-financial-services/> accessed 5 August 2017.
[309] 'The LIBOR Scandal: The Rotten Heart Of Finance' (*The Economist*, 2012) <http://www.economist.com/node/21558281> accessed 5 August 2017
[310] Surujnath (n 54) 300
[311] Steven L. Schwarcz, 'Systemic Risk' (2008) 97 Georgetown Law Journal 202
[312] Surujnath (n 54) 301
[313] See also *Core Principles For Systemically Important Payment Systems* (Bank for International Settlements 2001) 31

Finally, it may be still early to determine whether blockchain technology can be used for settlement finality. However, regulators are in charge for providing clarity around finality. Such regulators cannot sit back and assume that blockchain technology encompasses all the answers. If one thing is to be taken from the above, it is that decentralising clearing and settlement process does not prevent systemic risk. Rather, it only shifts the risk from institutions to markets themselves. Unlike markets with a centralised clearing structure which is based on the exposure of one institution towards another. Thus, systemic risk in a decentralised blockchain system might arise due to disputes with regard to finality.[314]

It is worth noting that there is a notion that regulators and auditors could act on a blockchain as limited permission nodes. By doing so, they would be able to monitor the market and its participants effectively. This would be an advantage to them as it allows for ongoing and real-time auditing, unlike the current regulatory regime.[315]

The present regulatory framework lacks coherence when it comes to regulating blockchain technology. Since blockchain technology poses to cause risk within financial markets, regulators may be required to find common ground when deciding to adapt current regulatory frameworks to such technology. Because of that, regulators will have to introduce new standards with regard to the use of blockchains and SCs to mitigate systemic risk.[316]

[314] Surujnath (n 54) 301, 302
[315] Nikiforos Mathews and Jonas Robison, 'Recent Blockchain Regulatory Developments' (*Derivatives in Review*, 2017) <http://blogs.orrick.com/derivatives/2017/01/31/recent-blockchain-regulatory-developments/> accessed 7 August 2017
[316] Surujnath (n 54) 302

Conclusion

Nakamoto's blockchain and Szabo's SCs have the potential to transform financial markets and the core of banking globally. Financial firms and regulators are still exploring how such technology can benefit capital markets. Once matured, the effect of blockchains will possibly be similar to how the internet changed our lives.[317] Although, some still question blockchain technology and believe it is a fad, as many once believed the internet was. Of course, the technology has not yet come to full fruition with the technology still evolving – similarly the web took decades to develop. However, the development is rapid, which can be attributed to the major commercial interest in the technology, unlike the internet at its infancy.

Even though several successful tests have been conducted within a regulated environment, this does not mean that operational flaws and vulnerabilities are non-existing. Regulators must tread lightly to make use of such technology and not seek to restrict it. According to Israel Kirzner, interventions may block or even divert the path of the entrepreneurial discovery process, and may prevent potential breakthroughs that we may never know about.[318]

We have discussed how, if markets were to use blockchain technology and SCs, it could prove to be beneficial. As it will aid in the reduction of several things and cause disintermediation. However, this does not come without a price. Decentralisation may create new systemic risks. Hence, regulators must be prepared to address such risks posed by the new technological developments. Security of technology is its greatest, yet it is also its downfall. As shown with Bitcoin and Ethereum, decentralised systems are not foolproof. Furthermore, this applies to not only public blockchains, but also private ones as well. The technology's development process requires an understanding of basic coding and its aspects in the same manner as we understand finance and the law.

[317] See also Joichi Ito, Neha Narula and Robleh Ali, 'The Blockchain Will Do To The Financial System What The Internet Did To Media' (*Harvard Business Review*, 2017) <https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media> accessed 11 August 2017 "The blockchain will do to the financial system what the internet did to the media."

[318] Israel M Kirzner, *Discovery And The Capitalist Process* (University of Chicago Press 1985) 121

Blockchain-Based Digital Commercial Bills: Advantages and Legal Challenges

LLB, LLM (Lon),
Amelie Shuhui Ruan

Introduction

Technological innovations have always been one of the main driving forces for the evolution of business models. In turn, the transformation of economic activities will inevitably call for changes in the legal system. For example, shipbuilding technology enabled cross-ocean commerce, thereby bringing major changes in shipping law. Another notable example is how the development of Internet Telecommunication (IT) technology, which dramatically boosted electronic commerce, led to according modifications to the legal system, such as e-payment and electronic signature law. More recently, distributed ledger technology (DLT), especially its "blockchain"[1] application, is bringing about profound changes to various aspects of modern society.

A notable transformation is the movement towards distributed payment systems with digital currency. The "killer application" that brought the blockchain technology to public attention is Bitcoin (BTC).[2] Over the years, more than 700 cryptocurrencies have been

[1] The terms "blockchain" and "distributed ledger(s)" are often used interchangeably when discussing the technology. This dissertation acknowledges that blockchain is just one of the possible applications of DLT. In fact, a distributed ledger is essentially a consensus of replicated, shared and synchronized data across involved parties, while a blockchain, comprised of immutable data encrypted in "blocks", is only one possible data structure that can achieve secure and valid distributed consensus.

[2] This decentralized cryptocurrency was initially introduced by an anonymous developer, Satoshi Nakamoto, in January 2009. The design was first described in a self-published paper by Nakamoto in October 2008. The genesis block was established on 3 January 2009. For a more detailed discussion, see Barber, Simon, Boyen, Xavier, Shi, Elaine, & Uzun, Ersin, 'Bitter to better - how to make bitcoin a better currency' (Lecture Notes in Computer Science, 2012), < https://crypto.stanford.edu/~xb/fc12/bitcoin.pdf> accessed 30 April 2017.

developed;[3] most of them are modelled on BTC and are thus labelled "altercoins". The rapid development of private cryptocurrencies has pushed central banks to acknowledge the inevitable trend of digital currency. Many countries have debated and tested central bank-issued digital currency (CBDC) initiatives, including China,[4] Sweden,[5] Canada,[6] the United Kingdom,[7] and Singapore.[8] The United States, however, has remained cautious about the feasibility of central bank-issued digital currency. Jerome H. Powell, a Governor

[3] Unpublished research results of Cryptocurrency research team, organised by Professor George Walker at Centre for Commercial Law Studies, Queen Mary University of London

[4] The People's Bank of China could launch its digital legal tender prototype system, "Demo", as soon as 2017. China Stock News, 'Central Bank Is Expected To Launch 'Demo' Next Year and a Pilot Project on Digital Bill' (2016)

[5] Cecilia Skingsley, 'Should the Riksbank Issue E-Krona?' (Fintech Stockholm 2016, Stockholm, 16 November 2016) <http://www.riksbank.se/Documents/Tal/Skingsley/2016/tal_skingsley_161116_eng.pdf> accessed 28 April 2017

[6] Ben Fung and Hanna Halaburda, 'Central Bank Digital Currencies: A Framework for Assessing Why And How' (Bank of Canada 2016) <http://www.bankofcanada.ca/wp-content/uploads/2016/11/sdp2016-22.pdf> accessed 29 April 2017

[7] The Bank of England has been publishing working papers on digital currency. See <http://www.bankofengland.co.uk/research/Pages/onebank/cbdc.aspx> accessed 29 April 2017. The UK Home Office responded to the UK Treasury's call for information on digital currencies indicating that central bank-issued cryptocurrency is necessary. Coindesk, 'The UK Government Wants To Create Its Own Digital Currency So It Can Track Peoples Transactions' (2015) <http://uk.businessinsider.com/the-uk-government-wants-to-create-its-own-digital-currency-2015-6> accessed 28 April 2017

[8] Singapore's central bank has completed a distributed ledger trial focused on inter-bank payments. Monetary Authority of Singapore, 'MAS Working with Industry To Apply Distributed Ledger Technology In Securities Settlement And Cross Border Payments' (2017)

of the Federal Reserve Board, has posited that such a system "would be a global target for cyber-attacks, cyber counterfeiting, and cyber theft".[9]

Another prominent trend is a combination of DLT and smart contracts to enable increased versatility of services, particularly in the financial services industry. The dematerialization of Money Market Instruments (MMIs) has become one of the notable trends in financial markets around the world since the beginning of 21st century.[10] The existence of financial assets in electronic form has enabled cross-border investments in bonds, Certificates of Depositors (CDs), Commercial Papers (CPs) and Bankers' Acceptances (BAs),[11] usually through centralized depository and clearing systems. However, with the advent of blockchain technology and smart contracts, it is likely that the existing financial infrastructure will gradually be replaced by a variety of distributed ledger systems. Both the public and private sectors around the world have been very active in exploring the optimal way of developing a new financial infrastructure.

There is, then, a universal awareness of DLT's potential disruptive effects on the financial industry. National and international institutions have been publishing reports on this topic, analyzing the potential of DLT.[12] More importantly, awareness is quickly being

[9] Jerome H. Powell, 'Innovation, Technology, and the Payments System' (Blockchain: The Future of Finance and Capital Markets? The Yale Law School Center for the Study of Corporate Law, New Haven, Connecticut, 2017)

[10] G.A. Walker, 'Financial Markets and Exchanges' (unpublished 2017)

[11] A banker's acceptance (BA) is a bill of exchange issued by a company that is drawn by a commercial bank.

[12] See China's Ministry of Industry and Information Technology (MIIT), 'China's Whitepaper on blockchain technology and the development of its application' (中国区块链技术和应用发展白皮书, October 2016); Deloitte and World Economic Forum, 'The Future of Financial Infrastructure' (2016); Pinna A and Ruttenberg

transformed into concrete efforts. As such, notable achievements are being made in digitalizing financial instruments. Examples abound. The first security issued through a blockchain was a 'crypto-bond' by Overstock CEO Patrick Byrne's start-up T0 in 2014.[13] In 2015, Nasdaq started investigating how to use blockchain technology for its stock exchange, and has since developed its own blockchain product, Nasdaq Linq.[14] Additionally, in August 2016, the Australian Securities Exchange (ASX) announced that it had completed the initial phase of DLT testing, which it expects will replace its 20-year-old clearing and settlement system.[15] In the commercial paper market, the consortium R3CEV completed a trial of a series of smart contract templates modelled for commercial

W, 'Distributed Ledger Technologies In Securities Post-Trading: Revolution Or Evolution?' (European Central Bank 2016); Hong Kong Monetary Authority, 'Whitepaper on Distributed Ledger Technology' (2016); UK Government Chief Scientific Adviser, 'Distributed Ledger Technology: Beyond Block Chain' (Office for Science, UK Government 2016); European Securities and Markets Authority, 'The Distributed Ledger Technology Applied To Securities Markets' (2017)

[13] The name alludes to the fact that security settlements moving across it happen immediately, instead of the typical 3-day wait for stocks.

[14] Pete Rizzo, 'Hands On With Linq, Nasdaq's Private Markets Blockchain Project', *Coindesk* (21 November 2015) <http://www.coindesk.com/hands-on-with-linq-nasdaqs-private-markets-blockchain-project/> accessed 1 May 2017

[15] Luke Parker, 'Major stock exchange completes blockchain trial for replacement settlement system', *Brave New Coin* (20 August 2016) https://bravenewcoin.com/news/major-stock-exchange-completes-blockchain-trial-for-replacement-settlement-system/ accessed 29 April 2017

paper transactions.[16] Moreover, in April 2016, IBM made a blockchain demo for trading CPs, IBM Bluemix, available online.[17]

China has integrated these two trends towards digital fiat currency and DLT-based financial infrastructure in its pilot project on digital commercial bill exchanges. On 15 December 2016, the People's Bank of China (PBOC) announced a successful trial run of blockchain-supported digital fiat currency that is developed on transactions and settlements of BAs[18], moving closer to become the first public issuer of sovereign digital currency. The PBOC aspires to use digital fiat currency not only for facilitating financial services, but also for cracking down on money laundering (AML) and tax evasion. [19] The trial run used central bank digital currency to enable delivery versus payment (DVP) and blockchain technology to cover the whole life cycle of a BA, including its issuance, acceptance, discount and discount transfer.[20]

---

[16] Stan Higgins, '40 Banks Trial Commercial Paper Trading in Latest R3 Blockchain Test' *Coindesk* (3 March 2016) <http://www.coindesk.com/r3-consortium-banks-blockchain-solutions/> accessed 23 March 2017

[17] IBM, 'Trading Commercial Paper via Blockchain with IBM Bluemix' (2016) < https://developer.ibm.com/tv/trading-commercial-paper-via-blockchain-with-ibm-bluemix/ > accessed 19 March 2017

[18] Bankers' Acceptance is one type of commercial bill. Another type is a trade acceptance, which is drawn by individuals or corporates.

[19] Brian Yap, 'PBOC Uses Blockchain Technology To Combat Money Laundering' *International Financial Law Review* (14 February 2017) <http://www.iflr.com/Article/3661468/PBOC-uses-blockchain-technology-to-combat-money-laundering.html> accessed 19 March 2017

[20] Caixin, 'Central Bank has Successfully Tested the Prototype of Digital Bill Exchange System (央行数字票据交易平台原型系统测试成功)' *Caixin* (25 January 2017) <http://finance.caixin.com/2017-01-25/101048999.html> accessed 26 March 2017

Although the fast-growing technology and its versatile uses are undoubtedly transformative, the challenges it presents should not be underestimated, especially in terms of the governing legal and regulatory framework. While DLT has the potential to bring benefits to many organizations, it is still in the early stages of development. Its unconventional features, as well as the corresponding changes to business paradigms that it will bring about, could give rise to unexpected legal challenges relevant to its eventual adoptability. The Hong Kong Monetary Authority (HKMA) has identified a number of legal issues including data privacy, litigation and legal disputes, rules and conditions in code, and compliance with laws and regulations.[21] Undoubtedly, without the adaptation and development of a sound governance framework, the benefits of technology innovation will be offset by uncontrolled risks.

This dissertation will thus focus on the legal considerations around a blockchain-based digital commercial bill exchange. Although the concepts have international implications, this dissertation will focus on China's pilot project. Section I will explain China's rationale for implementing such a project, particularly the structure of China's commercial bill market and its main challenges. The dissertation will introduce the project in detail in Section II, along with an analysis of its advantages. Section III will examine the potential legal challenges raised by the new transactional paradigms of digital bills. To maximize the benefits and mitigate the risks, Section IV will recommend the establishment of an

[21] Hong Kong Monetary Authority, 'Whitepaper on Distributed Ledger Technology' (2016) <http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf> accessed 26 March 2017

effective legal and regulatory framework to govern the digital commercial bill exchange system.

I. China's commercial bill market

1.1 Market size and structure

Since 1979 when the issuance of first commercial bill[22] was approved by the People's Bank of China, China's bill market has witnessed almost 40 years of development and there has

[22] In China, the legal concept of '票 据 ' (negotiable instruments), encompasses bills of exchange (draft), promissory notes, and checks (Negotiable Instruments Law of People's Republic of China, 2004 Amendment, Article 2). In some English media organizations, the term "票据" is translated as "commercial paper", which is misleading and inaccurate. In fact, China's Negotiable Instruments Law does not recognize promissory

been significant market growth ever since. In 2015, the total signing amount was 22.4 trillion yuan, which was 16.5 times greater than in 2001. At the end of 2015, the value of outstanding commercial bills amounted to 10.4 trillion Yuan, 19 times greater than 2001.[23]

More importantly, more and more bill transactions have moved from trade-based functions to the purpose of fundraising and investment, i.e. bill financing.[24] Because of its easy accessibility, low financing cost and high liquidity, the commercial bill has become an increasingly important financing tool for small and medium enterprises (SMEs) in China. There is a notable trend of substituting bill financing for short-term loans.[25] By late September 2016, the sum of bill financing had increased by 1.14 billion yuan compared to

notes signed by corporates; therefore, the Chinese concept of "commercial paper" only refers to promissory notes signed by regulated banks (Article 73). In practice, the term '票 据 ' typically refers to bills of exchange which can be classified into two types: bank acceptance and trade acceptance. American law identifies four basic kinds of negotiable instruments: promissory notes, drafts, checks, and certificates of deposit (Uniform Commercial Code, Article 3). In the UK, the 1882 Bills of Exchange Act codifies the law relating to bills of exchange, checks, and promissory notes, although a check is defined as a bill of exchange drawn on a banker and payable on demand (Article 73).

[23] Zhong Xu, 'Establish A Nation-Wide Integrated Platform For Commercial Bills Exchange (建设全国统一的票据交易平台)' *China Finance* (2017)

[24] A bill of exchange is an unconditional order made by a person or business (drawer), directing the recipient (drawee or acceptor) to pay a fixed sum of money to a third party (payee) at sight of the bill or at a future date. The bill can be drawn by individuals (trade drafts) or a bank (bank drafts). When presented with the bill, the drawee (acceptor) is obliged to pay the bearer. The bill is transferable by endorsement. Nowadays commercial bills are increasingly used for financing purposes in China, as the bearer can transfer the bill to a bank at a discounted value when he needs funds. The bank can then collect the face value from the payee or acceptor at the indicated future date.

[25] For a broader discussion of bill financing in China, see Li Yang and Robert Lawrence Kuhn, *China's Banking and Financial Markets* (Wiley 2012) 187.

the beginning of 2016 and accounted for 5.5% of total lending.[26] Concurrently, it has become a popular investment tool for banks, not only for its profit generating capacity, but also for managing liquidity, as well as assets and liabilities on the balance sheet. In addition to commercial banks, finance companies,[27] securities companies, funds, and asset management institutions have become increasingly active in the commercial bill market.

On January 26, 2017, the PBOC announced that it had completed a successful trial run of a digital bank acceptance exchange[28], and, as such, is likely to be the first central bank in the world to have its own digital currency use case.[29] Before the introduction of the blockchain-based digital bills, there used to be two types of products in China's bill market: traditional commercial bills and electronic commercial bills. [30] The PBOC established the Electronic Commercial Draft System (ECDS) in 2016.[31] The ECDS is a central depositary

[26] Gongsheng Pan, 'The Development And Regulation Of China's Commercial Bill Market (中国票据市场的发展与规范)' *China Financial Times* (2016)

[27] Chinese finance companies are usually affiliated to large corporate groups instead of commercial banks.

[28] It should be noted that Chinese press and PBOC officials' working papers, published in China Finance, Vol 17 (2016), only use the term "数字票据" without specifying whether it is for all commercial bills or only for bank acceptance. The English report of Caixin, which is China's biggest finance press, translates it as "digital bills" and indicates that it will be a "digital bank acceptance exchange platform". Considering the dominant position of bank acceptance vis-a-vis trade acceptance in China's financial markets, it is understandable that this pilot project begins with BAs.

[29] Zhang Yuzhe and Han Wei, 'PBOC Set to Be First To Issue Digital Bills' *Caixin Global* (26 January 2017) <http://www.caixinglobal.com/2017-01-26/101049103.html> accessed 12 April 2017

[30] In the first three quarters of 2016, commercial drafts in electronic form accounted for 60.9% of the bill market, according to the PBOC's data.

[31] The terms 'commercial bill' and 'commercial draft' are often used interchangeably when referring to bills of exchange.

system where commercial bills are issued and traded in purely electronic form. On 1 June 2016, the PBOC announced its plan of abandoning the paper form of traditional commercial bill in the next two or three years.[32] In December 2016, China launched a platform for centralized commercial bill trading, run by the Shanghai Commercial Paper Exchange Corporation (SCPE) [33] and overseen by the PBOC. The ECDS is connected to the SCPE's platform.

It is worth noting that the SCPE and the Digital Commercial Bill Exchange (DCBE) run two separate systems. The first trades bills in paper form and electronic bills within the ECDS, while the second one is only a pilot platform where a limited number of participants[34] conduct transactions of digital bills. The major difference between traditional bills, electronic bills and digital bills lies in its circulation infrastructure and means of settlement:

	Traditional bills	Electronic bills	Digital bills

[32] Global Finance, 'PBOC: Physical Commercial Bill Will Be Replaced In The Next Three Years (央行：三年内取消纸质票据)' (2016) <http://finance.huanqiu.com/roll/2016-06/8998349.html> accessed 7 April 2017

[33] The State Council of the People's Republic of China, 'China Launches Commercial Paper Exchange' (*English.gov.cn*, 2016) <http://english.gov.cn/news/video/2016/12/09/content_281475511650583.htm> accessed 15 March 2017. The translation can be misleading as "票据" is sometimes translated to "commercial paper", sometimes to "commercial bill". In fact, most secondary transactions of "票据" are based on BAs, which are essentially commercial bills.

[34] According a Caixin press report, confirmed participants include Industrial and Commercial Bank of China, Bank of China, Shanghai Pudong Development Bank, WeBank (a commercial bank led by TenCent) and Hangzhou Bank.

Circulation Infrastructure	Paper and signature[35]	Computer, Internet and electronic signature	Blockchain and smart contract
Means of settlement	Cash and bank balance	Bank balance	Central bank digital currency

An integrated commercial bill exchange platform is expected in the future. The PBOC aspires to have a nation-wide unified platform with 'the most comprehensive and accurate data of all bill transactions', covering all three types of commercial bills mentioned above. Physical bills will be registered online. The ECDS will be connected to this platform, as well as the system of blockchain-based digital bills. Discounting, price discovery, trust registration, settlement, clearing and collection will all be conducted on the consolidated national platform. [36]

1.2 Market problems

The fast-growing bill market poses many risks. In the first quarter of 2016, China's bill market has suffered from significant bill fraud. An alleged fraud of almost 1 billion yuan was discovered at China CITIC Bank, where an employee colluded with illegal brokers to fake documentation for companies to acquire quick funds. The Agricultural Bank of China announced a 3.9 billion yuan "risk incident" that was tied to a bill financing fraud by

[35] Though its issuance and transfers are in paper form, other transactions, including discounting and rediscounting, are primarily conducted online with scanned physical evidence.

[36]Zhong Xu (n23). Xu is the director of the Director of the Research Office of PBOC and the preparatory group responsible for developing the Digital Bill Exchange platform.

employees.[37] From these malpractices, we can identity four major problems with the Chinese bill market.

1.2.1 Market fragmentation

The bill markets include the markets of drawing[38], acceptance[39], discount[40], inter-bank discount[41], rediscount[42], brokering, rating and derivatives. In China, these markets are often isolated from each other due to insufficient market infrastructure for trading, trust registration, settlement, clearing, and information communication. The market infrastructure for bill transactions has long been outdated, considering the ever-growing market size and its diverse activities. At the moment, as cross-regional transactions of commercial bills become more and more popular, there is still no integrated bill exchange

[37] See Bloomberg News, 'China's Fraud Paper Trail Shows Flaws In Booming Funding System' *Bloomberg News* (January 28 2016) <https://www.bloomberg.com/news/articles/2016-01-28/paper-trail-of-fraud-shows-flaws-in-booming-china-funding-system> accessed 3 April 2017

[38] The drawing of a bill of exchange refers to the act whereby the drawer draws a bill and delivers it to the payee.

[39] 'Acceptance refers to the act whereby the payer promises to pay the amount of a bill at its maturity date.

[40] Discount refers to the act whereby the holder, prior to the maturity date of a draft, transfers its draft rights to a financial institution by endorsement, and the latter pays the agreed amount to the holder after deducting a certain amount of interest.

[41] Inter-bank discount refers to the act whereby a financial institution which holds a draft, prior to its maturity date, transfers its draft rights to another financial institution by endorsement, and the latter pays the agreed amount to the holder after deducting a certain amount of interest.

[42] Rediscount refers to the act whereby a financial institution which holds a draft, prior to its maturity date, transfers its draft rights to the central bank by endorsement, and the latter pays the agreed amount to the holder after deducting a certain amount of interest.

system in China. The fragmentation of bill markets generates several negative consequences.

Significant information asymmetry. Fragmented markets create considerable gaps in information dissemination, resulting in inefficiency in matching supply and demand among market participants. Thus, transaction costs are likely to be high and resource allocation is not carried out efficiently.

Delay in transactions. Due to the outdated market infrastructure, the circulation of commercial bills is usually separated from the transfer of funds. Therefore, there are higher risks of the bill or the funds being diverted to other uses before the conclusion of a transaction in process.

Non-effective interest rate. Market fragmentation makes it difficult for the market interest rate to wholly and accurately reflect industry dynamics, thereby reducing the transmission efficacy of the central bank's monetary policy in the money market.[43]

Regulation difficulties. Fragmented markets for bill transactions make it impossible for regulators to have timely access to comprehensive and authentic transaction data. Therefore, it is very difficult to conduct a consolidated supervision and regulation of the markets all over the country, especially in the case of China's large geographical scope.

The SCPE is tasked to help consolidate fragmented commercial bill markets. However, the ECDS connected to the SCPE does not currently trade physical commercial bills of

[43] Gongsheng Pan, 'The Development And Regulation Of China's Commercial Bill Market (中国票据市场的发展与规范)' *China Financial Times* (2016)

which the face value is lower than 3 million yuan.[44] Therefore, commercial bill intermediaries and fragmented markets of low-valued bill will continue to exist, especially with the rapid development of SME's demand for financing by commercial bills.

1.2.2 Illegal brokerage

In the non-transparent markets of the commercial bill, brokers act as information exchange intermediaries to match buyers with sellers. Many transactions of low-valued commercial bills are conducted over the counter (OTC). These licensed brokers are subject to due regulation and supervision and play an important role in reducing information asymmetry and improving market efficiency. However, there are also unlicensed and unregulated brokers that disturb market functions.

In fact, many unlicensed brokers have set up banks in rural areas or become beneficiary shareholders of rural financial institutions. That way, they can have legitimate access to the interbank bill market. However, they may set up false interbank trading accounts, forge commercial bills without real obligations of payment, or use one commercial bill for several parallel transactions, which they richly profit from, at a loss to the banks. The major fraud cases of 2016 have evidenced that some illegal brokers can subcontract the business of small and medium-sized banks and use false commercial bills to commit fraud.[45] Some

[44] According to the circular issued by PBOC on September 8th 2016, any commercial bill that exceeds 3 million yuan has to be traded through ECDS after 1 January 2017. The threshold will be lowered to 1 million after 1 January 2018. People's Bank of China, 'Circular On the Regulation And Promotion of Electronic Commercial Drafts (关于规范和促进电子商业汇票业务发展的通知)' (2016).

[45] Chengzhu Ji, 'Build Up the Version 2.0 Of Commercial Bill Market (票据市场"2.0 版"制度体系构建之思考)' (2016) 5 China Banking (中国银行业)

help the banks with regulatory arbitrage. Others may forge commercial bills in paper form to commit fraud against market players of integrity. Illegal brokerage has thus substantially increased risks for other regulated market players.

1.2.3 Non-compliant processes

As competition becomes fiercer in the bill market,[46] sometimes banks do not fully comply with the regulations, in order to improve their business performance. The "new normal" is external competition for information, clients, and source of commercial bills, as well as internal competition for FTP quota and the right of pricing.[47]

When competing for clients, banks can sometimes conduct business under a non-compliant process so that their contract formation and performance are less time-consuming than their competitors. For example, they can accept the transfer of a package of commercial bills from a broker without checking relevant details, something that is required by regulators. A simple official stamp from their counterparty bank on the package can give them enough assurance.[48] While this can sometimes be accepted market practice between creditworthy banks, it definitely increases the risks of fraud when illegal brokers intervene. As a result,

[46] Since 2013, the market profit margin has become less and less as the central bank decreased its benchmark interest rate, whilst more and more financial and non-financial institutions are present in the commercial bill market.

[47] Funds transfer pricing (FTP) is a process used in banking to adjust the reported performance of different business units of a bank, which is to adjust the profitability to incorporate true funding costs.

[48] China Bill Network, 'Commercial bill brokers suffered huge loss after stock market crash (股市暴跌引发的效应 票据掮客遭遇 "盛世"之劫)' (2016) <http://ww.zgpjw.com/news/newsdisp.asp?newsid=162211> accessed 4 April 2017

those who do not comply with due processes become the "industry champions" and promote the effect of "broken windows". The malpractices of bank employees not only augment the risks for the banks, but also for the economy as a whole, as they cause obstacles to the business of commercial bills with authentic payment obligations.

In addition, financial institutions do not have sufficient corporate governance structures nor an effective internal risk control system. There are few checks and balances among the departments dealing with bill transactions and compliance. The negative effects can be further amplified by the complexity of commercial bill transactions. Any fragment of the whole of a transaction can be exposed to risks of non-compliance and then contaminate other transactional actions.

1.2.4 Laggard legal framework

The legal framework for commercial bill regulation lags far behind the market developments. The *Negotiable Instruments Law of the People's Republic of China* was inaugurated in 1995 and amended in 2004[49]. In 2000, China's Supreme Court published *Rules on Hearing Cases around Negotiable Instruments.* Over the years, the regulations issued by the PBOC have become the main regulatory sources for transactions of commercial bills. In 1997, the PBOC issued the *Measures for the Regulation of Payment and Settlement*, which addressed the issues of using bills of exchange for payment and settlement. In the same year, the PBOC published the *Interim Measures for Regulating the*

[49] The 2004 amendment only deleted Article 75 of the original law, which required that the qualification of a promissory note drawer should be vetted by the PBOC.

Acceptance, Discount and Rediscount of Commercial Drafts[50], which requires the drawing of commercial drafts to be based on authentic payment obligations in commercial transactions, like, for instance, a sales contract.[51] With the implementation of an electronic commercial draft system, the central bank issued *Measures for the Regulation of Electronic Commercial Drafts Transactions* in 2009. In December 2016, the PBOC issued new *Measures for the Regulation of Commercial Drafts Transactions*, which aimed at regulating market participants' transacting capacity and forming an integrated market for commercial bill transactions.

The law and regulations made for regulating bill transactions revolve primarily around its functions of payment and settlement, whilst the financing function of commercial bills have become more important and complex as Chinese SMEs increasingly use commercial bills, especially BAs for short-term financing purposes. The current law and regulations do not sufficiently address the issues related to bill financing and the integrated management of commercial bill transactions. As a result, there is no officially recognized standard of market-entry, trading, settlement and clearing, nor effective and sufficient remedies for loss caused by illegal brokerage and non-compliant processes. Furthermore, the legal framework of commercial bills needs to be further developed to accommodate for the rapid

[50] In spite of the term "interim", this regulation is still effective.

[51] As the basic legal relationship of the instrument in question is separated from the legal relationship of the contract (non-causative principle), the defects of the contractual relationship have no influence on other relationships based on the endorsement or guarantee of the bill. However, the direct parties to the contract and the bill can use the defect as a defence.

innovation of financial technology (Fintech)[52]. The laws and regulations of commercial bill transactions need to be responsive to new transactional paradigms of digital commercial bills.

II. Pilot project on digital bills: a problem solver

[52] Fintech refers to the use of technology to conduct financial functions, including deposit taking, lending, payment, investment and insurance. For detailed analysis, see George Walker, 'Financial Technology Law-A New Beginning And A New Future' (2017) 50 The International Lawyer 137

Although the ECDS has partially solved the market problems identified in Section I, its functions are far from being sufficient to correct all the market deficiencies. Certainly, the ECDS has significantly reduced the risk of bill forgery and improved the manually intensive processes of transacting traditional bills. It is now more secure, standardized and efficient. However, the centralized operations of the ECDS considerably increase potential systemic risk, because an attack against the central depositor would cause changes to the single ledger providing data to all participants. Furthermore, the connection of the online banking system to the ECDS adds more operational risk, as cyber security is a pain point of traditional Internet-based infrastructure.[53] The ECDS has not solved the challenge of a lack of trust either. Information asymmetry continues to be an obstacle to the effectiveness of market functions. Searching for a better solution, the PBOC has been actively developing a digital bill exchange platform.

2.1 Basic mechanism

In this pilot project, a Digital Commercial Bills Exchange (DCBE) will be established to provide comprehensive financial services relating to digital bills exchange in a nation-wide scope. The exchange system will combine Internet telecommunication, blockchain technology, smart contract and digital fiat currency, covering the services for the whole life cycle of the commercial bill. It will become not only a center for the exchange of digital bills, but also the center for the payment and clearing, risk control, data collection and

[53] The concern over the cyber security of central systems is particularly highlighted in the recent Eternal Blue cyber-attack. See Sam Jones, Sarah Neville and Joshua Chaffin, 'Hackers use tools stolen from NSA in worldwide cyber attack' *Financial Times* (12 May 2017) <https://www.ft.com/content/e96924f0-3722-11e7-99bd-13beb0903fa3> accessed 13 May 2017

credit rating involved in the transactions. Nonetheless, it will not totally replace the current system of electronic commercial drafts. Instead, it will become part of money market infrastructure along with the existing system. The design of digital commercial bills exchange system (DCBES) mainly comprises of the following four elements: [54]

2.1.1 A permissioned blockchain

A blockchain is a 'record of all validated transactions grouped into blocks, each cryptographically linked to predecessor transactions down to the genesis block, thereby creating a "chain of blocks"' [55], which are essentially distributed ledgers that allow participants to create, disseminate and store immutable information in a transparent and secure manner. There are currently two types of blockchains: permissionless and permissioned.[56] In contrast to the permissionless blockchain where any participant can contribute data to the ledgers, i.e. the 'chain of blocks', and validate a transaction through mining[57], a permissioned blockchain, or private blockchain, is usually owned, controlled,

[54] The design is preliminary as the platform is still a pilot project. However, the basic mechanism and main characteristics are explained in Zhong Xu and Qian Yao, 'Preliminary design of digital bill exchange platform' (2016) 17 China Finance (数字票据交易平台初步方案' [2016] 中国金融), 31-33.

[55]Garrick Hileman and Michel Rauchs, 'Global Cryptocurrency Benchmarking Study' (Cambridge Centre for Alternative Finance, University of Cambridge 2017) 10 <https://zh.scribd.com/document/344316463/CCAF-Global-Cryptocurrency-Benchmarking-Study-2017#download&from_embed> accessed 5 April 2017.

[56] Blockchains can also be classified as public, private, and hybrid blockchains. A public blockchain is permissionless and a private blockchain is permissioned. The third type, the "hybrid blockchain", which is under development, extends the ability to read and write the records to a certain number of nodes.

[57] The typical use case is Bitcoin, which is usually considered the "killer application" of distributed ledger technology. Mining is a validation process of "proof-of-work", which involves all the validating nodes

and managed by a group of participants that act as a consortium. In the latter iteration, only authorized participants are allowed to take part in the control and maintenance of the permissioned blockchain. All participants keep distributed identical copies of ledgers.

The DCBES will adopt a private blockchain network where the central bank, DCBE, commercial banks and other eligible participants can transact. The DCBE will be responsible for authorizing the entry of commercial banks, insurance companies and other financial institutions. Accepted participants can all keep real-time identical records in the blockchain. However, different types of participants will be given different levels of permission: validating, bookkeeping (include updating) and read-only. Only blockchain nodes endowed with high-level credentials have the control and maintenance access to the ledger. Other ordinary nodes, once authenticated, only have the permission to use the data as reference for their transaction, i.e. read-only. Therefore, the DCBES is actually a distributed ledger system with a limited number of trusted validators. Insofar as public information disclosure, the permission mechanism and standards have not yet been defined.

Once a new digital bill is published on the chain or a new participant is accepted into the chain, its public information becomes open to every participant. However, the privacy protection technology also ensures that non-public details are only available to transactional parties, and subject to regulatory review when necessary.[58] Therefore, the blockchain network possesses a controlled anonymity mechanism.

competing to perform a computationally demanding calculation. The first node to solve the computational problem then gets to build a new transaction block.

[58] Caixin (n20)

2.1.2 Integrated identity management

An identity management institution[59] will be set up to provide independent identification services and eliminate any other intermediaries. This institution is also tasked to set the entry standard of the blockchain-based bill exchange platform. It provides services related to issuance, storage, validation and retrieval of ID certificate, i.e. a private key linked to a validated identity. With the private key, participants can log into the exchange platform, conduct encrypted transactions, and carry out data enquiries.

The public information contained in the digital ID will be accessible to all participants. Therefore, financial institutions can have access to the customer identity information without replicating Know Your Customer (KYC) checks.[60]

2.1.3 Smart contract

A smart contract is a self-executing contract whose terms and conditions are coded in a computing system instead of written in legal language.[61] It can add more versatility to DLT

[59] According to Xu's model, this institution is likely to be the DCBE.

[60] Caixin (n20)

[61] The term "smart contract" was first advanced by Nick Szabo in 1994 to emphasize the goal of bringing what he calls the "highly evolved" practices of contract law and related business practices to the design of electronic commerce protocols between strangers on the Internet. See Don Tapscott and Alex Tapscott, *The Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, And the World* (Penguin, 2016). Alexander Savelyev summarizes its main features as :1) solely electronic nature, 2) software implementation, 3) increased certainty, 4) conditional nature, 5) self-enforcement, 6) self-sufficiency. See Alexander Savelyev, 'Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law' (National Research University Higher School of Economics, 2016) <https://ssrn.com/abstract=2885241> accessed 18 April 2017

as nodes in the blockchain can enter self-drafted agreements and embed them in the records of the DLT network.[62] Smart contracts can have different triggering events to activate certain actions. For example, a payment can be triggered when the agreed-upon date is reached, or the legal title to an asset can be transferred once payment is received.

The DCBES is expected to cover all kinds of commercial bill business: issuance, trading, discounting, discount transfer, rediscounting, repurchase, etc. The terms and conditions of these transactions will be coded into smart contracts. In this way, the transactional steps, such as fund transfer, margin deposition, commission deduction, and transfer of legal ownership, can be executed automatically.

The smart contract embedded with business logic has been designed in such a way so that it will be separated from the smart contract that contains data, which means that the transactional coding program can be updated as conditions require it, without replicating all historical data. [63]

In addition, a regulatory program can be embedded in the smart contract, which can be designed as a condition precedent of contracts. If the content of the concerned transaction does not meet the requirements set in the regulatory program, it will be suspended immediately. Accordingly, the result of a compliance check will be published on the chain.

[62] The most evident example is Ethereum, which is a public Blockchain-based distributed computing platform, featuring smart contract functionality. It provides computing capacity (a decentralized virtual machine), that can execute peer-to-peer contracts using a cryptocurrency called "ether".

[63] Caixin (n20)

The DCBE will have the authority to issue smart contract templates[64] and regulatory programs in the DCBES.

2.1.4 Central bank-issued digital currency

The DCBES will use CBDC as means of payment. CBDC is a sovereign-backed cryptocurrency, which is a cash-equivalent token that is native to the DLT system. While cash is authenticated by its physical appearance and characteristics, and in the case of banknotes by serial numbers and other security devices, the authentication of CBDC is realized by cryptographic technology. Same as other kinds of fiat currency, CBDC is legal tender and a claim on the central bank. However, in the current pilot project, its effect of legal tender is limited to the transactions of digital bills within the DCBES.

A blockchain node will be set up to issue CBDC in the network. The node is backed up by a real currency account. Participants will transfer money to this account in exchange for digital fiat currency at the rate of 1:1. They will hold a certain amount of CBDC in their private wallet and send the required amount to the counterparty to fulfill the contract obligations and activate further steps set in the smart contract. Only CBDC will be used as means of payment in digital bill transactions for the purpose of delivery versus payment synchronization.

[64] As the industry has adopted a master agreement for bill transactions, it is likely that the templates will be designed to embed the business logics of the master agreement.

Example demonstration

Xu and Yao have demonstrated an example of an interbank discount.[65]

Step 1: Commercial bank A initiates an offer of transferring a discounted digital bill SDD-1 in its possession. Bank A changes the status of SDD-1 into 'wait for discount transfer' in the smart contract. In the meantime, Bank A also inserts the type and expected discount rate of the bill into the smart contract.

Step 2: Commercial bank B finds this on-chain offer in alignment with his expectations.

Step 3: Bank B accepts the discount transfer of SDD-1 and sends the required amount of CBDC to the address written in the smart contract.

Step 4: The smart contract ensures that the money is transferred to A. Then it transfers the control of SDD-1 to B. Now B becomes the controller (holder) of SDD-1.

2.2 Advantages of the digital commercial bill

The application of blockchain, CBDC and smart contract in the DCBES can significantly improve the market infrastructure for bill business, as well as creating new transactional paradigms. These technology innovations can be particularly advantageous in addressing the market deficiencies identified in Section I and the problems left unsolved by the

[65] Zhong Xu and Qian Yao, 'Preliminary Project of Digital Bill Exchange Platform (数字票据交易平台初步方案)' (2016) 17 China Finance (中国金融), 32

establishment of the ECDS. The benefits can be analyzed from both transactional and regulatory perspectives.

2.2.1 At transactional level

a. Increased information transparency

In the financial services, key transactions are typically concluded with data or messages being exchanged among them, very often involving intermediaries to facilitate the dissemination of information. That is how the brokering business emerged, and subsequently developed, with the advent increasingly complex and cross-regional transactions. Significant information asymmetry can arise from this process, where brokers intervene and play the role of facilitator. However, brokers performing in such roles can prove to be detrimental, as seen in the referenced bill fraud cases. The distributed ledger system, however, will change the communication model from a 'bilateral exchange' to 'public sharing'.

Distributed ledgers are essentially transaction records maintained collectively by participants, or 'nodes' in the network. Therefore, the participants can share an identical, accurate, verifiable and comprehensive ledger source in real time. The system is transparent in that all transactions are public,[66] traceable and permanently stored in the DLT network. In a permissioned blockchain, all stakeholders have common access to their set of common transactions. Once a new piece of information is added to the blockchain,

[66] The publicity of transactions is subject to rules of information restriction, which will be further discussed in section 5.2.3 (f).

it is broadcasted to all participants. The communication channel is no longer a bilateral exchange, but rather of public sharing. This evolution will bring two main benefits:

1) **Higher transaction efficiency.** In the demo transaction given above, the information is not exchanged bilaterally between bank A and bank B. Rather, when A changes the transactional status of a particular digital bill, it is broadcasting this offer to all potential transactional parties in the network. It this way, all participants of the DCBES can see this offer simultaneously. One of them, who finds the offer in alignment with its demand, will accept it and conclude the transaction. The public sharing model will thus make transactions more efficient and guarantee better resource allocation.

2) **Lower transaction costs.** Once a participant or an asset is vetted and accepted into the blockchain, all eligible members can see the public information of the new participant or asset. Therefore, members do not need to conduct repetitive Know Your Customer (KYC) checks; consequently, this will save substantial time and resources. Also, the particular design of smart contracts can streamline the transaction processes, reducing the cost of confirmation, and settlement and clearing.

b. Reduced legal disputes and forgery

As the HKMA explained in its white paper on DLT, the tamper-proof nature of distributed ledger system is achieved with two elements: a proof system and cryptographic technologies. [67]

[67] Hong Kong Monetary Authority (n21)

The proof system is essentially about how consensus is achieved to modify the shared ledger. In a blockchain network, a consensus mechanism is the way in which a majority (or in some mechanisms, all) of blockchain participants agree on the value of a piece of data or a proposed transaction, which then validates the new data or transaction and updates the ledger. In other words, the consensus mechanism is a set of rules and procedures that maintains a coherent set of facts among the participating nodes.[68] Any attempt to modify the blockchain records requires the perpetrator to present the proof of authority for this modification. In the permissioned blockchain of digital commercial bill exchange, such proof is given to a participant only when it has been vetted and trusted to make certain changes. [69]

The blocks in the chain are connected through links built through a hash function, in other words, computational algorithms. Any attempt to change the content of a block will cause changes to the value of its hash link. This breaks the chain, with the remaining chain being shorter than the original one. Other participants can immediately detect this abnormality and those who have bookkeeping authority will reject the changes and stick with the original chain. Therefore, the data, transactions, and messages recorded in the blockchain are immutable and retraceable.

---

[68] Tim Swanson, 'Consensus-As-A-Service: A Brief Report On The Emergence Of Permissioned, Distributed Ledger Systems' (2015) <http://www.ofnumbers.com/2015/04/06/consensus-as-a-service-a-brief-report-on-the-emergence-of-permissioned-distributed-ledger-systems/> accessed 22 January 2017.

[69] Permissionless blockchains use Proof of Work (PoW) mining where hashing power is offered to build trust. As long as 51% of the nodes are honest players, network consensus is reached. Permissioned blockchains can use Proof of Stake (PoS) which requires validators to prove ownership of certain amount of currency (their "stake" in the currency).

The DCBES adopted an enhanced proof system and cryptographic technologies, using a zero-knowledge mechanism and the SM2, SM3 cryptographic algorithms, which can better ensure the authenticity of the digital bills, as well as guarantee the integrity and immutability of transaction records. [70]

As the blockchain network is expected to produce immutable records of digital bill transactions, it can enhance the credibility of electronic evidence stored in the form of codes. Since the blockchain network can cover whole transaction history, distributed ledgers will provide a complete evidence chain that can help determine who is to bear the burden of proof and the responsibility for eventual loss. For example, when drawing a bill, the acceptor agrees to be the drawee of the bill, which involves a process of credit granting. This process can then be encrypted into a block, forming time-stamped evidence of the beneficiary's rights and the acceptor's liabilities. The cryptographic technology can thus prevent "cheating" and potential disputes.

When a commercial bill transaction is concluded through a smart contract, its control is transferred according to the coded terms and conditions. The control may contain the legal title to this asset or other beneficiary rights. Therefore, fraudulent transactions of selling or pledging one bill to several parties are unlikely to happen.

In addition, since the information of a commercial bill, such as the issuer, drawer (payer), payee, maturity date and signing amount, etc., can be encrypted into the blockchain, it will be impossible to forge a bill. Rather, due to the regulatory controls that can be embedded

[70] Caixin (n20)

into the smart contract, the bill will be duly examined. Therefore, ineligible bills, i.e. bills without an actual history of commercial transactions, cannot enter the blockchain-based bill market.

c. Whitelisted participants

One of the benefits that shared ledgers provide to financial services is granular access control.[71] In a distributed ledger system, 'keys' and electronic signatures are used to control who can do what to the shared ledger. Specific capacities are granted to the 'private keys' under certain conditions.

The key attribute of a permissioned system is to have legally accountable validators. [72] When a market player applies for the entry into a permissioned system, its legal capacity should be vetted. If the applicant cannot meet the eligible criteria, it will not be granted access to the system. If it meets the basic requirements, its legal capacity may be further vetted to decide the level of its access permission. Depending on the scope of its legal capacity in terms of entering into different contracts or conducting administrative tasks, it will be granted different levels of access, such as validating, bookkeeping, or read-only.

[71] UK Government Chief Scientific Adviser, 'Distributed Ledger Technology: Beyond Block Chain' (Office for Science, UK Government 2016) <http://www.ameda.org.eg/files/gs-16-1-distributed-ledger-technology.pdf> accessed 6 March 2017

[72] Robert Sams, 'Blockchain Finance' (Coinscrum: Tools for the Future #2, London, 2015) <https://www.slideshare.net/rmsams/blockchain-finance> accessed 28 March 2017

According to Xu Zhong's model, the vetting authority in the DCBES is likely to be DCBE.[73] Within the system, only trusted or vetted participants can participate in the control and maintenance of the ledger. Under this whitelisting mechanism, illegal bill brokers will be eliminated from the blockchain-based commercial bill market. Their interference with normal market functions will thus be curtailed. Furthermore, even if a financial institution or a corporate is admitted to the DCBES, it can only conduct permitted types of activities with its "private key". For example, a commercial bank has the "trade key" to discount a bill and transfer a discounted bill, while the central bank reserves the "key" to rediscount a bill. Therefore, the whitelisting mechanism of permissioned blockchain can better ensure that market players act within their duly authorized legal capacity.

d. Reduced counterparty risks

CBDC-enabled DVP can reduce counterparty credit risk. As the average span for settling a transaction is significantly shortened, the risk exposure decreases accordingly. Additionally, since the sovereign digital currency system is connected to the DCBES, the digital bill and CBDC are processed simultaneously under smart contracts, which achieves full DVP synchrony. In other words, the control of a digital bill is governed automatically by smart contracts and independently of external interference, and it will not be transferred unless the required amount of CBDC is sent to the transferor's account. Therefore, if a party does not hold enough CBDC in its electronic vault, it will not be able to conclude the transaction.

[73] Xu and Yao (n65) 33

When a bill is circulated among different parties, the requirements and restrictions of discounting, discount transfer, rediscount, and repurchase can be inserted into the smart contract through programming. The execution of these terms will thus be automatic and obligatory, which can reduce counterparty credit risk and operational risk.

For instance, when a commercial bill is drawn, its maturity date can be coded into its governing contract. When the bill matures, the programming control will automatically launch a collection request on behalf the bill holder to the acceptor. The collected amount will then be directly transferred to the payee's account. This transaction will then be concluded and a block containing the transaction data will be added to the blockchain. In this way, the automatic execution of a contract can prevent overdue collection or diverting any collected funds to other uses. Another example is the repurchase contract, or repo. As the agreed repo date is coded into the smart contract, the targeted bill will be automatically redirected to the original seller's possession and the corresponding amount of CBDC will be deducted from its account and transferred to the original buyer's account.

2.2.2 At regulatory level: consolidated supervision and coded regulation

Considering the enormous amount of data residing in the blockchain network and smart contract programming, a new model of regulation and supervision will likely come into being. The European Securities and Markets Authority (ESMA) has recognized that

distributed ledger technology could potentially facilitate the collection, consolidation, and sharing of data for reporting, risk management, and supervisory purposes.[74]

As all records are stored in the blockchain and are theoretically traceable across its history, it is possible to establish an ongoing monitoring system and external auditing system. Supervisory bodies can be granted special access to consult or retrieve the data without demanding them from the market players, which reduces the risk of deceit and pushes market players to comply strictly with relevant laws and regulations. However, the system can also alleviate market participants' burden of producing consolidated reports of their activities, as the transactional data will already be stored in an integrated way, i.e. in a chain of continuous evidence.

In addition, transactions can be better regulated with the application of smart contracts. DCBE will issue a common smart contract template, where a regulatory program can be inserted as a condition precedent for contract formation and execution. The smart contract template can serve as a master agreement to standardize the documentation in the blockchain-based market. The regulatory program can thus facilitate the implementation of regulatory policies and laws. For example, a bill repurchase contract should be valid at least longer than one day but less than its maturity date.[75] Therefore, if a contract obliges

[74] European Securities and Markets Authority, 'Report: The Distributed Ledger Technology Applied To Securities Markets' (2017) <https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf> accessed 10 February 2017

[75] PBOC, 'Regulatory Measures for Commercial Bill Transactions (票据交易管理办法)' (2016), Article 47

one party to repurchase the bill after its maturity date, the regulatory code embedding the rule will prevent the execution of this contract.

As the execution result will also be recorded in the distributed ledgers, the system can provide reference for regulatory review. Also, the accumulation of transactional data and failure record will establish a participant's credit history and provide reliable information for constructing a credit rating. With a transaction pattern analysis and credit rating mechanism, regulators can conduct targeted scrutiny and regulation, which will effectively deter market misconduct.

III. Legal challenges of digital commercial bills

As seen in Section II, digital commercial bills can be advantageous in enhancing information transparency, consolidating supervision and regulation, reducing fraud and counterparty risks, as well as eliminating ineligible participants. Nevertheless, digital bills also bring about many challenges, which may undermine its advantages if not properly dealt with. Just like the benefits, the risks and challenges of digital commercial bills can also be neatly divided into transactional and regulatory categories.

3.1 At transactional level

3.1.1 Definition of the digital bill and its "delivery"

As a very recent achievement of state-of-the-art technology, digital bills do not fit exactly into the traditional legal definition of a bill of exchange. At the very least, additional interpretation is necessary for such an instrument to be lawfully used.

Chinese law defines a bill of exchange as 'a negotiable instrument, signed and issued by the drawer, who authorizes the drawee to pay unconditionally a certain sum of money to the payee or the bearer at sight or on a specified date.' [76] An electronic commercial draft (ECD) is defined as 'a negotiable instrument made by the drawer in the form of data message within the ECDS to authorize the payer to unconditionally pay a determined amount of money to the payee or the holder on a specific date'.[77] ECD is only payable at a fixed date with maturity time up to one year.[78]

It is commonly acknowledged that a bill of exchange is essentially an order to pay. [79] There is no intrinsic value of the instrument itself, but it carries an enforceable claim for certain value in money. As a negotiable instrument, the legal title of a commercial bill in paper

[76] Translated from Negotiable Instruments Law 2004 Amended Article 19

[77] For the comparison of the traditional bill, electronic bill and digital bill, see Chart 1 in Section 1.1.

[78] PBOC, 'Measures for the Regulation of Electronic Commercial Drafts Transactions (2009), Article 13

[79] The legal definition of bill of exchange does not vary substantively across different jurisdictions. The English law definition of bill of exchange is 'an unconditional order in writing, addressed by one person to another, signed by the person giving it, requiring the person to whom it is addressed to pay on demand or at a fixed or determinable future time a sum certain in money to or to the order of a specified person, or to bearer'. Bills of Exchange Act 1882, Section 3(1). Following the recommendation of Bank of England, English law now recognizes the evidencing and transfer of title of dematerialized equivalents to money market instruments including bills of exchange. The Uncertificated Securities (Amendment) (Eligible Debt Securities) Regulations 2003. American UCC uses the term "draft" rather than "bill of exchange", which is an unconditional order made by the drawer to the drawee to pay a fixed amount of money to a certain person on demand or at a definite time. § 3-104, Uniform Commercial Code

form is transferred upon delivery. The transferee acquires a perfected ownership interest when she receives the bill, provided that there is no other defect.[80]

This transfer mechanism of legal title continues to apply to bills in electronic form, but with extended interpretation of "delivery". The "delivery" of an ECD means that 'a party to an ECD sends the draft to the assignee and the assignee signs for acceptance.'[81] The action of "signing" an ECD with an electronic signature is regulated by the Electronic Signature Law of 2004.[82] The legal title to an ECD is thus transferred upon "delivery" of a data message and the electronic signature. Since the ECD is traded in a centralized system, the transaction is recorded in the central administrator's ledger. [83]

The transfer mechanism of the legal title to a digital bill, however, necessitates further examination, given the features of blockchain technology and smart contracts. Distributed ledger systems can either record tokens or claims. When an asset is tokenized with cryptographic technology and inserted in the blockchain network, it becomes endogenous to the system. Only when such tokens are used will the settlement in the blockchain network be sufficient to discharge the two parties from their obligations. [84] If the blockchain represents property that exists off-ledger, however, the consequences of an

[80] For the function of bill of exchange and bill financing, see n24

[81] (n76) Article 20

[82] (n76) Article 15

[83] For the connection of ECDs with bills in paper form and digital bills, see Section 1

[84] Andrea Pinna and Wiebe Ruttenberg, 'Distributed Ledger Technologies In Securities Post-Trading: Revolution Or Evolution?' (European Central Bank, 2016) <https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf> accessed 5 March 2017

update to the distributed ledger are unclear in terms of the settlement finality and the effect on ownership rights. That is where efforts should be made to fill in the legislative gap. In the case of China's pilot project on digital bills, however, it has been expressly explained that digital bills are essentially independent series of codes programming business logics,[85] and therefore native to the DCBES.

Liu Xinwen classifies bills of exchange as special movable property representing certain enforceable claims for money.[86] Following this classification, traditional commercial bills represent enforceable claims materialized in paper form and ECDs represent dematerialized claims that are registered with a central depositor. As for digital bills, they may be interpreted as tokens representing certain enforceable claims for money, i.e. tokenized order to pay. The token itself is intangible property without intrinsic value, but it embodies the value of enforceable claims that are encrypted into it. The transfer of legal title or other beneficiary rights should be finalized upon delivery, i.e. the change of control over a digital bill, which is governed by smart contracts and conducted on a peer-to-peer basis. However, there is currently no legal recognition of transferring legal title or other beneficiary rights upon "delivery" using cryptographic coding in a decentralized blockchain system, as the regulation of ECDs only recognizes the "delivery" in data message form in a centralized depository system. Therefore, there is currently no legal

[85] Xu and Yao (n65) 31

[86]According to Liu, while the ownership of the bill is regulated by China's Property Law, the enforceability of the claims and other beneficiary rights should be governed by Negotiable Instruments Law. Liu X, *Law Of Negotiable Instruments* (3rd edn, CUPL Press 2015) 20

basis for the completion of "delivery" and the transfer finality of legal title or other beneficiary rights.

3.1.2 New operational risks

Threats to the blockchain-based digital bill exchange platform can come not only from flaws in smart contracts, but also from the failure of components. It is advisable to remain cautious as to the operational risk in a DLT-based network.

ESMA indicates that the technology is at an early development stage and largely untested. Although it is currently considered unlikely that the encryption algorithms will collapse, it is not impossible for such an accident to happen. In addition, technical innovations such as quantum computing may render the security schemes inherent to a blockchain network irrelevant through time. Also, the security of the entire network remains dependent on its 'weakest link'; for example, a hacker could step into the breach by one single unsecured node.[87] Finally, the fact that DLT-related knowledge and skills are currently concentrated in the hands of a small number of people increases the security concerns.

It is worth noting that there is no sufficient empirical evidence to evidence the absolute stability and security of a blockchain network. In fact, the risks of market infrastructure failure will always be part of operational risk when a new infrastructure is introduced. Both the infrastructure provider and users should develop risk control strategies to deal with the new risks. In the current pilot project, all kinds of digital bill transactions are concluded in a single network, which is the DCBES. The risk of overdependence on a single blockchain-

[87] European Securities and Markets Authority (n74) 10-11

based market infrastructure is thereby amplified by the variety of covered services. Although the collapse of the whole infrastructure is unlikely to happen, as the central bank would not implement such an unstable and risky project, unexpected failures of certain components are still technically possible. It is still unclear what the results and available remedies are when the holder loses control over a digital bill, that is to say, when the holder's private key does not match with the digital bill.

As the DCBE will be responsible for the maintenance of the blockchain-based network for all digital bill transactions, it is expected to assume the responsibility of ensuring the stability and security of the system. The extent of the DCBE's liability when losses emerge from infrastructure failures stands to be seen. When liabilities are well defined, a remedy regime should be implemented to provide compensation to those who have incurred losses. When losses result from a malicious attack by a third party, there should be contingencies in place to implement efficient retrieval procedures. If the third party attack was facilitated by the DCBE's gross negligence or intentional actions, then the DCBE should bear contributory liability.

3.2 At regulatory level

3.2.1 Compliance risk

In the DCBES, the DCBE will be tasked to provide comprehensive market support services. Compared to a traditional exchange, its role as an information and trust intermediary will

be less important, as the blockchain network itself will serve as the perfect solution for asymmetric information and trust problems. However, it will be granted new functions.[88]

a. Non-public information exchange

The DCBE will be involved in the exchange of confidential data to facilitate the transactions. The DCBE is thus expected to comply with information restriction rules on commercial bill transactions. [89] To be specific, in the blockchain system, though the block containing certain a piece of information is added to the distributed ledgers held by every participant, only parties with the right 'private key' can read the content of the information. [90] Others are only aware of its existence in the network. Therefore, an exchange channel of confidential information should be established to facilitate the negotiation or transaction process. When the DCBE exchanges confidential information, there will be concerns of information security and conflicts of interest. For example, if a DCBE staff member, who is a government official, negligently leaks a piece of confidential information to an unauthorized party and thus distorts the market order, he or she should be held liable for malpractice and breach of anti-unfair competition law. If the staff abuses its "regulatory key" to acquire illegitimate benefits for a relative, this should constitute an

[88] The main roles are mentioned in Zhong Xu and Qian Yao's article 'Preliminary Project of Digital Bill Exchange Platform'.

[89] Negotiable Instruments Law 1995 Chapter 2; Regulatory Measures For Transactions of Electronic Commercial Drafts Chapter 4

[90] Tessa Hosser, 'Blockchain Basics, Commercial Impacts and Governance Challenges' (2016) 68 Governance Directions 608

illegal abuse of power. Depending on the nature and involved sum of money of the committed malfeasance, the staff would be subject to civil or criminal charges.

b. Identity management

The DCBE is also the identity management authority that sets admission requirements and verifies the off-chain identification of participants, which will inevitably involve the KYC process. Although a KYC check is strictly speaking an obligation of financial institutions, they expect to rely on the authenticated digital identity of their counterparties in the DCBES. Therefore, the burden of KYC compliance will partially (if not totally) be transferred from market players to a governmental institution. If the DCBE wishes to decrease this burden, it can claim that the certification of a new participant only involves a formal examination rather than the examination of substantive authenticity. This would, however, unfortunately reduce the level of trust in the blockchain network and the benefits of shared KYC sources, since participants would still have to conduct substantive checks of their counterparty's identity information. If the admission process is supposed to verify the relevant information substantively, the DCBE will need considerable human resources and other vetting resources at its disposal, and bear more of the burden of KYC compliance. It can be argued that the traditional KYC process should be rephrased as KYP, i.e. Know Your Participants, in the case of a permissioned blockchain that provides a shared KYC source.

c. Issuance of digital commercial bills

A similar situation will happen in the issuance of digital bills. Insofar as public information is concerned,[91] it is unclear whether the creation of a digital bill is subject to DCBE's approval or only its supervision. If it is only supervision, the obligation of checking the payment obligation underlying the commercial bill remains with the transactional parties. If the creation process needs DCBE's approval, the DCBE will be responsible to examine the eligibility of the concerned digital bill. As the DCBE will be responsible for publishing the template of the smart contract governing the creation of a digital bill, the formality requirements will already be coded into the template and further approval is unnecessary.

The remaining question, then, is who is responsible for checking the authenticity of payment obligations underlying the commercial bill. To enhance the trust in the blockchain network, the payment obligation background of a digital bill should be examined before the token is published on the chain. This examination process cannot simply be a process of apparent examination. Though theoretically the drawer can submit the evidence of such a background to the blockchain network and meet the formal requirements, its effect as a single accurate source of truth will be undermined if the evidence is not subject to a substantive examination of its authenticity. Needless to say, if the DCBE assumes the responsibility of substantively examining the payment obligation, its compliance burden is likely to increase significantly.

Therefore, the extent to which the DCBE is responsible for examining the authenticity of participants' identity and digital bills before they are admitted to the network needs to be

[91] Mainly from working papers of PBOC officials and respected press report to August 1st, 2017.

clarified. The underlying regulatory principles may need to be revised according to the unique features of permissioned blockchain and new transactional patterns.

3.2.2 Systemic risk

Smart contract coding problems can potentially increase the systemic risk in the DCBES. Blockchain-based smart contracts can be defined as "a piece of code which is stored on a blockchain, triggered by blockchain transactions, and which reads and writes data in that blockchain's database."[92] It enables automatic contractual performance by the involved parties. This new paradigm of contractual parties' interaction transforms the traditional contracting process and contract performance. While they increase efficiency and reduce transactional costs and default risks, smart contracts can become problematic due to their reliance on computational coding programs. New operational risks can arise from coding flaws and systematic risks may be amplified by the increasing interconnectedness between parties and the application of one smart contract in numerous transactions.

For example, in December 2016, investors faced a multimillion-dollar loss because they missed a loophole in a smart contract's coding.[93] The crowd-funding technology was based on an Ethereum public blockchain. The loophole, known as the "recursive call vulnerability" or the "race to empty", was exploited to divert funds from the investors'

[92] Gideon Greenspan, 'Beware Of The Impossible Smart Contract' *Blockchain News* (12 April 2016) <http://www.the-blockchain.com/2016/04/12/beware-of-the-impossible-smart-contract> accessed 18 April 2017

[93] Peter Sayer, 'A Blockchain "Smart Contract" Could Cost Investors Millions' *IDG News Service* (20 June 2016) <http://www.pcworld.com/article/3086211/a-blockchain-smart-contract-could-cost-investors-millions.html> accessed 18 April 2017

account to another account.[94] It enabled the exploiter to issue instructions which transferred funds from the collective investors' account to a different account which only he controlled, and thus "defrauded" the other investors of that money. Although the "DAO" (Decentralized Autonomous Organization) crises happened in a public blockchain network where no central authority is tasked to judge and award remedies, in contrast to the permissioned blockchain of China's pilot project, these coding flaws are inherent to smart contracts regardless of whether the blockchained is permissionless or permissioned.

3.2.3 Reputational risk

At the development stage of a permissioned blockchain, a specialized entity will usually be responsible for setting a smart contract template for blockchain-based transactions and maintaining the stability of the underpinning infrastructure. As far as the DCBES is concerned, the DCBE will be the publisher of smart contract templates and the entity responsible for the maintenance of the permissioned blockchain system. As such, the DCBE may assume an implied responsibility of ensuring that there are no loopholes in the smart contracts that threaten transaction security. However, technical flaws are not always anticipated and solutions are often developed after the fact to rectify the loopholes. Therefore, the DCBE will be exposed to high reputational risk in its role of publishing the

[94] Ethereum Foundation proposed changing the underlying rules, introducing the equivalent of a constitutional amendment to freeze the account to which the DAO's funds were diverted. This proposal can be seen as a centralized operation, and as such, it would breach the decentralization principle of the blockchain network. The mechanism of simple majority voting to amend the underlying rules is also problematic from a socio-political perspective.

smart contract template. The DCBE can try to reduce its reputational risks by stipulating that the template is purely optional, like a master agreement that is made for reference only.

However, this would leave the parties to develop their own smart contracts, which may produce diverse flaws that undermine the efficiency of smart contract transactions. In addition, as few market participants will have the technical resources to develop their own templates, an official referencing version published by a government agency will likely to be the choice of most, if not all, market players. It can be argued that the participants involved in the pilot project are sophisticated financial institutions with rich resources, but the scalability of this project will be impeded by the existence of different smart contract templates. Furthermore, as the project is expected to be part of a nation-wide bill exchange platform, a standardized template will be necessary for the purpose of promoting uniform market standards and enhance the trust in the system. Therefore, the burden of producing smart contract template seems to inevitably fall on the DCBE. However, if users suffer a loss because of the flaws in the template, the redress mechanism and loss allocation regime are unclear for the moment. The subsequent reputational damage will render the DCBES less popular and market players may return to traditional bill transactions, where we have already identified many market deficiencies.[95]

[95] See Section 1.2

IV. The way forward: critical issues for digital commercial bills

As discussed in previous section, there are many legal challenges to be dealt with before digital bills can fully deliver their potential benefits. Although most legal concepts and policies related to commercial bills continue to apply to digital bills, the unique characteristics of digital bills should be taken into consideration when designing a legal framework to ensure the proper operation of the digital bill exchange system.

4.1 Definition of digital commercial bills and transfer finality

Digital bills do not fit exactly into the traditional definition of commercial bill in paper

form or electronic bills.[96] The lack of a clear definition will make digital bills subject to disputes and make their associated rights and obligations ambiguous. Therefore, a new definition is needed. Considering the innovative features of blockchain, digital commercial bills should be defined as:

> A negotiable instrument prepared by the drawer in the form of cryptographic token within the Digital Commercial Bill Exchange System (DCBES), to authorize the payer to unconditionally pay a determined amount of money to the payee or the holder on a specific date.

As a negotiable instrument, the legal title of a commercial bill, regardless of its medium, is supposed to be transferred upon delivery. However, since the delivery method of digital bill is different from commercial bills in paper or electronic form,[97] the transfer mechanism of digital bills also requires a redefinition. Taking into consideration the application of digital fiat money and smart contracts in transacting digital bills, the "delivery" of digital bills should be defined as occurring when:

> The transferee sends the due amount of digital fiat currency to the transferor's digital address, following which the transferee becomes the controller of the digital bill,[98] which is recorded in the governing smart contract of the digital bill.

[96] See Section 3.1.a

[97] Ibid

[98] The digital bill is now matched with the private key of the transferee.

After defining a digital commercial bill in a DLT-based network and how it is transferred between parties in transactions conducted with smart contracts and sovereign digital currency, further explication should be made as regard to the rights and obligations of the involved parties.

4.2 Clarification of rights and obligations

Although the digital bill system may to some extent change the transactional medium and paradigm, the nature of the acts and rights[99] on the commercial bill remain the same under general negotiable instruments laws.[100] Nevertheless, some changes or ambiguity may arise in the rights and obligations of parties involved in the digital bill exchange.

It should be noted that not all financial institutions can enter into the DCBES, considering the limited availability of the infrastructure and the stringent qualification requirements. The parties to the digital commercial transactions can thus be categorized as:

1. financial institutions with direct validation and bookkeeping authority (direct participants), or;

2. financial institutions or other legal persons with read-only authority (indirect participants).

In addition to the transacting parties, the system operator, the DCBE, also plays an essential

[99] The acts include issuance, acceptance and endorsement. The rights include the right to claim payment and the rights of recourse.

[100] Negotiable Instruments Law 1995; Measures for Payment and Settlement 1997; Temporary Measures for Accepting, Discounting and Rediscounting Commercial Drafts 1997; Regulatory Measures For Transactions of Electronic Commercial Drafts 2009; Regulatory Measures for Commercial Bill Transactions 2016.

role and has obligations in ensuring the smooth conduction of transactions.

4.2.1 Direct participants

Direct participants should continue to be responsible for examining the authenticity of digital bills in their transactions, as well as the information of their counterparties. In these processes, they may have the public information in the DLT network as reference. However, the information should not be considered as a representation made by the infrastructure provider (the DCBE in this case) to the general public. Although the technology is designed to ensure the traceability and authenticity of information, for now, participants should not conduct business on the assumption that the truth is guaranteed. As far as current empirical exploration and tests indicate,[101] the information stored in the DCBES is only supposed to reduce the KYC burden rather than eliminate it. Nevertheless, blockchain technology will predictably help provide reliable sources for the KYC check when the technology is mature and a sound guarantee mechanism is in place.[102]

Direct participants should bear responsibility for providing a reliable internal system that is connected to the DCBES and high-quality digital bill services to its clients. They should also register and open an account with the DCBE, which would put them under the DCBE's

[101] The absolute reliability of a DLT-based network in providing truthful information has not been supported by enough empirical evidence.

[102] Digital identity service providers, such as I/O Digital, Sho Card, Uniquid, Onename and Ascribe Gmbh, can offer banks the ability to scan customer documents and identity information and then generate private and public keys to seal them before the data is encrypted and sent to the blockchain. Bradley Cooper, 'Blockchain Tech Powers Identity Management' *Blockchain Tech News* (10 August 2015) <https://www.blockchaintechnews.com/articles/blockchain-tech-powers-identity-management/> accessed 26 February 2017

regulatory authority.

Once its identity and legal capacity is authenticated by the DCBE, a direct participant can conduct authorised business of digital bills, including acceptance, discounting, inter-bank discounting, and rediscounting. They are permitted to validate transactions and add "blocks" to the network. Therefore, they are responsible for the authenticity and compliance of the digital bills that they publish in the system.

4.2.2 Indirect participants

The rights and obligations of indirect participants remain the same as parties to traditional commercial bill transactions.[103] However, they should be registered with the DCBE and subject to due supervision and regulation by this new authority.

It should be highlighted that all participants, regardless of its authority level, should comply with strict rules of bill financing, such as the examination of debt obligations underpinning bill drawing and the discounting and inter-bank discounting procedures.

4.2.3 Digital Commercial Bill Exchange (DCBE)

Different from the SCPE established under the authority of the central bank, the DCBE is not a central counterparty to the transactional parties in the digital bill business. However, the DCBE should assume important responsibilities in the following areas, where its mismanagement may result in liabilities:

[103] Negotiable Instruments Law 1995 Chapters 2-6

a. Authorization.[104]

The entry of commercial banks, insurance companies, and other financial institutions into the DCBES is subject to the examination and approval of the DCBE. In this process, the DCBE should clarify the entry standards for applicants and check their qualifications rigorously.[105] However, once an institution is accepted to the network, it would be responsible for its own activities. The publication of each new digital bill is no longer subject to the authorization of the DCBE.

b. Identity management.[106]

The DCBE should be responsible for providing services such as issuance, storage, validation, and retrieval of an ID certificate, namely, through a private key linked to a valid identity, which participants can use to log onto the DCBES and conduct transactions in the network.

c. Retrieval of digital bills

It should be within the DCBE's mandate to retrieve the digital bills that are lost, whether they were lost from infrastructure failures or from hack attacks. The record in the DLT network can help the DCBE verify the ownership and other rights related to the digital bill. When it is impossible to restore a holder's control of a digital bill, the holder may apply to invalidate the lost bill and create a new one with same content and

[104] See Section 2.1.1

[105] See Section 3.2.1

[106] See Section 2.1.2

equivalent rights.

d. System maintenance.[107]

The DCBE is expected to maintain the security and stability of the distributed ledger system. It should regularly check and upgrade the system according to technological changes and potential new vulnerabilities. More importantly, a substitution plan should be developed, in case the failure of the unique system causes irrecoverable loss.[108]

e. Smart contract template publication.[109]

The DCBE should assume the duty of publishing an effective and reliable smart contract template to be commonly used in the DCBES. The template is expected to establish market standards on transactional procedures. Also, the smart contract template will be embedded with the regulatory program carrying the conditions of commercial bill transactions, and thus the acceptance of the transaction will be contingent on its compliance with the regulatory requirements. In this way, the DCBE is making regulation in the form of coding programs.[110]

f. Digital fiat currency issuance.[111]

The DCBE will be in charge of exchanging sovereign digital currency (CBDC) with

[107] See Section 3.2.3

[108] For detailed discussion of substitution planning, see Walker (n52) Section 8(1)

[109] See Sections 2.1.3 and 3.2.2

[110] Lawrence Lessig discusses the problems with code being law in *Code v2* (Basic Books, 2006)

[111] See Section 2.1.4

real currency held by the parties, which will be subject to central bank monetary policy.[112] In this process, the DCBE, as an entity, will inevitably fall under anti-money laundering rules, as the exchange will involve large amounts of capital flows.

g. Confidential information communication.

Following the principles of commercial bill transactions in China, different parties should have access to different pieces of information on the bill. [113] However, as the blockchain-based digital bill system broadcasts the information on a bill to the entire network, an information protection and inquiry regime should be implemented. **[114]** The DCBE should provide non-public information to relevant parties only after due examination of their qualifications. Specifically, the acceptor may inquire the face information[115] on a digital bill before receiving a request for payment and may inquire all information after receiving the request. The payee, the endorsee, and the guarantor can ask for the act information and the previous draft information. The holder

[112] For the influence of digital fiat money on central bank monetary policy, see John B and Michael K, 'The macroeconomics of central bank issued digital currencies' (2016) Bank of England staff working paper No. 605 <https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies.pdf?la=en&hash=341B602838707E5D6FC26884588C912A721B1DC1> accessed 18 March 2017

[113] Ibid

[114] See Section 3.2.1.a

[115] The information on a commercial bill includes the information on the bill itself (face information) and the information on the acts associated with this bill (act information).

(controller) of a digital bill can have access to all draft information. During the stage of recourse, the person against whom recourse is exercised can inquire all information.

4.3 Liabilities and loss allocation

After clarifying the rights and obligations of different parties, liabilities should also be clearly defined and an effective compensation regime should be established in addition to the general liabilities and remedies that exist in the digital bill business. Authorities may issue a warning or impose a fine depending on the nature and seriousness of the circumstances.

4.3.1 Direct participants[116]

Direct participants should be held liable if they fail to examine the basic information of their clients, as well as the authenticity and regulatory compliance of the bills that they digitalise into the DCBES.

They should also be liable for flaws in their internal systems that cause loss to its principals or cause a widespread failure in the DLT network to which it is connected. Specifically, if they collectively manipulate the validation mechanism, they should be liable for engaging in market abuse and face substantial fines.[117]

[116] Most of their liabilities are the same as in traditional commercial bill transactions. As for indirect participants, since their authority is read-only, their liabilities are not increased by the implementation of the digital bill system.

[117] Although this is highly difficult as the proof system is enhanced in the digital bill exchange system (see Section 2.2.1.b), it is still theoretically possible. Further empirical evidence is thus needed to support this discussion.

Additionally, if direct participants hold insufficient funds (either in real currency or CBDC) for clearance, which subsequently causes a loss to the payee to the commercial bill, they should also provide appropriate compensation. However, if the lack of funds is caused by a delay in exchanging real currency to CBDC with the DCBE, the compensation should be provided by the latter.

4.3.2 DCBE

As the operator and maintainer of the digital bill system, different liabilities of the DCBE may arise from its different roles. However, certain limitations should be placed upon the DCBE's liabilities, considering the limited resources at its disposal and the fact that participants are voluntarily assuming by engaging in the new system.

The DCBE should face categorical responsibility when it fails to vet the qualification of an applicant and accepts an unqualified party into the system. It should be stressed that this examination process should not be limited to formal requirements, but also the substantive authenticity of all submitted information and the business history of the applicant. As the subsequent introduction of commercial bill products by the parties is not subject to the DCBE's approval, the entry examination and identity verification process is critical to the market order in the digital bill system.

In addition, if the parties suffer a loss as a result of the improper design or maintenance of the blockchain network, loopholes in the smart contract template, or due to delays in the exchange of real currency to CBDC, the DCBE should also be held liable. However, as the DCBE is an administrative body and has no enforceable possessions, it is difficult to impose a fine on it or provide compensation to the victims. It can be argued that since it is

a governmental institutions, the state should provide compensation for the victim's loss. However, this will expose taxpayers to losses incurred in the digital bill market. Thus, a better alternative would be to implement a collective compensation scheme that can allocate risk among risk-makers in a more reasonable way than a unilateral liability scheme. To be specific, each participant that subscribes to the digital bill system would pay a membership fee, which would in turn be directed to the collective compensation scheme. In addition, parties may also contribute money to the collective compensation scheme for each transaction they conduct in the system. The proportion should not be too large that parties are deterred from using the system; rather, it should reflect the balance of benefits and risk in being engaged in the new system of digital commercial bill transaction.

Conclusion

China's fast-growing commercial bill market, which centers increasingly on bill financing, has witnessed many deficiencies in its traditional transaction paradigms, as seen in Section I. Major problems include market fragmentation, illegal brokerage, non-compliance of

market players, as well as a laggard legal framework. One of the solutions to these challenges has been the establishment of an Electronic Commercial Draft System (ECDS), and a nation-wide unified exchange platform is in development. To fully address the market's many problems, a pilot project on digital commercial bills has been developed using emerging disruptive technologies, including distributed ledger technology (DLT) and smart contracts. In the pilot project, blockchain-based digital commercial bills will be issued, and the transactions in the system will be supported by central bank issued digital currency.

This will bring a lot of benefits for both market players and regulators as analysed in Section II. For transactional parties, they can have higher transaction efficiency and lower transactional costs because of the public information sharing scheme that characterizes a DLT-based network. Also, they will be faced with less legal disputes and fraud risk since the distributed ledger system is expected to produce inalterable evidence and eliminate undue interference. Thus, transactions can become more secure and trustworthy, because the market participants will undergo an initial vetting procedure when they are admitted to the permissioned blockchain network, and their acting capacity within the network is technologically controlled by their private key. This can ensure that every participant acts within its legal capacity and with due authorization. In addition, parties can be less worried about counterparty risk. Since the use of digital fiat currency can enable DVP in the blockchain, the settlement interval in transferring commercial bills by endorsement can become almost zero. The automatic execution of smart contracts can also prevent malicious practices such as diversion of funds or overdue collection of funds. As for the regulators, they can conduct consolidated supervision with the integration of traceable and

unchangeable information stored in the network. Also, they will be able to code regulatory requirements into the smart contract template and thus regulate the transactions through coding programs.

However, the new transactional and regulatory paradigms raised by the digital commercial bill exchange system can have potential legal challenges and risks as examined in Section III. First, without a clear legal definition of what a digital bill is, it is difficult to establish the relevant rights and obligations of parties, such as a transferee's right to receive payment. It is also impossible to make the blockchain-based transactions legally binding without the acknowledgment of "delivery" in the network. Secondly, since there is no empirical evidence to support the absolute reliability of the new technology, parties could suffer losses as a result of coding flaws and component failures. Without an adequate protection and remedy regime, users and their clients can be unfairly exposed to unknown damages. Furthermore, when assuming different functions,[118] the DCBE must comply with the rules related to information inquiry restrictions. The extent to which this institution should assume the responsibilities of providing KYC sources, and whether it should examine new commercial bills in their compliance with formal or substantive requirements, is also debatable. In addition, smart contract coding flaws can potentially increase the DCBE's reputational risk and the systemic risk in the DCBES. Therefore, it is also worth discussing whether the smart contract template published by the DCBES should be implemented as the single, mandatory standard contract template for the system.

[118] Including non-public information exchange, identity management and issuance of digital commercial bills.

Considering the aforementioned benefits and challenges, these critical issues have to be properly dealt with so that blockchain-based digital commercial bills can maximize advantages and minimize risks. As such, Section IV advanced a suitable legal basis for digital commercial bills and their delivery completion, to support transfer finality and the crystallization of the relevant rights and obligations of involved parties. Section IV also clarifies what additional rights and obligations are introduced by the new transactional paradigms in the DCBES, and how they affect different parties, including direct and indirect participants. [119]

As to the new governmental agency, the DCBE, its duties should also be clarified. The paper advances recommendations on a number of its functions, such as authorization, identity management, retrieval of lost digital bills, system maintenance, smart contract template publication, digital fiat currency issuance, and confidential information communication.

After clarifying the duties of the diverse parties, the paper advanced an explanation of the liability regime and availability of remedies in the digital commercial bill business. The party that bears responsibility in a particular case should provide reasonable compensation. However, faced with the emerging risks of a new technology, it is advisable to establish a collective compensation regime, as no one can fully predict the potential weakness or failure of this ever-developing technology. The collective compensation funds should be comprised of basic membership subscription fees and additional contributions that are

[119] Needless to say, traditional rights and obligations under the commercial bill transaction continue to exist.

proportionate to the transaction volume of different parties in the digital commercial bill market.

The application of blockchain, digital fiat currency, and smart contracts to the transaction of commercial bills is just one of the many possibilities of these technologies. Since Bitcoin brought DLT to public attention, the technology has grown out of its infancy and is now on the way towards widespread deployment,[120] especially in the banking and finance sector. This injects momentum to the development of financial technology (Fintech), which has been transforming many aspects of people's daily life and transactions. Legal and regulatory innovation, therefore, should catch up with the current technology-driven period of industry innovation.

Legislators and regulators must be aware that open dialogue with industry players is indispensable in order to comprehend the fast-changing nature of the new paradigms in different sectors. The legal and regulatory framework should respond to the new features presented by emerging business models, and balance regulation with innovation. In this process, legislators, regulators and market players should prepare themselves for the next revolution of modern society, where distributed systems will transform many aspects of the society, and coding is expected to partly or entirely replace laws.

[120] The World Economic Forum, for example, has identified the possible application of DLT in global payments, claim processing, syndicated loan, trade finance, automatic compliance, proxy voting, etc. See Deloitte and World Economic Forum, 'The Future of Financial Infrastructure' (Future of Financial Services Series, 2016) <http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf> accessed 1 April 2017

The Shift to a Derivatives Markets in Fintech

LLB, LLM (Lon),
MSc (Auth),
Eleni Samara

INTRODUCTION

Derivatives markets are secondary markets of trading of financial products that derive their value from an underlying asset, such as a commodity, currency or security. Their current infrastructure commenced in 1981, and they boomed after 2000, reaching the size of $700 trillion before the 2007 global financial crisis.

In the aftermath of the Great Recession, derivatives were severely criticised as causing or at least aggravating the crisis, due to their inherent characteristics, including their complexity, the lack of market transparency, the interconnectedness of market participants, and so on. The main focus was on the over-the-counter (OTC) derivatives markets, since these were the less regulated ones. OTC derivatives will be the main focus of this paper as well, since exchange-traded derivatives are subject to very strict rules and are traded in specific venues, leaving little to no room for innovations at this time.

Thus, in the first chapter I will primarily attempt to unfold the series of events that led to the 2007 global financial crisis, in order to critically examine the views expressed concerning the interrelation between the OTC derivatives markets, as they existed and functioned until 2006, and the causes of the crisis. In the second chapter, I will point out the main characteristics and core obligations that the after-crisis regulation posed in the US (Dodd-Frank Act) and the EU (EMIR, etc.), as the most representative jurisdictions, along with their aspired objectives. On the other hand, these regulatory initiatives, though in the correct track, seem to overburden market participants, but at the same time, they have not yet crystallised to ensure a legally certain environment, and their ensuing complexity and ambiguousness leads to wide disputes.

Since legislatures around the world do not seem capable of regulating derivatives markets efficiently, a quest for other solutions has led to FinTech as an alternate resort. Financial Technology comprises the technological methods implemented to bring about various financial solutions. Although the term lately became widespread, the concept behind it exists for decades; for instance, e-banking can be easily included under its umbrella. Nevertheless, during the last 3-4 years, the abbreviation FinTech refers to a rapidly augmenting industry, which reaches figures in the spectrum of

approximately $200 billion, if traditional financial institution transacting via technology are considered within its scope.

An aspect of FinTech that can have wide implications for derivatives markets is blockchain, or more generally distributed ledger technology (DLT). The third chapter focuses on the basic notions of distributed ledgers and smart contracts, and their specific implementation and potential in a derivatives environment. In the early stages, it is probable that only post-trade procedures of the derivatives markets may enjoy the deployment of DLT, as successful experiments have already shown, but a bolder scenario of a total replacement of central counterparties in the long run should not be out of the question.

In any case, I argue that substantial perils may originate from the implementation of FinTech in the derivatives markets, among which are technological, business and legal risks. Chapter IV will address these concerns and attempt to either dispute some extravagant objections or suggest possible solutions. Furthermore, the chapter includes some considerations about the timely and appropriate intervention of the regulator, in order to avoid any unnecessary disruptions of industry progress and achieve the long-desired efficient transformation of the derivatives markets.

The attempted analysis might be premature, as FinTech initiatives in the derivatives markets have only recently started to take place. Conversely, it might be considered overdue, as the use of DLT has been soaring during the last four years, obliging big players in the derivatives markets to organise special experimental networks for its testing. In the face of this, regulatory authorities and organisations, such as ESMA, SEC, the UK Government Chief Scientific Adviser, and others, have had to repeatedly issue discussion papers and reports, to avoid being overhauled by the reality of the market. Regardless of the timing, the sole fact that numerous parties have been constantly occupied with this issue demonstrates its utmost significance beyond a shadow of a doubt.

CHAPTER I - THE DERIVATIVES CHARACTERISTICS CONTRIBUTING IN THE 2007 CRISIS

After the eruption of the recent and still ongoing global financial crisis, there has been an effort by many scholars, politicians, businessmen and generally many

participants –or not- in the global financial markets to pinpoint its causes, to learn from the past mistakes and avoid –if possible- any similar crises in the future. During this time, derivatives have been demonized by some as the main cause of the crisis, but it is by now mostly agreed that, although derivatives may be blamed for exacerbating it, it would be an exaggeration to fully attribute the crisis to the derivatives markets. In view of that, the wide scale and evolution of the crisis itself is indicative of the course of action one should adopt in studying the crisis; that is, to take into account the full continuity of the historical facts and not partially on cherry-picked facts so as to put the blame on a certain –predetermined- sector of the markets.

The Unfolding of the Crisis

There was a plethora of investments in Western economies that originated in China and Japan starting in the late 1990s, as a result of the low levels of domestic consumption and investment in these countries in comparison to their earnings. This amounted to a ready availability of capital and hence a reduction of the cost of credit, but also of the yields of traditional investments, which further resulted in an unprecedented accumulation of household debt in Western economies, especially in the United States, and in a quest for higher yields by investors.[1] The latter led to the creation or extreme expansion of innovative financial instruments, primarily in the form of securitised debt instruments.

In an environment of extremely positive economic conditions, the low levels of inflation and the low interest rates led to the vast availability of credit, which in turn created a housing bubble, especially in the US market, as both mortgages and consumer credit skyrocketed, along with property prices. This tendency was accompanied by growing financial imbalances partially provoked by the foreign origins of many investments. Simultaneously, to achieve the much-desired higher yields, underwriting standards decreased significantly, leading to the rise of subprime mortgage lending in the US from $ 180 billion in 2001 to $ 625 billion in 2005[2] and the

[1] Simon Firth, *Derivatives: Law and Practice* (Sweet & Maxwell 2017)
[2] The High-Level Group on Financial Supervision in the EU, *Report* (Brussels, 25 February 2009)

formation of complex financial instruments for higher returns, such as asset backed securities (ABS) or collateralised debt obligations (CDOs).

Nevertheless, in mid-2006, inflationary pressures emerged in the US, due to which it became obvious that it was necessary to tighten the monetary policy. However, the rise of interest rates would soon prove to be fatal and trigger a domino effect. The subprime mortgages started to default at alarming levels, resulting in HSBC and BNP Paribas announcing unacceptable default rates in March and August 2007, respectively. The market confidence began to tremble, causing many investors to withdraw their funding from lower-quality mortgages, but eventually also from firms originating higher-quality mortgages, such as Northern Rock. Financial institutions subject to mark-to-market accounting were obliged to write down assets in their balance sheets and amidst constant revisions of credit ratings, in order to cope up with the imposed quantity and risk-weighted capital requirements, they had to proceed to large scale "fire sales". This brought about a further decline in asset prices and transformed a temporary liquidity problem into a solvency one.[3] As a consequence, through the rest of 2007 and the beginning of 2008, major banks and financial institutions including Citibank, Merrill Lynch, UBS and Bear Stearns, issued successive reports that detailed huge mortgage-related losses. Bear Stearns suffered such severe losses that it had to be acquired by JPMorgan Chase, with the assistance of the Federal Reserve. MBIA and Ambac, engaged in the mortgage insurance business, lost their AAA ratings in June 2008. IndyMac, one of the largest mortgage originators in the US, soon followed, failing in July, and it was in turn followed by Fannie Mae and Freddie Mac in September.[4]

Confidence in the market had totally evaporated, and after Lehman Brothers filed for bankruptcy in September 2008, inter-bank lending and the money markets froze. This was followed by the widely-debated rescue of AIG, through the outlay of vast sums of taxpayer money, and state-funded recapitalisation interventions in other countries to prevent systemically important banks from failing and the risk of contagion. Cumulatively, all of the aforementioned incidents effected tremendous

[3] Ibid

[4] Bruce Tuckman, 'Derivatives: Understanding Their Usefulness and Their Role in the Financial Crisis' (2016) 28 (1) Journal of Applied Corporate Finance 62

declines in the stock markets and consumption rates, the restriction of investments and business entrepreneurship in general, and finally a deep and widespread recession, bearing also a severe blow to weaker economies and countries with highly leveraged financial institutions. These highly leveraged financial institutions had to be rescued by their respective countries, transforming a corporate crisis into a sovereign debt crisis, which is still present and unresolved.[5]

Derivatives: The Source of all Evils

In the ambivalent financial environment that emerged from the crisis, an intense 'witch-hunt' ensued, in order to attribute responsibilities to people accountable for provoking it, and to pinpoint and eliminate the culpable financial instruments for the destruction. Many have identified derivatives as the main cause of this crisis.

In particular, the main fault is placed upon Credit Derivatives, and more specially on Credit Default Swaps, as some argue that through them the key players in the derivatives markets, e.g. Lehman Brothers, Bear Stearns and AIG, accumulated major risk positions in a very short period of time, without any capital or collateral backing, which in turn resulted in unacceptable systemic risk. In addition, the opaqueness of these instruments led both to the manipulation of the market by these significant market participants, away from the restrictions of regulatory authorities, and to the proliferation of a lack of confidence when things started to collapse, as market participants could not accurately predict their exposure (which later proved to be far less than anticipated during the days of panic). What is more, the growth of the CDS market contributed substantially to the increase of interconnectivity in global financial markets. By creating interdependencies between financial institutions, insurance companies, investors from various backgrounds, and everyday businesses in all industries, and by enhancing global scalability for financial markets, the CDS market made any failure or collapse of a major participant in one market an inherent risk of

[5] Firth (n1)

instant and broader spread of the contagion to a number of other participants and markets as well.[6]

Similarly, naming this crisis a subprime mortgage crisis was inaccurate, as the total value of all subprime mortgages in the US amounted to a mere $1.3 trillion, meaning that even if all of them defaulted, it would not have been enough to escalate to such a major global financial crisis. Instead, it was the legalisation and removal of the legal obstacles of speculative trading in OTC derivatives effected through the 2000 Commodities Futures Modernization Act (CFMA) that resulted in the rapid multiplication of the relevant market. In essence, some claim that lawful OTC derivatives speculation on mortgage-backed bonds amplified the initial $1.3 trillion weakness in such a scale as to offer a legitimate accusation of the CFMA as the main 'culprit', since it allegedly caused spill over effects big enough to bring down the banking industry and several sovereign borrowers.[7]

The supporters of this view attempt to prove it through the use of three examples, namely, Bear Stearns, Lehman Brothers, and AIG. The first of them was allegedly one of the most leveraged firms on Wall Street, whilst the second was one of the largest CDS market counterparties. Both failed at the first signs of default of the underlying assets —mortgage-backed bonds— of the derivatives they held in vast numbers. Finally, AIG had a reputation of assuming riskier investments, differentiating itself from more conventional insurance firms. It was highly involved in the market for mortgage-backed securities and had concluded numerous CDS contracts for low-quality underlying assets, amounting to exposures of $513 billion, all without taking offset positions in the CDS market. Consequently, even from the first specimens of defaults of the underlying assets, AIG was called by its counterparties upon posting billions of dollars of collateral. At the escalation of the crisis, this amounted to such unanticipated figures that the firm was faced with urgent and insurmountable liquidity adversities. It could not overcome them despite its $1 trillion in assets –held mainly by its subsidiaries- and its efforts to access funds from capital markets, which in light

[6] Walaa I. Alnassar, Eatessam Al-shakrchy and Mahmoud K. Almsafir, 'Credit Derivatives: Did They Exacerbate the 2007 Global Financial Crisis? AIG: Case Study' (2014) 109 Procedia, Social and Behavioural Sciences 1026

[7] Lynn A. Stout, 'Derivatives and the Legal Origin of the 2008 Credit Crisis' (2011) 30 (12) Banking & Financial Services Policy Report 13

of the circumstances proved unsuccessful.[8] Finally, policymakers adopted the only viable solution, which consisted of a bail-out by the Federal Reserve at the expense of hundreds of billions of taxpayer money.

Derivatives: The Source of all Evils… NOT!

The above opinion seems to distort some facts, placing the beginning of the crisis in events that were in fact symptomatic of it,[9] and omitting to consider many facts or factors that contributed at least equally to the crisis.

First of all, MBSs and CDOs, which contributed significantly to the crisis, are **not** derivatives, as in both cases investors pay for the securities in advance and expect the subsequent revenues in the future, whereas in derivatives there is rarely any up front monetary transaction, apart from posting margins to guarantee performance. Instead, the counterparties agree for a future monetary transaction depending on certain predetermined events or conditions. Indicative of the misconception is the fact that Bear Stearns was mainly engaging in these kinds of mortgage-backed securities, rather than derivatives, which renders the whole example as at least misplaced.

What is more, the crisis did **not** commence with the failure of Lehman Brothers, which was the first time that derivatives were actually inserted in the equation,. Rather, it began long before that, as described above. Specifically, the first signs started emerging right after the tightening of US monetary policy in mid-2006. All of the announcements that signalled growing mortgage defaults or firms' failures before Lehman's were related to the subprime mortgage market, and were more than enough to shake the markets to the ground and wipe out any seed of confidence in them.[10] These caused severe liquidity problems to all kinds of financial institutions and businesses, even those that were less leveraged or had high-quality leverage. In addition, the longevity of this situation was bound to lead to solvency problems as well and eventually spill over to other financial sectors , especially since governments

[8] Alnassar et al. (n6)
[9] Alastair Hudson, *The Law on Financial Derivatives* (5th Edition, Sweet & Maxwell 2012) 843
[10] Alan N. Rechtschaffen, *Capital Markets, Derivatives and the Law: Evolution After Crisis* (Oxford University Press 2014)

were swept into the ensuing panic and rushed to bail-out any institutions perceived as too-big-to-fail, risking their own financial stability in the process.

In this environment of uncertainty, the constant revision of credit ratings by credit rating agencies deteriorated the situation, forcing financial institutions into consecutive fire sales to conform with their capital requirements and sovereigns into urgent liquidity injections. All in all, a vicious circle had taken form, the continuity of which seemed to be irreversible.

Furthermore, to be precise, even Lehman's failure was not caused by its derivatives positions, but by its high leverage combined with its extreme exposure to real-estate related assets. Of course, it is undeniable that this failure triggered the liquidation of its derivatives contracts, which subsequently exacerbated the whole problem, especially since Lehman's debt was insured through CDSs, leaving the interconnected sellers of the protection in a seriously tight spot. However, even then, it was the previous loss of confidence owed to the subprime crisis that induced the greater damage than the contagion through Lehman's derivatives transactions themselves. This is because, as is usual in the CDS market, CDS positions are offsetting; that is to say, a dealer makes sure to balance the protection bought from a client with the protection sold to another. This proved to be the case with Lehman as well, where, little more than a month after the bankruptcy filing, it came to light that after netting, only $6-8 billion was in fact owed from protection sellers to protections buyers.[11]

Even in the case of AIG, the contribution of derivatives was exaggerated: of the total of $527 billion of CDS protection sold, the overwhelming majority was on high-quality assets that did not default. The problem resided in the $78 billion of protection sold on low quality mortgage-based CDOs. Although most of these underlying assets were in fact triple A-rated securities, the extent of the subprime crisis was such that it affected them as well. Still, out of the total $99 billion in losses in 2008, only $29 billion derived from CDS positions, which explains why only 28% of the government bailout funds were channelled into liquidating these positions. Furthermore, the alarm of contagion to its derivatives' counterparties was overstated, as individually they varied only from 1.3 % of equity, in the case of Rabobank, to 7.6

[11] Tuckman (n4)

% concerning obligations to Société Générale, meaning that the repercussions would be far less and more confined than initially feared.[12]

Finally, the blame upon synthetic CDOs, which indeed constitute derivatives, seems to be misplaced as well, considering that they consisted only 8-15 % of the total residential mortgage risk, which is too small a portion to create such huge problems.[13]

BUT still derivatives played a crucial role and cannot be acquitted

Although we know by now that derivatives were not the sole or the primary cause of the financial crisis, it is true that they contributed in exacerbating it further in its later stages.[14]

The implementation of CFMA in 2000 changed established industry practices by allowing speculative trading of derivatives without simultaneously imposing any limitations. This led to their out of control multiplication, reaching the notional amount of $673 trillion in 2007. Furthermore, as an innovative tool, they were immediately linked with and fuelled the mortgage-securitisation sector. Thereby, they multiplied further the risks inherent in that sector, as numerous investors were presented with the opportunity to buy derivatives for every single MBS or CDO, which disproportionately proliferated the notional amounts. This happened without necessary protective measures in place, such as capital requirements, posting of collateral, etc.[15] The lack of transparency and understanding of these complex financial instruments enhanced the mistrust towards them and the financial institutions involved with them, creating greater diffusion.[16]

The concentration of these instruments in a restricted number of financial institutions worked against one of their basic advantages, namely, the redistribution of risk.[17] Furthermore, there is a moral hazard inherent in the modern derivatives market because it is controlled by the so-called too-big-to-fail institutions, which are

[12] Ibid
[13] Ibid
[14] A. Feldman, 'The Current Economic Crisis and Derivatives' (2009) 52 Problems of Economic Transition 3
[15] The Financial Crisis Inquiry Commission, *The Financial Crisis Inquiry Report – Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States* (Official US Government Edition 2011)
[16] Chiara Oldani, *Governing Global Derivatives – Challenges and Risks* (Ashgate 2008)
[17] Firth (n1)

bound to be bailed-out in case of imminent failure. Both of these factors resulted in excessive risk-taking and disregard towards counterparty risk and other risks of the capital markets.[18] There were further contributors to this risk-taking: the ease of the transfer of risk to the next link of the chain through a derivative contract,[19] the preferential regime even in comparison to secured creditors in a Chapter 11 bankruptcy,[20] the constant pursuit for higher yields that was supported by the regulators, the belief that this market could be self-regulated,[21] and finally, the fact that derivatives solved the problem of achieving the intensely-desired need for prosperity in an economic environment of falling margins and per capita income in ageing western societies.[22]

Thus, while derivatives were not the main cause of the 2007 crisis, they may well be considered as a catalyst, but only because of the characteristics that market participants artificially attributed to them, and because of glaring regulatory omissions. The inherent features of derivatives still consist a useful and powerful tool for hedging risks and for managing banks' balance sheets and capital requirements efficiently,[23] as long as they are used prudently. As Mulaudzi establishes statistically,[24] the losses in the markets during the crisis were significantly reduced when CDO tranches were hedged, instead of the other way around.

CHAPTER II - DERIVATIVES REGULATION AFTER THE 2007 CRISIS

In view of the above contribution of OTC derivatives to the global financial crisis, it became obvious that certain procedures should be rectified and that the sector needed comprehensive reform. Although OTC derivatives never stopped gaining

---

[18] Jonathan McMillan, *The End of Banking – Money, Credit and the Digital Revolution* (1st Zero/One Economics GmbH 2014) 100-101

[19] MP. Mulaudzi, MA. Petersen and J. Mukuddem-Petersen, 'Credit Derivatives and Global Financial Crisis' (2013) II Proceedings of the World Congress on Engineering and Computer Science 925

[20] Mark J. Roe, 'The Derivatives Market's Payment Priorities as Financial Crisis Accelerator' (2011) 63 (3) Stanford Law Review 539

[21] Hudson (n9) 841-842

[22] Lucy Badalian and Victor Krivorotov, 'Looking for a Single Root-Cause of Both Crises: the 2008 Crisis of Derivatives and the Unfolding European Debt Crisis. A New Reading of the Ricardian Law of Diminishing Returns' (2011) 2 (8) Journal of Innovation Economics & Management 173

[23] Claude Brown and Timothy Cleary, 'Impact of the global financial crisis on OTC derivatives in structured debt transactions' (2010) 5 (2) Capital Markets Law Journal 218

[24] Mulaudzi et al. (n19) 927

ground in terms of value and volume, only effective regulation could bridle the markets and the continuing malpractices. Consequently, there have been many regulatory initiatives in the US, the European Union, and in other countries as well, most of which seek to address the main issues that derivatives have been blamed for.

This regulatory reform can be traced to the G20 statement in Pittsburgh regarding to the improvement of the OTC derivatives markets, as indicated in the recitals of the basic European Regulation. The summit resulted in the following resolution:

> All standardised OTC derivative contracts should be traded on exchanges or electronic trading platforms, where appropriate, and cleared through central counterparties by end-2012 at the latest. OTC derivative contracts should be reported to trade repositories. Non-centrally cleared contracts should be subject to higher capital requirements. We ask the FSB and its relevant members to assess regularly implementation and whether it is sufficient to improve transparency in the derivatives markets, mitigate systemic risk, and protect against market abuse.[25]

It is thus clear that the G20 countries adopted the following aims for regulatory reform: the transparency of the market, the strengthening of operational efficiency, and the mitigation of risks. The means towards achieving those goals have been roughly determined as the standardisation of OTC derivative contracts, their trade execution on a regulated facility, their central clearing, their reporting to trade depositories, and the addition of capital requirements to non-centrally cleared products.

Apart from some expected deviations and adjustments to the particularities of each country's legal system, the approaches have more similarities than differences, a fact manifested by a comparison between the US and the EU legislative initiatives.

---

[25] 'G20 Leaders' Statement – The Pittsburgh Summit' (24–25 September 2009) <https://www.g20.org/Content/DE/StatischeSeiten/Breg/G7G20/Anlagen/G20-erklaerung-pittsburgh-2009-en.pdf?__blob=publicationFile&v=1> accessed 17 July 2017

In the US, Title VII of the 'Dodd-Frank Act',[26] passed in July 2010, reforms the derivatives market. In the EU, it is the European Market Infrastructure Regulation ('EMIR'),[27] as amended by Regulation 600/2014/EU,[28] as well as Directive 2004/39/EC[29] (MiFID) and Directive 2014/65/EU on Markets in Financial Instruments (MiFID II),[30] which comes into full force on January 3, 2018. Whereas the US regime focuses on swaps or security-based swaps, as the most common ones, the EU has adopted a general framework that applies to all kinds of derivative contracts.

The Clearing Obligation

Article 4 (1) of EMIR provides for counterparties in OTC derivative contracts that have been authorised for clearing by ESMA to mandatorily subject them to clearing. The obligation depends on two conditions: the first is that one of the counterparties to the contract is a financial counterparty or a non-financial counterparty whose OTC positions exceed certain thresholds, and the second is the time of conclusion of the contract, and whether the time is on or after the dates set forth in its provisions.

Similarly, Section 723 of the Dodd-Frank Act defines the omission of clearing for standardized derivatives, as determined by the CFTC and the SEC, as unlawful. The clearing has to be performed through a derivatives clearing organisation (DCO) or a security clearing agency (SCA), depending on whether the contract is a swap or a security–based swap, as Section 763 dictates.

Of course, there are some differences in the details of clearing between the two regimes, such as in the review process of the contracts that are subjected to mandatory clearing, the application to already existing contracts, the exemptions

[26] The Dodd-Frank Wall Street Reform and Consumer Protection Act of July 21, 2010 Pub. L. 111-203 H.R. 4173

[27] Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories [2012] OJ L201/1

[28] Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 [2014] OJ L173/84

[29] Directive 2004/39/EC of the European Parliament and of the Council of 24 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC [2004] OJ L145/1

[30] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173/349

applicable, etc., but the main concept is that OTC derivatives, when standardized, ought to be subjected to the process whereby one central counterparty (CCP) becomes the counterparty to both the parties of a derivative contract. This is usually done through two separate contracts, and it ensures the performance of the initially agreed transaction, thereby minimizing counterparty risk, the systemic risk in case of a contracting party's default, and the operational risk, due to the robust documentation and enhanced margining procedures of the central clearing houses.[31] The risks are further reduced by a provision stating that to abide by the clearing obligation, a party to a derivative contract has to either become a clearing member itself or a client to a clearing member, thereby establishing a more controllable system, as CCPs impose preconditions before accepting clearing members and clearing members have to bear or alternatively hedge for the risk of their clients.

On the other hand, there is the risk of affording too much power to CCPs and creating new too-big-to-fail institutions, as nobody can escape the default of a CCP. To prevent such a danger, CCPs are to be authorised and strictly regulated.

Another important innovation of the above legislation is that it includes extraterritorial provisions regarding clearing, wisely considering that the derivatives markets are more international than domestic. EMIR, in Article 4 (1) (iv-v) provides that entities not established in the EU are also subject to the clearing obligations, as long as the contract has "a direct, substantial and foreseeable effect within the Union". The Dodd-Frank Act, in Sections 722 and 772, provides for its application to activities outside the United States if they "have a direct and significant connection with activities in, or effect on, commerce of the United States." Counterintuitively, these similar provisions might complicate things further, since one transaction may have to be cleared according to both regimes. This would be the case for a contract between an EU and a US company, governed by the law of a third jurisdiction. Accordingly, there have been some announcements by the competent authorities in both jurisdictions to resolve these overlaps, along with some significant initiatives, including the development of the Principles for Financial Market Infrastructures (PFMIs), which are of a non-compulsory nature. However, it is premature to hope for

[31] Firth (n1)

a definite solution. Hence, it is crucial to seek for alternatives that could alleviate these contradictions, as the success of the individual regimes lies on the international cooperation and coordination between them,[32] especially since both include provisions that allow the recognition of equivalent regulatory regimes, in order to avoid imposing duplicative obligations.[33]

The Standardisation of Derivatives

A precondition to the clearing obligation in both the above US and EU regulatory regimes is to standardise, as much as possible, the derivatives contracts that are bought and sold over-the-counter. The push towards standardisation is palpable in numerous recitals of EMIR (e.g. 21 & 92), but also in Article 5 (4) (a), whereby ESMA is dictated to primarily consider, before including a derivative contract into those eligible for the clearing obligation, "the degree of standardisation of the contractual terms and operational processes of the relevant class of OTC derivatives".

In Section 723 (a) (3) of the Dodd-Frank Act, concerning the determination that a class of swaps is eligible for clearing, there is an analytical description of the characteristics of standardised derivatives. In fact, the legislator has defined the liquidity, adequate pricing data, and the availability of a rule framework consistent with the main terms and conventions of trading the particular contract, as key features to determine whether a class of swaps should be subject to clearing. All in all, the US legislature selected a more descriptive approach than the EU, but ended up at the same result.

The standardisation of OTC derivatives is one of the most important aspirations of legislators. The lack of standardised contracts in the market causes uncertainties in price discovery and in the estimation of the exposure of counterparties, it endangers the reduction of operational risks, and hinders the adoption of necessary practices such as trade reporting and collateral posting, all of which have been deemed necessary to avoid a repetition of the 2007 crisis. Apart from increasing the use of

[32] Jerome Powell, 'A Financial System Perspective on Central Clearing of Derivatives' (2014) <https://www.federalreserve.gov/newsevents/speech/powell20141106a.htm> accessed 23 June 2017

[33] PWC, 'FS Regulatory Brief – Derivatives – Enter EMIR, You're going to need a bigger boat' (2013) <http://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/pwc-fs-reg-brief-derivatives-emir.pdf> accessed 14 July 2017

clearing, standardisation would in general contribute to the procedural improvement of OTC derivatives transactions. It would enhance the execution of trades in organised and authenticated trading platforms, whilst simultaneously promoting the further comparability of trade information.[34]

The Reporting Obligation

Article 9 of EMIR sets forth the details of the reporting obligation, which includes the recordkeeping obligation as well, imposing it both on counterparties to a transaction and CCPs. It pertains to both cleared and uncleared derivative contracts, has a strict time limit of one working day after the conclusion, amendment, or termination of the contract, and it designates trade repositories registered under Article 55 as the recipients of the reports.

The Dodd-Frank Act places an equally important value on the reporting obligation; Section 725 imposes an obligation on the derivatives clearing organisations to provide the Commission with all necessary information latter to perform efficient oversight. Additionally, Section 727 provides for real-time public reporting, whereby there is an obligation to report all data in relation to a swap transaction, including price and volume, "as soon as technologically practicable after the time at which the swap transaction has been executed." Similar to the EU regime, there is no differentiation between cleared and uncleared derivatives, and the recipients of the reports are swap data repositories (SDRs) regulated by the CFTC or SEC. The importance of the reporting obligation to the US regulator is evident because of the fact that it is the most broadly applicable of all the Title VII provisions. Also, a series of supplementary rules have been issued to regulate these reporting duties in greater detail: the final SDR data reporting and recordkeeping rules, the real-time CFTC public data reporting rules, the historical swap data reporting and recordkeeping rules, the large-trader commodity reporting, the recordkeeping rules for swap dealers and major swap participants

[34] FSA & HM Treasury, 'Reforming OTC Derivative Markets – A UK Perspective' (2009) <http://www.fsa.gov.uk/pubs/other/reform_otc_derivatives.pdf> accessed 23 June 2017

(MSPs), and the Regulation SBSR data reporting rules for security-based swaps (SBSs).[35]

The reporting duty in both regimes includes extended data of the derivatives transactions, such as counterparty information, key economic terms, daily valuations, aggregated trading information, etc. It is obviously aimed at greater transparency of the OTC derivatives market, since the market's opacity was one of its main flaws before the crisis. The reporting duty gives the relevant competent authorities an adequate picture of the market positions of the entities they are responsible for regulating and allows for better risk monitoring.[36]

On the other hand, there still remain some issues that can be handled more efficiently, such as duplicative reporting requirements, deriving either from different counterparties of the same transaction or even from different clearing entities. To avoid duplicate reporting, it is advisable to use unique trade, product and counterparty identifier codes, but their use is not widespread enough yet and needs further encouragement by regulatory authorities. Likewise, the harmonisation of common standards concerning data access and aggregation has to improve in some jurisdictions in order to overcome the barriers erected by bank secrecy and privacy laws or international agreements.[37]

As described above, another aspect of the reporting obligation is recordkeeping, whereby all counterparties have to maintain accurate and detailed records of derivatives transactions for a period of five years, thereby further enhancing the ability of the regulatory authorities to supervise efficiently and prevent malpractices or other cases of market abuse.

The Risk Mitigation Obligation

---

[35] Practical Law Finance and Practical Law Corporate & Securities, 'Summary of the Dodd-Frank Act: Swaps and Derivatives' <https://uk.practicallaw.thomsonreuters.com/3-502-8950?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1> accessed 23 June 2017

[36] Deloitte, 'CFTC and EU OTC Derivatives Regulation – An Outcomes-based Comparison' (2013) <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-fs-cftc-and-eu-otc-derivatives-regulations.pdf> accessed 14 July 2017

[37] Eric Heitfield, 'OTC Derivatives Market Reform: Looking Back and Looking Forward' (2015) <https://www.business-school.ed.ac.uk/waf/crc_archive/2015/OTC%20Derivatives%20Market%20Reform%20Looking%20Back%20and%20Looking%20Forward.pdf accessed 14 July 2017

The risk mitigation obligation is the most multifaceted of these statutory obligations, as it is divided into operational risk mitigation, the exchange of collateral, and the demand for additional capital requirements for regulated institutions. In fact, operational risk mitigation is further separated into the timely confirmation of trades, their daily valuation in accordance to mark-to-market accounting, the provision for dispute resolution processes, and the so-called portfolio reconciliation and compression.[38]

Section 731 of the Dodd-Frank Act clearly states that swap dealers and MSPs shall conform with the regulated standards in relation to 'timely and accurate confirmation, processing, netting, documentation and valuation of all swaps.' Likewise, Article 11 (1) (a, b) of EMIR requires the parties to a transaction to implement all necessary procedures to allow for the 'timely confirmation, where available, by electronic means, of the terms of the relevant OTC derivative contract[,]' and to 'monitor the value of outstanding contract.' Subparagraph (b) demands formalised procedures for the identification and resolution of disputes, which is also featured in Section 735 of the Dodd-Frank Act. These provisions focus on non-cleared OTC derivatives, and they are geared towards market and transactional transparency; consequently, increased transparency should lead to a reduction of the operational risk that was so flagrant during the financial crisis, when there were no approximate estimations of the exposure of participants in the derivatives market.

These measures are further enhanced by the reconciliation and compression processes, already included in the 2013 ISDA Protocol. Through reconciliation, the parties to a contract prearrange the terms and conditions to exchange each party's valuation of the derivative contract, so that both can identify any differentiations or discrepancies between their records, and at the same time adopt transparent methods for calculating margin. Through portfolio compression, parties perform transaction reductions through a biannual offset, provided that certain thresholds are surpassed. This way credit risk is significantly relieved, and both regulators and market participants acquire a more accurate picture of the magnitude of outstanding transactions and the market.[39]

---

[38] Firth (n1)
[39] Ibid

To supplement these rules, and prevent further taxpayer bailouts, a provision that addressed the exchange of collateral was considered essential. This would minimize any negative consequences deriving from a market participant's insolvency by offsetting the relevant losses of its counterparties. Both regimes, in regulations supplementing their main legislations, provide for the obligation of an initial and a variation margin. The former is posted at or before the beginning of the transaction and is intended to cover potential future exposure, whereas the latter is intended to protect from current exposures. Collateral should be highly liquid, and thus has to be provided for mainly in cash.[40] The segregation of the collateral is also regulated in both regimes through different methods; either CCPs or counterparties are required to keep separate records and accounts of the clearing members or even their clients, in order to protect the posted collateral in case of a default.[41] Clearly, the above measures address –in a rather photographic way- the fear of another AIG or Lehman failure; that is to say, they aspire to mitigate any systemic risk arising from a too-big-to-fail market participant, especially since in AIG's case it was the lack of collateral and the subsequent spiralling request for it that led to the firm's near-collapse, whereas in the case of Lehman, the ascertainment of almost adequate collateral —even in the long run— downsized the initially anticipated losses and mitigated the consequences of its default to its counterparties.

Finally, the above rationale also led to additional capital requirements for participants involved in uncleared OTC derivatives transactions, since their inherent risk is far greater than when dealing with an authorised central counterparty. Thus, counterparties should hold a proportionate amount of capital to manage the risk that might exceed the value of the posted collateral.[42] Since holding regulatory capital is relatively expensive, this provision also acts as a discouraging factor against speculative derivatives transactions of a bespoke nature, which are the most difficult

---

[40] SIDLEY, 'US and EU OTC Derivatives Regulation – a Comparison of the Regimes' (2012) <https://www.sidley.com/en/insights/newsupdates/2012/04/us-and-eu-otc-derivatives-regulation--a-comparison-of-the-regimes> accessed April 14, 2017.

[41] Robert Dilworth and others, 'Comparison of the Dodd Frank Act Title VII and the European Market Infrastructure Regulation' (2014) <https://media2.mofo.com/documents/140128-comparison-of-the-dodd-frank-act-title-vii.pdf> accessed July 14, 2017.

[42] SIDLEY (n40).

to regulate and are considered to be the most dangerous in terms of creating financial uncertainty.

Other Obligations

Both regimes prioritise various other obligations, but the ones gaining most ground lately are the rules imposing mandatory trading on certain trading venues and position limits.

Regarding the first one, MiFID II requires that liquid derivatives shall be traded exclusively through specific trading venues, like regulated markets, multilateral trading facilities (MTFs), and organised trading facilities (OTFs), whereas in the US the equivalent eligible venue for clearing swaps will be a swap execution facility (SEF) or a designated contract market (DCM).[43]

As for the second obligation, the CFTC has adopted position limits pursuant to the Dodd-Frank Act, which are focused mainly on certain referenced commodity derivatives, while the EU regime, created by MiFID II, will adopt the most extensive position limits in the world, setting requirements for any market participant that, regardless of its location or regulatory status, trades in any EU trading venue.[44]

It is more than obvious that the above provisions are meant to provide regulators with the tools to ensure trading transparency and prudent market conduct. As far as market participants are concerned, the provisions furnish them with a centralised pool of liquidity, but at the same time, they prevent parties from incurring obligations they are not equipped to take on, and they avoid the creation of too-big-to-fail institutions and the associated moral hazard dilemma.

To summarize, the above provisions have benevolent intentions, but their intended objectives have yet to be achieved, since further amendments seem to be required to accomplish market transparency without complex statutory procedures that act as barriers to entry due to the high costs they entail. The latter is necessary to allow the

[43] Dilworth (n41)

[44] Adam Topping – Ellie Kirby (HFW, 'MiFID II position limits and reporting regimes: an update' (2017) HFW Commodities Bulletin <http://www.hfw.com/downloads/HFW-Commodities-Bulletin-July-2017.pdf> accessed 18 July 2017

entry of smaller participants in the market, and to mitigate the market's inherent risks. What is more, there are further issues that need to be addressed. For instance, imposing customary derivative disclosures might not, by itself, indicate the actual exposures of a firm in complex credit derivatives, as the experience of Ambac with respect to the PG&E downgrades in 2001 and its CDO downgrades illustrated.[45] Thus, the usefulness of the reporting obligation and of information disclosure requirements is doubtful. In addition, the derivatives most blamed for exacerbating the crisis derivatives, synthetic CDOs and mortgage-backed CDSs, are not liquid enough to be centrally cleared; thus, it would seem that the remedial measures are a little disoriented.[46] They seem particularly misguided since they inextricably lay the ground for the creation of a complex network of highly interconnected CCPs and clearing members, established in multiple jurisdictions, without appropriate legislative harmonisation, where the failure of a single member might have far-reaching results for the whole system. After all, as Jerome Powell concludes, "the system as a whole is only as strong as its weakest link."[47] Consequently, although the regulation is headed in the right direction, the derivatives industry has signalled that —as Scott O'Malia aptly summarized— "the reforms could be further improved by eliminating duplication, complexity and unnecessary compliance burdens that damp the ability of financial institutions to fund the growth of the real economy."[48]

CHAPTER III – DISTRIBUTED LEDGERS: A NEW PERSPECTIVE FOR THE DERIVATIVES MARKETS

The exhaustive and ongoing regulatory reform of the global derivatives markets has so far not managed to achieve one of its initial aspirations, namely, the restoration of trust and faith in the financial system. The same holds true for the majority of the other sectors of the financial markets, such as lending. Simultaneously, the fact that

[45] Robert Bartlett, 'Inefficiencies in the Information Thicket: A Case Study of Derivative Disclosures During the Financial Crisis' (2010) 36 The Journal of Corporation Law 1
[46] Tuckman (n4)
[47] Powell (n32)
[48] Joe Rennison and Philip Stafford, 'US Derivatives Industry Anticipates Modest Dodd-Frank Changes – Wholesale Repeal of Post-2008 Financial Crisis Rules Finds Little Industry Appetite' *Financial Times* (7 February 2017) <https://www.ft.com/content/1f6ccfbe-ed2e-11e6-ba01-119a44939bb6> accessed 23 June 2017

the contagion effect of the crisis resulted in widespread unemployment and a number of yet-unresolved sovereign debt crises does not help consign the crisis to oblivion. In addition, the ensuing regulatory hurricane, which ranged from the imposition of differentiated capital requirements on banks, to the introduction of new, untested concepts, such as recovery or resolution plans (living wills), bail-in, convertible bonds (Cocos), has not reassured the market and consumers. Rather, it has demonstrated governmental uncertainty as to how to avoid a future crisis, reshaped the business models and structures of financial institutions, and ballooned the compliance costs for the financial sector. Consequently, this succession of events spurred a quest for other, more cost-efficient financing alternatives, as the post-crisis environment had led banks and important financial institutions to withdraw their funding from SMEs and consumers due to the ensuing liquidity crunch. Since they were concentrating on fully complying with the ever-changing regulatory framework, banks and established financial institutions were left unable to compete with and react to the sweeping wave of innovation. This, in turn, created fertile terrain for a new generation of market participants seeking credit and investments in alternative routes, establishing a new paradigm, the so-called FinTech firms.[49]

Distributed Ledgers and Smart Contracts

The breakthrough for FinTech was the launch of the Bitcoin cryptocurrency in 2009, which deployed and combined long existing technologies, such as distributed ledgers and cryptography. Soon enough, people realized that the underlying technologies of Bitcoin and their innovative utilisation had the potential to fundamentally transform financial markets. Derivatives have become a sector of primary focus for the exploitation of distributed ledger technology (DLT) and blockchain, the underlying system of Bitcoin.

But what is a distributed ledger or a blockchain? Since so many researchers have elaborated these concepts and this is not the core topic of this paper, it is sufficient to

[49] Douglas Arner, Janos Barberis and Ross Buckley, 'The Evolution of Fintech: A new Post-Crisis Paradigm?' (2016) 47 (4) Georgetown Journal of International Law 1271

provide a limited general explanation of the terms, since the analysis will revolve around their meaning, their applications, and their possible benefits and risks concerning derivatives specifically.

A simple definition of distributed ledger is found in a report by the UK Government Chief Scientific Advisers, where it is explained as:

> An asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of 'keys' and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network.[50]

A blockchain, on the other hand, is a type of a distributed ledger that combines a certain number of records in a block and chains successive blocks to each other, after they are validated through some prearranged form of consensus among its participants. So, the main difference compared to the distributed ledger lies in the accumulation of transactions in blocks rather than one by one,[51] which is so insignificant a distinction that the two terms are used interchangeably.

In practice, a distributed ledger is innovative, as it diverges from the traditional need for a centralised trusted third party for the validation of transactions, which is instead effected by multiple authorised parties in the distributed ledger. This allows parties to transfer assets, represented as tokens, between one another in a trustless, yet tamper-proof environment, with immutable transaction records that are validated

---

[50] UK Government Office for Science, 'Distributed Ledger Technology: beyond Block Chain – A Report by the UK Government Chief Scientific Adviser' (2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> accessed 22 July 2017

[51] Michael Mainelli and Alistair Milne, 'The Impact and Potential of Blockchain on the Securities Transaction Lifecycle' (2016) SWIFT Institute Working Paper No. 2015-007 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2777404> accessed 5 March 2017

through a consensus mechanism and secured cryptographically.[52] The contents are accessible to the participants, in accordance to the network's rules, through identical shared versions of the ledger.[53]

What is more, because a distributed ledger is programmable, it has enabled the use of "smart contracts". As these have been aptly described:

> A smart contract is an agreement whose execution is both automatable and enforceable. Automatable by computer, although some parts may require human input and control. Enforceable by either legal enforcement of rights and obligations or tamper-proof execution.[54]

In other words, smart contracts comprise both the conventional legal agreement, with the agreed terms and conditions between the parties, as well as their codification in a comprehensible computer language. Smart contracts link automatic contract performance to the occurrence of reference conditions,[55] which derive from information received from internal or external sources —via programmes called oracles—, and eliminate the need for any external intermediation.[56]

Of course, there is the possibility of making use of certain other technology innovations, which will be considered without further analysis in this paper, such as APIs (Application Programming Interfaces), as they might prove invaluable in terms of interoperability and compatibility between legdgers with different protocols or even between ledgers and legacy systems.[57]

---

[52] Deloitte, 'The Future of Asset Servicing: Shaped by Three Disruptive Technologies' (2017) <https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/performancemagazine/articles/lu_future-asset-servicing-012017.pdf> accesses 23 July 2017

[53] Deloitte, 'Over the Horizon: Blockchain and the Future of Financial Infrastructure' (2016) <https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-over-horizon-blockchain-future-financial-infrastructure-281116.pdf> accessed 23 July 2017

[54] Christopher Clack, Vikram Bakshi and Lee Braine, 'Smart Contract Templates: Foundations, Design Landscapes and Research Directions' (2016) <https://arxiv.org/abs/1608.00771> accessed 4 March 2017

[55] Jo Van de Velde et al., 'Blockchain in Capital Markets – The Prize and the Journey' (2016) <https://www.euroclear.com/dam/Brochures/BlockchainInCapitalMarkets-ThePrizeAndTheJourney.pdf> accessed 20 February 2017

[56] Dong He et al. (IMF Staff Team), 'Virtual Currencies and Beyond: Initial Considerations' (2016) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> accessed 22 July 2017

[57] David Mills et al., 'Distributed ledger technology in payments, clearing and settlement' (2016) Board of Governors of the Federal Reserve System Finance and Economics Discussion Series 2016-095 <https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2881204> accessed 23 February 2017

Permissioned v Permissionless Ledgers

Although Bitcoin's innovative blockchain technology took the form of an open network consisting of participants allowed to perform all the activities of the network, including the validation process, commonly known as a permissionless blockchain, it is in fact permissioned distributed ledgers that are perceived as the appropriate application for the financial industry and, by extension, the derivatives markets. In permissioned ledgers, access is allowed only to a restricted number of trusted parties, who have been previously checked to verify if they fulfil the prerequisites of the network, e.g. credit, authorisation, and other requirements. Furthermore, not all the participants in a permissioned blockchain have the authority to perform the totality of the procedures in the network. There are differential levels of access, as different sets of participants have access to certain records, usually through different layers of encryption, and can participate in specific transactions, such as the transfer of assets, validation of transactions, updates to the ledger, and so on.[58] These ledgers are preferred in financial transactions, especially due to the sensitivity and the significance of financial data,[59] as the participating entities are identifiable, bound contractually through their participation in the network, and usually liable to special requirements and authorisations outside the ledger. This way, the transparency and accountability of any wrongdoer vis-à-vis the regulators is secured, whilst other legal provisions are complied with, such as privacy protection, know-your-customer laws, and confidentiality rules. Even in these systems, where only certain participants are authorised to perform updates of the ledger, a consensus mechanism is still a valuable characteristic to further enhance their cyber resilience.[60] Alternatively, it can be replaced by an equally secure method, such as a notary node trusted by everyone in the system,[61] or it can be enhanced through a PoS system with collateral, whereby assets of participants are kept in escrow by a trusted third party, and the assets of

[58] Ibid

[59] Imogen Garner et al., 'FinTech: Analysing the Changing Nature of Financial Services' (2016) 140 Compliance Officer Bulletin 1

[60] Andrea Pinna and Wiebe Ruttenberg, 'Distributed Ledger Technologies in securities post-trading' (2016) European Central Bank Occasional Paper Series 172 <https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2770340> accessed 23 February 2017

[61] James Chapman et al., 'Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?' (2017) Financial System Review 59.

which are immediately forfeited in the event of an illicit transaction or malevolent action.[62]

Deploying DLTs and Smart Contracts in Post-Trade Procedures of Derivatives Markets

Combining all the above, there is a general consensus that a distributed ledger protocol may provide the necessary conditions regarding confirmation, netting, clearing and settlement, risk mitigation, reporting and recordkeeping of derivatives transactions to transform and ameliorate prevalent practices in the derivatives market.

Currently, when a derivative is sold over-the-counter, the underlying asset may be a repeatedly rehypothecated percentage of a collateral, without any further knowledge of the total rehypothecation percentage of the asset or the transactions concerning either the underlying asset or its derivatives preceding this transfer. As a result, there is no certainty as to the ownership and the collateral value, whilst the total value of the pledge ends up exceeding both the origination value and the legal restrictions. Consequently, as there is no regulatory reporting of the transaction history within the secondary markets, there is an opaque regime for both regulators and participants, leading to enhanced counterparty and systemic risk.

In a DLT environment, on the other hand, any collateral is immediately tokenised and the transaction history of any underlying asset is recorded in detail along with that of its derivatives. In addition, the smart contracts attached to the ledger controlling the transactions embody the full details of the counterparties and of the preceding transactions, making recordkeeping automated and facilitating subsequent counterparties to acquire a full and clear picture of their data, including their value, as well as regulatory transparency, via real-time access, preventing the violation of rehypothecation limits.[63]

---

[62] Pinna (n61)

[63] World Economic Forum and Deloitte, 'The Future of Financial Infrastructure – An Ambitious Look at How Blockchain can Reshape Financial Services' (Future of Financial Services Series, 2016) <http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf> accessed 23 July 2017

It is almost certain that when blockchain technology is employed in derivatives markets, it will be implemented through a permissioned network, in which only authorised market participants will be provided with nodes in the ledger, and where participants will be allocated with different sets of rights in the network, depending on the category of the clearance they fall in. Obviously, the parties to the transaction shall have to agree the terms and conditions of the deal, as in any conventional contract, and record them using their cryptographic keys in the ledger, where the members with the respective clearance shall subsequently validate them, making the record definite. Smart contracts, along with oracles, will allow for the automation and self-execution of the terms of the contract and could specifically perform regular —at least once a day— valuations of the asset, trigger netting, clearing and settlement processes between the participating members, and initiate the exchange of supplementary collateral as needed. Specifically, collateral posting shall be provided either by escrowing cash on an interoperable cash ledger or through the allocation of assets on interconnected asset ledgers.[64] Reporting and recordkeeping shall be executed simultaneously and more securely, as the ledger shall provide for a permanent record in separate nodes, making disruptions far more difficult, if not impossible, and the system immune to possible cyberattacks. At the same time, this will open the door to real-time monitoring by regulators and automatically prohibit surpassing legal limits or restrictions. Compression shall be performed automatically as well, in prearranged intervals, which may be as short as desired, whereas reconciliation between counterparties is by definition unnecessary in DLT, as the valuations shall be executed instantaneously through smart contracts in order to trigger the respective margin calculations.[65] And, as the smart contracts have the additional ability of escrowing cash or other assets, they can enable "a fully autonomous and disintermediated contract."[66]

---

[64] de Velde (n56)

[65] Jenny Cieplak and Mike Gill, 'How Distributed Ledgers Impact Post-Trade in a Dodd-Frank World' *Coindesk* (9 July 2016) <http://www.coindesk.com/distributed-ledger-cftc-post-trade-dodd-frank> accessed 28 June 2017

[66] Shayan Eskandari et al., 'On the Feasibility of Decentralized Derivatives Markets' <https://bitaccess.co/pdfs/Bitaccess_research_Velocity_On_the_feasibility_of_decentralized_derivatives_markets.pdf> accessed 22 July 2017

For instance, Stark considers the case of a call option, whereby Alice buys from Bob a smart options contract to purchase 100 shares of Acme Inc. at $50 per share before a certain expiry date. The code of the contract will first attribute the following denominations:

- Strike Price = $50
- Holder = Alice
- Seller = Bob
- Asset = 100 shares of Acme Inc
- Expiry Date = August 16th, 2017

Then, at any date before the expiry date, the holder (Alice) shall be able to exercise her option, only by sending an (usually) encrypted message, if the following prerequisites of the code are satisfied:

- If Message Sender = Holder **and**
- If Sending Date < Expiry Date

Provided that both these preconditions are true, then automatically $5000 will be sent to the Seller and the Asset will be received by the Holder. If, on the other hand, one of them is not true, then the smart contract shall not allow any exchange of cash or assets. Of course, it almost goes without saying, that this is the simplest case scenario, whilst in fact a smart derivatives contract should be tested against any set of possible outcomes and inputs, in order to translate them in the encoded language of the smart contract, and have all different outcomes automated and self-executable, exactly in analogy to software developers, who will test the code results to predict all the possible ramifications.[67]

Benefits of Deploying DLTs in Derivatives Markets

The adoption of these technologies in the derivatives markets would bring along a host of benefits that EMIR in the EU and Dodd-Frank in the US have failed to achieve for almost a decade now. First of all, the basic limitations of the current system will be overcome, as DLT provides the possibility of a single "golden" record, instead of multiple perspectives of the truth, which lead to the rise of several disputes. It also

[67] Josh Stark, 'How Close are Smart Contracts to Impacting Real-World Law?' (2016) <https://www.coindesk.com/blockchain-smarts-contracts-real-world-law> accessed 27 July 2017

addresses the vulnerability of existing infrastructure to technology threats, the current system's extreme complexity, and its lack of compatibility for the reality of 24/7/365 processing, far more efficiently.[68]

What is more, DLT can accelerate the clearing – netting – settlement processes, by making them automated and simplified, simultaneously reducing counterparty risk, since the possible outcomes of each transaction would be explicitly prearranged in order to perform execution orders in the code of the smart contracts. In addition, the cash exchange transactions from a derivative contract could be settled almost in real-time, i.e. as soon as the validation is completed, along with the creation of an immutable record of the ownership of transferred assets. Consequently, clearing can be shortened down to minutes or even seconds.[69] Thus, the whole process becomes not only more efficient but error-free, since human interventions are restricted to the minimum, bringing about huge cost reductions. Netting may be also performed automatically after the completion of each transaction, leaving no doubt as to the open positions of the market participants at any given time. Furthermore, the automation of compression and the redundancy of reconciliation in DLT will further increase speed and efficiency and reduce operational costs —including compliance burdens— for the counterparties.[70] All in all, it is estimated that blockchain technology could alleviate financial institutions from the burdens of the post-crisis regulatory framework up to an amount of $20 billion annually.[71]

As a consequence, the above will inextricably lead to reduced counterparty risk, as the exposure to longer settlement time spans will be significantly reduced and, in addition, the parties have at their disposal richly detailed transaction and counterparty history before the closing of any deal. Simultaneously, the shortening of time —through real-time netting and settlement— for collateral retention and margin

[68] DTCC, 'Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape' (2016 Whitepaper) <https://www.finextra.com/finextra-downloads/newsdocs/embracing%20disruption%20white%20paper_final_jan-16.pdf> accessed 29 July 2017

[69] de Velde (n56)

[70] Mills (n58)

[71] Kurt Fanning and David Centers, 'Blockchain and Its Coming Impact on Financial Services' (2016) 27 (5) Journal of Corporate Accounting & Finance 53

calculation, and the subsequent release of assets to be used in further transactions, shall ameliorate collateral management and advance market liquidity.[72]

Even more beneficial is the fact that due to the distributed and shared character of the ledger, all the above is achieved in a far more secure environment, which is resilient to cyber-attacks and immune to system disruptions. This is because of the numerous existing nodes of the ledger, where the failure of one or even a number of them cannot affect the records, and where a cyber-attack will require the control of at least 2/3 of the entirety of the nodes, rendering it virtually impossible. The traceability of every single transaction, the multiple validation mechanism leading to extreme accuracy, and the equivalent reliability on the records enhanced by the use of efficient encryption methods,[73] all make DLT the ideal way forward for the reform of derivatives markets.

Nevertheless, what might prove to be the most important advantage of deploying DLT in derivatives markets is the long sought-after, but never achieved, wide and efficient oversight by the regulatory authorities. DLT makes not only automatic reporting and recordkeeping of all the details of each transaction possible, but regulators have the opportunity of monitoring the market through real-time access using their clearance passes. This includes the ability to monitor, at any given time, not only the notional values of the transactions, but also the adjusted values after clearing and compression, giving regulators a far less distorted picture of the markets. As ISDA has reported, the increase of 8,9% during the first semester of 2016 in outstanding volumes in the derivatives markets detailed by the Bank of International Settlements, is in fact estimated to amount to a mere 5,5% after it is adjusted for clearing and compression.[74] Additionally, DLT provides the regulators with a clear image of the net exposures of the participants in the ledger, enhancing financial stability through a programmable economy, where participants are not allowed to

---

[72] ESMA, 'Report: The Distributed Ledger Technology Applied to Securities Markets' (2017) <https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf> accessed 22 July 2017

[73] Taketoshi Mori, 'Financial Technology: Blockchain and Securities Settlement' (2016) 8 (3) Journal of Securities Operations & Custody 208

[74] ISDA, 'IDSA Research Note: Derivatives Market Analysis: Interest Rate Derivatives' (2016) <http://www2.isda.org/attachment/OTA2NQ==/OTC%20Derivatives%20Market%20Analysis%20-%20DEC%202016%20-%20V3.pdf> accessed 12 January 2017

assume greater risks than what they can handle, fraudulent activities are prevented or promptly restricted, and the regulator can intervene in a timely manner much more easily and reverse accumulating imbalances that might pose systemic risks. Simultaneously, the governance and compliance costs of the participants are significantly reduced.[75] Enhanced surveillance could induce beneficial outcomes to physical markets as well, through the combination of traceable audits of both the derivatives transactions and their underlying commodities with satellite imaging and monitoring sensors. As such, this can enable the timely spotting of systemic market developments causing extreme risk and the manipulative behavior of any participant in the commodities markets.[76]

Finally, the dynamism of electronic technologies, as previously proved by the wide and sweeping expansion of the Internet, might be able to overcome the harmonisation and globalisation hurdles that regulation has faced in the post-crisis years. As such, they might spur uniformly regulated interconnected networks, with uniform, non-duplicative legal reporting and recordkeeping. Commissioner Christopher Giancarlo admits that in 2008, regulators had to use primitive methods, like telephoning brokerage firms to find out the extent of Lehman's exposure; if they had "viewed a real-time distributed ledger… they may have been able to recognize anomalies in market-wide trade activity and diverging counterparty exposures indicating heightened risk of bank failure."[77] Furthermore, he states that with DLT, the regulatory interference would not only have been prompter and more efficient, but that in the (more unlikely due to real-time monitoring) event of Lehman's failure, its counterparties would have been saved years of litigation, as the settlement of Lehman's positions would have been almost instantaneous.[78]

Examples of Early Implementation

[75] UK Government Office for Science (n51).

[76] Henry Engler, 'INTERVIEW: U.S. Derivatives Regulator Engages "Fintech" World Seeking Better Oversight, Compliance' *Reuters* (6 June 2017) <http://www.reuters.com/article/bc-finreg-fintech-oversight-idUSKBN18X20T> accessed 27 July 2017

[77] Christopher Giancarlo, 'If Allowed to Thrive, Blockchain May Finally Give Regulators Transparency' (Keynote address before the Cato Institute, 2016) <http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-14> accessed 25 July 2017

[78] Ibid

The allure of realising the aforementioned benefits has already led many market participants to some early adoption initiatives in their effort to best the competition in what appears to be an inescapable future scenario.

The first announcement of a successful test implementation took place in April 2016, when Axoni, DTCC, Markit, and the Multi-Bank Working Group implemented blockchain technology and smart contracts to manage the post-trade activities for standard North American credit default swaps. The experiment was conducted with 85 structured test cases and achieved a 100% success rate in its management of the entire post-trade lifecycle, in the provision of real-time transparency availability to regulators, along with efficient interoperability with external systems, and ledger resiliency and security, all the while preserving the privacy of the counterparties.[79]

Soon after, in June 2016, ART, Allianz Group, and Nephila Capital announced the successful pilot implementation of blockchain and smart contract innovations for trading natural catastrophe swaps. The pilot project proved efficient enough to accelerate and simplify the whole transaction, with a uniform platform being the base for merging the previously delayed and segregated systems of information flow, accounting, payments, etc., while simultaneously increasing reliability due to reduced human intervention. What is more, the defined parameters of the contract, as embodied in the smart contract code, left no room for doubt or dispute, automatically triggering the next step of the contract when conditions precedent were satisfied, resulting in quick and automated payments, and, subsequently, in greater customer satisfaction.[80]

The Possibility of CCP's Abolishment

The capabilities of the DLT in the derivatives markets, and the successful experiments referenced above, seem to render disintermediation of the markets fully applicable, eliminating the need for intermediaries and the costs they imply.[81] Principally, this occurs because trust and security is established by the technology

[79] DTCC, 'Successful Blockchain Test Completed by Axoni, DTCC, Markit and Multi-Bank Working Group' (2016) <http://www.dtcc.com/news/2016/april/07/successful-blockchain-test-completed> accessed 27 July 2017

[80] Kate Smith, 'Smart Swaps' (2016) 7 Best's Review 72

[81] World Economic Forum & Deloitte (n64).

itself, which efficiently addresses the problem of double-spending, making the presence of a trusted third party seem redundant. [82]

Consequently, in a DLT framework, the central counterparty could be totally replaced by a consortium of clearing members forming a distributed clearing house. Clearing, netting, and settlement would be purely bilateral, but with advanced safety nets that would be fully automated and self-executing via the implementation of smart contracts. Such safety nets would be combined with the condition of pre-funding, according to which any cash or other type of collateral that may be traded must pre-exist in escrow. All of the other back-office or post-trade functions would be executed either in the same network or via its interconnectivity with other ledgers.[83] For instance, the exchange of collateral could be performed through the automatic transfer of cash or assets held in escrow in separate ledgers that are interoperable with the main one. The total replacement of the central counterparty will not cause any problem to the transparency of transactions and regulatory oversight either, due to the technological features of the DLT, which have been analysed above.

On the other hand, there is a possibility that the above model is not feasible, or at least not yet. The failed experiment of Velocity, which was an ambitious plan for the creation of an autonomous, open source platform for derivatives, demonstrated the project's difficulty in implementation. As theorized in the project's white paper, their customers would be able "to buy and hold collar options contracts which are issued and settled autonomously".[84] Nevertheless, the project faced practical problems that trounced their expectations: the price feed, which should be done "in a fully decentralized trustless way to prevent fraud and market manipulation by the feed provider," is not plausible yet, as all the current solutions "have a central point that can manipulate data, it is either the exchange API or the component responsible to publish the price."[85] In addition, the fact that smart contract technology is still in the

---

[82] Trevor Kiviat, 'Beyond Bitcoin: Issues in Regulating Blockchain Transactions' (2015) 65 (3) Duke Law Journal 568

[83] Hossein Kakavand, Nicolette Kost De Sevres and Bart Chilton, 'The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies' (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251> accessed 23 February 2017

[84] Vignesh Sundaresan and Daniel Cawrey, 'Velocity: An Autonomous, Open Source Platform for Derivatives (Whitepaper)' <https://bravenewcoin.com/assets/Whitepapers/velocity-whitepaper.pdf> accessed 22 July 2017

[85] Eskandari (n67)

proof of concept stage, and the barriers for people to possess the necessary crypto-currency to work with relevant systems, pose additional hurdles towards having such a revolution succeed.[86]

CHAPTER IV – CHALLENGES, RISKS AND SUGGESTED TECHNICAL AND REGULATORY SOLUTIONS

Apart from the reported barriers that have been observed in practice, some suggest that DLT may pose a series of other challenges or risks that dictate a more careful consideration of its use and the postponement of its implementation in a $700 trillion plus derivatives market. On the other hand, others submit that some alleged risks are the result of pure exaggeration and others are manageable either through technical or regulatory actions.

Legal and Technical Code

Prior to any analysis, it is useful to refer to Lawrence Lessig's argument that in a digital environment, both the legal and the computer code, comprising of legal provisions and software/hardware respectively, regulate activity, which means that the impact of both of them has to be considered when constructing a theory of regulation.[87] One core difference between these two is that compliance to the legal code is managed via the provision of consequences in case of infringement, whereas the technical code is self-executory, meaning that compliance is achieved via the operation itself, as the installed software will not allow for any activity outside the pre-programmed framework.[88]

Although the current financial system is already sufficiently digitalised, its governance is primarily pursued by producing and amending the legal code, either through private or public rule-making. On the other hand, distributed ledgers have been functioning so far mainly without any external rule-making interventions, but rather purely in accordance with the provisions and within the limitations set by their intrinsic technical code. Nevertheless, it is self-evident that their wider expansion or

---

[86] Ibid

[87] Lawrence Lessig, *Code and Other Laws of Cyberspace, Version 2.0* (2nd Edition, Basic Books 2006)

[88] UK Government Office for Science (n51)

their implementation in the gargantuan scale necessary for the handling of the derivatives markets, where much broader and extremely crucial interests are involved, shall render their regulation essential, in order to fortify them against systemic and other risks or market failures.[89] Thus, especially if the central counterparty will be gradually rendered obsolete, these ledgers will have to function under a combination of the most robust, resilient, and efficient internal technical code, along with public regulation of ledger activity that takes into account technical code and its intrinsic features, benefits, and risks.

Technology Related Challenges & Operational Risks and How to Address Them

Considering the size of the derivatives markets, some argue that the deployment of DLT can only be gradual, making the manifestation of its benefits totally dependent upon its widespread adoption, where market participants will be progressively persuaded by the success that other derivatives players enjoy in a DLT environment.[90] In my opinion, this reservation is unjustified, since consecutive successful initiatives, and the announcements of others to come, have already demonstrated the substantial interest of market participants for these technologies, the realisation of their huge potential, and the strong intent towards their adoption. It may be useful to remember that the same reservations were expressed at the dawn of the internet revolution.

In addition, due to the stepwise adoption of DLT, some claim that lack of interoperability of distributed ledgers with legacy systems, and with each other, shall pose further obstacles to their widespread adoption, along with the fear that their capacity or scalability might prove to be insufficient to support the tremendous volumes of everyday transactions that are completed in the derivatives markets.[91] These fears also seem to be unfounded, as they rely on a false perception: they mistake the technical capabilities of ledgers such as Bitcoin, which began as a small scale experiment with totally different aspirations, and try to adjust them to the financial markets. Nevertheless, technology has evolved so much since 2009 and

[89] Ibid
[90] ESMA, Report 2017 (n73)
[91] Ibid

progresses at an exponential pace, so that the minor challenges that yet exist to a DLT-based system are at the same level —if not even a better one— with the ones faced by central digitised current systems. This view additionally disregards the fact that derivatives markets are already digitised enough, which will indeed facilitate the interoperability with any innovative computer based systems. In fact, OTC derivatives markets are considered to be much more decentralised systems with long settlement times, which would be "significantly improved using a DLT-based platform if they could be integrated with a core wholesale payment system, resulting in the transfer of cash payments using central bank money."[92] In any case, the fast-improving APIs, when they are standards-based and combine interoperability protocols, may bridge successfully emerging and legacy systems.[93] Alternatively, a combination of solutions is plausible, such as the one adopted in Project Jasper, whereby the validation function is performed by the parties to the transaction, confirming its details, and the uniqueness function is managed by a notary, in this case the Bank of Canada, which —having unlimited access to the ledger— is responsible for verifying the availability of funds.[94]

Another related issue is the ability of the ledgers to provide Delivery versus Payment settlement with the use of central bank money[95] or —to generalise even more— their competence of control of real assets, using smart contracts, without physically securing them. This is a manageable concern as well, since already in cryptocurrency ledgers there have been models or interconnected ledgers that transform cryptocurrencies into central bank money, creating an equivalent to a DvP system, and there is even the alternative of enabling fully digitised assets, which will be owned and transferred through the control of cryptographic keys.[96]

One more feature of distributed ledgers that is considered to be problematic is that they are append-only databases; in other words, after the records of the transactions are created and validated, they become immutable.[97] And, although this in fact

[92] Chapman (n62)
[93] Mills (n58)
[94] Chapman (n62)
[95] ESMA, Report 2017 (n73)
[96] Stark (n68)
[97] Ibid

enhances their security and resilience, it is true that financial transactions may need to be modified, cancelled, or revoked in some instances, due to operational or other mistakes. There is already an effort to invent and apply recourse mechanisms, but it should be intensified to allow greater expansion.[98]

In addition, ESMA attributes a so-called cyber risk to DLT, reasoning that since the technology is at an early stage, there is a possibility of "cracking" the encryption algorithms, that other technical developments may render DLT irrelevant in the future, and that the security of the DLT depends on its 'weakest link'.[99] These arguments are somewhat exaggerated, and linked to a tendency to confront and fear technology which is incomprehensible to the majority of people, and especially regulators, generally with undue suspicion, and without acknowledging the tremendous advances in cybersecurity in the last few years. To be fearsome of technology results only in the deprivation of its benefits and the hindering of evolution, especially if these reservations are not specific and well-founded. One cannot block development by claiming that there is a possibility of infringing cryptographic methods that have been tamper-proof since the 1990s. One cannot dread the danger of the weakest link in a system which is inherently protected from targeted attacks due to its distributive nature rather than in a centralised one. Black swans, random misfortunes, or meteorites capable to destruct a whole continent are always possible, but these are never assumed as valid reasons to delay progress.

Other acclaimed technology risks, such as the safekeeping of digital keys, will not be analyzed in this paper, as I do not even think that they could be construed as such, since such alleged risks are inherent in any form of possession, e.g. even physical ownership of assets, and thereby innate in all transactions or simple course of actions. Consequently, they are not in fact attributable to DLT itself, but to trading in general. The same goes for software common threats, such as bugs and viruses, that are already existent in the digital maintenance of derivatives records. This is even more true for distributed ledgers, that, as shown before, present greater assurances of safety than current centralised systems.

---

[98] ESMA, Report 2017 (n73)
[99] Ibid 10-11

This does not mean, of course, that there are no unresolved security or technical issues, such as the so-called "Re-entrance Vulnerability" spotted in the DAO case, a renowned case of attack, or other sets of denial of service attacks, such as the "Mishandled Exceptions."[100] But the latest estimates say that technology only restricts the adoption of DLT in derivatives markets at a rate of 20%, with most problems being immediately resolvable, whereas the biggest obstacles lay with the inability of regulators and the markets to comprehend and cooperate efficiently with the technology experts.[101] In any case, as in the case of the internet, the development of technology will find its way through efficiency in technical coding, and of course it bears stressing that no system is absolutely secure. Therefore, we should always keep in mind that the goal is to have a more secure and efficient system than the current one, not perfection.

Market Related Challenges & Risks and How to Address Them

Another point of consideration is generally the fact that derivatives markets have been operating for decades under certain standards and practices and the implementation of new techniques might collide with them.

As mentioned above, one of the most attractive reasons for deploying DLT in derivatives markets is the ability for near real-time clearing, netting, and settlement. This would then inextricably lead to the automated calculation of margins, self-executing exchange of collateral, and so on. Some claim, however, that the current longer settlement periods have nothing to do with the incompetence of the existent methods, but are exclusively linked to the inability of the markets to support such a model. This owes to the fact that at the time of the trade, counterparties in fact may not possess the cash or assets necessary, and need the T+2 or T+3 days of the settlement to sort it out. Additionally, accounting and management reporting will possibly encounter problems depicting offsets of near real-time settlement, instead

[100] Eskandari (n67)
[101] Mori (n74)

of daily ones.[102] On the other hand, the implementation of DLT in derivatives transactions does not necessarily mean that settlement should take place in near real-time, as this is a condition that can be negotiated and embodied in the smart contract, adopting, if the parties so desire, the current settlement timeframes. There could also be a transition period to move on from the current system to a near real-time settlement one, as it has been done in the past, when settlement times were longer and subsequently shortened. In the meantime, counterparties can harvest the rest of the fruits of a DLT based derivatives market, including the certainty of settlement, the automatic execution of supplementation of collateral, and the rest of the post-trade functions, whilst avoiding failures of transactions owed to collateral or cash not being in place promptly.[103]

Another concern expressed is that since the use of DLT for derivatives transactions will incorporate a series of automated triggers, it might aggravate market downfalls in periods of difficulty and stress. Also, in combination with shorter settlement periods and the facilitation of connectivity between markets and their participants, there may be a severe exacerbation of liquidity and systemic risk.[104] Particularly, in markets where settlement procedures and guarantees were assumed and managed centrally by duly-authorised and regulated intermediaries, their sudden replacement and subsequent lack of guarantees by a trusted party might disrupt the liquidity management of the counterparties, and hence the efficient mitigation of the counterparty credit risk.[105] My perception, however, is that even if there is a speck of consistency in these reservations, it concerns only a limited timeframe: until the markets fully transition to the wide implementation of DLT and its structures. In other words, as soon as the diminution of settlement times and the automation of collateral exchange become the norm, market participants will adjust their practices to the new market requirements. This happened in a much larger scale with Dodd-Frank and EMIR, and indeed with greater costs to bear and benefits that accrued solely to the financial system as a whole and not the market participants directly. Such a

[102] Mainelli (n51),
[103] Ibid.
[104] ESMA, Report 2017 (n72).
[105] Missl (n57).

monumental reform would be easier to succeed in the case of DLT, where market participants will have a lot more to gain in terms of cutting down costs and enhancing safeguards against various risks. Consequently, I firmly believe that DLT will essentially result in the rationalisation of the markets, as it will inextricably establish a more prudent management of capital by market participants, who will be obliged to have available funding in the beginning of transactions, and will simultaneously have the right to free up assets sooner than before, thereby being able to handle their liquidity more efficiently.

Legal Challenges & Risks

Finally, there is a set of legal considerations to take into account before adopting DLT, which derive mainly from the fact that blockchain is almost totally unregulated so far, meaning that although derivatives markets are highly regulated, some legal issues that have been definitively resolved over the course of the years may seem to arise again under the mechanisms of the DLT.

First of all, the fact that DLT provides securely maintained records of the transactions performed between the participants, with specific and detailed audit trails, is one of its most inspiring benefits to regulators, as it could automate reporting or real-time monitoring of derivatives markets and indisputable recordkeeping. The problem is, however, that these records need to acquire legal authority to be binding to the parties on the one hand, and submittable to court, tax and other public authorities on the other hand.

Furthermore, there is great controversy about the legal nature and ownership regime of digital tokens in the distributed ledger framework. Tokens are a precondition for each transaction, and they either are issued as such directly, or even constitute the digital representation of physical assets. To have a valid transaction, the ownership of transferrable assets has to be previously clear beyond a doubt.

Similarly, there is a problem with the enforceability of smart contracts, which mainly rely on the automation and self-execution of actions without taking into consideration basic legal doctrines, such as the invalidation of unconscionable

contracts or the alteration of contractual terms in light of changed circumstances.[106] Therefore, it is crucial for the legal community to thoroughly examine smart contracts and determine their legal and evidentiary status.

There is also the issue of ensuring definite legal settlement finality in a distributed ledger, where the finality of settlements is probabilistic, meaning that the longer a transaction is considered settled by the respective nodes of the network, the less likely it becomes to be reversed.[107] It is obvious, though, that loose ends of this sort are unacceptable in legal transactions, especially when they are concerning agreements of billions of dollars, and should thus be specifically regulated.

Additionally, governance issues will need to be addressed in order to facilitate the shift from networks organised around trusted parties to distributed ones, ensuring that further provisions will be implemented concerning participation in permissioned ledgers, levels of clearance, licensing of participants, as well as the definition of responsibilities towards system maintenance and the stipulation of the circumstances that could lead to amendments of the ledgers and their protocols.[108] An interrelated issue is the privacy protection of participants, the safeguarding of which is a sine qua non requirement in the financial markets, especially for avoiding unfair competition or market manipulation conduct.[109] It requires special attention due to the fully transparent nature of distributed ledgers.

The above mentioned legal risks may be addressed either contractually or through regulation. In fact, this is the pattern that legal challenges are resolved anyway, as usually the legislature displays slower reflexes towards pending legal considerations. This approach might prove to be more efficient in a digital environment, because it would avoid any unnecessary hindrance in efficiently transforming the derivatives markets.

Addressing Legal Risks. Is Regulation in order?

[106] Mills (n57).
[107] Ibid.
[108] Ibid.
[109] ESMA, Report 2017 (n72).

As it has been aptly argued, "virtually all wholesale financial services are regulated."[110] In other words, since market participants and the transactions of derivatives are exhaustively regulated concerning clearing, netting, settlement, trade venues, etc., it is advisable to exercise caution before burdening the industry with further provisions to address the execution of derivatives transactions in distributed ledgers.

It is important to regulate in a timely fashion to avoid having innovators see their efforts go to waste or to impede the adoption of a beneficial technological innovation. The example of e-banking, which pre-existed 20 years before its proper regulation, is quite an informative one.[111] The emergence of DLT is so recent that it is transforming constantly, as networks and markets realize its potential and try to configure its technical code to suit the needs of the markets. It would be premature to regulate it before things settle down and there is evidence of its wider adoption.[112]

For the time being, a thorough examination is necessary to ascertain if DLT can be implemented with the existing provisions of law or structured in ways compatible to it, to avoid the creation of a new regulatory regime which may quickly become obsolete due to the emergence of new technology.[113] Simultaneously, already existing regulation such as MiFID II, which states that upon its implementation all trading platforms in Virtual Currency derivatives which constitute financial instruments shall be authorised,[114] should be reappraised with the assistance of technical experts, to determine its suitability or need for revision.

Nevertheless, when the time is right, regulators should be technologically neutral and focus on the desired outcome of a technology.[115] A wait-and-see approach is the ideal one, combined with the do-no-harm approach that was successfully implemented with the regulation of e-commerce.[116] The UK "sandbox" regulatory

---

[110] Mainelli (n52)
[111] Arner (n50)
[112] Ibid
[113] Thomas Keijser, 'Financial Collateral Arrangements in the European Union: current state and the way forward' (2017) 22 (1) Uniform Law Review 258
[114] Mark Kalderon, Ferdisha Snagg and Claire Harrop, 'Distributed ledgers: a future in financial services?' 31 (5) Journal of International Banking Law and Regulation 243
[115] Arner (n50)
[116] Harold Primm, 'Regulating the Blockchain Revolution: A Financial Industry Transformation' (2016) 36 (1) Review of Banking and Financial Law 75.

regime would be extremely helpful, as well, as it provides for a safe environment to address issues that indeed arise in practice, with the active contribution of regulators, business, and technological experts, achieving the best equilibrium possible between their positions and interests. It is even advisable to estimate the necessity of certain aspects of existing infrastructures and legislation of derivatives markets in the DLT framework, so as to minimize existing exhaustive interventions and simplify the regulatory regime, taking into account the intrinsic guarantees of a distributed ledger infrastructure, due to which the penalties for actions that a smart contract would automatically block will become superfluous.

In the meantime, private players will lead the way, by contractually predicting and resolving system malfunctions during the transitional period in which derivatives transactions move to the blockchain, as experience has shown with other technological initiatives, such as cloud services, electronic bills of lading, etc. The challenge to the regulators and the various industry organizations is to align these private initiatives with appropriate common standards, set by the competent organizations (IOSCO, FSB, etc.), on certain design points, technical aspects, business practices, and legal rules of the ledgers.[117]

Finally, underlying the success of this entire process is the need for international regulatory coordination,[118] both in terms of soft law and in mandatory provisions should be fundamentally prioritized, as the main characteristic of DLT and modern technology is the globalisation of markets. Consequently, lack of its consideration shall immediately render any regulatory attempt irrelevant and obsolete.

CONCLUSION

Derivatives have been a feature of the financial markets since at least 1972, when the first financial futures contract was introduced by the Chicago Mercantile Exchange, although futures markets in agricultural commodities and metals have existed since the mid-19th century. However, the foundation of the modern derivatives market began in 1981, with a currency swap between the World Bank and

[117] de Velde (n56)
[118] Giancarlo (n79)

IBM, after which the growth of derivatives took off and has not stopped since, reaching figures of hundreds of trillions of dollars before the global financial crisis a decade ago.

Even though they were blamed for immensely exacerbating the crisis,and were subsequently targeted by legislative efforts that resulted in an exhaustive, complex and still evolving regulatory framework, the derivatives markets never ceased to expand in size and modalities.

Nowadays, the challenge is to deploy distributed ledger technology, at the very least in post-trade procedures, where the burdens for market participants in terms of cost and effort have been immensely multiplied by post-crisis legislation. The potential of blockchain technology is already obvious, but as always there are adverse risks that should be handled beforehand to safeguard from any unpleasant surprises, especially since their manifestation in a system that handles a multitrillion dollar market could possibly lead into a new, more intense financial crisis.

However, considering that the dynamic of progress cannot be withheld, specifically since DLT offers a real prospect for the absolute unification and globalisation of derivatives markets, cooperation between technology experts and regulators is indispensable to deploy the full benefits of the new technology in derivatives markets and dispose of the numerous flaws of the current infrastructures once and for all. UK's "sandbox" example should lead the way in the effort of promptly and appropriately regulating the transition of derivatives markets to distributed ledgers, whereas global cooperation is also essential, especially considering the 2019 completion of BREXIT, as UK is one of the most significant derivatives hubs. This geographical separation of the markets will emphatically dictate the need for the immediate deployment of a purely global technology, such as DLT, even sooner than anticipated, and by then it will be an indispensable requirement to have the essential infrastructures and frameworks for its undisturbed function already in place.

Finally, in the course of regulatory transformation it is crucial to consider the innovative application of technology to regulation itself, the so-called RegTech, in order to achieve the best possible granularity in risk assessment, and the ideal outcome in regulatory oversight, all without obstructing technological

breakthroughs.[119] As Andy Haldane, Chief Economist of Bank of England, put it when articulating his vision of a data-led regulatory system:

> I have a dream. It is futuristic, but realistic. It involves a Star Trek chair and a bank of monitors. It would involve tracking the global flow of funds in close to real time (from a Star Trek chair using a bank of monitors), in much the same way as happens with global weather systems and global internet traffic.[120]

[119] Arner (n50)

[120] Andy Haldane, 'Managing Global Finance as a System' (Speech at the Maxwell Fry Annual Global Finance Lecture, 2014) <http://www.bankofengland.co.uk/publications/Documents/speeches/2014/speech772.pdf> accessed 5 August 2017