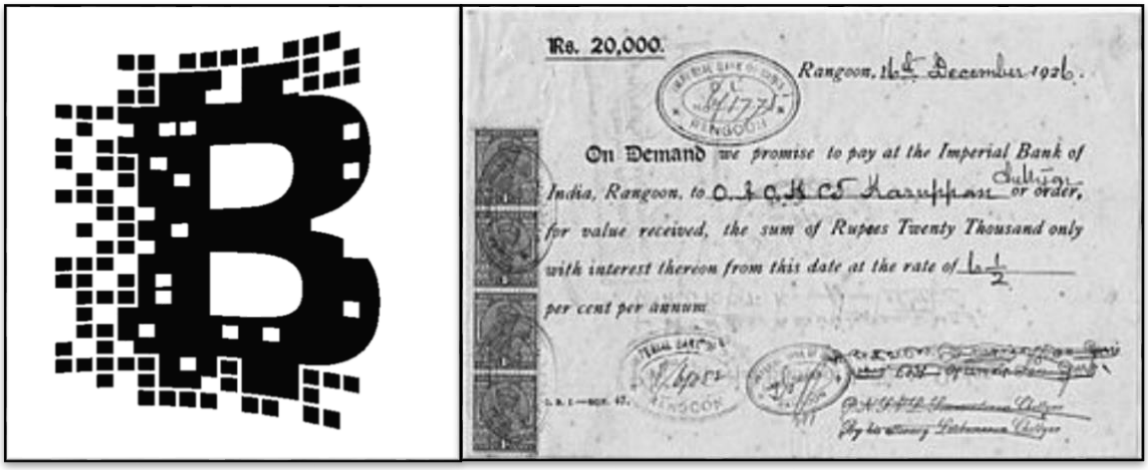
Redefining Negotiable Instruments with Blockchain: Modernisation through Digitalisation

A study analysing the technical and legal compatibility of Blockchain-based negotiable instruments with digital ecosystem, UNCITRAL legislations and payment system environment



LL.M. Thesis by Levent Aslan

Supervised by Ivona Skultetyova

ANR: 754954

Table of Contents

Introduction **3**

1 Negotiable Instruments **5**

1.1 A Short History of Negotiable Instruments **5**

1.2 Main Principles and Functions of Negotiable Instruments **8**

1.3 Fall of Negotiable Instruments **11**

1.3.1 Regulatory Environment 11

1.3.2 Financial Environment 12

2 Blockchain **15**

2.1 Main Attributes of Blockchain **15**

2.1.1 Distributed database 15

2.1.2 Peer-to-peer transmission 15

2.1.3 Transparency with pseudonymity 16

2.1.4 Irreversibility of records 16

2.1.5 Computational logic 16

2.2 Main Operations of Blockchain **16**

2.2.1 Data storage & security 16

2.2.2 Consensus algorithms 18

2.2.3 Privacy 19

2.3 Types of Blockchain **20**

2.4 Blockchain's Role in Banking System **21**

2.5 Challenges for the implementation and use of Blockchain **22**

3 Compatibility of Blockchain with Negotiable Instruments **25**

3.1 Technical Compatibility **25**

3.1.1 Creation of Negotiable Instruments 26

3.1.2 Validation of Negotiable Instruments 26

3.1.3 Governance of Blockchain 29

3.1.4 Endorsements 30

3.1.5 Identification 33

3.2 Legal Compatibility **34**

3.2.1 Scope of Applications 36

3.2.2 Functional Equivalency of Data Message / Electronic Record to Paper Instrument 38

3.2.3 Functional Equivalency of Electronic Record to Negotiable Instrument 41

3.2.4 Interpreting Blockchain as a platform 47

Conclusion **49**

Bibliography **51**

Introduction

Throughout our history as humankind, we constantly thrived for new technologies to make our lives more developed and efficient. We created technologies that redefine the ecosystems they were built for, and sometimes even redefine the centuries they were built in. The end of 20th century and the very beginning of 21st century were defined by Internet, with its various applications transforming different aspects of certain fields like finance, media, business etc. With a new technology, Blockchain, becoming a serious candidate to define the rest of the 21st century, its enthusiasts' research intensifies around the possible native applications that would increase the development speed in different fields. As the legal field has been comparatively slow-paced, it particularly needs such acceleration of development to accommodate advances in artificial intelligence and machine-learning technology (The Law Society, 2016).

Smart contract is one attempt to revitalise law which uses modern technology like Blockchain, yet "LegalTech" has the potential to widen even further and become mainstream. However, current smart contract structure has limited applicability and serious concern about its legal compatibility. Complexities of both legislations on contract law and smart contract structures necessitate legislative restoration and further technological development to reach mainstream applicability of smart contracts. In the meantime, an actual regulative response to smart contract can be taken only for specific forms of contracts. A legal institution that would benefit from its introduction to LegalTech and smart contracts is negotiable instruments, which are defined as "*documents that contain a guarantee or promise to pay a specific amount of money to a person or entity in possession of the instrument, whether on a specified date or on demand*". Although heavily regulated, even the most popular negotiable instrument, check, has become an outdated payment method which cannot compete with other, digital-based payment systems.

Buckminster Fuller once said: *"You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete".* Negotiable instruments will eventually have to go through a comprehensive reform, or follow Fuller's advice to an overhaul to sustain its relevancy. My research question is to what extent could the implementation of the Blockchain infrastructure into negotiable instruments mitigate their fundamental flaws and revive their use in business practice. Blockchain, as a new "value exchange" network, can offer what current models of negotiable instruments and its modern substitutes do while adding new features and improving the existing ones. There may be some scepticism towards this model as some argue Blockchain has been overhyped and does not

validate its "century-defining" title[1]. Indeed, transforming current negotiable instruments' system with a complete adaptation to Blockchain technology would be illogical and inefficient as certain attributes of Blockchain and negotiable instruments do not mesh. However, an adaptation with modifications in both Blockchain's technology and negotiable instruments' law has the potential to become a sustainable, efficient and accessible model. Modernisation of negotiable instruments through Blockchain can also be a two-way street: in addition to making negotiable instruments relevant again, this can also become a pioneer example on how to regulate Blockchain and its applications.

First chapter will be dedicated to a brief introduction of negotiable instruments system – its history, main principles and functions – with a closer look on the reasons behind its demise as the leading payment system it once was. Understanding negotiable instruments and especially their purpose is vital for configuring the extent of its compatibility with Blockchain.

Second chapter will deal with Blockchain technology and elaborate on its characteristics to offer a brief, yet in-depth insight on how Blockchain works. Since a separate paper or even a book can be (and were by many) written solely on Blockchain, this chapter focuses on certain attributes that complements or hinders the compatibility with negotiable instruments system without going into über-technical details.

Third chapter, subsequently, will consist the optimistic attempt to model the "Negotiable Instruments 2.0" while discovering the ways this modelling uniquely offers – or has the potential to offer - that eliminates the current problems faced by the entirety of payment systems. After the modelling process, which aims to sustain technical compatibility of Blockchain technology with negotiable instruments, the legal compatibility of the created system with concerning UNCITRAL legal instruments will be analysed.

[1]Kai Stinchcombe, 'Blockchain is not only crappy technology but a bad vision for the future' (Medium, 5 April 2018)

1 Negotiable Instruments

Before the invention of money, barter economy was the norm with the basis mechanism of commodity exchanges. Each combination of commodities required a different exchange ratio to produce just results for transacting parties, and determination of each exchange ratio necessitated the consideration of various factors unique for each commodity and combination. Due to these attributes earlier economies had a limited potential and weren't suitable for complex transactions, which required an intermediary "medium" that eliminated the bartering and its exchange mechanism: Money. Defined by Harari as *"anything that people are willing to use in order to represent systematically the value of other things for the purpose of exchanging goods and services"*[2], money was the medium that converted, stored and transported "value" cheaply and easily, allowing commercial markets and networks to get exponentially bigger while offering more dynamic and efficient transactions.

Following Harari's definition, money's earlier versions before the invention of coinage include barley, salt, cattle and even one of the currently existing negotiable instruments, "promissory notes". The fact that in former times promissory notes – and other negotiable instruments - were used as money profoundly influenced their governing law as well[3]. Thus, to fully understand the current negotiable instrument system alongside some of its attributes that may seem as out-of-place and/or meaningless, and to have a healthy trajectory of future development, acknowledging the historical progress of negotiable instruments is indispensable.

1.1 A Short History of Negotiable Instruments

Throughout their history negotiable instruments have coexisted with money and served specific needs. First prototypes of negotiable instruments date back to ancient times around 17th century BC as Babylonians had documents with debt obligations stated on them named as *hudu*[4]. Ancient Greeks used legal instruments similar to medieval European bills of exchange in 400 BC[5] and check payments were already widespread as early as 100 BC[6].

[2] Yuval Noah Harari, Sapiens: A Brief History of Humankind (Penguin Random House 2011) 197
[3] J. Rogers, The End of Negotiable Instruments: Bringing Payment Systems Law Out of the Past, (Oxford University Press 2011) 32
[4] Sergii Moshenskyi, History of the Weksel Bill of Exchange and Promissory Note (New York: Xlibris 2008) 28
[5] ibid 37.
[6] ibid 39.

Around Middle Age it was common for merchants to use bills of exchanges for arranging the payment after distribution of their goods. As an example, assuming a merchant in Bruges had shipped goods to his representative in Venice who had sold them on commission, with Venetian merchant had done the same vice-versa; if amounts gained by agents through sales were equal, accounts could have been settled by Bruges agent pay money to the merchant in Bruges and Venetian agent paying money to Venetian merchant. A bill of exchange allows for such transaction to take place and, in essence, transferring value of any kind between distant locations.

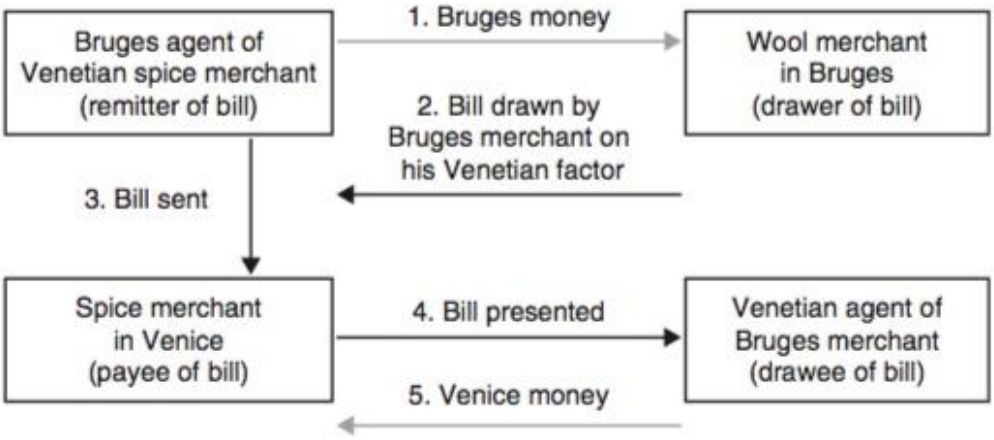


Figure 1: A typical exchange transaction from the late Middle Ages[7]

In 18th century using bank notes for payments were to become a banking standard, as depositing money or taking out a loan resulted in receiving notes issued by the bank, which were basically promissory notes representing bank's promise to pay money to its bearer. Although receiver of such notes could demand payment, as long as people's trust in bank's solvency prevailed, it was much common to use such notes in making payments for other transactions till their retirement from the banking system in 1930s[8].

(A side note: Currently, instead of all commercial banks like in the past, usually one central power – in USA case, Federal Reserve – has the competence to issue bank notes, with exceptions including the UK and the EU[9]. American Dollar, Turkish Lira, Japanese Yen have all in fact notes issued by their respective central powers (US Federal Reserve, Turkish

[7] J. Rogers, The End of Negotiable Instruments: Bringing Payment Systems Law Out of the Past, 25
[8] ibid 33.
[9] K. Scheller Hanspeter, The European Central Bank – History, Role and Functions (European Central Bank 2004) 103-104

Republic Central Bank, Bank of Japan) and their value depends on people's trust in solvency of their issuers. Federal Reserve Bank of Boston's "Putting It Simply" report simplifies the issuance of notes, stating: *"When you or I write a check there must be sufficient funds in our account to cover the check, but when the Federal Reserve writes a check there is no bank deposit on which that check is drawn. When the Federal Reserve writes a check, it is creating money"*[10]. So, in a way, paper money is a form of negotiable instruments – promissory notes - that is perceived and regulated in complete separation from the rest.)

Another type of note circulation was gaining mass-usage starting from the early 19th century, with creditors transferring the mercantile notes and bills - which represented the obligations of debtors - in return for cash rather than waiting until the maturity of debt. This "discounting" of notes lead to the creation of "accommodation bills", instruments appearing to represent genuine mercantile transactions which were, in reality, simply a means of borrowing for the sake of raising money[11]. Subsequently, the practice of raising money through discounting accommodation bills was replaced by the practice of the borrower directly appearing as the person obligated to pay, to prevent irregular denominations – accommodation bills vary in their value – while offering legal clarity and transparency for both borrowers and lenders[12].

During the late 19th century – early 20th century multiple negotiable instruments laws were codified in multiple countries (India's 1882 *Negotiable Instrument Act*, UK's 1882 *Bills of Exchange Act*, Germany's 1933 *Scheckgesetz*) with 1930s witnessing the first attempt to unify the law of negotiable instruments through the Geneva Conventions on the Unification of the Law Relating to Bills of Exchange and Checks. Although many European and South American states in addition to Japan were parties, exclusion of countries including the USA and members of the British Commonwealth prevented the Convention to reach its potential and eventually deemed it ineffective[13].

Technological developments in the area started to gain pace through the patent of a standard for machine-readable characters (MICR) in 1959, which facilitated the automation of clearing process for checks through the automated reader/sorting machines. The subsequent result was the exponential growth of check volumes, and by the late 20th century billions of checks were

[10] Federal Reserve Bank of Boston, Putting It Simply, (1984) 57
[11] J. Rogers, The End of Negotiable Instruments: Bringing Payment Systems Law Out of the Past, 36
[12] ibid 37.
[13] United Nations, 'Progressive Development of the Law of International Trade: Report of the Secretary-General of the United Nations' (Jus UiO, 1966)

processed yearly already, making them the most popular non-cash payment method in the world.

Another attempt at unifying the negotiable instruments' system came within European jurisdiction with the introduction of *Eurocheck* in 1969. Initially designed for international payments with its coverage of multiple currencies and lower cross-border clearing cost, *Eurochecks* - in its apex – were mainly used domestically as international payments rarely accounted for more than 5% of all *Eurocheck* transactions. However, this experimentation also came to an end with *Eurochecks* issuance ceasing in 2002 (Investopedia).

Volume of transactions with checks was in its all-time-high during late 1980s and 1990s, however the rise of electronic payment methods de-popularised checks and their number started to fall. Consequently, mid-1990s saw the first attempt to digitalise checks, which were only paper-based at that time, through laws enabling *check truncation*. By converting checks into electronic form, physical nature of checks was eliminated while their transfer became more efficient and cheap.[14]

1.2 Main Principles and Functions of Negotiable Instruments

A famous definition of negotiable instruments given in an English case back in 19th century exhibits some of the main principles: "*where an instrument is by the custom of trade transferable like cash, by delivery, and is also capable of being sued upon by the person holding it, it is entitled to the name of a negotiable instrument, and the property in it passes to a transferee who has taken it for value and in good faith"*.[15]

One of the core attributes of negotiable instruments, as their name suggests, is the "negotiability". Negotiability usually refers to transferability of an instrument – although transferability and negotiability are two different concepts. Every negotiable instrument is transferable, but not every transferable instrument is negotiable due to the "holder in due course" doctrine. Negotiable instruments are transferred by delivery, but *bonafide* transferee can acquire a better title than the transferor – which is not the case for non-negotiable transferable documents.[16]

[14] Moneycontrol, 'What is Cheque Truncation System' (Moneycontrol, 5 February 2013)
[15] Crouch v. The Credit Foncier of England, Ltd., L.R. 8 Q.B. 374,381 (1873)
[16] D.P. Whiting, The Concept of Negotiability (Macmillan Master Series 1985) 122

Another important principle for negotiable instruments is "reification", the requirement of a sole, original physical representation, with an authentic signature necessary for the birth of rights. Reification principle also suggests the rights can only be transferred through physical delivery, whereas destruction of the instrument is the single way to abolish them[17].

For the most commonly used negotiable instruments, check, transfer requires an endorsement from the holder, which can be accomplished through different methods with each offering certain levels of negotiability[18]. Regardless of the method, each endorsement requires the signature of the holder on the back of the check. After the original endorsement by the drawer, checks usually receive multiple secondary endorsements before being cashed in, which creates a chain of title that can be traced back to previous holders and eventually, the drawer. This traceability is imperative for the enforcement of liability when a check is dishonoured, not paid or not accepted.

The most common, negotiable and least secure endorsement method, blank (also called general) endorsement obligates only the holder's signature; meaning the bearer of a blank-endorsed instrument has full competence to cash or endorse it. Since negotiability and security are inversely proportional, the holder of a check can partially limit the negotiability through restrictive endorsement, by specifying the means the checks can be used for in addition to his/her signature as a safeguard.[19] A common example is "for deposit only", which restricts the negotiation to deposit in a specific account. However, the human element in clearing the negotiable instruments creates possible unwanted consequences as an inattentive teller may fail to properly respond to the restriction or the instrument might be deposited into wrong account.[20]

Another endorsement method, full (also called special) endorsement simply transfers the check from the holder to another party without any negotiability limitation, yet with full restriction on the bearer's identity chosen by the ex-holder. The new holder has full competence to cash or endorse it – like the bearer of a blank-endorsed check.[21]

Apart from limiting negotiability or identity, it is also possible to restrict the liability for an endorser through qualified (also called conditional) endorsement in case check is not paid.

[17] J. Rogers, The End of Negotiable Instruments: Bringing Payment Systems Law Out of the Past, 45
[18] Center for Financial Training, Banking Systems. 2nd ed. ed., (South-Western Cengage Learning, 2010) 160
[19] ibid 161.
[20] ibid 161.
[21] ibid 161.

Mostly used by representatives to transfer checks received from third parties for their clients, qualified endorsements often include a guarantee to pay if person with primary liability fails to, while it is also possible to set certain conditions upon which's realisation liability will rise for the endorser. The conditionality on the finality of the transfer rather than the endorser liability is however ineffective for the endorser and endorsee as well as for the subsequent endorsees.[22]

In general, negotiable instruments have multiple functions: they are substitutes for money and regarded by some as "currency substitutes", while also acting as a credit device with certain forms extending credit from one party to another, and keeping records that are used for financial statements and tax returns.

Statistics on negotiable instrument exhibit the communality of aforementioned functions and certain areas where it still holds the upper-hand over alternative payment systems. Global market size for payments made in checks and cash by small retailers is $19 trillion, whereas only $15 trillion worth of payment were made electronically[23]. In France, a country that is abnormally accounted for 71 percent of all EU checks alone in 2013[24], checks are commonly used for business-to-person (B2P) payments alongside electronic fund transfers thanks to the easier storage of payment records and securer bulk payments for large number of employees[25]. On the other hand, person-to-business (P2B) payments are mostly done through electronic payment methods as they are considered safer by consumers with an avoidance of carrying cash and quicker in comparison to paper-based payments[26]; however, with no setup requirement and percentage fee, checks can be financially favourable to some businesses.

Payment Type Flow	Overall Total Electronic Payments Transaction Value (USD 'M)	Electronic Payments (Value %)	Electronic Payments (Volume %)
P2B	535,407	64%	54%
B2B	369,321	85%	72%
B2P	44,899	78%	n/a

Figure 2: Electronic payments' role under different payment type flows in France[27]

[22] United Nations Convention on International Bills of Exchange and Promissory Notes [1988], Article 18
[23] World Bank Group, Cash vs Electronic Payments in Small Retailing Estimating the Global Size (International Bank for Reconstruction and Development / The World Bank 2016) 3
[24] Committee on Payments and Market Infrastructures, Statistics on payment, clearing and settlement systems in the CPMI countries: Figures for 2015 (Bank for International Settlements 2016)
[25] World Bank Group, Cash vs Electronic Payments in Small Retailing Estimating the Global Size, 54
[26] ibid 51.
[27] ibid 47.

1.3 Fall of Negotiable Instruments

With the birth of alternative payment systems like wire transfers, ACH, PayPal and Apple/Samsung/Android Pay, negotiable instrument started to lose its relevancy. The recent developments on this area that partially automatise and electronise the paper-based process did not realise its potential since the logic behind is still paper-based, according to the former CEO of Citigroup Vikram Pandit.[28] Indeed, negotiable instruments law is constructed on the embodiment of abstract rights in piece of paper, which is physically delivered for the transfer of rights. In addition, one of the aforementioned developments, substitute check system, degraded the paper-based system through the introduction of an accurate representation of Magnetic Ink Character Recognition (MICR) line, in which the essential information of the payer bank's identification, the drawer's account number and the amount is encoded. This information, not the physical object, is the basis of this payment system; making the paper-based check largely irrelevant.[29]

1.3.1 Regulatory Environment

Regulated under Article 3 of Uniform Commercial Code in the US, and under Directive 2014/65/EU and Regulation 600/2014 in the EU, the negotiable instruments law is still locked under nineteenth-century concepts such as negotiability[30], and rules that resembles "beans in your ears" law, the old saying which states it is illogical to tell children not to put beans in their ears, because they would otherwise not even have thought of trying[31]. Modernising the regulatory environment is not an easy task either; for instance, United States' banking system is highly fragmented with over 10000 depositary institutions and thousands of different banks, some of which may be less willing to invest and/or adapt to modernise, with a Federal Reserve that doesn't possess the regulatory power to mandate a change on negotiable instruments.[32] Although banking industry consensually concludes the necessity of total electronisation, even a small percentage of banks unprepared to receive electronic presentments prevents the transition to electronic means of processing payments initiated by negotiable instruments.[33] At

[28] Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, (2016) 149
[29] J. Rogers, The End of Negotiable Instruments: Bringing Payment Systems Law Out of the Past, 60
[30] Steven L. Harris, Introduction to Rethinking Payments Law, 83 Chi.-Kent L. Rev. 477 (2008) 10
[31] J. Rogers, The End of Negotiable Instruments: Bringing Payment Systems Law Out of the Past, 190
[32] Katie Robertson, 'Why Can't Americans Ditch Checks?' (Bloomberg, 26 July 2017)
[33] J. Rogers, The End of Negotiable Instruments: Bringing Payment Systems Law Out of the Past, 61

the same time, the urgency to create a uniform set of rules governing electronic check exchange infrastructure will increase with more banks willing to engage in this business.[34]

The regulative problematics of negotiable instrument law combined with the various alternative payment systems that disrupt the entirety of payment systems' legislative environment necessitate a comprehensive solution. As Harris puts, "t*he increasing use of nonbank payment intermediaries coupled with the uneven regulatory treatment of payment intermediaries in regard to allocation of risk in the processing of payments may be creating unacceptable systemic risk to the soundness and reliability of the various payment mechanisms".*[35] Different jurisdictions adopt different approaches with their regulative responses; United States for instance were historically market-driven, supporting competition between public and private solutions to determine the evolution of different payment systems and the subsequent legal response.[36]

1.3.2 Financial Environment

Data regarding payments with the most commonly used negotiable instrument, check, shows a significant decline in different jurisdictions. In USA, total commercial checks paid decreased by number 3.1 percent a year between 2012 and 2015 to 17.9 billion. In comparison, automated clearing house (ACH) network payments increased by number 4.9 percent to 19.3 billion while card payments increased by number 7.5 percent to a whopping 103.5 billion[37].

One should bear in mind the fact that USA market uses checks much more than the rest of the world - more than half of business-to-business payments are still made by checks[38]. However, 51 percent of respondents to Bank of America's Consumer Mobility Report 2017 found paying via check painful, while 38 percent were annoyed by delayed checks or check that are never cashed. Americans made, on average, 38 check transactions annually whereas the number is 18 for Canada, 8 for UK and almost zero for Germany[39]. There are even more extreme examples, with Finland stopping issuance of checks in 1993, Netherlands in 2002 and Denmark in 2017.

[34] Steven L. Harris, Introduction to Rethinking Payments Law, 19
[35] ibid 11.
[36] Faster Payments Task Force, The U.S. Path to Faster Payments Final Report Part Two: A Call to Action, 27
[37] Federal Reserve Board, The Federal Reserve Payments Study: 2017 Annual Supplement (Federal Reserve System 2017)
[38] Katie Robertson, 'Why Can't Americans Ditch Checks?' (Bloomberg, 26 July 2017)
[39] Committee on Payments and Market Infrastructures, Statistics on payment, clearing and settlement systems in the CPMI countries: Figures for 2015 (Bank for International Settlements 2016)

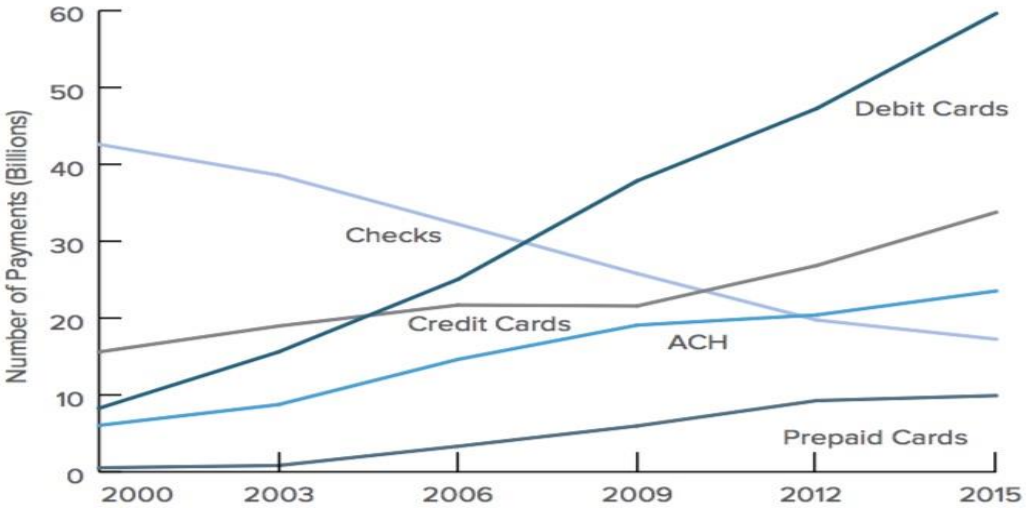


Figure 3: Trends in Non-Cash Retail Payments by Number and Type of Transaction[40]

Common theme in banking industry on checks is that their survival, along with other negotiable instruments, depends on their structural and legal reform[41]. Currently there are different "value transfer system" alternatives, like automated clearing house (ACH) networks and wire transfers that take place in electronical ecosystems.

Structurally, there is room for improvement: A 2014 Federal Reserve study found that "at least 29 billion transactions, or 12 percent of all U.S. payments annually, could benefit from faster authorization, clearing, settlement and/or availability of funds"[42]; meaning beyond negotiable instruments the entirety of current payment system is in need of structural advancement. Indeed, consumers at the bottom of the financial pyramid cannot afford minimum account balances, minimum payment amounts or transaction fees,[43] with approximately 1.7 billion people excluded from the global financial system[44] due to the cost structure. Even with the Internet, the infrastructure costs make micropayments and microaccounts mostly unfeasible.

Person's control over his/her bank account is also a debatable concept. Mougayar argues that banks provide an illusion of access and activity visibility to bank account owners. As banks are the higher authority with their database that points to the entry that states a person has a certain

[40] Faster Payments Task Force, The U.S. Path to Faster Payments Final Report Part One: The Faster Payments Task Force Approach
[41] Steven L. Harris, Introduction to Rethinking Payments Law, 19
[42] Faster Payments Task Force, The U.S. Path to Faster Payments Final Report Part One: The Faster Payments Task Force Approach, 32
[43] Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, (2016) 125
[44] Demirgüç-Kunt, Klapper, Singer, Ansar, Hess, The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution (International Bank for Reconstruction and Development/The World Bank 2018) 4

amount of money, the ownership is only an illusion; which is also the case for moving money, pay someone or deposit money, where bank is providing explicit access to the person that gave his implicit trust over his/her affairs.[45]

[45] Mougayar, William, Buterin. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, (John Wiley & Sons, Incorporated, 2016) 62-63

2 Blockchain

First mention of Blockchain was in Satoshi Nakamoto's whitepaper[46] for Bitcoin in 2008, coincidentally(?) around the same time the global financial crisis occurred. Blockchain can be defined as "*a distributed, public, time-stamped asset ledger that keeps track of every transaction ever processed on its network, allowing a user's computer to verify the validity of each transaction such that there can never be any double-counting".*[47] Originally designed to propose an alternative value storage and medium of exchange system, this technology was subjected to various applications in separate fields since.

2.1 Main Attributes of Blockchain

2.1.1 Distributed database

Entire database and its complete history is accessible to all parties of Blockchain, with no singular control over the data. An intermediary is unnecessary as all parties can verify the records directly.[48] Blockchain's decentralised virtual network allows each "node" (user) to record transactions on a public "block", with each successive block containing a "hash" (a unique fingerprint) of its predecessor, leading to a "chain" of sequential data blocks, the Blockchain.

As a "state machine", Blockchain's each state indicates the stored information at a specific time, and the database structure offers traceability between the transitions of states in an immutable way thanks to Blockchain's distributed nature. In comparison, regular databases do not always offer audit trails; and even if they do, these trails are not tamper proof – they can be destroyed or lost.[49]

2.1.2 Peer-to-peer transmission

Communication between peers occurs without an intermediary as the information is stored in and transferred through Blockchain. Hash codes of each block securely authenticate transaction source without a trusted third party while encrypting user identities.

---

[46] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (Bitcoin, October 2008)
[47] Mougayar, William, Buterin. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, 33
[48] Dhillon, Metcalf, Hooper, Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You, (1st Apress Berkely, CA, USA, 2017) 185
[49] Mougayar, William, Buterin. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, 35

2.1.3 Transparency with pseudonymity

Users have the competence to remain anonymous or provide proof of identity, which constitutes a 30-plus-alphanumeric address. On the other hand, transactions between Blockchain addresses and their associated values are, in principle, visible within the system, offering transparency.

2.1.4 Irreversibility of records

The moment of a transaction record and transacting accounts' update is "time-stamped" - a permanent, irrefutable and immutable registration with computational algorithms ensuring a chronological order and network-wide availability.[50] This mechanism also assures a singular presence for each transaction and prevents multiple entries in other blocks.

2.1.5 Computational logic

The digital nature of Blockchain creates room for computational logic, meaning users can set up algorithms and rules that automatically trigger different transactions. This computational logic can also be used in smart contracts, computerised transaction protocols whose execution of terms are automatable and self-enforceable. Minimising the threat of malicious and accidental exceptions, smart contracts facilitate the entirety of a contracting process and increase its efficiency by monitoring the contracting parties' past behaviour.[51]

2.2 Main Operations of Blockchain

2.2.1 Data storage & security

Cryptography science provides security and efficient storage of information within Blockchain network under the concepts of hashing, keys, and digital signatures. Each block has a unique fingerprint (hash) that verifies the authenticity of information on transactions without disclosing the information itself; as any change to the original data within a block will result in a new hash value, indicating the corruption. Content of a hash includes time-stamp, nonce, previous block's hash and the root hash of a data structure called "Merkle tree" storing the information of all the transactions in a block[52]. Each transaction within a block is coupled and hashed together to obtain an output hash that carries both transaction's information. These output hashes are

[50] Dhillon, Metcalf, Hooper, Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You, 185
[51] Kolvart, Poola, Rull, Smart Contracts. in Kerikmae, Rull (ed), The Future of Law and eTechnologies (Springer International Publishing Switzerland 2016) 134
[52] Joseph J. Bambara and Paul R. Allen, Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions (McGraw-Hill Education 2018) 20

repeatedly coupled and hashed again, with each level containing all information of the level below, until one hash, the Merkle root hash, carries the information of entire transaction list. The root hash allows to determine the presence of a particular transaction within a block efficiently, offering data consistency without compromising the input of a transaction. In addition, the virtual impossibility to reverse engineer a hash and uncover the input adds extra security to this process.[53] Lastly, validity of a block can be easily tested by checking the validity and existence of referenced previous block, comparing their time-stamps (previous block's time-stamp value should be lower) and testing the consensus algorithm.

Private keys are generated using the SHA-256, a hashing algorithm that receives any data and creates a cryptographically secure 256-bit digest / number, which will eventually be transformed into a base58 key.[54] Each private key corresponds to a single address, though the correspondence is secret; private key creates the corresponding public key, which subsequently creates the address through hashing function, preventing any reverse process to reach one's private key through the knowledge of her public address or public key.[55]

Authenticity of a message or document is provided through "digital signature", a mathematical computation consisting the hash of the document encrypted with the private key of the document/message owner, which can be verified by using his/her public key.

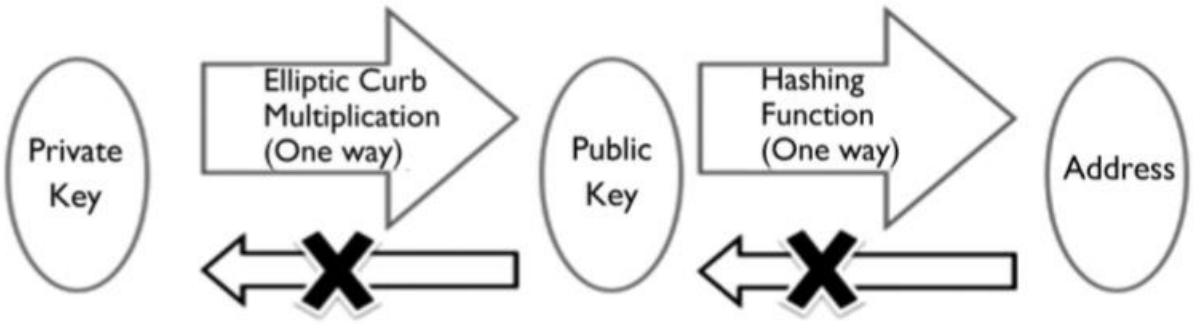


Figure 4: Process of Creating Public Key and Public Address[56]

Apart from authenticity of transaction, authenticity of communication also has to be sustained without compromising their identities or their private keys. Creating trust between two parties

[53] Dhillon, Metcalf, Hooper, Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You, 22
[54] Hector Lopez, 'How is a private key created for Bitcoin?' (Medium, 16 November 2017)
[55] Koji Takahashi, 'Blockchain technology and electronic bills of lading' [2016] 22 The Journal of International Maritime Law 209
[56] Ibid.

in a digital environment without a trusted intermediary is a challenge that Blockchain succeeds using the Diffie–Hellman key exchange (DH)[57], a method which allows two parties with no prior knowledge to establish a shared, secret key over an insecure channel. Similar to the hashing mechanism, this exchange method ensures the authenticity of transacting parties' communication without disclosing their private keys to their counterparty.

In a digital environment, matching real-life identities with digital avatars is vital for legal matters as well as eliminating the threat of Sybil attacks[58], which may compromise the initial generation of digital identities, and whitewashing attacks[59], which may corrupt reputation-based system through constant discarding and receiving identities to escape bad reputation. Blockchains' inability to access data outside their network necessitates integration of off-chain data sources called "smart oracles" to receive authentic information on user identity and real-life occurrences. These oracles act as trusted identification authorities, providing information to Blockchain to be used in smart contracts.

2.2.2 Consensus algorithms

As mentioned earlier Blockchain is a state machine, and with each broadcast of a transaction, the network has to decide whether the transaction is authentic and should be included to the current state of the distributed ledger. This consensus within the network can be procured through a consensus algorithm, which's purpose is to "distribute the right to decide what the state of the blockchain is to a decentralized set of users".[60] Each algorithm achieves distribution of rights through different mechanisms, with efficiency and security usually being reversely proportional. The consensus algorithm play a key role in Blockchain, as its failure may cause the "double-spending" problem[61] and addition of invalid transactions to the distributed ledger.

There are various consensus algorithms[62], with the most popular one being proof-of-work (PoW) algorithm used by the Bitcoin Blockchain. Here the right to decide whether a transaction should be included is earned through the process of "mining" – miners compete against one

[57] Christopher Demicoli, 'Introduction to the Diffie-Hellman Key Exchange' (blog.cdemi, 8 June 2016)
[58] John R. Douceur, 'The Sybil Attack' (UIowa, 2003)
[59] Feldman, Papadimitriou, Chuang, Stoica, Free-Riding and Whitewashing in Peer-to-Peer Systems (3rd Annual Workshop on Economics and Information Security (WEIS2004) 2004)
[60] Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, (2016) 538
[61] Investopedia, 'Double Spending' (Investopedia)
[62] Zane Witherspoon, 'A Hitchhiker's Guide to Consensus Algorithms' (Hackernoon, 13 February 2018)

another on solving a mathematical problem using their computing power; with the winner adding his "block" to the Blockchain and earning "Bitcoin" as a reward. Blockchains with proof-of-work algorithms are criticised for the required massive energy consumption[63] caused by the competition of computing powers and relatively slow transaction confirmation speed[64] which limits the scalability.

Within another popular algorithm, proof-of-stake (PoS) energy consumption is not an issue – competition is on the amount of "coins" one hold, and each successful "validator" of a block receives transaction fees directly from the transacting parties. Unlike proof-of-work, all coins exist from the very beginning, with more coins one possess, more likely he will be given the right to add his block to the chain. Critics of proof-of-stake algorithm underline the "nothing-at-stake" problem (Buterin, 2014), however cryptography science offers certain PoS-embedded solutions[65] and variations of PoS like Delegated PoS[66] as a counter.

2.2.3 Privacy

As mentioned earlier, within Blockchain users normally possess pseudonymity - although private identities are securely encrypted, proof of validations are public to prove the existence of transactions and/or parties without revealing the underlying encrypted data[67]. Recent developments in this area lead to various technologies providing more privacy beyond the pseudonymity: Quorum, an enterprise-grade permissioned version of Ethereum, introduces private transactions and contracts using "a peer-to-peer messaging daemon that can direct the flow of private information to the appropriate network participants" called Constellation[68]. In addition, an inherently private transaction type, IsPrivate was presented to its users. Another technology called "Zero Knowledge Succinct Non-Interactive Arguments of Knowledge" (zk-SNARKs) creates proof of validation for smart contract conditions without revealing the condition[69]. Here "succinct" means efficient computing in a reasonable amount of time, an

[63] Digiconomist, 'Bitcoin Energy Consumption Index' (Digiconomist)
[64] Raul Amoros, 'Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?' (Howmuch, 10 January 2018)
[65] Beau Stoner, 'Ethereum's Future Proof-of-Stake Casper Upgrade | A Detailed Overview' (Cryptocurrency Australia, 15 March 2018)
[66] Dhillon, Metcalf, Hooper, Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You, 155
[67] Joseph J. Bambara and Paul R. Allen, Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions, 80
[68] Dhillon, Metcalf, Hooper, Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You, 175
[69] ibid 176.

important asset for verification; "non-interactive" refers to SNARKs not needing prover interrogation by the verifier, with prover publishing in advance the proof, which's correctness can be checked by the verifier similar to hashing; and "adaptive argument of knowledge" stands for proof of knowledge through computation.[70] These "zero knowledge proofs" can be created through zk-SNARKs' cooperation with smart oracles, receiving information on real-life occurrences that conditions are based upon to test their realisations.

2.3 Types of Blockchain

Contrary to public perception there are multiple types of blockchain, each with different properties. The most known type, public blockchain does not require permission to access and transact within its network – everyone can contribute to the consensus process and receive awards in return without offering any credentials as is the case for Bitcoin Blockchain, which tend to increase the transaction fee.

On the other hand, the private blockchain, also known as permissioned blockchain, only allows credited users to operate and participate in the consensus process. This permission-based model makes private blockchains rather centralised which attenuates the core decentral, non-authoritarian character Nakamoto has envisioned for Blockchain. Public readability can also be restricted or fully excluded for more privacy which can be the case for internal databases.

Leaving the control of the consensus process to preselected nodes (users) with a set of preformed rules in a private blockchain creates what is known as a "consortium blockchain". Exemplified by the R3 Blockchain,[71] a consortium of identified users like banks approves each block as to provide validation.

Both private and consortium blockchain offer certain advantages in comparison with public blockchain. With the numbered participants of consensus process pre-identified, the risk of an attack on this validation process is greatly reduced as third-parties cannot intervene and bad validators can be easily identified. This also provides faster consensus reachability and cheaper (or free) transactions since a limited number of nodes verify instead of everyone on a public network. Protection against a distributed denial-of-service (DDoS) attack is also possible with

[70] Matt Luongo, 'Zero-knowledge proofs, Zcash, and Ethereum"' (Keep Network, 19 September 2017)
[71] r3, 'Blockchain for business: Delivering the world's only blockchain built specifically for the enterprise' (r3)

the validated nodes, who can change the rules of Blockchain when deemed necessary and revert transactions or modify account balances.[72]

2.4 Blockchain's Role in Banking System

Before the hype for cryptocurrencies, Wall Street's opinion of Blockchain technology was already overwhelmingly positive, with 94 percent of respondents in a study believing Blockchain could play an important role in finance sector.[73] According to Blythe Masters, a former executive at JPMorgan Chase, Blockchain could be an efficient and cheap model for financial service infrastructure "by allowing multiple parties to rely on the same information rather than duplicating and replicating it and having to reconcile it".[74]

A FinTech report by Spanish bank Santander suggests that with both clearing and settlement process for peer-to-peer value transfers continually occurring on a Blockchain network, banks can decrease their back-office expenses by an estimated $15-20 billion without changing their underlying business model.[75] Not coincidentally, Santander became one of the first banks to apply Blockchain to payments, enabling customers using their application to make overseas payments that clear within 24 hours. Bitcoin networks require even fewer time, with an average of ten minutes necessary to clear and settle all transactions through the consensus process. In comparison, the current numbers are three to seven days for remittances, two to three days for stock trades, twenty-three days for bank loan trades[76] and more than a few days for ACH system, which annually handles trillions of dollars of U.S. payments.[77]

Blockchain can also provide a more efficient, cheap and sustainable trust network between banks comparing to the current trust system, which tend to be expensive due to regulatory obligations and complexity of integrating each banks' proprietary systems. This may enable network-wide transactional analysis to combat money laundering more effectively comparing

[72] Joseph J. Bambara and Paul R. Allen, Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions 175
[73] Matthew Leising, 'The Blockchain Revolution Gets Endorsement in Wall Street Survey' (Bloomberg, 22 July 2015)
[74] Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 155
[75] Santander, Innoventures, Oliver Wyman, Anthemis Group, 'The Fintech 2.0 Paper: rebooting financial services' (Finextra, 2015)
[76] Matthew Leising, 'The Blockchain Revolution Gets Endorsement in Wall Street Survey'
[77] Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 157

to current anti money laundering (AML) paradigm which heavily depends on customer due diligence.[78]

Aside from AML measures, banks also have the obligation to know and verify the identity of their customers (KYC). Storing customer identity documentation, account and payment information in a tamper-proof block in the Blockchain can lead to a standardisation of account requirements, improvement of data quality and also easier compliance with AML regulations by more accurate suspicious transaction identifications. The standardised KYC data may also be shared through the aforementioned trust network, decreasing resource required for account-related activities while increasing their efficiency. Access to private data, on the other hand, may be strictly limited to its owner through providing a private key.[79]

2.5 Challenges for the implementation and use of Blockchain

As mentioned earlier, scalability of Blockchain can be challenging depending on the consensus algorithm, especially for PoW. While mainstream payment networks can process around 2000 transactions per second, Bitcoin network with its PoW algorithm can only process seven. Changing the block size limit parameter can accelerate process time, yet this change would impair the decentral character of such Blockchains since bigger blocks require more energy in PoW ecosystems, preventing average users from running Blockchain. Aforementioned "zero-knowledge-proofs" can offer a more comprehensive and multi-dimensional solution, with a miner / validator processing transactions and publishing a proof of computation, which solely needs to be verified instead of each transaction by the users.[80]

PoW algorithms' massive energy requirement may limit the scalability as well; however Bitfury's founder Valery Vavilov claims technological development will gradually make Blockchain more environmentally friendly and energy efficient in general, with strategical implementations including relocations to areas with cheaper, renewable energy decreasing general costs.[81] In addition, direct interoperability between different Blockchains should greatly

[78] Mougayar, William, Buterin. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, 85
[79] Joseph J. Bambara and Paul R. Allen, Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions 29-37
[80] Vitalik Buterin, 'Ethereum/wiki/problems' (GitHub, 25 August 2014)
[81] Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 661

enhance scalability with the establishment of network-of-blockchain solutions which would connect multiple Blockchains through an external, decentralised system.[82]

Irreversibility of transactions and unvoidability of smart contracts set a legal challenge against Blockchain, since current legal ecosystem designed with considerations to non-performance risk, breach of contract and damages - which is not the case for Blockchain.[83] Privacy of personal information stored in Blockchain is another challenge with data protection regulations like GDPR emphasising the "right to erasure" and "right to be forgotten". In principle, destruction of the private key in an auditable way renders any data within that block unreadable, though whether this unreadability satisfies the aforementioned rights or not is yet to be seen.[84] Zero-knowledge proof of computations would also be beneficial as they only reveal the legitimacy of transactions, hiding the transaction from everyone but its parties.[85]

Apart from privacy, Blockchain's accessibility to average person is also questionable with various applications consisting numerical, user-unfriendly interfaces.[86] Bound to digital devices, Blockchain-based applications struggle to reach masses with low digital literacy or scepticism towards digital payments due to the uneducated fear.[87]

As a social and digital network, Blockchain's creation and governance requires human involvement. The definitive protocol, consensus algorithm and other inputs that establish Blockchain all have to constructed as well as developed through integration of technological improvements and patching of vulnerabilities. These obligations / powers are the matters of governance; and a decentral approach, governance by the network through certain cooperation and coordination mechanisms can be successful only if these mechanisms are robust, fair and predictable. [88]

---

[82] Joseph J. Bambara and Paul R. Allen, Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions, 228

[83] Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 653

[84] Joseph J. Bambara and Paul R. Allen, Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions, 80

[85] Vitalik Buterin, 'Ethereum/wiki/problems' (GitHub, 25 August 2014)

[86] Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 646

[87] Dannielle Correa, 'Security concerns are inhibiting mobile payment adoption worldwide' (SC Magazine, 07 October 2016)

[88] Odysseas Sclavounis, 'Understanding Public Blockchain Governance' (Oxford Internet Institute, 17 November 2017)

With each new (potentially) disruptive technology comes these kinds of problems to deal with, and the regulatory response to applications using Blockchain would have to take these into consideration. On paper, public blockchains' transparency combined with pseudonymity and immutable time stamps allows regulators to monitor and act in accordance. On the other hand, Mougayar humorously compares the variety of financial services regulatory authorities around the world to the number of ice cream flavour varieties, stating "more than 200 regulatory bodies exist in 150 countries, and many of them have been eyeing the blockchain and pondering regulatory updates pertaining to it".[89] A harmonised response thus seems hard to achieve, especially with private parties taking initiative in Blockchain technology to create applications with different attributes for different industries.

[89] Mougayar, William, Buterin. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, 84

3 Compatibility of Blockchain with Negotiable Instruments

Blockchain technology has mostly been identified with Bitcoin and other cryptocurrencies in financial ecosystem, which would eventually replace the traditional fiat currencies. However, as seen with initiatives taken by regulators and the banks, traditional financial actors, Blockchain can very well be the new technical infrastructure that would modernise and digitalise the traditional payment systems that use fiat money, which is defined by American economist and Penn State professor Neil Wallace as *"an intrinsically useless object that serves as a medium of exchange".*[90] Transformations within banking sector, from using books to computers for book keeping, from using physical money to electronic substitutes, are continuous; and with each new disruptive technology, as their full potential is discovered and they mature beyond their hype, such transformations will eventually take place.

In payment sector the Faster Payments Task Force ("Task Force" hereinafter) envision the transformation from existing payment systems to new actors that carries certain characteristics. The payment system they project should be fast, allowing its end users fast access to funds; secure with minimal fraud and error; ubiquitous, reaching users including unbanked and underserved; safe and efficient.[91] Their recommendation, in their report, is to establish a faster payments governance framework, rules, standards and baseline requirements by 2020[92]. I argue that the Blockchain-based Negotiable Instrument 2.0 may satisfy the requirements set by Task Force and is compatible with the legal and financial ecosystems. Before this analysis, the technical construction of Negotiable Instrument 2.0 with Blockchain technology will be elaborated and the unique compatibility between these two seemingly unrelated institutions will be explained.

3.1 Technical Compatibility

Negotiable instrument is a special type of contract with standardised terms and the unique attribute of transferability. The standardisation and transferability can be achieved in a digital environment; with the Negotiable Instrument 2.0 being a legal contract that is formed electronically, signed digitally and some of its terms enforced by a smart contracting process. Establishing the digital substitutes for all functions related to negotiable instruments requires

[90] Neil Wallace, Fiat Money, 1-9. 10.1057/978-1-349-95121-5_454-2 (2008)
[91] Faster Payments Task Force, The U.S. Path to Faster Payments Final Report Part Two: A Call to Action 16
[92] ibid 31-32.

an illustration of each function and how each substitute will be functionally equivalent or superior.

3.1.1 Creation of Negotiable Instruments

A negotiable instrument carries the following information: an unconditional order of payment, signature of the maker or drawer, name of the drawee and statement of time when payment is to be made whether on demand or on a specified date. As the drawer of a paper-based negotiable instrument simply fills this information on a standardised template, the Negotiable Instrument 2.0 will be an electronic template on which the user will determine the amount, the addressee's pseudonymous identity and payment time. Determination of payment time can be more flexible in comparison to traditional negotiable instrument thanks to smart contract feature, which may detect real-life information on time through smart oracles. Any pre-determinable time period can therefore be set as time of payment.

3.1.2 Validation of Negotiable Instruments

Currently banks act as the provider of payment systems and are responsible for the clearance and settlement of payments. Elimination of intermediaries for transactions is a key feature of Blockchain; however as mentioned earlier, validating transactions and recording them within Blockchain requires a delicate consensus algorithm which shall be both secure against Sybil and tyranny of majority attacks as well as efficient and comparatively decentral. Determining such algorithm is challenging as newer and arguably better algorithms are mostly security-wise unchallenged, thus Blockchain enthusiast like Blockstream's ex-CEO Austin Hill believes conservative, very-well established algorithms should be preferred.[93]

On the other hand, most popular consensus algorithms, proof-of-work and proof-of-stake have both well-documented, aforementioned issues regarding their efficiency and/or security. Attempts to better consensus algorithm see different approaches, with one attempt's design, Semada, being ostensibly a suitable model upon which validation of transferring negotiable instruments can be achieved through certain modifications.

Semada's design philosophy is based on reputation, incentivising productive cooperation by *"tying an expert's reputation to their proof of ability and productive contributions as verified*

[93] Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 100

by validation pools generated by public fees sent to the system".[94] System consists of sub-tokens representing reputation and bench of experts who stake their sub-tokens to answer validation requests in the validation pool, which is the mechanism that creates and distributes reputation. Semada infrastructure allows for different expertise outside the network through posting off-network works' evidence to validation pool where other experts decide on approving or disapproving the work's integrity and authenticity. However, for negotiable instrument sole required expertise is simpler like any other cryptocurrency which is the creation of a block consisting transactions; thus, while the proposed process will implement main principles of Semada, there will be certain deviations from Semada's Whitepaper.

Although Semada's original model is more "developed" as to offer the opportunity to accommodate expertise outside the network, for Negotiable Instruments 2.0, the sole expertise is the efficient, automated and technically sound transaction validation by the experts, who will be the banks for reasons explained in the next sub-chapter. The competition on the areas of reputation and fees between experts (banks) would incentivise them to lower their fees while still ensuring a sound automated transaction validation process. The elements of proof-of-authority consensus mechanism, where reputation of validators are staked, are particularly compatible for this proposal as for banking industry, within whom offers are predominantly intangible and service-based, the ability to provide superior service is valuable from customers' perception and thus creates a significant competitive advantage.[95]

The process starts with the endorser of the negotiable instrument choosing an expert based on his reputation and his asked fee. Here multiple options may be given within the simple user interface; my proposition would include the options of the lowest fee, highest reputation or the equilibrium of both. The pre-existing options may also facilitate automatisation of this stage as a user pre-determines his preference for all his transactions. Semada's whitepaper indicates fees should be on Ether currency as Semada is founded on Ethereum Blockchain, however in this visioned model representation of fiat currency on Blockchain is projected; therefore, the fee in

[94] Calcaterra, Craig and Kaal, Wulf A. and Andrei, Vlad, Semada Technical Whitepaper - Blockchain Infrastructure for Measuring Domain Specific Reputation in Autonomous Decentralized and Anonymous Systems (February 18, 2018) 4

[95] Babic-Hodovic, Mehic, Arslanagic, Influence of Banks' Corporate Reputation on Organizational Buyers Perceived Value (7th International Strategic Management Conference, Elsevier Ltd 2011) 358

fiat currency should be distributed among all experts weighted according to their holdings of expertise tokens.[96]

In second stage the system mints new reputation tokens on a pre-set conversion ratio with the fee and stakes half of it in the chosen expert's name, incentivising work accuracy. The other half is staked against the expert and left unassigned. After the expert's posting evidence-of-work, a validation pool is created where all experts stake their reputation tokens to approve or disapprove the work. In the most efficient case, an automatisation of this validation process and choosing correct vote through algorithms is envisioned.[97] Winners of this process split losers' stake weighted according to their holdings of expertise tokens, with upvotes winning ties. If post is approved, the previously unassigned minted reputation tokens are also split among approvers, whereas in case of non-approval these tokens are destroyed.

As a result, Semada's unique reputation-based consensus algorithm has multiple upsides: Element of competition on fees to attract the user ensures lower fees, with staking half of the newly minted reputation tokens for the chosen expert further incentivising all experts to lower their fees as to substantially increase the amount of their reputation tokens, which will lead to obtaining a higher ratio on fee received through splitting. On the other hand, the competitiveness is restricted to the cost of validation, since it is financially infeasible and from competition law perspective perceivably predatory to offer fees lower than the cost.

Semada's algorithm is also resistant against Sybil and tyranny-of-the-majority attacks. Sybil attacks consist obtaining multiple expert accounts to unjustly profit from the system; however as Semada's model is weighted by reputation, the amount of reputation token solely determines the power: An account with 1000 reputation token has the same power or even more power as 1000 accounts with one token.[98] The other threat, tyranny-of-the-majority describes corruption in a system that *"manifests itself in decisions made with a greater concern for following what is perceived as popular than what is right and just".*[99] A solution within Semada's model is to adopt a weighted voting system where those with greater reputation accrues more power,

[96] Calcaterra, Craig and Kaal, Wulf A. and Andrei, Vlad, Semada Technical Whitepaper - Blockchain Infrastructure for Measuring Domain Specific Reputation in Autonomous Decentralized and Anonymous Systems, 6
[97] ibid 7.
[98] ibid 13.
[99] ibid 13.

making the popular decision also the right one as the powerful expert has the reputation to make the right decision and favours precedent and predictability.[100]

Since staking the reputation tokens is one of the basis dynamics within Semada's model, the "nothing-at-stake" problem of the traditional proof-of-stake algorithm comes into mind; though Semada's incentivises experts to act in the interest of the system through the validation pool. With losers' stake of reputation tokens splitted by the winners, the process disincentivises experts from corruption attempts, which will eventually lead to low reputation and lack of attraction from the users.

3.1.3 Governance of Blockchain

Validating the transactions is only one dimension of Blockchain governance. Constructing the network itself through the establishment of the infrastructure and a set of rules is *ipso facto* required by the "platform provider(s)". First examples of Blockchain applications had platform providers that were informally organised groups of individuals, though today many Fintech startups and even banks[101] venture into setting up Blockchain networks. Being the platform provider bears great responsibility as the designer of the entire system including the security measures, and the only suitable point of entry for network-wide regulatory and legal rules. A platform provider has to sustain a sound and continuous software platform while aligning platform's internal rules concerning rights' acquisition and contract execution with private law. Requirements on integrity, safety, availability continuity of service and any similar rule that necessitates central implementation must be enforced by the platform provider. In addition, *ex ante* regulatory measures are vital for avoiding any loophole or bug, though prevention of any flash crashes and bubbles through software updates and reporting mechanisms is required for the system stability. Preventative measures before the materialisation or the reversal of any incorrect outcome derived from a faulty code is necessary for the systemic stability at the cost of immutable character of Blockchain[102], which was the case for Ethereum and the DAO

[100] Calcaterra, Craig and Kaal, Wulf A. and Andrei, Vlad, Semada Technical Whitepaper - Blockchain Infrastructure for Measuring Domain Specific Reputation in Autonomous Decentralized and Anonymous Systems, 14
[101] Anna Irrera, 'Bank-backed R3 launches new version of its blockchain' (Reuters, 3 October 2017)
[102] Philipp Paech, The Governance of Blockchain Financial Networks (December 16, 2016) 18

hack.[103] For all these listed reasons, Blockchain platform providers should be legal persons who are regulated by the State.[104]

In comparison, the providers of the check payment system are banks, whether payer or depositary.[105] As the providers, they should *de jura* bear the risk of any systemic loss beyond users capabilities, incentivising them to adopt an appropriate yet cost-efficient level of security.[106] In parallel, the platform providers for Negotiable Instruments 2.0 should be banks, as well as the aforementioned experts whose power of influencing the validation system are reputation based. Paech argues that when nodes are entities not regulated as financial institutions, or individuals which is the case for Negotiable Instruments 2.0, the sole entity with the capability to apply the relevant regulatory and legal rules to the network and its nodes is the platform provider, who, as the addressee of these rules, should be a fully regulated financial institution like a bank, controlling the network through network software programming and access control.[107] Although this would undermine the decentralised character of Blockchain, the accounts are solely controlled by their respective nodes / users, which would be an improvement over the existing central database model Mougayar heavily criticised.[108] On a better note, it is technically possible to program the complex and central risk management process[109] for eliminating threats against users' recorded assets inside the network, which is required for any financial market, into the Blockchain network as smart contracts.[110]

3.1.4 Endorsements

In blank endorsements, negotiability can be partially restricted through determination of means the instrument can be used for. The smart contract feature of Blockchain may help with the establishment of this feature negotiable instruments uniquely have unlike other payment systems, enforcing a functional implementation of a particular requirement and showing

[103] Antonio Madeira, 'The DAO, The Hack, The Soft Fork and The Hard Fork' (Cryptocompare, 20 May 2018)
[104] Philipp Paech, The Governance of Blockchain Financial Networks, 34
[105] J. Rogers, The End of Negotiable Instruments: Bringing Payment Systems Law Out of the Past, 119
[106] Ibid., 124
[107] Philipp Paech, The Governance of Blockchain Financial Networks, 35
[108] See page 13
[109] Basel Committee on Banking Supervision, 'International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version' (Bank for International Settlements, June 2006)
[110] Philipp Paech, The Governance of Blockchain Financial Networks, 18

proof[111]. Blank endorsements require only the signature of the holder; offering full competence to the bearer of the blank-endorsed instrument to transfer or cash in. Signature information can be found in the Blockchain-based negotiable instrument, which also gives the person in control total competence on the electronic record. Critically, the sole requirement of obtaining the possession of a blank-endorsed instrument without defining the next holder's identity makes the paper-based instrument vulnerable against the violations of proprietary rights. Considering in addition the Blockchain's digital infrastructure non-compatibility with lack of transferee identification, the institution of blank endorsement may not be included in "Negotiable Instruments 2.0". On the other hand, its "determination of means" function can be applicable for other types of endorsements as it offers the unique opportunity to technically limit the negotiable instrument's potential usage. Full endorsement, which identifies the next holder, is compatible with Blockchain infrastructure and the digital obtainment is protected against any outside interventions. Similarly, qualified endorsement is also compatible and serves the important purpose of restricting the liability of an endorser in case of a payment failure. This limitation of liability is possible to code within the smart contract of negotiable instrument. Authenticating previous endorsements and referring when necessary is possible through digital signature used validating that transaction; meaning the evidentiary requirement is satisfied through this blockchain receipt for each specific endorsement.[112]

One of the main principles in traditional negotiable instrument system is the holder in due course doctrine, which is also labelled as the difference between transferability and negotiability. From a conventional policy perspective, purpose of the holder in due course rule is to encourage transactions in negotiable instruments through stripping defences[113] such as refusal of payment by the maker based on a legal ground or claim of ownership by a third party[114]. Although this encouragement is supposed to facilitate the creation of substitution for cash[115], the existing problematic and non-cohesive implementation of this doctrine creates legal vagueness and vulnerability. Rogers' explanation of the current status quo with holder in due course doctrine under US legislation and jurisdiction is enlightening on this regard. Per U.C.C. statute, Rogers concludes that the revision of Article 3, which abrogates holder in due course

[111] Mougayar, William, Buterin. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, 46
[112] Joseph J. Bambara and Paul R. Allen, Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions, 88
[113] Gregory E. Maggs, The Holder in Due Course Doctrine as a Default Rule, 10
[114] Lary Lawrence, An Introduction to Payment System, S 53 (1997)
[115] Gregory E. Maggs, The Holder in Due Course Doctrine as a Default Rule, 13

doctrine in consumer sales, also lead to the recognition and approval of precedent cases where a refusal to apply the statutory holder in due course rule. In addition, Rogers underlines the non-limitation and non-definition of cases where the holder in due course doctrine should not be applied. Although consumer cases and their unjust results of applying the doctrine non-discriminatively were mainly the reason why this doctrine needed this kind of exception, case law was not limited to consumer transactions. Conclusively, Rogers argues that what statute says to judges is "*Apply this statute unless you think you shouldn't. We legislators leave it to you judges to figure out whether it does or does not make sense to apply the statute in any particular class of transactions*".[116] This has resulted in courts refusing to apply holder in due course doctrine where it appeared to produce unjust results through strained reasoning on matters such as the requirements for qualifying as a negotiable instrument[117] or debtors pointing out some random words written on the instrument by the creditor[118].

3.1.4.1 Smart contract feature

The smart contract feature can enforce a functional implementation of a particular requirement and show proof. For Negotiable Instrument 2.0 the functional implementations are the endorser liability and determination of means negotiable instrument can be used for, both standardised implementations. Considering the fact that standards manage costs of contract formation, general standardisation within negotiable instruments is crucial, which is also vital for facilitating the application of smart contracts. As a concept, smart contract is currently seen as vulnerable[119], insecure and inefficient[120] by some. This greater technical and financial costs stem from smart contracts attributes of being precisely written in fully defined code as they are unmodifiable once executed; and favouring anonymous and one-off transactions.[121]

The immutable and unmodifiable character is derived from smart contract terms being decentralised and distributed to every node within Blockchain, meaning the transactional relationship created by smart contract must be completely formed and defined, which might be

[116] J. Rogers, The End of Negotiable Instruments: Bringing Payment Systems Law Out of the Past, 90
[117] ibid 93.
[118] ibid 110.
[119] Nikolic, Kolluri, Sergey, Saxena, Hobor, Finding The Greedy, Prodigal, and Suicidal Contracts at Scale (Arxiv.org 2018)
[120] Kai Stinchcombe, 'Ten years in, nobody has come up with a use for blockchain' (Hackernoon, 23 December 2017)
[121] Jeremy M. Sklaroff, Smart Contracts and The Cost of Inflexibility, (University of Pennsylvania Law Review) 12

not possible in volatile and uncertain environments of contracting process.[122] Even if that is not the case, it will still cause high technical / financial ex-ante costs of drafting and negotiating over precise terms. Parties will have to allocate greater resources against greater uncertainties to project future state of the world and set these projections within smart contract, which may discourage contracting parties from using smart contracts in the first place.[123] However, the smart contract feature in Negotiable Instrument 2.0 is fully standardised and comparatively simple; meaning the non-modifiability is rather a strength, eliminating the possibility of exploiting the liability chain or pre-determination of means and decreasing the financial and technical cost.

The enforcement inflexibility of smart contracts prevents contracting parties to avoid litigation and informally resolve contractual disputes for the sake of bootstrapping the business relationship and constraining any opportunistic behaviour.[124] In comparison, the nature of negotiable instrument transactions is fully financially driven and non-changeable implementation of smart contract terms is in favour of contracting parties' interest.

3.1.5 Identification

As previously explained, within Blockchain, all users have pseudonymous identities with their private identities securely encrypted. However, one requirement of financial markets is the verification of identifications. With the development of network-of-blockchain solutions connecting multiple Blockchains through an external, decentralised system; each identity provider may inject the credentials into their private Blockchain, which subsequently can provide real life information as smart oracles to Negotiable Instruments 2.0 Blockchain when necessary. This would also greatly decrease maintenance cost of databases for these identity providers as expensive call centres or websites would no longer be deemed necessary.[125]

Another Blockchain solution for digital identification can be based on the so-called self-sovereign ID, where users can certify their identity by sharing their verifying public key while collecting different identification instruments like medical records, social security information, financial history under one Blockchain record. Sharing the public key, which matches the information that needs to be verified, without disclosing its content is the main focus for self-

[122] Jeremy M. Sklaroff, Smart Contracts and The Cost of Inflexibility, 6
[123] ibid 7.
[124] ibid 6.
[125] Alex Batlin, 'Digital Identity on Blockchain: Alex Batlin's "prediction"' (Fintech Switzerland, 15 September 2015)

sovereign ID solutions.[126] Solutions like eID+ by Procivis offers high level of security with use of biometrics and Blockchain, which provides tamper-proofness for identity information.[127] eID+ also facilitates authentication of data entered by users through government offices and is already in the implementation phase, with Swiss Canton of Schaffhausen adopted eID+ for its e-government services as an access tool.[128]

Existence of several standards organizations including the National Institute of Standards and Technology (NIST), Fast Identity Online Alliance (FIDO), Identity Assurance Framework (The Kantara Initiative), and the National Strategy for Trusted Identities in Cyberspace (NSTIC) is facilitative for the establishment of a digital identification framework.[129] Further, the European Union is in a favourable position for mass implementation as the EU passport is connected to authorisation and continued supervision of financial service providers.[130] Negotiable Instruments 2.0 Blockchain may benefit from this connection not only in providers' home Member State but rather in the entire EU jurisdiction through its platform providers consisting of banks, which is in line with Paech's thinking who argues this model would be suitable for platform providers authorised as a financial institution like a payment service provider. [131]

3.2 Legal Compatibility

Evaluating the legal compatibility of Blockchain-based "Negotiable Instruments 2.0" with the existing international legal instruments requires a comparative and argumentative approach, one that can be exemplified by Prof. Takahashi's "Implications of the Blockchain Technology for the UNCITRAL Works" which he presented in the Congress of the United Nations Commission on International Trade Law Vienna 2017[132], as there are multiple works of United Nations Commission on International Trade Law (UNCITRAL) which overlap with and/or complement one another in the field of electronic commerce. Related instruments covering negotiable instruments are the Convention on International Bills of Exchange and Promissory

[126] Roger Aitken, 'Blockchain To The Rescue Creating A 'New Future' For Digital Identities' (Forbes, 7 January 2018)
[127] Procivis, 'eID+ is' (Procivis, 24 January 2017)
[128] Procivis, 'Trusted interaction between citizens and government' (Procivis, 24 January 2017)
[129] Faster Payments Task Force, The U.S. Path to Faster Payments Final Report Part Two: A Call to Action 20
[130] European Banking Authority, 'Passporting and supervision of branches' (European Banking Authority)
[131] Philipp Paech, The Governance of Blockchain Financial Networks, 37-38
[132] Proceedings of the Congress of the United Nations Commission on International Trade Law Vienna. Modernizing International Trade Law to Support Innovation and Sustainable Development, 4-6 July 2017, Volume 4: Papers presented at the Congress.

Notes (BEP) and Convention Providing a Uniform Law for Cheques (ULC); whereas for electronic trade instruments include the Model Law on Electronic Commerce (ECM), the Model Law on Electronic Signatures (ESM), Convention on the Use of Electronic Communications in International Contracts (ECC) and the Model Law on Electronic Transferable Records (ETR).

Purpose of Model Laws is to offer a pre-existing legal template on areas UNCITRAL deem a legislative response necessary but not to the extent of a fully harmonised international approach. Lawmakers of national governments may freely modify and adopt Model Laws as part of their domestic legislation.

Conventions, on the other hand, are binding instruments under international law of UN Member States and any treaty-making entities that choose to become a party. Deviating from the original text is possible only if the related Convention permits reservations on its provisions.[133] In conventions regarding trade law, reservations are mainly prohibited or minimised in an attempt to not to undermine conventions' realisation of purpose.[134]

Before the analysis of compatibility one should bear in mind certain guiding principles of UNCITRAL in its legislative acts. Principle of technological neutrality refers to the non-requirement and non-assumption by the law of a particular technology for the electronic generation, communication or storage of information.[135] In ECC, technological neutrality is emphasised for its accommodation of future technological development and innovations[136] - which is also the case for other UNCITRAL instruments - ; thus, a technology like blockchain, which was not invented in the time of these instruments' creation, can be included within the scope of application.

Another principle, functional equivalency indicates that any electronic-commerce technique that can satisfy the criteria provided by the paper-based requirement's purposes and functions should enjoy the same level of legal recognition as corresponding paper document with the same function.[137] Repudiation of such techniques solely on the ground of their electronic nature

[133] United Nations Commission on International Trade Law, 'FAQ - UNCITRAL Texts' (UNCITRAL)
[134] ESM, Guide to Enactment, para 27
[135] ECC, Explanatory Note, para 47
[136] ibid, para 48.
[137] ECC, Explanatory Note, para 51

is not allowed under ECM[138], ETR[139] and other instruments. As mentioned in ECM's Guide to Enactment[140] and ECC's Explanatory Note[141], a system of electronic records - like the one provided with Blockchain – can provide more security, reliability and speed in comparison with the traditional paper-based system in terms of its purposes and functions.

3.2.1 Scope of Applications

3.2.1.1 Convention on International Bills of Exchange and Promissory Notes (BEP)

The first modernisation of international uniformed negotiable instruments law saw BEP replacing the League of Nation's Convention Providing a Uniform Law for Bills of Exchange and Promissory Notes. As the name suggests this Convention does not address international checks to accommodate civil law jurisdictions which considered these instruments separately; however, modernisation of the other half of the "Geneva Conventions", Convention Providing a Uniform Law for Cheques was not realised due to "checks losing their relevancy in international payments".[142]

Considering conventions' binding nature, BEP is comparatively loose since it only applies to international instruments that contain the phrases "International bill of exchange (UNCITRAL Convention)" or "International promissory note (UNCITRAL Convention)"; making its application scope optional.[143]

3.2.1.2 Model Law on Electronic Transferable Records (ETR)

Aforementioned principles of technological neutrality and functional equivalence approach are embraced by ETR, which adopts a *"system-neutral approach, enabling the use of various models whether based on registry, token,* ***distributed ledger*** *or other technology".*[144] National laws determine which documents or instruments are transferable[145], with ETR's definition of electronic transferable records aiming to cover any electronic record functionally equivalent with these nationally-determined transferable documents or instruments. This equivalency reaches beyond the nationality as electronic transferable records cannot be deemed illegal,

[138] ECM, Article 5
[139] ETR, Article 7.1
[140] ECM, Guide to Enactment, para 16
[141] ECC, Explanatory Note, para 134
[142] BEP, Explanatory Note, para 12
[143] ibid para 12.
[144] ETR, Explanatory Note, para 18
[145] ETR, Explanatory Note, para 10

invalid or unenforceable solely due to their issuance or usage abroad,[146] facilitating cross-border payments in an electronic environment.[147]

Not included in ETR are the electronic transferable records that do not possess a paper-based equivalent[148], and any document or instrument under the scope of the Convention Providing a Uniform Law for Bills of Exchange and Promissory Notes (which was eventually replaced with BEP) and of the Convention Providing a Uniform Law for Cheques.[149] Requirement of having an equivalent transferable document or instruments provides compatibility with the numerus clausus principle, whereas exclusion of negotiable instruments from ETR as well as from ECC is due to technical difficulty of creating an "electronic equivalent of paper-based negotiability, […] for which special rules would need to be devised.[150] Blockchain's eligibility to offer such electronic equivalent allows UNCITRAL to eradicate the technical obstacle and realise their intention to devise special rules. ETR's (and ECC) avoidance of covering negotiable instruments leads to a legal gap for electronic negotiable instruments, meaning another modernisation of international uniformed negotiable instruments law necessitates creation of new UNCITRAL instrument, or modification of existing ones. UNCITRAL's intention to monitor technical, legal and commercial developments to modify ETR complements this process.[151]

3.2.1.3 Convention on the Use of Electronic Communications in International Contracts (ECC)

Similar to ETR, ECC does not require any communication or a contract to be made or evidenced in a specific form, applying the technological neutrality principle.[152] Complementing ETR, ECC was also designed to not create regime duality between paper-based contracts and electronic transactions.[153]

Aforementioned exclusion of negotiable instruments and similar documents from ECC's scope[154] is further explained in its Explanatory Note; stating that preventing unauthorised

[146] ETR, Article 19
[147] ETR, Explanatory Note, para 8
[148] ibid para 87.
[149] ibid para 28.
[150] ECC, Explanatory Note, para 7
[151] ETR, Explanatory Note, para 9
[152] ECC, Article 9.1
[153] ECC, Explanatory Note, para 221
[154] ECC, Article 2.2

duplication of documents of title and negotiable instruments has to be sustained.[155] A mechanism combining legal, technological and business solutions to ensure uniqueness and singularity of these documents must be established,[156] as well as constructing an electronic-based documentation that is functionally equivalent to traditional paper-based ones in order to extend ECC's scope of application. If a unique electronic record that could be exclusively held by a holder and transferred to another without replication down the negotiating chain can be created, the essential feature of uniqueness for a transferable instrument can be reached. Notions of "written form", "originality", "signature", "endorsement", "time stamp", "consent", "identification", "contract" etc. to encompass electronic solutions have been extended in ECC[157], with the opportunity to facilitate the coverage of Blockchain-based solutions' through future modifications and additions.

3.2.2 Functional Equivalency of Data Message / Electronic Record to Paper Instrument

Defined as "*information generated, sent, received or stored by electronic, optical or similar means"* in ECC, ECM and ESM; the notion of data message covers not only communications but also computer-generated records not intended for communication[158], thus same definition is applicable for "electronic records" of ETR. Information kept within Blockchain can be classified under these definitions, though evaluating Blockchain-based tokens representing negotiable instruments requires further interpretation. Transferable electronic records comply with five requirements set by ETR Article 10 are considered as functionally equivalent with traditional transferable documents or instruments.

3.2.2.1 Storing information

First requirement is to contain information stored in such documents; with ETR neither imposing any additional information requirement nor preventing the inclusion of additional information that may not be found in traditional transferable documents or instruments due to media difference. In the case of negotiable instruments, following information can be found on the paper-based document: Unconditional order of payment, signature of the maker or drawer, name of the drawee and statement of time when payment is to be made whether on demand or on a specified date. According to Article 17, substantive law can deem certain information as

[155] ECC, Explanatory Note, para 80
[156] ibid para 81.
[157] ibid para 50.
[158] ECM, Guide to Enactment, para 30

unnecessary to be contained in the electronic record.[159] Blockchain-based version can carry the essential information of the unconditional payment (transaction), statement of date (time-stamp), signature (digital signature) and name of the drawee (pseudonymous identity).

3.2.2.2 Reliability

Second requirement for electronic transferable records is to consist a method that satisfies the general reliability standard set by ETR Article 12. Functional equivalency should be provided within this standard, which's elements listed as not numerus clausus. First element, data integrity is one of the strongest attributes of Blockchain-based system as any corruption of data will be visible through the hash value change. Second element, prevention of unauthorised access is also given as access to an account without the private key is simply impossible. Third element, security of hardware and software is sustained through the consensus algorithm that prevents any foreseeable breaches to the governance of Blockchain as well as the validation process of transactions, which also covers the fifth element, regular audits by an independent body. Here, reputation-based-elected validators can arguably conform the notion of "independent body", since independency is needed for neutral evaluation of system – which aforementioned validators conduct in line with the game theory logic.

3.2.2.3 Identification of electronic transferable record

Third requirement is to uniquely identify an electronic transferable record for the purposes of traceability as well as transparency. Here Blockchain-based system is again advantageous since each record has an inherently unique hash value that cannot be copied or corrupted.

3.2.2.4 Integrity of electronic transferable record

Fourth requirement is regarding the integrity of an electronic transferable record. Criteria for integrity assessment can be found both in ETR and ECC, which define integrity as the maintenance of the information contained in the electronic transferable record in complete and unaltered form, apart from any authorised changes (like endorsements)[160] or changes that occur in normal course of communication, storage and display.[161]

Combining the first element of this definition with the previous requirement of record

[159] ETR, Explanatory Note, para 164
[160] ECC, Article 9.5(a)
[161] ETR, Article 10.2

identification results in the retained originality of the record, which is vital for international commerce as to satisfy the functional equivalency of originality for the paper-based transferable instruments, without which detection of alteration is significantly harder; leading to lack of confidence in transferable electronic records' content.[162] The Blockchain-based record is suitable hereof as hash values of records are unique and alteration to the original content of records can easily be detected through the change of hash value. The second element of integrity concerning the necessary additions to the original record is also compatible with Blockchain, since UNCITRAL compares additions of supplemental data like endorsements or data necessary for transmission to the supplemental pieces of paper (like allonge) or the envelope/stamp used to send the original paper. Per ETR Explanatory Note paragraph 58, this additional information can consist of metadata or a unique identifier, as well as dynamic information which may change periodically or continuously based on an external source. Accordingly, in Blockchain-based system addition of information such as nonce and hash of the previous block are necessary for the transmission of new block to the Blockchain.[163] The smart contract feature that determines endorser liability and means instrument can be used for also consist dynamic information with each endorsement transforming the chain of liability. In fact, these additions facilitate the identification of the origin, destination and time of the information which is required for the retention of an electronic record.

Retaining the electronic record in an integral form also obligates accessibility to the information when necessary for future references[164]. In traditional paper-based documents this accessibility is sustained through written form[165], which's other functions in national laws are listed non-exhaustively in ETR's Explanatory Note paragraph 74; legibility, authentication through signature, acceptability to public authorities and courts, finalisation of intent, easy storage, facilitation of control and audit for accounting, tax or regulatory purposes. Blockchain's nature of storing information readably, authenticatably, irreversibly, efficiently, incorruptibly, detectably and permanently fulfils all these functions; providing functional equivalency of its records with the notion of "writing".

[162] ECC, Explanatory Note, para 167
[163] ECC, Explanatory Note, para 170
[164] ECM, Article 8.1(b), Article 10.1(a); ECC, Article 9.4(b)
[165] ECM, Article 6.1; ECC, Article 9.2; ETR, Article 8

3.2.2.5 Capability of being controlled

Last requirement for functional equivalency is the capability of being subject to control from creation to cease of validity or effect, with its first element, the establishment of exclusive control by a person, is provided within Blockchain-based systems through private keys. Second element, namely the identification of that person as the person in control[166], is further elaborated on in ETR's Explanatory Note. Here, requirement of identifying the person in control can be satisfied through a certain method that performs the identification function without the electronic transferable record containing such information or naming the person in control, since ETR's structure facilitates anonymity when necessary.[167] Paragraph 117 of the Explanatory Note explains that *"certain electronic transferable records management systems, such as those based on* ***distributed ledgers****, may identify the person in control by referring to pseudonyms rather than to real names. That identification, and the possibility of linking pseudonym and real name, if need be, would satisfy the requirement to identify the person in control. In any case, anonymity for commercial law purposes may not preclude the possibility of identifying the person in control for other purposes, such as law enforcement".* Smart oracles feeding real-life information on identity to the Blockchain may provide the link between pseudonymous names and real identities for law enforcement / regulatory purposes (e.g. anti-money laundering) as well as commercial reasons like detection of the endorsement chain or Know-Your-Customer practice.

3.2.3 Functional Equivalency of Electronic Record to Negotiable Instrument

As mentioned earlier, paper-based negotiable instruments in general contain following information: Unconditional order of payment, statement of date and place where document is drawn, signature of the maker or drawer, name of the drawee and statement of place where payment is to be made. Assessing the functional equivalency of a Blockchain-based substitute requires a comparative analysis of each contained information with legal instruments concerning electronic transferable records, and whether a Blockchain infrastructure would be compatible.

3.2.3.1 Unconditional order of payment

The unconditionality of payment order means a sole payment demand is required for the

[166] ETR, Article 11.1
[167] ETR, Explanatory Note, para 116

finalisation of transaction without any reservations or conditions that ambiguate the payment. Although there is the possibility of creating conditionality within contracts in Blockchain through smart contracts, a regular transaction includes an unconditional order of payment which needs to be validated to be included within a block.

3.2.3.2 Statement of time and place

Statement of time and place with a reliable method in an electronic transferable record satisfies the functional equivalency per ETR Article 13. The technological equivalency principle indicates the compatibility of time and place statements through "*registry, token, **distributed ledger** or other technology"*[168]. As each transaction is time-stamped by the validators while getting included in a certain block, this information will be present for future references in a reliable way, which is necessary for establishing the sequence of the obligors in the action of recourse for negotiable instruments.

Per ETR Explanatory Note paragraph 144, the electronic nature may enable automation of certain action related to time, e.g. negotiable instrument can be presented for payment automatically on its due date through smart-contractualisation and setting the time of presentation as a variable.

3.2.3.3 Drawer's signature

Signature of maker's / drawer's is defined by BEP Article 5(k) as a handwritten signature or an equivalent authentication. Per ESM Article 2(a) and ECC Article 9(3), the functionally-equivalent electronic signature is data in electronic form that reliably identifies the signatory and indicates his approval of information in the data message. The equivalently reliable foreign electronic signatures are also encompassed under this definition per ESM Article 12(3), complementing to a common future international financial infrastructure for negotiable instruments in Blockchain.

Under EU Regulation No 910/2014, which is better known as eIDAS (electronic IDentification, Authentication and trust Services), standards for digital signatures were established for all EU Member States bindingly with three tiers of electronic signatures are defined, each offering higher level of signer ID verification, non-repudiation and security. A regular electronic signature covers all forms, advanced electronic signatures that only the signing party could

[168] ETR, Explanatory Note, para 143

create reflect changes to the original data by getting invalidated in case of data corruption; and qualified electronic signatures are created using a qualified certificate and backed by a Trust Service Provider (TSP) – the only type universally recognised by all EU Member States and is a legal equivalent of handwritten signature.[169] UNCITRAL's functionally equivalent digital signatures can be classified under advanced electronic signatures, which is more suitable for public blockchains. However, smart oracles can be functionally equivalent with TSP's to the extent that both serves to verify identity and match these identities with digital signatures.

Requirement of identifying the signatory could have been legally challenging for Blockchain, however as was the case with identifying the person in control of an electronic record, ETR structure is suitable considering the ETR's Explanatory Note paragraph 78, which states that *"certain electronic transferable records management systems, such as those based on distributed ledgers, may identify the signatory by referring to pseudonyms rather than to real names. That identification, and the possibility of linking pseudonym and real name, including based on factual elements to be found outside distributed ledger systems, could satisfy the requirement to identify the signatory".*

For the reliability aspect of identification, UNCITRAL's approach is that a challenge to the reliability of a certain method cannot lead to invalidation of entire contract if identity of the signatory and authenticity of the signature are non-disputable[170]. Within Blockchain digital signatures are reliable as their authenticity can only be infringed due to keyholder's personal carelessness to the extent of sharing his private key with third parties, only way to obtain the digital signature.

ESM enlists three additional requirements for electronic signatures. Firstly, signature creation data should be linked solely to the signatory at the time of signing to prevent unauthorised transactions. Uniqueness of each signature is vital for satisfying this requirement, and within Blockchain private keys are generated in a way that assures uniqueness, which subsequently leads to unique digital signatures. Second requirement is the detectability of any alteration made to the electronic signature after signing, with last requirement being the detectability of any alteration made to the information for which the signature is used to provide assurance of its integrity. As mentioned earlier, any changes made to the information within a block is

[169] Jacob Boersma, 'Legally binding Blockchain transactions: Can we stop using handwritten signatures already?' (Deloitte, 31 October 2017)
[170] ECC, Explanatory Note, para 164

detectable through hash values; and a changed hash value will automatically indicate the corruption of a digital signature, which is used to encrypt transaction.

3.2.3.4 Drawee's name

For negotiable instruments name (identification) of the drawee is naturally necessary for the transferability of the document. In Blockchain-based system the identification of the drawee by the drawer can be established through the aforementioned self-sovereign ID solution where the public key of the drawee satisfies the verified identification requirement without revealing the information.

3.2.3.5 Making negotiable instrument

A negotiable instrument is created by the drawer, who then transfers the instrument to the drawee. A functionally equivalent definition of drawer can be found in ECC Article 2(c), which defines the "originator" of a data message / electronic record as the person generating data message prior to storage and transfer. Since drawer is the creator of a negotiable instrument, which may have a functionally equivalent electronic transferable record, the generator of such record is functionally equivalent with the drawer. ECC's Explanatory Note further facilitates this argument by stating that notion of "originator" excludes a recipient who store a data message, who is the drawee in negotiable instruments' case. The drawee, on the other hand, has a functional equivalent in the "addressee" of the electronic record, who is defined as the person intended by the originator to receive the record. Here ECC differentiates an addressee from an intermediary, who may be compared to the validator of transactions in Blockchain-based system.

3.2.3.6 Transfer of negotiable instrument

As described in Chapter 1, transfer of a negotiable instrument requires the delivery of paper-based instrument and, if last endorsement is not blank, an endorsement by the holder to the endorsee. Per ETR Article 10(2), if law requires transfer of possession of a transferable instrument, transfer of control over the electronic transferable record meets such requirement. Transfer of control here implies exclusive control to create functional equivalency with the notion of "possession".

Under UNCITRAL instruments, electronic records are deemed composite by nature, meaning association of information can take place any time regardless of the issuance time of the

electronic record. This attribute complements the endorsement system of negotiable instruments without harming the integrity and the originality of the electronic record.[171] Functional equivalency for endorsement is determined under ETR Article 15, which states any information required for endorsement should be included in the electronic transferable record while complying with the written form and signature requirement which were previously analysed.

Per ULC Article 19, the possessor of an endorsable check (or in general, negotiable instrument) is the lawful holder if check consists an uninterrupted series of endorsement. Similarly, the person in control of an electronic transferable record representing a negotiable instrument is the lawful holder if record consists an uninterrupted chain of endorsement, detected through the hash value.

3.2.3.7 Contractual formation

Aside from the functional equivalency, determination of contractual formation is necessary for Negotiable Instrument 2.0. ECM Article 11 reflects UNCITRAL's technological neutrality principle by allowing the expressions of offer and acceptance of an offer through data messages, and not denying validity or enforceability to a contract solely due to usage of data messages.

Rules on the formation of contract is distinguished between instantaneous and non-instantaneous communications of offer and acceptance, with non-instantaneously communicated contracts have multiple theories on when an offer or an acceptance became effective. Face-to-face engagements are one example of instantaneous communication, and, although they are exchanged at a distance, digital engagements within Negotiable Instrument 2.0 can also be classified as instantaneous, simplifying the determination of effectiveness moment.

Under an information system its participants may interact through "electronic communication", which includes any *"statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, made by electronic, magnetic, optical or similar means in connection with the formation or performance of a contract"* per ECC Explanatory Note paragraph 5. The remedy for an error concerning the electronic communication attributable to a natural person is dealt with under UNCITRAL instruments; with the withdrawal of the portion of the electronic communication in which the error was made under certain circumstances rather than correction

[171] ETR, Explanatory Note, para 34

of error.[172] Here UNCITRAL preferred nullification that is better suited for digital environment over correction of an electronic communication which requires modification, a feature incompatible with Blockchain's irrevocable and permanent records. Although nullification of a record is similarly not possible, same result can be achieved with a reversed transaction that would nullify the consequences created by the error.

The right to withdraw an electronic communication cannot be exploited for repudiating disadvantageous transactions or escaping valid legal commitments through nullification, with the right is solely justified if a reasonable person aware of the error at that time would not have issued the electronic communication in the position of the originator.[173] However, if the withdrawn portion contains information without which the electronic communication would be sufficiently definite under United Nations Sales Convention, the entire communication may become invalid or ineffective for purposes of contract formation[174]. For the withdrawal to be effective it has to occur "as soon as possible" and not later than the time when the party has used the value obtained from the other party.[175]

Aside from type of communications, Negotiable Instrument 2.0 has the smart contract feature that arranges liability of endorser which's legal classification has been debated. Under ECC Article 4(g), "automated message system" is defined as a *"an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person each time an action is initiated or a response is generated by the system",* which bears similarity with the smart contract, which can be defined as *"a computer protocol that facilities the transfer of digital assets between parties under the agreed-upon stipulations or terms […] (and) enforce the agreed-upon obligations automatically".*[176] The automatic initiation of action without the review or intervention of a natural person regarding an electronic record is indeed the function of the smart contract feature with the failure of payment automatically initiating the pre-programmed liabilities of previous non-qualified endorsers regarding that negotiable instrument. Attribution of these actions are also addressed in ECM Article 13(2)(b) and ECC Explanatory Note paragraph 213, with the legal entity / person, on whose behalf automated message system is acting on behalf, is in

[172] ECC, Explanatory Note, para 239
[173] ibid para 236.
[174] ibid para 241.
[175] ibid para 246.
[176] Techopedia, 'Smart Contract' (Techopedia)

principle regarded as attributable. However, a technical fault that is beyond the control of the concerned entity / person shall be attributed to the Blockchain's governance, since actions and circumstances caused by a dysfunction in the infrastructure should be attributed to its creator, as it is the case in current traditional payment systems with banks.

3.2.4 Interpreting Blockchain as a platform

As the platform on which Negotiable Instruments 2.0 is built, Blockchain's dynamics and structural mechanisms also require legal interpretation under UNCITRAL instruments. Both in ECM and ECC, an "information system" is defined as a *"system for generating, sending, receiving, storing or otherwise processing data messages"*[177], with the notion covering any technical mean that satisfies the listed functions such as a communication "network"[178]. Similarly, Blockchain establishes a platform on which electronic transferable records of negotiable instruments can be generated, sent, received, stored and processed.

Using such platform requires consent from all parties involved, as the digital transformation can only occur with participation of actors actively regulating and controlling the payment systems (regulators, banks etc.) as well as users who will be subjected to change their habits and adapt. Per ETR Explanatory Note paragraph 66, consent to the use of electronic transferable records in systems without a centralised operator like "distributed ledger-based systems", consent can be implicitly given through actions such as exercise of controlling the record or performing a related obligation.

ECC's definitions allows automated message systems as part of information systems, differing two notions with information systems facilitating exchanges leading to contract formation and automated message systems negotiating and concluding contracts without review or intervention by natural person at one of the ends of negotiation chain. The consensual usage of electronic transferable records combined with the interpretation of information system as Blockchain and automated message system as smart contract establishes the legal foundation upon which Negotiable Instruments 2.0 can be found.

Determining the law applicable for the rights and assets within the Negotiable Instruments 2.0 Blockchain network is vital for a clear legal framework. The *lex rei sitae* rule is incompatible as location of nodes is both in principle indeterminable and even if they were determined, that

[177] ECM, Article 2(f); ECC, Article 4(f)
[178] ECC, Explanatory Note, para 101

would lead to application of various laws within the same network. On the other hand, establishing a function of the jurisdiction which regulates the platform provider and the network, or the law chosen by the platform provider would be more compatible as to ensure legal clarity and predictability. Whichever of both is preferred, the law should be incorporate into the network's internal rule, determining the transfer of assets and rights' execution.[179] To avoid forum shopping by the platform provider for the second case, the choice of law should be restricted to the jurisdictions where major operations or the incorporation of platform provider are present. **[180]**

[179] Philipp Paech, The Governance of Blockchain Financial Networks (December 16, 2016) 39-40
[180] Hague Securities Convention (n 182), Article 4(1)

Conclusion

Negotiable instrument has been around for centuries, shaping the financial landscape while being shaped by it as well. Throughout its lifespan different functionalities of it become prominent; from the facilitation of keeping records or allowing exchanges between distant locations to act as a currency substitute or credit device. Today, negotiable instruments still hold certain value with their ability to store payment records, secure bulk payments for large number of people and act as a viable payment method for technologically illiterate; however, the rise of alternative payment systems, combined with failed attempts to modernise negotiable instrument's structure and regulatory environment has limited the its usage to the extent of extinction in certain jurisdictions. On the other hand, the payment system environment is also in need of structural modernisation and open to disruption from technological advancements.

Blockchain technology has the potential to disrupt various industries, including banking and the payment systems. The unique and previously unthinkable combination of irreversible, decentralised, anonymous yet traceable data storage and transmission has made Blockchain the technology that may rival Internet in terms of transforming the entire world. A young technology with an exponential rate of development, Blockchain has still multiple areas where further work is necessary (consensus algorithms, privacy, GDPR compatibility, user friendliness,…) for it to be a more mature, mass-adopted technology whose applications are regulated without limiting their technological advancements.

Compatibility of Blockchain with negotiable instruments can be perceived as challenging and unusual, since one is a new, disruptive technology that threatens the status quo in different sectors, whereas the other is an old, outdated payment system that has lost its relevancy to its counterparts. Yet, the technical analysis has shown that these two constructs conform one another in various areas while eliminating the disadvantages both possess. Negotiable instruments, although mainly lost its relevancy in practice, are still mostly regulated which offers legal clarity and transparency; something Blockchain-based applications mostly lack. Blockchain technology offers the concept of smart contract, automated and self-enforceable computerised transaction protocol, which can be featured in electronic negotiable instruments for liability chain establishment and determining means of instrument. From a legal perspective the aforementioned conformation is pursued, with multiple instruments of UNCITRAL already consisting concepts and institutions that can accommodate the Blockchain-based negotiable

instrument payment system; especially with their guiding principles of technological neutrality and functional equivalency.

Blockchain can be the technology that will eliminate the disadvantages of negotiable instruments against their counterparts, while negotiable instruments, with their record-keeping, easy-to-digitise character, can be the payment system that will adopt Blockchain to its full potential in finance industry. The same financial industry has already spent over $1.4 billion on research into Blockchain technology[181], indicating how Blockchain, a relatively young technology, can pioneer the transformation in this field. Two main features of Blockchain, decentralised data controlled solely by its owner and the digital interface are vital for the mass adoption of the so-called "Negotiable Instruments 2.0". An Ernst & Young survey revealed nearly half of consumers will limit access to their data in the near future and over the half of them are already providing less data, including self-driven social media censor, than in the previous five years.[182] In addition, the "Digital in 2017 Global Overview" report from We Are Social and Hootsuite indicates half of the world's population uses a smartphone, with 1.75 billion new users over the next eight years expected to be added to mobile internet market through cheaper smartphones and data plans, reaching a milestone of 5 billion mobile internet users in 2025. If Blockchain-based negotiable instrument payment system can comply with data protection regulations such as GDPR while offering a digital interface that is accessible through smart phones with mobile internet, it may very well become the payment system of the future.

[181] R. Jesse Mcwaters, 'The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services' (World Economic Forum, 12 August 2016)
[182] Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, (2016) 98

Bibliography

Alex Batlin, 'Digital Identity on Blockchain: Alex Batlin's "prediction"' (Fintech Switzerland, 15 September 2015) <http://fintechnews.ch/blockchain_bitcoin/digital-identity-on-blockchain-alex-batlins-prediction/803/> accessed 5 June 2018

Anna Irrera, 'Bank-backed R3 launches new version of its blockchain' (Reuters, 3 October 2017) <https://www.reuters.com/article/us-r3-blockchain/bank-backed-r3-launches-new-version-of-its-blockchain-idUSKCN1C80MS> accessed 4 June 2018

Antonio Madeira, 'The DAO, The Hack, The Soft Fork and The Hard Fork' (Cryptocompare, 20 May 2018) <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/> accessed 4 June 2018

Babic-Hodovic, Mehic, Arslanagic, Influence of Banks' Corporate Reputation on Organizational Buyers Perceived Value (7th International Strategic Management Conference, Elsevier Ltd 2011). Available at: https://ac.els-cdn.com/S1877042811015916/1-s2.0-S1877042811015916-main.pdf?_tid=663bc89c-77f5-4a49-a79e-924788448663&acdnat=1528187307_b62941f5bc1a0fb8774e27745d18a4ac

Basel Committee on Banking Supervision, 'International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version' (Bank for International Settlements, June 2006) <https://www.bis.org/publ/bcbs128.pdf> accessed 5 June 2018

Beau Stoner, 'Ethereum's Future Proof-of-Stake Casper Upgrade | A Detailed Overview' (Cryptocurrency Australia, 15 March 2018) <https://cryptocurrencyaus.com/2018/03/15/ethereum-casper/> accessed 4 June 2018

Board of Governors of the Federal Reserve System, The Federal Reserve Payments Study: 2017 Annual Supplement. Available at: https://www.federalreserve.gov/paymentsystems/2017-December-The-Federal-Reserve-Payments-Study.htm

Calcaterra, Craig and Kaal, Wulf A. and Andrei, Vlad, Semada Technical Whitepaper - Blockchain Infrastructure for Measuring Domain Specific Reputation in Autonomous Decentralized and Anonymous Systems (February 18, 2018). Available at SSRN: https://ssrn.com/abstract=3125822 or http://dx.doi.org/10.2139/ssrn.3125822

Center for Financial Training, Banking Systems. 2nd ed. ed., (South-Western Cengage Learning, 2010)

Christopher Demicoli, 'Introduction to the Diffie-Hellman Key Exchange' (blog.cdemi, 8 June 2016) <https://blog.cdemi.io/introduction-to-the-diffie-hellman-key-exchange/> accessed 4 June 2018

Committee on Payments and Market Infrastructures, Statistics on payment, clearing and settlement systems in the CPMI countries: Figures for 2015 (Bank for International Settlements 2016). Available at: https://www.bis.org/cpmi/publ/d155.pdf

Crouch v. The Credit Foncier of England, Ltd., L.R. 8 Q.B. 374,381 (1873)

D.P. Whiting, The Concept of Negotiability (Macmillan Master Series 1985)

Dannielle Correa, 'Security concerns are inhibiting mobile payment adoption worldwide' (SC Magazine, 07 October 2016) <https://www.scmagazine.com/security-concerns-are-inhibiting-mobile-payment-adoption-worldwide/article/548120/> accessed 4 June 2018

Demirgüç-Kunt, Klapper, Singer, Ansar, Hess, The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution (International Bank for Reconstruction and Development/The World Bank 2018). Available at: https://globalfindex.worldbank.org/

Dhillon, Metcalf, Hooper, Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You, (1st Apress Berkely, CA, USA, 2017)

Digiconomist, 'Bitcoin Energy Consumption Index' (Digiconomist) <https://digiconomist.net/bitcoin-energy-consumption> accessed 4 June 2018

European Banking Authority, 'Passporting and supervision of branches' (European Banking Authority) <https://www.eba.europa.eu/regulation-and-policy/passporting-and-supervision-of-branches> accessed 4 June 2018

Faster Payments Task Force, Faster Payments Effectiveness Criteria. Available at: https://fedpaymentsimprovement.org/wp-content/uploads/fptf-payment-criteria.pdf

Faster Payments Task Force, The U.S. Path to Faster Payments Final Report Part One: The Faster Payments Task Force Approach. Available at: https://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-final-report-part1.pdf

Faster Payments Task Force, The U.S. Path to Faster Payments Final Report Part Two: A Call to Action. Available at: https://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-final-report-part1.pdf

Federal Reserve Bank of Boston, Putting It Simply, (1984); reported in Peter Cook, Federal reserve, fractional reserve and interest-free government credit explained in question and answer form, (1991)

Federal Reserve Board, The Federal Reserve Payments Study: 2017 Annual Supplement (Federal Reserve System 2017). Available at: https://www.federalreserve.gov/newsevents/pressreleases/files/2017-payment-systems-study-annual-supplement-20171221.pdf

Feldman, Papadimitriou, Chuang, Stoica, Free-Riding and Whitewashing in Peer-to-Peer Systems (3rd Annual Workshop on Economics and Information Security (WEIS2004) 2004). Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1.1493&rep=rep1&type=pdf

Gregory E. Maggs, The Holder in Due Course Doctrine as a Default Rule, (32 Ga. L. Rev. 783 1998)

Hector Lopez, 'How is a private key created for Bitcoin?' (Medium, 16 November 2017) <https://medium.com/@hlopez_/how-are-public-and-private-keys-created-in-bitcoin-f90b2b88f40a> accessed 4 June 2018

Investopedia, 'Double Spending' (Investopedia) <https://www.investopedia.com/terms/d/doublespending.asp> accessed 4 June 2018

Investopedia, 'Eurocheck' (Investopedia) <https://www.investopedia.com/terms/e/eurocheque.asp> accessed 5 June 2018

J. Rogers, The End of Negotiable Instruments: Bringing Payment Systems Law Out of the Past, (Oxford University Press 2011). Retrieved 7 Feb. 2018, from http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199856220.001.0001/acprof-9780199856220.

Jacob Boersma, 'Legally binding Blockchain transactions: Can we stop using handwritten signatures already?' (Deloitte, 31 October 2017) <https://www2.deloitte.com/nl/nl/pages/risk/articles/legally-binding-blockchain-transactions.html> accessed 4 June 2018

Jeremy M. Sklaroff, Smart Contracts and The Cost of Inflexibility, (University of Pennsylvania Law Review). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3008899

John R. Douceur, 'The Sybil Attack' (UIowa, 2003) <http://www.divms.uiowa.edu/~ghosh/sybil.pdf> accessed 5 June 2018

Joseph J. Bambara and Paul R. Allen, Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions (McGraw-Hill Education 2018)

K. Scheller Hanspeter, The European Central Bank – History, Role and Functions (European Central Bank 2004). Available at: https://www.ecb.europa.eu/pub/pdf/other/ecbhistoryrolefunctions2004en.pdf

Kai Stinchcombe, 'Blockchain is not only crappy technology but a bad vision for the future' (Medium, 5 April 2018) <https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-c1ca122efdec> accessed 5 June 2018

Kai Stinchcombe, 'Ten years in, nobody has come up with a use for blockchain' (Hackernoon, 23 December 2017) <https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100> accessed 4 June 2018

Katie Robertson, 'Why Can't Americans Ditch Checks?' (Bloomberg, 26 July 2017) <https://www.bloomberg.com/news/articles/2017-07-26/why-can-t-americans-give-up-paper-checks> accessed 4 June 2018

Koji Takahashi, 'Blockchain technology and electronic bills of lading' [2016] 22 The Journal of International Maritime Law <https://www1.doshisha.ac.jp/~tradelaw/PublishedWorks/BlockchainTechnologyElectronicBL.pdf> accessed 5 June 2018

Kolvart, Poola, Rull, Smart Contracts. in Kerikmae, Rull (ed), The Future of Law and eTechnologies (Springer International Publishing Switzerland 2016)

Lary Lawrence, An Introduction to Payment System, S 53 (1997)

League of Nations Convention Providing a Uniform Law for Cheques [1931]

Matt Luongo, 'Zero-knowledge proofs, Zcash, and Ethereum'" (Keep Network, 19 September 2017) <https://blog.keep.network/zero-knowledge-proofs-zcash-and-ethereum-f6d89fa7cba8> accessed 4 June 2018

Matthew Leising, 'The Blockchain Revolution Gets Endorsement in Wall Street Survey' (Bloomberg, 22 July 2015) <https://www.bloomberg.com/news/articles/2015-07-22/the-blockchain-revolution-gets-endorsement-in-wall-street-survey> accessed 4 June 2018

Moneycontrol, 'What is Cheque Truncation System' (Moneycontrol, 5 February 2013) <https://www.moneycontrol.com/news/business/stocks/-1778499.html> accessed 4 June 2018

Mougayar, William, Buterin. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, (John Wiley & Sons, Incorporated, 2016) ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/uvtilburg-ebooks/detail.action?docID=4516142.

Neil Wallace, Fiat Money, 1-9. 10.1057/978-1-349-95121-5_454-2 (2008)

Nikolic, Kolluri, Sergey, Saxena, Hobor, Finding The Greedy, Prodigal, and Suicidal Contracts at Scale (Arxiv.org 2018). Available at: https://arxiv.org/pdf/1802.06038.pdf

Odysseas Sclavounis, 'Understanding Public Blockchain Governance' (Oxford Internet Institute, 17 November 2017) <https://www.oii.ox.ac.uk/blog/understanding-public-blockchain-governance/> accessed 4 June 2018

Philipp Paech, The Governance of Blockchain Financial Networks (December 16, 2016). (2017) 80(6) Modern Law Review 1073–1110; LSE Legal Studies Working Paper No. 16/2017. Available at: https://ssrn.com/abstract=2875487

Proceedings of the Congress of the United Nations Commission on International Trade Law Vienna. Modernizing International Trade Law to Support Innovation and Sustainable Development, 4-6 July 2017, Volume 4: Papers presented at the Congress. Available at: www.uncitral.org/pdf/english/congress/17-06783_ebook.pdf

Procivis, 'eID+ is' (Procivis, 24 January 2017) <http://procivis.ch/eid/what-is-eid/> accessed 4 June 2018

Procivis, 'Trusted interaction between citizens and government' (Procivis, 24 January 2017) <http://procivis.ch/eid/use-cases/> accessed 4 June 2018

R. Jesse Mcwaters, 'The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services' (World Economic Forum, 12 August 2016) <https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services/> accessed 4 June 2018

r3, 'Blockchain for business: Delivering the world's only blockchain built specifically for the enterprise' (r3) <https://www.r3.com/> accessed 4 June 2018

Raul Amoros, 'Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?' (Howmuch, 10 January 2018) <https://howmuch.net/articles/crypto-transaction-speeds-compared> accessed 4 June 2018

Roger Aitken, 'Blockchain To The Rescue Creating A 'New Future' For Digital Identities' (Forbes, 7 January 2018) <https://www.forbes.com/sites/rogeraitken/2018/01/07/blockchain-to-the-rescue-creating-a-new-future-for-digital-identities/ - 71a8e82e5492> accessed 4 June 2018

Santander, Innoventures, Oliver Wyman, Anthemis Group, 'The Fintech 2.0 Paper: rebooting financial services' (Finextra, 2015) <https://www.finextra.com/finextra-downloads/newsdocs/the fintech 2 0 paper.pdf> accessed 5 June 2018

Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (Bitcoin, October 2008) <https://bitcoin.org/bitcoin.pdf> accessed 5 June 2018

Sergii Moshenskyi, History of the Weksel Bill of Exchange and Promissory Note (New York: Xlibris 2008). Available at: https://archive.org/details/bub_gb_8UBDndXgNIYC

Simon Kemp, 'Digital in 2017: Global Overview' (We Are Social, 24 January 2017) <https://wearesocial.com/special-reports/digital-in-2017-global-overview> accessed 5 June 2018

Steven L. Harris, Introduction to Rethinking Payments Law, 83 Chi.-Kent L. Rev. 477 (2008). Available at: https://scholarship.kentlaw.iit.edu/cklawreview/vol83/iss2/3

Tapscott, Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, (2016)

Techopedia, 'Smart Contract' (Techopedia) <https://www.techopedia.com/definition/32499/smart-contract> accessed 4 June 2018

The Law Society, 'Legal system must keep pace with technology to be fit for the future, says the Law Society' (The Law Society, 22 June 2016) <http://www.lawsociety.org.uk/news/press-releases/legal-system-must-keep-pace-with-technology-to-be-fit-for-the-future/> accessed 4 June 2018

United Nation Convention on the Use of Electronic Communications in International Contracts [2007]

United Nation Model Law on Electronic Commerce with Guide to Enactment [1996]

United Nation Model Law on Electronic Signatures with Guide to Enactment [2001]

United Nation Model Law on Electronic Transferable Records [2017]

United Nations Commission on International Trade Law, 'FAQ - UNCITRAL Texts' (UNCITRAL) <http://www.uncitral.org/uncitral/en/uncitral_texts_faq.html> accessed 4 June 2018

United Nations Convention on International Bills of Exchange and Promissory Notes [1988]

United Nations Convention on the Law Applicable to Certain Rights in respect of Securities Held with an Intermediary, “Hague Securities Convention” [2006]

United Nations, 'Progressive Development of the Law of International Trade: Report of the Secretary-General of the United Nations' (Jus UiO, 1966) <http://www.jus.uio.no/lm/un.sg.report.itl.development.1966/1.html> accessed 5 June 2018

Vitalik Buterin, 'Ethereum/wiki/problems' (GitHub, 25 August 2014) <https://github.com/ethereum/wiki/wiki/Problems> accessed 4 June 2018

World Bank Group, Cash vs Electronic Payments in Small Retailing Estimating the Global Size (International Bank for Reconstruction and Development / The World Bank 2016). Available at: http://pubdocs.worldbank.org/en/219031465585757849/WBG-Electronic-Payments-Small-Retailing.pdf

Yuval Noah Harari, Sapiens: A Brief History of Humankind (Penguin Random House 2011)

Zane Witherspoon, 'A Hitchhiker's Guide to Consensus Algorithms' (Hackernoon, 13 February 2018) <https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3> accessed 4 June 2018