

BLOCKCHAIN TECHNOLOGY AND SMART CONTRACTS FROM A FINANCIAL LAW PERSPECTIVE

BLOCKCHAIN TECHNOLOGY IN FINANCIAL TRANSACTIONS:
REGULATING A REVOLUTION?

Maurice Demeyer

Student number: 01310663

Supervisor: Prof. Dr. Michel TISON

Commissary: Mr. Evariest CALLENS

A dissertation submitted to Ghent University in partial fulfillment of the requirements for the degree of Master of Laws.

Academic year: 2017 - 2018

ACKNOWLEDGMENTS

This Master's dissertation demarks the final moments of my law studies at Ghent University and therefore, it is the ideal opportunity to express my sincere gratitude to everyone who participated in making the past five years exciting, intellectually enriching and simply exceptionally beautiful.

I would like to acknowledge the Institute of Financial Law at Ghent University for decisively inciting my interest through the various advanced legal courses offered on capital markets, private banking law and corporate law. I am especially thankful to my thesis supervisor, professor Michel TISON, for granting me the opportunity to immerse myself in the intriguing topic of distributed ledger technology and for his continuous guidance, advice and enthusiasm.

My parents have always given me all chances and freedom, and my family has steadfastly encouraged me during stressful periods of deadlines and exams. They play a crucial role in my life and I am very grateful for their love and support.

I would also like to thank my friends in computer engineering, Wout, Nathan and Dries, for answering my many questions and assessing my statements, for proofreading my work and for all enlightening discussions we had together.

Finally, I wish to acknowledge the friendly people of Living Tomorrow, Becon, Larcier, Intersentia and the IFR for hosting blockchain and fintech conferences and for kindly welcoming me at these outstanding events, where I have gathered numerous important insights for my research.

Maurice Demeyer

Ghent, 15 May 2018

ABSTRACT (ENGLISH AND DUTCH)

Through extensive study of literature, this Master's dissertation aims to identify the opportunities created by the advent of first and second generation distributed ledger technology in the context of the financial sector. It also assesses the regulatability of various distributed ledger configurations, and their relation to the pre-existing legal framework. Finally, it identifies a number of priorities for suggested future law changes.

Our research leads to a categorization of possible distributed ledger technology applications, based on a varying degree of decentralization: from highly decentralized native crypto-asset blockchains to permissioned interbank payment and settlement ledgers; from irreversible smart contracts that are meant to embody the legal agreement to smart contracts with a point of entry for judicial intervention and which co-exist with a prevailing traditional contract.

This dissertation establishes that all degrees of decentralization are or can be regulated by one way or another and that certain changes to the existing legal framework are desirable to maximally benefit from the unique capacities of distributed ledger technology.

Deze Masterscriptie is erop gericht om, op basis van een uitgereide literatuurstudie, de mogelijkheden te identificeren die “gedeeldgrootboektechnologie” (*distributed ledger technology*) van de eerste en tweede generatie biedt in de financiële sector. Het evalueert bovendien de vatbaarheid voor regulering van verscheidene *distributed ledger* constellaties, alsook hun verhouding tot het positief recht. Ten slotte duidt deze scriptie een aantal prioriteiten aan voor de voorgestelde toekomstige wetswijzigingen.

Ons onderzoek leidde tot een categorisering van de mogelijke *distributed ledger* toepassingen, gebaseerd op hun verschillende graad van decentralisatie: gaande van uiterst gedecentralizeerde *native* crypto-activa netwerken tot beperkt toegankelijke interbank betaal- en afwikkelingssystemen; en gaande van onomkeerbare *smart contracts* die beogen de onderliggende juridische overeenkomst te vervangen tot *smart contracts* die rechterlijke tussenkomst toelaten en die naast een primerend traditioneel contract bestaan.

Deze dissertatie stelt vast dat alle gradaties van decentralisatie aan regulering onderhevig zijn of op de één of andere manier voor regulering vatbaar zijn, en dat bepaalde wetswijzigingen wenselijk zijn teneinde maximaal maatschappelijk voordeel te halen uit de unieke capaciteiten van *distributed ledger technology*.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	iii
ABSTRACT (ENGLISH AND DUTCH)	v
TABLE OF CONTENTS	vii
TITLE 1. INTRODUCTION.....	11
TITLE 2. BLOCKCHAIN EXPLAINED	15
A. INFORMATION TECHNOLOGY	15
B. PRINCIPAL CATEGORIZATIONS.....	18
1. Network access	18
2. Stages of development	23
3. Consensus mechanisms	26
C. DLT APPLICATIONS	29
TITLE 3. CRYPTO-ASSETS.....	31
CHAPTER 1. CRYPTOCURRENCIES	31
A. HIGHLY DECENTRALIZED AND PUBLIC – <i>electronic cash</i>	32
1. Qualification by an economist	32
2. Qualification by a lawyer	34
3. Regulation?.....	36
B. PERMISSIONED AND PRIVATE – <i>blockchain-based interbank payment solutions</i>	38
1. Interbank financial communication network	39
2. Interbank money remittance network.....	41
3. Regulation?.....	42
a. Individual nodes.....	44
b. Blockchain as an entity	45
c. Transactions.....	47
C. CONCLUSION	48
CHAPTER 2. CRYPTOSECURITIES.....	50
A. THE MODERN SECURITIES MARKET – <i>intermediaries, origins and problems</i>	50
1. Trade lifecycle.....	50

2. Origins	52
3. Deficiencies of the intermediated infrastructure	54
4. The blockchain alternatives	55
B. HIGHLY DECENTRALIZED AND PUBLIC – <i>token sales, ICOs and</i>	56
1. vs. cryptocurrencies?	56
2. Regulation?	59
a. Issuance and market infrastructure	59
b. Transactions	61
3. Conclusion	62
C. PERMISSIONED AND PRIVATE – <i>blockchain-based interbank securities clearing and settlement</i>	64
D. CONCLUSION	68
TITLE 4. SMART CONTRACTS	71
CHAPTER 1. ORIGINS	71
CHAPTER 2. CODERS’ APPROACH – <i>code is law</i>	73
CHAPTER 3. SMART LEGAL CONTRACT – <i>law is law, and code is code</i>	74
A. RELEVANT DISTINCTIONS	76
1. Operational vs. non-operational contract clauses	76
2. Automatable vs. non-automatable contractual rights and obligations	78
3. Strong vs. weak smart contract code	78
4. External vs. internal smart contract models	79
B. IN PRACTICE	79
1. External smart legal contract	80
a. Setup and use	80
b. Non-operational and non-automatable distortions	81
c. Smart bugs: disputes and unwanted output	82
2. Internal smart legal contract	83
a. Setup and relevance	83
b. Non-operational and non-automatable distortions	84
i. <i>General non-operational clauses</i>	84

ii. <i>Ambiguous clauses</i>	85
iii. <i>Non-automatable elements</i>	86
c. Smart bugs: disputes and unwanted output	86
i. <i>Strong internal smart contract</i>	86
ii. <i>Weak internal smart contract</i>	88
C. CONCLUSION	88
TITLE 5. CONCLUDING CONSIDERATIONS	93
BIBLIOGRAPHY	95

TITLE 1. INTRODUCTION

Liberty in cyberspace will not come from the absence of the state. Liberty there, as anywhere, will come from a state of a certain kind.¹

– L. LESSIG, *Code 2.0*

1. In 2009, when Satoshi NAKAMOTO first introduced *Bitcoin*, the world was absorbed by the revolutionary idea of a ‘virtual currency.’^{2,3} Besides physical money, funds held in accounts in commercial banks and electronic money, a new way to transfer, receive and even create value was born. The virtual currencies appeared to be groundbreaking because of their advantages regarding transaction speed around the globe, security, low cost and high privacy. ‘*Bitcoin*’ was and still is a buzzword. In fact, the expectations it created and the 2017 ‘investor’ excitement overshadowed the relatively simple but ingenious design of the coin’s software. Nearly ten years after its release, *Bitcoin* and its many varieties are still too volatile to lastingly reshape the landscape of established currencies. Focus now shifted to the implementation behind the virtual currency transactions: a distributed system of information ledgers called the ‘blockchain’.⁴ The variety of this technology’s potential applications is virtually unlimited and stretches far beyond the original idea of coins and currencies. Some authors predict that this method to exchange and record information will innovate almost every aspect of our daily life and economic activities. Accordingly, PETERS and PANAYI claim that blockchain is the latest disruptive technology.⁵ The view presented by Gartner is more cautious but this organization’s well-known ‘Hype Cycle’ positions

¹ L. LESSIG, *Code version 2.0*, New York, Basic Books, 2006, 4. Available at <http://codev2.cc/download+remix/Lessig-Codev2.pdf>, last accessed 3 February 2018.

² S. NAKAMOTO, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. Available at <https://bitcoin.org/bitcoin.pdf>, last accessed 6 March 2017.

³ ‘Satoshi NAKAMOTO’ is a pseudonym adopted by the individual or group behind the original *Bitcoin* concept.

⁴ Blockchain technology is also referred to as distributed ledger technology (DLT) or as a decentralized ledger, decentralized network. However, to be precise, blockchain is the first fully functional manifestation of DLT. A DLT is a distributed database and blockchain is a DLT which is organized as a chain of blocks that contain transactional data.

⁵ G.W. PETERS and E. PANAYI, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money” in P. TASCA, T. ASTE *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016, 276.

blockchain past the peak of inflated expectations with a mainstream adoption horizon of five to ten years.⁶

2. Large numbers of new articles and insights on the subject are published on a weekly basis. However, this literature and the ideas described therein are characterized by the frequent use of phrases expressing hesitation like “could be”, “might become”, “would mean” ... This dissertation has the ambition to identify whether and by what means the distributed ledgers truly justify the use of the word “disruptive”, and how the law answers to it. Because developments are generally first driven by market dynamics and later sanctioned by the law, we believe that a legal approach particularly suitable in order to identify blockchain applications that are more likely to actually cause substantial transitions in the near to middle long future. This research focusses on how these transitions thrive in a pre-existing legal framework and how both the innovation and the law mature together, in a process based on dialogue, growing insight and experience. Indeed, new internet technology like DLT does not simply emerge in a legal vacuum.⁷ The finding that its architecture relies on libertarian ideas about abolishing the middleman (and other external forms of control) does not affect this legal reality.

3. One domain of law where the role of the middleman is of particular relevance, is financial law. The modern banking infrastructure is continuously under development because of the consistently increasing volume, speed, global spread and complexity of executed transactions. While monetary payments are executed through their own electronic settlement architectures (*e.g.* the TARGET2 service operated by the European Central Bank (ECB) or the Continued Linked Settlement (CLS) system for foreign exchange), the dematerialization on securities allowed for increased liquidity on securities markets as well.⁸ Nowadays however, the degree of liquidity in this context is challenged by efficiency limits. The dematerialized security assets are held and transferred through an international settlement network characterized by its patchiness and its complex pyramidal structure. Its operation is based on an intricate array of accounts and registers as well as an interplay of

⁶ X., “Gartner Hype Cycle for Emerging Technologies”, 2017. Available at <https://blogs.gartner.com/smarterwithgartner/files/2017/08/Emerging-Technology-Hype-Cycle-for-2017-Infographic-R6A.jpg>, last accessed 20 February 2018.

⁷ L. LESSIG, *Code version 2.0*, New York, Basic Books, 2006, 4. Available at <http://codev2.cc/download+remix/Lessig-Codev2.pdf>, last accessed 3 February 2018.

⁸ For the sake of clarity, we will be using the term “securities” interchangeably to refer to different kinds of negotiable financial assets; only making distinctions where it is essential.

many intermediaries whose regulation and supervision are shared amongst a corresponding number of jurisdictions. The introduction of DLT opened the door for a new massive step in the ongoing development of the securities market architecture: after dematerialization comes *cryptonization*.⁹ Analogous to the *Bitcoin* procedure, today's dematerialized securities could be converted to assets represented by bits and bytes in a network that permits direct, speedy and inexpensive transfers from one user to another. This network may substitute both the registers and the role of the intermediaries thanks to its revolutionary technical design. Such innovation poses challenges for – or, if you like: is challenged by – many aspects of the existent, dense financial regulation. We believe that the abundant number of important policy considerations renders financial law the ideal subject for legal research on how disruptive DLT really is.

4. The next paragraphs provide a brief summary of how this research endeavour is structured. First, we inevitably need to explain the crucial aspects of what blockchain is, and how and why it works. This section on computer science is kept to the essential information required for the reader to further understand the impact of the technology from a financial-legal point of view. It also sets out some of the key technical categorizations of blockchain varieties existing thus far. Indeed, the individual characteristics of the code at the basis of a certain blockchain software application have important repercussions on its legal analysis.

Subsequently, this paper is organised in a way that follows the evolutionary steps of blockchain itself. As discussed in paragraphs 16 to 19, three development stages or 'generations' of distributed ledger technology currently coexist: crypto-assets, smart contracts and decentralized autonomous organizations. The reader will observe that the red line running through these chapters exists in the question how these novelties may be useful to contemporary financial transactions and actors; and, how such applications fit in the existing legal framework. As the development of the third category depends on the gradually maturing groundwork of the first two categories, we will highly limit our analysis to the legal questions and challenges faced by crypto-assets and cryptosecurities. We will thereby

⁹ This relatively new term has been used in relation to cryptocurrencies (see for example O. J. MANDENG, "Cryptocurrencies, monetary stability and regulation: Germany's nineteenth century private banks of issue", *LSE Institute of Global Affairs* 2018. Available at <http://www.lse.ac.uk/iga/assets/documents/research-and-publications/LSE-IGA-WP-5-2018-Ousmene-Mandeng.pdf>, last accessed 11 March 2018.), not so much in relation to securities. Its conceptual meaning is equally applicable and forms a logical next step after the dematerialization of various kinds of assets.

try to establish to which extent new blockchain-based financial procedures assimilate with contemporary financial processes and traditional legal concepts; and whether a need exists for specific regulations of a whole new nature: the domain *Lex Cryptographia*.¹⁰

¹⁰ For the origin of this term, see: A. WRIGHT and P. DE FILIPPI, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia”, 2015. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

TITLE 2. BLOCKCHAIN EXPLAINED

A. INFORMATION TECHNOLOGY

5. The outset of this research will explain the main characteristics of the distributed ledger's unique setup. We will commence with a simplified practical description of the blockchain, followed a brief theoretical clarification. We will then lay out some important classifications based on the technical particularities of the existing blockchain varieties. Finally, this chapter will describe several interesting blockchain applications to further illustrate the technology and its broad potential for practical use.

6. A blockchain network is in fact nothing but a collective, chronological and public bookkeeping of information via the internet.¹¹ This information can be anything – for example, it may consist of numerous changes of possession regarding an asset that is represented by a digital file of data. Since digital goods are essentially easy to copy, they are particularly subject to the risk of double spending.¹² Public bookkeeping of all transactions in a database helps to mitigate this risk as it enables other actors to verify who most recently acquired the digital asset. It is however not always easy to preserve the authenticity of the information in the books, especially in situations where everybody can access them. Hence, in a blockchain, all transactions are recorded in one shared ledger which is simultaneously accessed, saved and updated locally by every user participating in the network, which makes it a 'distributed' ledger. This distributed arrangement is what makes the blockchain novel in comparison to a traditional database. The different participants in a certain network are called 'nodes'.¹³ Users who wish to take in upholding the network can become a node themselves and start verifying and saving the entire bookkeeping.

¹¹ This comparison is inspired by one of the earliest easy-to-understand explanatory videos on blockchain: DUTCHCHAIN, "The real value of bitcoin and crypto currency technology - The Blockchain explained", video, 2014. Available at <https://www.youtube.com/watch?v=YIVAluSL9SU>, last accessed 6 March 2017.

See also, a more recent video: WESTPAC BANKING, "Blockchain Demystified", video, 2016. Available at <https://youtu.be/LdOcXXB48fI>, last accessed 6 March 2017.

¹² D. DRESCHER, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, New York, Springer Science+Business Media, 2017, 51.

¹³ We will only consider users who participate in the validating DLT transactions to 'run a node'. In our definition, users who take part in these transactions do not necessarily need to be a node themselves.

7. In order to secure the integrity of the contents of the database, it is structured as a chronological and interconnected chain of packages of data, the blockchain. The software will only allow an irreversible addition of new information to the decentralized ledger if the nodes reach consensus on the correctness of the new data. Control over validating a new addition is essentially shared among nodes in a blockchain – it is not allocated to any central authority. Consequentially, trust is factually distributed, decentralized in a distributed ledger, preventing malevolent nodes or intruders from unilaterally manipulating its contents.

8. The particular procedure that governs the approval of a transaction by the network is called a ‘consensus mechanism’. It does not necessarily rely on singular voting rights per node – it depends on the individual software which is built to meet the needs and purpose of a certain application. The influence or ‘weight’ of each node is calculated in accordance with the standards of the specific blockchain. In situations where nodes do not know each other, and therefore, trust is absent, this factor is often derived from calculations performed by the nodes to the network: ‘one-CPU-one-vote’.¹⁴ *Bitcoin* is the prime example of a blockchain based on this mechanism, called ‘proof-of-work’. Each node automatically collects the new transactions that are to be confirmed in a package of data, a block, then starts confirming this block. The *Bitcoin* nodes invest considerable amounts of computational power (hence ‘one-CPU-one-vote’) to solve the mathematical ‘hash puzzles’ generated based on the data in the block and on the solution of the puzzle of the preceding block of transactions.¹⁵ The complexity of the puzzle is adapted to the desirable completion time; in case of *Bitcoin*, this is ten minutes for each block of transactions. It is difficult to predict who will solve the puzzle first – this procedure is often compared to a lottery; but once the block of transactions has been verified, it is easy for the rest of the network to verify the correctness of the solution to its puzzle. The solution, a ‘hash’, is then attached to the block. It functions as the block’s unique signature or fingerprint and it makes the information tamper-proof: any change to the transactions would invalidate the correspondence between the block and its signature.¹⁶ Even if it were possible to manipulate the complexly generated signature instantaneously, the coherence with the preceding and consecutive block in the

¹⁴ S. NAKAMOTO, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, 3. Available at <https://bitcoin.org/bitcoin.pdf>, last accessed 6 March 2017.

¹⁵ This puzzle is called a ‘hash function’ and its output is a ‘hash’ – the data inside is literally hashed, mixed-up until it is no longer intelligible.

¹⁶ D. DRESCHER, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, New York, Springer Science+Business Media, 2017, 84.

chain would be damaged and the interference would be obvious.¹⁷ Moreover, the puzzle is a cryptographic hash function, making it impossible to trace the input based on the output.¹⁸ The finalized new block of data is subsequently broadcasted to all other nodes in the network. They can verify the correctness of the hash instantaneously and they will add the new block to their local copy of the blockchain and the new, longest chain of transactions will be deemed authoritative. A rewards-based system incentivizes the nodes of a blockchain network to participate in supporting the calculations. In the *Bitcoin* context, this exists in rewarding virtual currency to the participant solving the puzzle – he ‘mines’ a (fraction of a) new coin. Besides the proof-of-work consensus mechanism described above, other voting systems exist which may be more suitable to meet the requirements of different blockchain appliances, e.g. proof-of-stake.^{19, 20}

9. Note that, thanks to its unique structure, the distinctive features of a blockchain and DLT systems in general are its:

- Distributed trust: new transactions are confirmed by the aggregate of all network participants pursuant to the blockchain’s consensus mechanism. There is no need for a trusted third party.
- Immutability: the data structure of interlinked blocks, each with a cryptographic signature attached to it, makes it very difficult to secretly change the ledger’s contents.
- Durability: all nodes hold a local copy of the blockchain – the number of backups of the data is equal to or greater than the number of nodes in the network.

These features are essential to every blockchain or DLT, but the underlying architecture and algorithms differ to meet the specific needs of every application’s individual purpose. The next paragraphs will discuss the most important variations.

¹⁷*Ibid.*, 86.

¹⁸ For more details about cryptographic hash functions, see S. FRIEDL, “An Illustrated Guide to Cryptographic Hashes”, 2005. Available at <http://www.unixwiz.net/techtips/iguide-crypto-hashes.html>, last accessed 15 April 2018.

¹⁹ The proof-of-work consensus mechanism now takes approximately. 7 minutes to validate a Bitcoin transaction, although now it is coded to confirm a block in around 10 minutes. It takes substantially more time to confirm more sizable packages of information through proof-of-work (like coded contracts, *infra*, 18).

²⁰ *Infra*, 22.

B. PRINCIPAL CATEGORIZATIONS

10. In order to increase the reader’s insight in the diversity of blockchain designs, this section highlights three prevailing structural blockchain classifications. The distinctions are based on the access to the network, the transactional complexity and the used consensus mechanism. We invite the reader to bear this typology in mind as it will facilitate understanding the impact of a blockchain’s individual design on the legal analysis in the subsequent chapters.

1. Network access

11. Distributed ledger networks can firstly be classified based on who is allowed to access or participate in the network. These are two distinct questions – users can access the contents of the ledger and submit new information to it while network participants are nodes, responsible for validating new information thus executing the consensus mechanism. Network access as a user is determined by the distinction between public and private networks whereas access as a node depends on the permissioned or permissionless character of the network.^{21, 22} In many blockchains, there is an overlap between both criteria because users also have an interest in keeping the network up and running. The distinction between public and private ledgers is however independent from the question whether a network is permissionless or not.

12. Most of the well-known blockchains in existence are of the permissionless kind. This means that any aspiring participant can become a node in the network straight away, without the need for prior authorisation. As it is the case in the *Bitcoin* network, anyone with a computer can start supporting the network as a node, by verifying new transactions, thus start mining new coins.

²¹ Note that a singular interpretation of these discerning characteristics does not yet exist among authors. Many sources use private, public and permissioned, permissionless in an intertwined manner (see for example J.D. CAYTAS, “Developing Blockchain Real-Time Clearing and Settlement in the EU, U.S. and Globally”, *Columbia Journal of European Law: Preliminary Reference* 2016, 6-7). We hereby establish an important distinction between both concepts, which we consistently rely on throughout this research.

²² G.W. PETERS and E. PANAYI, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money” in P. TASCA, T. ASTE *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016, 244.

Some enthusiasts argue that this designed openness and impartiality is the only sensible option for a true blockchain, in line with its anti-institutional, libertarian philosophy.²³ The ultimate goal is to exclude any sort of ‘corruption’ – either by distortion of what the parties really wanted to achieve, or in the traditional meaning of the word – in transactions between parties, caused by an intervening and authoritative actor.²⁴ This view is grounded on the conviction that restricted access to the network undermines the functioning of its specific processes. The architecture depends on the combined computational power of the participants, which is essential to ensure trust among them. The absence of a process confirming the legitimacy of new participants also allows for a pseudonymous blockchain environment.²⁵ Users in the network need not reveal their true identity – the transactions they engage in are attributed to their pseudonymous identity which they personally access through their private key and which is consistently represented by their public key.²⁶ The actor saves the private key locally, electronically or even by writing it down, depending on its complexity. The nodes and other users can only verify this actor’s pseudonymous identity through the presence of the unique public key. Hence, the private key to an account is cryptographically attached to its public key. The lack of a central authority contributes to the state-remote character of open and permissionless networks. They are in fact self-governing by design – the internal processes are deemed to make any intervention of a central authority unnecessary and undesirable.²⁷ It is more challenging to regulate a network when the network fundamentally governs itself.

13. Contrary to the above, permissioned blockchains only include trusted party nodes, who were verified and admitted to the network by a preselected central authority. The European Securities and Markets Association (ESMA) expressed its preference for these closed systems in the context of securities markets for reasons of governance, scale and risk

²³ An example is the point of view presented by T. MARCKX (co-founder *TheLedger.be*) at “Blockchain: disrupting markets & governments”, Ghent, 25 October 2017.

²⁴ E. TJONG TJIN TAI, “Smart contracts en het recht”, *NJB* 2017, 92(3), 179.

²⁵ P. HACKER and C. THOMALE, “Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law”, 2017, 31. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, last accessed 12 February 2018.

²⁶ A user signs a transaction with his individual public key, which is only possible by using the correct private key. Nodes can verify whether a transaction is signed with a matching pair of keys. Furthermore, a user can create different addresses to transact from, all of them connected to a single pair of cryptographic keys.

²⁷ P. PAECH, “The Governance of Blockchain Financial Networks”, *Mod. L. Rev.* 2017, 1084.

of illicit activities.²⁸ Likewise, the Belgian bank KBC only considers a permissioned setup in the development of the bank's very own blockchain-based solution.²⁹ Indeed, both varieties of the technology serve entirely different purposes and accordingly, they are characterized by a different spirit. The networks developed by for-profit market players and the fintech start-ups they collaborate with mean to facilitate existing processes and to weed out inefficient business practices among a defined group market participants among whom a certain level of trust already exists.^{30,31} These ledgers are purpose-built in accordance with the specific needs of the commissioning institutions. The practice of whitelisting selected actors to a permissioned blockchain platform may for instance be helpful to administer a financial institution's know your customer policy.³²

14. Clearly, there is an important split between the open and closed approaches: institutions whose business currently exists in playing an intermediary role do not act in pursuit of the libertarian philosophy of permissionless blockchains. Both varieties of the technology serve entirely different needs and a permissioned design is more relevant to facilitate trusted information exchanges among established financial market participants with a real-world reputation.³³ Nevertheless, exceptions exist: *Ripple* (in its standard version) is one of the leading 'altcoins' (*i.e.* alternatives to *Bitcoin* and open to a broad audience) but it is open to discussion whether or not it can be considered a real cryptocurrency.³⁴ *Ripple* is public – everybody is eligible to obtain an individual private key as a user and thus to take part in transactions on the network – but it is built on a blockchain that is *de facto* permissioned.³⁵ Consequently, transaction speed is higher than on the permissionless *Bitcoin*

²⁸ ESMA, "The distributed ledger technology applied to securities markets", report, 2017, 4. Available at https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf, last accessed 7 April 2018.

²⁹ C. MUYLDERMANS (counsel regulatory affairs KBC) at the "Becon Blockchain Conference", Brussels, 8 March 2017.

³⁰ P. PAECH, "The Governance of Blockchain Financial Networks", *Mod. L. Rev.* 2017, 1091. See also: R. VERHAERT, *Blockchain, de overheid aan of in de ketting?*, Brugge, Vanden Broele, 2016.

³¹ D. MILLS, K. WANG *et al.*, "Distributed ledger technology in payments, clearing, and settlement", *Finance and Economics Discussion Series* 2016, 12. Available at <https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf>, last accessed 17 April 2018.

³² T. SWANSON, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems", 2015, 5. Available at <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>, last accessed 7 April 2018.

³³ *Ibid.*, 44.

³⁴ *Ripple*, <https://ripple.com/>, last accessed 7 April 2018.

³⁵ The ECB even categorizes *Ripple* as a "centralised virtual currency scheme", see ECB, "Virtual currency schemes – a further analysis", report, 2015, 15. Available at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, last accessed 15 April 2018.

blockchain.³⁶ It has its own cryptocurrency, but its network is also open for use to transfer any other virtual or (non-native) traditional currency through a specific system of gateways.

15. For the sake of clarity, the following scheme summarizes the definitions we adhere to when we label a certain DLT network private or public, permissioned or permissionless.

³⁶ D. SCHWARTZ, N. YOUNGS and A. BRITTO, “The Ripple Protocol Consensus Algorithm”, *Ripple Labs Inc* 2014, 8. Available at https://ripple.com/files/ripple_consensus_whitepaper.pdf, last accessed 15 April 2018.

	Permissionless	Permissioned
Public	<ul style="list-style-type: none"> - Anyone can run a node and thus participate in executing the consensus algorithm. Incentive to do so exists in financial benefit. - Anyone is eligible to create an individual private and public key pair and an address, and thus is accepted to execute transactions in the network; as well as to access data in the network. - <i>e.g. Bitcoin.</i> 	<ul style="list-style-type: none"> - A designated authority (or: the collectivity of the nodes) decides on who is allowed to run a node as a trusted party. Incentive may exist in a financial benefit or in supporting the common interest. - Anyone is eligible to create an individual private and public key pair and an address, and thus is accepted to execute transactions in the network; as well as to access data in the network. - <i>e.g. Ripple.</i>
Private	<ul style="list-style-type: none"> - Anyone can run a node and thus participate in executing the consensus algorithm. Incentive to do so exists in a financial benefit. - A designated authority decides on granting a private and public key pair and an individual address to applicants who wish to transact in the network and access its data. - <i>e.g. a fintech bank that entirely distributes trust by giving nodes a financial incentive (e.g. cryptosecurities issued by the bank itself) and that offers hyper-secure, virtually risk-free savings accounts to its paying clients.</i> 	<ul style="list-style-type: none"> - A designated authority decides on who runs a node as a trusted party (likely: the actors establishing the DLT). Incentive exists in supporting a common interest. - A designated authority decides on granting a private and public key pair and an individual address to applicants who wish to transact in the network and access its data. (likely: the actors establishing the DLT). - <i>e.g. a consortium of banks that agrees to establish a DLT network to settle payments among each other. All participating banks run a node in the network.</i> - <i>e.g. 2: Corda.³⁷</i>

³⁷ R3 Corda is specifically designed to meet the needs of the financial industry, <https://docs.corda.net/key-concepts-ecosystem.html>, last accessed 5 May 2018.

2. Stages of development

16. Another important typology concerns the different evolutionary steps in the complexity of the DLT and its capacities. Most authors generally discern two generations of the technology: crypto-assets and smart contracts. A third category, decentralized autonomous organizations (DAOs³⁸), is often seen as a combination of smart contracts. However, as Jane ZHANG righteously suggested, DAOs are fundamentally more far-reaching and thus deserve to be ranked as a third stage of development.³⁹

17. The first generation does not need an extensive introduction. Basic virtual currencies like *Bitcoin* belong to the first materialization of blockchain and DLT. These networks facilitate almost instantaneous and cost-efficient remittance of digital or crypto-assets.⁴⁰ All reassignments from one node to another are immutably logged to the database. This information makes it possible to consistently identify the public key belonging to the final holder of the rights regarding the value or the crypto-asset.⁴¹ A pure first-generation blockchain thus only contains data on transfers, thereby identifying the most recent asset holder and banning the double spending risk.⁴² In a more advanced configuration, this transaction data can be represented in a complete list of individual accounts.⁴³

Further distinction can be made between native and non-native crypto-assets: while native crypto-assets only virtually exist the blockchain register's data, the non-native entries represent a separate asset in the world outside the ledger. These assets can range from traditional currencies to intellectual property rights or property titles. *Bitcoin* is an example of a native blockchain – the coins only exist by virtue of the data on the distributed ledger.

³⁸ Not to be confused with “*The*” *DAO*, that is, a specific DAO-application which was set up as an investment vehicle. Due to a loophole in the blockchain's coding, one node was able to drain 70 million dollars of value from *The DAO*. The consecutive “hard fork” to reverse these malevolent transactions caused major polemics among the platform's users. See also E. TJONG TJIN TAI, “Smart contracts en het recht”, *NJB* 2017, 92(3), 180. English commentary on the event: P. HACKER and C. THOMALE, “Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law”, 2017, 31. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, last accessed 12 February 2018.

³⁹ I concur with the viewpoint presented by J. ZHANG (founder and CEO at *Shellpay*) at “Becon Blockchain Conference”, Brussels, 8 March 2017.

⁴⁰ Cost-efficient to the user – some consensus algorithms are disproportionately energy-consuming. *Infra*, 19.

⁴¹ D. DRESCHER, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, New York, Springer Science+Business Media, 2017, 65.

⁴² *Supra*, 6.

⁴³ *Ethereum*, for instance. E. TJONG TJIN TAI, “Smart contracts en het recht”, *NJB* 2017, 92(3), 178.

18. More developed applications that go far beyond this first cryptocurrency function have appeared more recently. A second-generation blockchain does not just serve as a decentralized logbook of transfers, it also supports the performance of encoded computation on the network platform.⁴⁴ A widely known example is *Ethereum* project, which serves as a smart contract programming environment.⁴⁵ This means that the transactions regarding the virtual currency can be tailored to the needs of the user: two nodes can agree that a remittance of value between them will only occur contingent on the fulfilment of certain pre-determined conditions. These platforms feature their own extended script language and they make it possible to construct self-enforcing programs that are computed and executed on the blockchain, so-called smart contracts.⁴⁶ The purpose of the distributed ledger remains the same as with first-generation varieties. Registering the source code of the smart contract to the blockchain makes its clauses immutable and their execution, in principle, irreversible. Thus, the self-executing program runs without anyone having the power to alter or to revoke it. Parties may however choose to deliberately design for flexibility and adaptability by enabling the processing of external inputs to the contract, or even by encoding a self-destruct function.⁴⁷

Potential smart contract applications are wide-reaching and go beyond traditional two-party-contracts. They may for instance be used to construct self-enforcing voting and dividend rights for the holders of ‘digital shares’ of a company.⁴⁸ Thanks to the immutability of the blockchain, nodes can always retrieve and recycle completed smart contracts that already proved their worth. They can be reused as building blocks and combined together to encode new and even more sophisticated smart contracts.⁴⁹

⁴⁴ G.W. PETERS and E. PANAYI, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money” in P. TASCA, T. ASTE *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016, 240.

⁴⁵ *Ethereum*, <https://www.ethereum.org/>, last accessed 7 April 2018.

⁴⁶ N. SZABO, “Smart Contracts”, 1994. Available at <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>, last accessed 24 April 2018.

⁴⁷ G. JACCARD, “Smart Contracts and the Role of Law”, *Justletter IT* 2017, 23, 7; and *infra*, 68 and 77-78.

⁴⁸ See for example stock issuance by Overstock.com as described in C. VAN DER ELST and A. LAFARRE, “Blockchain and the 21st Century Annual General Meeting”, *European Company Law Journal* 2017, 4, 173.

⁴⁹ G.W. PETERS and E. PANAYI, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money” in P. TASCA, T. ASTE *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016, 247.

19. Further sophistication and interconnection of smart contracts may eventually develop a third and currently final stage of blockchain implementations: DAOs. A variety of coded contracts can be bound together in a coordinated manner in order to create a decentralized organization by itself.⁵⁰ This concept corresponds with JENSEN's and MECKLING's agency theory of the firm, stating that corporations essentially exist in the accumulation of their internal and external contractual and other relationships.⁵¹ Accordingly, a DAO is defined by and operates pursuant to the smart contracts it consists of. Such arrangement permits to do business through the set of coordinated smart contracts, without incorporating into a traditional business entity without being owned or controlled by a single person, yet these DAOs can theoretically operate in the market.⁵² In the context of the emerging Internet of Things, people may even become redundant and a business could just be made up of the DAO and the machines it administers.

Yet, these futuristic perspectives remain unfeasible for the time being. Both legal and technical impediments will need to be tackled before fully independent DAOs can possibly materialize. The necessary tools for a DAO to directly participate in the traditional business landscape are currently lacking as it is unclear how these entities would be recognized by law and how they can be governed; for instance, it is necessary to appoint identifiable 'nearest persons' to make it possible for the DAO to be held liable.⁵³ We will not go into further details on this topic because we believe that these questions can be traced back to analogous problems in relation to crypto-assets and smart contracts – DAOs exist in intertwined combinations of these building blocks and the governance of DAOs depends on the governance of first and second generation blockchains. A problem of an entirely different nature exists in the scalability issues connected to computation-intensive consensus mechanisms, and therefore mainly faced by permissionless blockchain setups. These blockchain structures ensure trust among nodes through processes that require heavy and

⁵⁰ A. WRIGHT and P. DE FILIPPI, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015, 15. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

⁵¹ M. JENSEN and W. MECKLING, "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure", *Journal of Financial Economics*, 1976, 3(4), 311.

⁵² P. PAECH, "The Governance of Blockchain Financial Networks", *Mod. L. Rev.* 2017, 1084.

⁵³ S. BLEMUS, "Law and Blockchain: a legal perspective on current regulatory trends worldwide", *RTDF* 2017, 4, 15; and, A. WRIGHT and P. DE FILIPPI, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015, 55. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

competitive computation on all network nodes.⁵⁴ This process is very energy-consuming which prevents mass adoption. Recent reports even estimate that the *Bitcoin* network exceeds Ireland's total energy consumption per year.⁵⁵ Some authors are optimistic and expect future advances in computer processing speed to deal with scalability bottlenecks.⁵⁶ We believe however that the solution does not exist in stronger computers; instead, ingenious new consensus mechanisms and network architectures will empower widespread usage of blockchain networks.

3. Consensus mechanisms

20. The aforementioned proof-of-work procedure undoubtedly is the most recognized consensus mechanism, a logical consequence of Satoshi NAKAMOTO applying it to the original *Bitcoin* concept.⁵⁷ It also is the mechanism responsible for the scalability issues. We earlier explained how consensus is the instrument to create trust among participants in the network. Consequently, the recommended standard for this mechanism depends on the relationship between the nodes. As the Belgian researcher Kristof VERSLYPE labels it, trust is *decentralized* in a permissioned network whereas it is *distributed* in a permissionless network.⁵⁸ The principle of adopting a voting mechanism to share the responsibility of validating a block of new data is identical but its scale is different. If anyone can freely join the operation of the network, trust is indeed distributed to anyone who asks for it – who guarantees that nobody will register a million accounts to seize control? To the contrary, when authority is merely decentralized among a closed group of individually identified and approved participants, it is easier to assert that at least half of them will remain diligently updating the chain in the common interest.

⁵⁴ G.W. PETERS and E. PANAYI, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money” in P. TASCA, T. ASTE *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016, 240.

⁵⁵ A. HERN, “Bitcoin mining consumes more electricity a year than Ireland”, *The Guardian*, 27 November 2017. Available at <https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland>, last accessed 8 March 2018.

⁵⁶ E. KARAINDROU, “Distributed ledger technology and the future of payment services”, 2017, 26. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078523, last accessed 10 March 2018.

⁵⁷ *Supra*, 1; and for an earlier comment on proof-of-work: *supra*, 8. For good understanding: even though proof-of-work is built on the cryptographic process of determining a block's hash, the consensus mechanism is independent from the blockchain's immutable data structure. The consensus algorithm is the operationalization of the distributed trust to validate new blocks.

⁵⁸ As pointed out by K. VERSLYPE during his lecture “Bitcoin, Blockchain & Smart Contracts – Inleiding voor juristen”, Ghent, 26 October 2017.

21. Complicated consensus procedures based on rewarding nodes for actively validating blocks in an honest manner, like the ones based on computational power, are appropriate only if trust is distributed. In a closed, permissioned blockchain environment with identified participants, it may be more sensible to implement a one-node-one-vote standard. It has no impact on the immutable character of the blockchain, but it removes the competition to outperform one another in the confirmation process. Hence, there is no need to reward the nodes validating the transaction – the blockchain will work fine as long as half of the participants remains acting in good faith. Absent the need for rewards, the blockchain can in certain circumstances exist without having its own cryptocurrency, token or other carrier of value.

However, this approach is insufficient if the purpose of the distributed ledger requires a permissionless setup. A more sophisticated consensus protocol is then essential to protect it against nodes trying to add erroneous transactions to the chain. Such protocol will basically demand some sort of effort from the nodes to prove that they belong to the network of trustworthy participants backing the right information. This mechanism raises the barrier for an intruder to distort the update of the blockchain – the intruder will have to exceed fifty percent of the total effort contributed by all network participants in order to succeed. Besides the effective but inefficient proof-of-work, new solutions are continuously being explored and built. Below we will discuss both an increasingly common and a particularly interesting alternative algorithm.

22. Proof-of-stake an alternative algorithm and its importance is growing since the leading permissionless second generation blockchain platform *Ethereum* adopted a similar consensus mechanism named *Casper*.^{59, 60} Nodes are expected to ‘stake’ funds while confirming new transactions, at the risk of losing their stake if the confirmed transaction turns out to be inaccurate. The higher the value of a node’s stake, the higher the chances that this particular node will finally confirm the transaction and generate a new block. He will then be rewarded with a fixed commission fee. The cost to acquire an influential stake of the ledger’s value makes it disproportionally expensive to attack its contents, parallel to how

⁵⁹ *Casper*, <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/>, last accessed 8 March 2018.

⁶⁰ An example of a successful first-generation ledger entirely relying on proof-of-stake is *NXT*, see https://nxtwiki.org/wiki/Nxt_Wiki, last accessed 8 March 2018.

an attack on a proof-of-work ledger would require a disproportionate investment in computational power – indeed, both mechanisms rely on a rational cost-benefit analysis. A cheating participant will be deterred from compromising and jeopardizing the network he himself invested so much in.

While proof-of-stake is not as energy-costly as proof-of-work, it also features some major drawbacks. Since more wealth means more votes, hoarding is encouraged and this tendency risks to ultimately cause the centralization of the blockchain's value. Major stakeholders accumulating influence over time may eventually obtain control over the network, undermining the distributed trust among nodes.⁶¹ The formation of such monopoly position inherently defeats the basic purpose of a distributed ledger. Proof-of-work ledgers risk facing the same problem in the long run because certain pools are gradually acquiring a majority of CPU power.

23. An interesting approach to deal with these issues is found in the *Obelisk* algorithm. It is the consensus mechanism supporting the advanced *Skycoin* blockchain and it is built on the web-of-trust concept. Nodes connect themselves to other nodes they personally trust, and the density of a node's interconnections determines its voting power in the validation of new transactions. Each participant's activity and influence on the ledger is transparent which enables the community to react to malicious nodes. The creators describe this process as a continuous audit by the *Skycoin* community.⁶²

24. The reader should now better understand the basics of how the blockchain works. An overview of DLT categorizations brings us to the conclusion that there is no such thing as 'the blockchain' – the specific features of every DLT application are determined by its unique underlying architecture. Importantly, even though the invention of *Bitcoin* and the technology concept it is built on are often assimilated, it is necessary to consider that the *Bitcoin* use case is a very specific emanation of DLT; and that blockchain networks with an entirely different setup may support many other applications with each a very different, individual purpose and spirit. We will briefly introduce some of these other use cases for

⁶¹ L. LEE, "New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market", *Hastings Business Law Journal* 2016, 12(2), 108.

⁶² *Obelisk*, <https://www.skycoin.net/blog/statement/obelisk-the-skycoin-consensus-algorithm/>, last accessed 11 March 2018.

illustration purposes before commencing a more detailed legal analysis of financial DLT applications.

C. DLT APPLICATIONS

25. The following three promising use cases mean to further demonstrate what blockchain technology is, among others, meant for. We mainly aim to establish that possible applications go far beyond cryptocurrencies and monetary matters in general – we invite the reader to bear in mind the diversity of this technology’s potential, even though the scope of this thesis is limited to financial law.

Land registries – The Swedish land registry authority, the Lantmäteriet, started an experiment in June 2016, aiming to put real estate transaction such as transfers of property and deeds of mortgage on a blockchain.⁶³ The project now entered its second phase where a testbed-platform is being built.⁶⁴ By developing a land registry in a decentralized ledger, the Swedes intend to reduce paperwork, costs and fraud, and to speed up the transaction processes.

Documenting a supply chain – An interesting private initiative is *Modum*, a Switzerland-based startup that makes supply chain processes more efficient by combining blockchain technology with another IT-revolution, the Internet of Things (IoT).^{65, 66} The company currently operates an application in pharma logistics. *T-Mining* is a Belgian example implementing blockchain technology to improve the efficiency of international transport and logistics.⁶⁷ In the future, this startup believes that a decentralized network allows for a safer and faster online administration of documents related to international shipments such as bills of lading and letters of credit.

⁶³ G. CHAVEZ-DREYFUSS, “Sweden tests blockchain technology for registry”, *Reuters*, 16 June 2016. Available at <http://www.reuters.com/article/us-sweden-blockchain-idUSKCN0Z22KV>, last accessed 10 March 2017.

⁶⁴ LANTMÄTERIET *et al.*, “The Land Registry in the blockchain – testbed”, report, 2017. Available at https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf, last accessed 9 April 2017.

⁶⁵ *Modum*, <https://modum.io/about-us/>, last accessed 9 April 2017.

⁶⁶ IoT refers to the networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence.

⁶⁷ N. WAUTERS (co-founder and CEO *T-Mining*) at “Becon Blockchain Conference”, Brussels, 8 March 2017.

Copyrights – A decentralized network permits to exclude central intermediation in a variety of situations where the role of the middleman is crucial until today. The copyright sector is an example of such a densely intermediated environment. *Jaak* is a second generation blockchain project built on *Ethereum* and by storing rights and smart contracts to the blockchain, it aims to facilitate and automate copyright management and royalty payments for using the content.⁶⁸

26. The virtually unlimited variety of blockchain possibilities demands for a firm demarcation of the research. For the reasons discussed above and in view of our specific area of interest, we will analyze the legal issues possibly arising from the two fundamental generations of blockchain applications for financial purposes, so-called fintechns.⁶⁹ We will thereby establish whether traditional legal concepts and methods of regulation are adequate to govern these fintech innovations and to ensure their reliability in the context of the contemporary financial industry.

⁶⁸ *Jaak*, see <http://musically.com/2017/02/20/blockchain-startup-jaak-unveils-m%C3%9C%E2%82%AC-plans-pilots/>, last accessed 7 March 2018.

⁶⁹ *Supra*, 3.

TITLE 3. CRYPTO-ASSETS

CHAPTER 1. CRYPTOCURRENCIES

27. Financial crypto-assets consist of both cryptocurrencies and cryptosecurities. We will treat these subjects separately because of the distinct legal questions raised. Note however that practice shows that cryptocurrencies are often used for speculative objectives, as if they were investment assets.⁷⁰ David YERMACK compares the behavior of average *Bitcoin* buyers to the speculative investment pattern targeting internet stocks in the late 1990s.⁷¹ In the light of the first part of our research however, we will draw the line in accordance with their initial apparent purpose – Satoshi NAKAMOTO, for instance, referred to his creation as ‘electronic cash’ from the very beginning.^{72, 73} While the electronic cash component serves holders to pay for external goods and services, the utility component of cryptosecurities or ‘tokens’ is limited to accessing an internal function provided by their issuer.⁷⁴

⁷⁰ S. ATHEY, I. PARASHKEVOV, V. SARUKKAI and J. XIA, “Bitcoin Pricing, Adoption, and Usage: Theory and Evidence”, working paper, 2016, 30. Available at <https://www.gsb.stanford.edu/faculty-research/working-papers/bitcoin-pricing-adoption-usage-theory-evidence>, last accessed 14 April 2018.

⁷¹ D. YERMACK, “Is Bitcoin a real currency? An economic appraisal”, working paper, *National Bureau of Economic Research Working Paper Series* 2013, 2. Available at <http://www.nber.org/papers/w19747>, last accessed 14 March 2018.

⁷² S. NAKAMOTO, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. Available at <https://bitcoin.org/bitcoin.pdf>, last accessed 6 March 2017.

⁷³ See *infra*, 49, for a discussion of distinctive characteristics inherent to cryptosecurities.

⁷⁴ P. HACKER and C. THOMALE, “Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law”, 2017, 12. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, last accessed 12 February 2018.

A. HIGHLY DECENTRALIZED AND PUBLIC⁷⁵ – *electronic cash*

28. Some authors state that cryptocurrencies compete with traditional central bank-issued fiat money.^{76, 77} In this regard, note that a performant cryptocurrency must be constructed as a public blockchain. Assets on a private blockchain can only be transferred to a selected group of users and as we will discuss below, a currency is fundamentally characterized by a high degree of versatility and acceptance. The following paragraphs will discuss to what extent a cryptocurrency indeed succeeds at fulfilling the functions and the distinguishing requirements of a currency – consecutively from an economical and from a legal point of view. We will then analyze how the underlying highly decentralized blockchain application relates to the EU legal framework regarding payment services.

1. Qualification by an economist

29. From an economical perspective, money is defined by the following functions it fulfils:

- a measure of value and a unit of account;
- a medium of exchange; and,
- a store of value or wealth.⁷⁸

Looking at most established virtual currencies at the time of writing, their capacity to meet these purposes is – at least – highly debatable.⁷⁹ The main explanation for this failure lies in their extreme volatility; which has been a consistent characteristic for all cryptocurrencies since their surge in 2009. The *Bitcoin* volatility index varied between 4 and 10% over the

⁷⁵ While many cryptocurrencies are permissionless, some (*e.g. Ripple*) have a particular consensus mechanism which is not carried out by all users but by a select group of nodes with a uniquely operational task. These permissioned varieties are still highly decentralized due to the unlimited access for users (*i.e.* public).

⁷⁶ H. NABILOU and A. PRÜM, “Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies”, 2018, 5. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3121918, last accessed 11 April 2018.

⁷⁷ ECB, “Virtual currency schemes – a further analysis”, report, 2015, 21. Available at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, last accessed 15 April 2018.

⁷⁸ C. PROCTOR, *Mann on the Legal aspects of money*, Oxford, Oxford University Press, 2012, 10.

⁷⁹ As also presented by J. RICHELLE (*Lawsquare*) at “Studiedagen Instituut Financieel Recht: Fintech”, Brussels, 16 January 2018.

past eight years, reaching peaks of as much as 15%.⁸⁰ These fluctuations are mainly caused by the absence of a credible obligor behind the cryptocurrency (a central bank authority, for instance) combined with the non-existent intrinsic value of the private keys to the blockchain wallets. The fixed supply schedule intrinsic to the rewards-based mining procedure of most cryptocurrencies today adds to the price volatility.⁸¹ As a consequence, cryptocurrencies are currently very unwieldy as a measure of value or as a means of exchange – their value compared to other currencies swings up and down every day and it would be very costly for traders to bear or mitigate these risks. Since consumers always need to double check the currency’s actual value in order to understand prices, it is also very confusing in the context of payments.⁸² The extreme volatility furthermore prevents the cryptocurrency’s capacity to act as a store of value. For comparison purposes, gold serves as a reasonable alternative way to store value. The 30-days volatility index of this precious metal ranged between 0.50 and 1.50% over the past eight years, with an occasional peak of 2.50% in 2011 – far less than *Bitcoin*’s variation between 4 and 10%.⁸³ Holding cryptocurrencies, for even a very brief period of time, is very risky, which collides with the function of storing value.⁸⁴ Additionally, it is very difficult to protect the key to a person’s funds of cryptocurrencies against operational risks like loss and theft.⁸⁵ The key is in fact the ‘weak link’ of a cryptocurrency wallet: it is nothing more than a numerical code and the owner has the responsibility to keep and protect it – this includes the need for a very robust IT security when accessing the cryptocurrency account. Absent a legal claim on an intermediary, one

⁸⁰ Based on the 30-days BTC-USD volatility index; a measure of the *Bitcoin* value variation compared to US dollars. Available at <https://www.buybitcoinworldwide.com/nl/volatiliteits-index/>, last accessed 13 April 2018. Note that, while the example of *Bitcoin* is by far the most important cryptocurrency in terms of market capitalization, the other top five varieties (*Ethereum*, *Ripple*, *Bitcoin Cash* and *Litecoin*) face the same problem of extreme volatility. See also <http://cryx.io/> (last accessed 13 April 2018) and <https://www.sifrddata.com/cryptocurrency-volatility-index/> (last accessed 13 April 2018) on their volatility indices.

⁸¹ H. NABILOU and A. PRÜM, “Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies”, 2018, 26. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3121918, last accessed 11 April 2018.

⁸² J.L. VERHELST, “Zijn cryptomunten munten? Een analyse van Bitcoin” in M.E. STORME and F. HELSEN (eds), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia, 2017, 55-56 & 67; see also: D. YERMACK, “Is Bitcoin a real currency? An economic appraisal”, working paper, *National Bureau of Economic Research Working Paper Series* 2013, 11. Available at <http://www.nber.org/papers/w19747>, last accessed 14 March 2018.

⁸³ Based on the 30-days Gold-USD volatility index. Available at <https://www.buybitcoinworldwide.com/nl/volatiliteits-index/>, last accessed 13 April 2018.

⁸⁴ J.L. VERHELST, “Zijn cryptomunten munten? Een analyse van Bitcoin” in M.E. STORME and F. HELSEN (eds), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia, 2017, 68.

⁸⁵ ECB, “Virtual currency schemes – a further analysis”, report, 2015, 22. Available at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, last accessed 15 April 2018.

cannot rely on a bank to assume the security risk of a digital wallet analogous how bank accounts for traditional currencies are held.⁸⁶

Apart from the volatility issue affecting the three functions of money and the practical problem with the required safety of a store of value, two more impediments of a practical nature exist that restrict the functions of means of exchange and unit of account. In the first place, cryptocurrencies do not have a single straightforward value. They can be bought and sold from one of the numerous different online exchange platforms called ‘markets’ and each of them applies an individual ‘current market price’. The difference between the highest and lowest individual prices quoted by the active *Bitcoin* platforms with the highest trading volumes usually ranges from 3 to 10%.⁸⁷ This disparity makes it almost impossible to find a single reference point. Instead, the value of most cryptocurrencies is usually assessed through opaque 24-hours price aggregations that fail to indicate the true cost of procuring or selling the currency at the present time. The second and last cumbersome factor pertains to the relatively high cost of a single unit of the currently established cryptocurrencies compared to the price of most ordinary products and services. Retail prices quoted in two or even four or more (*Bitcoin*) decimals are simply puzzling. The mathematics are transparent, but consumers tend to fail finding reference points due to the presence of many leading zeros.⁸⁸

2. Qualification by a lawyer

30. The economic reality discussed above seems to coincide with the legal reality, both in literature and in the dominant interpretation by the EU lawmakers. There is no universal legal definition of money, nor is there a pragmatic functional approach like the one applied by economists. MANN established that different ‘theories of money’ exist that are used to demark the legal concept.⁸⁹ The most important ones are the ‘State theory of money’, which bases the quality of money on the role of the State establishing it in its monetary system;

⁸⁶ D. YERMACK, “Is Bitcoin a real currency? An economic appraisal”, working paper, *National Bureau of Economic Research Working Paper Series* 2013, 14. Available at <http://www.nber.org/papers/w19747>, last accessed 14 March 2018.

⁸⁷ *Ibid.*, 12. See <https://www.cryptocompare.com/coins/btc/markets/USD> (last accessed 14 April 2018) to consult current *Bitcoin* prices quoted by the different markets. Given its volatility, it is important to only consider the markets involved in recent transactions (*cf.* left column).

⁸⁸ *Ibid.*, 13.

⁸⁹ C. PROCTOR, *Mann on the Legal aspects of money*, Oxford, Oxford University Press, 2012, 13.

and the ‘Societary theory of money’, where it is the attitude of society rather than the authority of the state that defines money through its public acceptance and the confidence of the people.⁹⁰ The ‘Institutional theory of money’ is more recent and inspired by the creation of the euro. It focuses the role of the central bank that controls the money rather than on the state acting through legal tender laws.⁹¹ Cryptocurrencies, to the contrary, are essentially built on a principle of disintermediation. They have no ties with states or central banks; nor are they currently publicly accepted by any society. Consequentially, cryptocurrencies do not fit in any of the legal definitions stipulated by MANN.

Two reports by the ECB are consistent with our foregoing analysis founded on MANN’s legal definitions. In 2012, the ECB distinguished cryptocurrencies from electronic money.⁹² The latter is defined in the Electronic Money Directive, as a monetary value represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and accepted by entities other than the electronic money issuer.⁹³ The ECB points out that cryptocurrencies are only accepted within the issuing virtual community – it is not a claim on the issuer.⁹⁴ In addition, cryptocurrency is not always issued on receipt of funds since varieties built on reward-based consensus mechanisms also assign value to mining nodes.⁹⁵ Later, in its 2015 report, the ECB established that an interpretation of cryptocurrencies may not even include the word ‘money’ because of the lacking high degree of liquidity and the minimal current level of acceptance as a means of payment.⁹⁶ These considerations lead to ECB’s refined definition of cryptocurrencies as a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money.⁹⁷ The European Court of Justice (ECJ) however seemed to adhere to a diverging approach in *Skatteverket v David*

⁹⁰ *Ibid.*, 15-25.

⁹¹ *Ibid.*, 27.

⁹² The ECB refers to cryptocurrencies as ‘decentralized bi-directional virtual currency schemes’.

⁹³ Article 2 (2) Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

⁹⁴ ECB, “Virtual currency schemes”, report, 2012, 16. Available at <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, last accessed 15 April 2018.

⁹⁵ *Supra*, 8.

⁹⁶ ECB, “Virtual currency schemes – a further analysis”, report, 2015, 25. Available at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, last accessed 15 April 2018.

⁹⁷ *Ibid.*, 25. See also: P. ATHANASSIOU, “Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks”, *ECB Legal Working Paper Series* 2017, 19. Available at <https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf?344b9327fec917bd7a8fd70864a94f6e>, last accessed 15 April 2018.

Hedqvist.⁹⁸ This case involved a tax dispute between the Swedish Tax Authority and a Swedish national exchanging traditional currency for *Bitcoin* and the other way around. The national court was uncertain whether such exchange activities fall within the scope of the Common VAT Directive exemption for ‘transactions of negotiation, concerning currency, bank notes and coins used as legal tender...’.⁹⁹ The ECJ considered that although *Bitcoin* is no legal tender, it is a means of payment accepted between parties. Moreover, the court finds that in the underlying relations, *Bitcoin* has no other purpose than to be a means of payment.¹⁰⁰ The ECJ decided not to classify the cryptocurrency as anything that is statutorily recognized, and the court seemingly intentionally avoided to call it money. Instead it classifies cryptocurrencies under a narrower category of liquid payment instruments like electronic and bank account money.¹⁰¹ This does not mean that *Bitcoin* has this same status. While the euro as a currency takes the form of – besides scriptural money, banknotes and coins – widely accepted electronic money, cryptocurrencies use their own denominations, which are currently not backed by the law or declared legal tender in any state.^{102, 103} Hence, it appears that the ECJ chose to solve the tax dispute pragmatically without leaving a decisive impact on the cryptocurrency typology.¹⁰⁴ Lastly, the ECB notes that even though cryptocurrencies currently cannot be labeled money, it remains possible that a different analysis applies to safer, more efficient and more reliable cryptocurrencies that may be developed in the future.¹⁰⁵

3. Regulation?

31. Despite the fact that the existent cryptocurrencies are incompatible with both the economical and legal demarcations of the money concept, a number of transactions still

⁹⁸ Judgment of 22 October 2015, *Skatteverket v David Hedqvist*, C-264/14, EU:C:2015:718, paragraphs 50-57.

⁹⁹ Article 135 (1) (e) Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax.

¹⁰⁰ *Hedqvist*, *op. cit.*, paragraph 52.

¹⁰¹ P. HACKER and C. THOMALE, “Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law”, 2017, 30. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, last accessed 12 February 2018.

¹⁰² ECB, “Virtual currency schemes – a further analysis”, report, 2015, 24. Available at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, last accessed 15 April 2018.

¹⁰³ *Hedqvist*, *op. cit.*, paragraph 49.

¹⁰⁴ A. A. GIKAY, “Regulating decentralized cryptocurrencies under payment services law: lessons from European Union law”, *Journal of Law, Technology & the Internet* 2018, 9, 23.

¹⁰⁵ ECB, “Virtual currency schemes – a further analysis”, report, 2015, 25. Available at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, last accessed 15 April 2018.

involve a payment through a cryptocurrency. This finding leads to the question whether the relevant blockchain networks could in any way be subject to law in relation to payment services. A preliminary problem however concerns the question how to connect a national set of rules to a decentralized payment ledger. States developing such regulatory framework will likely want to govern the operation of all cryptocurrency blockchain applications accessible for users within their jurisdiction. The cryptocurrencies are designed to surmount these very jurisdictions and the permissionless blockchain platforms as such are often built by anonymous individuals. If, for this reason, an important cryptocurrency platform would indeed escape necessary regulation, a state can resort to blocking access to the internet webpages through which the blockchain application operates.¹⁰⁶

32. The practical challenge of subjecting a decentralized network to national laws aside, it is questionable whether any existing laws relating to payment systems can apply to cryptocurrencies, given their very limited resemblance to traditional currencies. From an EU perspective, the second European Payment Services Directive (PSD2) harmonizes the European payments market by regulating payment service providers by submitting them to the requirement of retrieving prior authorization, supervision by the competent home member state authority and various rules of a prudential nature.¹⁰⁷ These rules mean to ensure these actors' reliability. Cryptocurrency blockchain applications however fall out of the scope of these rules.¹⁰⁸ The currently dominant refusal to view cryptocurrencies as a form of funds excludes them from the definition of payment services as applied by PSD2.¹⁰⁹ Note that the ECJ cautiously labeled *Bitcoin* a 'means of payment' instead of a 'payment instrument', which is a defined concept under PSD2, in the above-cited *Hedqvist* case.¹¹⁰ The scope of PSD2 is intentionally broad compared to the initial PSD dating from 2007, in order to ensure equivalent operating conditions to existing players and to new market

¹⁰⁶ A. WRIGHT and P. DE FILIPPI, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015, 55-56. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

¹⁰⁷ Articles 5-37 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2).

¹⁰⁸ For a more elaborate analysis of the status of *Bitcoin* under PSD; see: C. HAUBEN, "Bitcoin en EU-recht: de virtuele vreemde eend in de bijt" in M.E. STORME and F. HELSEN (eds), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia, 2017, 83.

¹⁰⁹ *Ibid.*, annex I.

¹¹⁰ *Hedqvist*, *op. cit.*, paragraph 50. See also: A. A. GIKAY, "Regulating decentralized cryptocurrencies under payment services law: lessons from European Union law", *Journal of Law, Technology & the Internet*, 2018, 9, 23.

entrants who introduce technically innovative payment products or services.¹¹¹ However, it does also not apply to cryptocurrencies. Among other changes, PSD2 thus created a regulatory level playing field for both the banks and the fintechs, notably the payment initiation and account information service providers.^{112, 113} These new actors create tools that enable the consumer to rely on payment instruments provided by service providers other than the bank where he or she holds an account in order to make online, immediate credit transfers. These providers will also be able to offer to consumers a consolidated view of their different payments accounts – by consequence, consumers would only need to possess one payment service account. Cryptocurrencies are a different type of fintech, even though they could serve a similar purpose of effectuating direct online payments without the need to rely on the service provided by an established bank. In fact, cryptocurrencies are way more far-reaching than the third-party service providers regulated by PSD2. Whereas PSD2 permits the payment initiation and account information services to compete with the banks' payment services by establishing cooperation between traditional and new actors, the philosophy behind cryptocurrencies is grounded on a radical split from established actors. The ECB confirms this analysis in its latest report on cryptocurrencies. The phenomenon is still new and evolving which makes it difficult to create tailor-made legislation. Additionally, the ECB states that such efforts would not be proportional given the limited usage of cryptocurrencies today.¹¹⁴ It must be noted however that the above analysis only applies to pure cryptocurrencies, *i.e.* crypto-assets that are solely used as a means of payment and that do not serve an investment-related purpose to the buyer, nor to the issuer – other regulations may apply if these conditions are not fulfilled.¹¹⁵

B. PERMISSIONED AND PRIVATE – *blockchain-based interbank payment solutions*

33. An approach fundamentally different from peer-to-peer transferable cryptocurrencies is reflected by initiatives exploring the possibilities to adopt blockchain-

¹¹¹ Recitals 3-6 PSD2.

¹¹² P. BERGER (Baker McKenzie) at “Studiedagen Instituut Financieel Recht: Fintech”, Brussels, 16 January 2018.

¹¹³ Annex I and article 4 (3) PSD2.

¹¹⁴ ECB, “Virtual currency schemes – a further analysis”, report, 2015, 24. Available at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, last accessed 15 April 2018.

¹¹⁵ *Infra*, 53-58.

based solutions to improve the current interbank payment infrastructure. Contrary to cryptocurrencies, such ledgers only play an indirect role in payment transactions; they are to be used by the actors underpinning payment services and not directly by the payors and payees involved. They serve as a tool to enhance the operation of the modern financial system.¹¹⁶ Such blockchain is thus likely constructed as a private and permissioned interbank network – other options are theoretically possible but unfeasible at the time of writing due to reasons of system integrity and legal compliance.¹¹⁷ In the current, centralized constellation, accounts on different levels can be involved in the transfer of one and the same asset, from the commercial bank accounts held by the payor and payee to, in some instances, the accounts held with an intermediating central clearing bank at the top of the pyramid. The payment data is validated and reconciled – sometimes even manually – by all different actors involved. This is a labor-intensive and costly process and moreover, it is prone to errors.¹¹⁸ We discern two scenarios for the adoption of distributed ledger technology in the interbank payment infrastructure: a more basic and a radical one.¹¹⁹ The first scenario involves the introduction of decentralized technology to support or replace an interbank telecommunication network that facilitates clearing between financial institutions. With a network of more than 11,000 financial institutions, SWIFT currently is the leading actor providing this service.¹²⁰ The second option involves the replacement of the complete interbank payment infrastructure. It does not only support the clearing function, but it also provides for interbank settlement, like the ECB’s TARGET 2 system does for transfers denominated in Euro.

1. Interbank financial communication network

34. A blockchain that merely serves as an interbank data transmission network does not contain information on deposits or accounts. It provides for the transmittance of standardized messages between banks. One of these message types, the MT103, is used to transmit payment instructions from one bank to another, in the clearing process of a payment between

¹¹⁶ P. ATHANASSIOU, “Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks”, *ECB Legal Working Paper Series 2017*, 26. Available at <https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf?344b9327fec917bd7a8fd70864a94f6e>, last accessed 15 April 2018.

¹¹⁷ *Ibid.*, 28.

¹¹⁸ *Ibid.*, 27.

¹¹⁹ E. KARAINDROU, “Distributed ledger technology and the future of payment services”, 2017, 14-18. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078523, last accessed 10 March 2018.

¹²⁰ SWIFT, <https://www.swift.com/about-us/discover-swift/messaging-standards>, last accessed 15 April 2018.

their respective customers. Such message is merely an instruction and entails no immediate transfer of funds from one account to another. This happens later through debiting and crediting of the accounts held by the banks themselves, usually with an intermediary central bank they rely on. In a 2016 whitepaper, SWIFT states that the discerning characteristics of distributed ledger technology have the potential to be advantageous for its services.¹²¹ These strengths include, according to the paper, the efficient propagation to all nodes in near to real-time, the full traceability and immutability of transactions recorded in the chain and possibly automated reconciliation. Also, SWIFT notes that the decentralized setup of a blockchain guarantees trust in the integrity of the ledger and accuracy of the recorded transactions. This last advantage implies a highly decentralized blockchain setup in which, for instance, every participating financial institution is a node. This prompts the question how SWIFT sees the actual implementation of the network, and what its own role in this network is. The paper serves as a preliminary assessment and it does not yet provide details on this matter. It only cautiously states that “DLT-based services could be provided by SWIFT, our community or third parties”.¹²² Nevertheless, this organization emphasizes its status as an industry cooperative and declares that thanks to its governance model, it is best positioned to control the access to the permissioned network by taking up the task of preselected central authority.^{123,124} The whitepaper furthermore stresses the importance of a high degree of standardization in order to allow for straight-through processing and interoperability.¹²⁵ Again, SWIFT refers to its business knowledge and experience with ISO standards, establishing its qualities to realize an industry-standard distributed ledger.¹²⁶ The interim results of a proof of concept distributed ledger, launched by SWIFT and thirty-three leading global banks are said to be “encouraging for this business use case” in a recent report.¹²⁷ Strengthened by this initial project, SWIFT reasserts it is in the industry’s interest that the distributed ledger innovation is integrated in the contemporary interbank infrastructure, so it can be further developed based on agreed standards.¹²⁸

¹²¹ SWIFT, “SWIFT on distributed ledger technologies”, position paper, 2016, 4. Available at <https://www.swift.com/resource/swift-distributed-ledger-technologies>, last accessed 15 April 2018.

¹²² *Ibid.*, 3.

¹²³ *Ibid.*, 17.

¹²⁴ *Supra*, 13.

¹²⁵ *Ibid.*, 9.

¹²⁶ *Ibid.*, 14.

¹²⁷ SWIFT, “gpi Nostro Proof of Concept”, interim report, 2017, 3. Available at <https://www.swift.com/news-events/press-releases/swift-tests-show-blockchain-has-potential-for-global-liquidity-optimisation>, last accessed 15 April 2018.

¹²⁸ *Ibid.*, 21.

35. Despite SWIFT's efforts and experience, it has also been argued that it is outdated and unable to adopt the wider changes the financial telecommunications sector needs.¹²⁹ In 2016, the above-mentioned initiative of *Ripple* engaged in a collaboration with a number of banks to build an interbank network on the *Ripplenet* blockchain.¹³⁰ This endeavor could perform the services offered by SWIFT but it would be designed as a more accessible application; and its capacity is not necessarily limited to processing payment information, it would also be able to provide settlement services for any transaction with regard to digitally represented assets.^{131, 132} This larger prospect leads us to the second and more radical scenario for the adoption of distributed ledger technology in the interbank payment infrastructure, *i.e.* in a full-fledged interbank money remittance network.

2. Interbank money remittance network

36. A distributed ledger application that aims to also replace the interbank settlement infrastructure operates as a master-record, held by all banks in the network. Unlike the data transmission network described in the previous paragraph, this blockchain application is comprised of entire accounts and balances but contrary to the cryptocurrency schemes, it would not compete with traditional currencies. Indeed, rather than to replace commercial money, its purpose is to represent money held in accounts with commercial banks in one common distributed ledger.¹³³ The ledger is continuously updated with all transactions or balance adjustments and every bank in the network has direct access, eliminating all labor-intensive reconciliation processes. The participants may choose to use a second distributed ledger to increase internal efficiency, a blockchain within a node that is compatible with the ledgers operated by other banks and with the master-ledger.¹³⁴ Despite the absence of a trusted third party responsible for the processing and monitoring of transactions in this master-ledger, the state of the accounts held therein is regarded accurate and thus

¹²⁹ C. SKINNER, "Will the blockchain replace SWIFT?", *American Banker*, 8 March 2016. Available at <https://www.americanbanker.com/opinion/will-the-blockchain-replace-swift>, last accessed 16 April 2018.

¹³⁰ Global Payments Steering Group (CPSG), see <https://ripple.com/insights/announcing-ripples-global-payments-steering-group/>, last accessed 15 April 2018.

¹³¹ K. JEMIMA, "Blockchain insiders tell us why we don't need blockchain", *Financial Times*, 2 May 2018. Available at <https://ftalphaville.ft.com/2018/05/02/1525253799000/Blockchain-insiders-tell-us-why-we-dont-need-blockchain/>, last accessed 2 May 2018.

¹³² E. KARAINDROU, "Distributed ledger technology and the future of payment services", 2017, 18. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078523, last accessed 10 March 2018.

¹³³ *Ibid.*, 14.

¹³⁴ *Ibid.*, 15.

authoritative.¹³⁵ This confidence requires a carefully designed consensus mechanism that either relies on a limited number of nodes that are deemed to be especially trustworthy (to the example of *Ripple*) or which encourages all participating banks to diligently remain updating the chain in the network's common interest.

The solution where a comprehensive blockchain-based application replaces the entire contemporary back-end payment infrastructure is in fact the conceptual midpoint between a society widely adopting pure, permissionless cryptocurrency blockchains (and thereby dismissing banks) on the one hand and a group of banks giving their interbank communication system the 'blockchain facelift' on the other hand. According to Elli KARAINDROU, this is the most plausible and interesting scenario – she considers the initial libertarian ideology behind the blockchain bygone and she claims that “one might say that the question is no longer how DLT will disrupt the regulated sector, but rather how it will become part of it.”¹³⁶ This insight presumes a scenario where not only the nodes, but also the distributed ledger itself is regulated.

3. Regulation?

37. The regulatability of the permissioned decentralized payment network is indeed a crucial ingredient for its success. Philipp PAECH trusts that blockchain applications in the financial industry will operate within the reach of relevant laws, regulators and courts.¹³⁷ Given the densely regulated character of the financial sector, it is difficult to create a viable interbank payment network that escapes the regulatory framework of the states of which the financial industry is affected. Measures of a globally relevant nature like know your customer (KYC) and anti-money laundering (AML) rules as well as tax-related requirements are particularly relevant in this context because their enforcement may be threatened by the

¹³⁵ P. ATHANASSIOU, “Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks”, *ECB Legal Working Paper Series* 2017, 27. Available at <https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf?344b9327fec917bd7a8fd70864a94f6e>, last accessed 15 April 2018.

¹³⁶ E. KARAINDROU, “Distributed ledger technology and the future of payment services”, 2017, 19. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078523, last accessed 10 March 2018.

¹³⁷ P. PAECH, “The Governance of Blockchain Financial Networks”, *Mod. L. Rev.* 2017, 1110.

pseudonymous character of a primitive blockchain.^{138, 139} Additionally, the 2008 financial crisis revealed major vulnerabilities of the global financial integration and to some extent, liberalization.¹⁴⁰ International organizations like the Basel Committee and their member states responded by promoting rules that would reinforce market integrity and financial stability. The EU, for instance, adopted a more stringent regulatory framework with qualitative and quantitative prudential standards for, and adequate supervision on, financial institutions.¹⁴¹ The extensive set of KYC, AML and tax-related laws as well as the principles bolstering the financial sector would likely also apply to an interbank blockchain network; most certainly if it covers the EU and US. While these laws put substantial compliance duties on the shoulders of the nodes, failing to abide by them risks to trigger draconian measures by affected states, like forcing the internet service providers to block data passing through the distributed ledger, thus effectively disabling the application.¹⁴² PAECH proposes that alternatively, an interbank blockchain network could be set up among participants in jurisdictions that barely or not regulate financial institutions and payment services, thereby excluding the EU and the US.¹⁴³ This fallback option is inadequate as it clashes with the main objective of blockchain-based payment services; that is, executing cheap, swift and secure international payments by eliminating the intermediary steps in the process. It is clear that the reality of regulation is inevitable for a blockchain-based payment network with a global reach. Less clear is the issue of how to control a body that lacks any form of central power and that is identically geographically present at the address of every node. LESSIG summarizes that “To regulate well, you need to know (1) who someone is, (2) where they

¹³⁸ A. WRIGHT and P. DE FILIPPI, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia”, 2015, 22. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

¹³⁹ P. ATHANASSIOU, “Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks”, *ECB Legal Working Paper Series* 2017, 31. Available at <https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf?344b9327fec917bd7a8fd70864a94f6e>, last accessed 15 April 2018.

¹⁴⁰ S. CLAESSENS and L. KODRES, “The Regulatory Responses to the Global Financial Crisis: Some Uncomfortable Questions”, *IMF Working Paper* 2014, 6-8. Available at <https://www.imf.org/external/pubs/ft/wp/2014/wp1446.pdf>, last accessed 16 April 2018.

¹⁴¹ Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms; and, Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms.

¹⁴² A. WRIGHT and P. DE FILIPPI, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia”, 2015, 51. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

¹⁴³ P. PAECH, “The Governance of Blockchain Financial Networks”, *Mod. L. Rev.* 2017, 1104.

are, and (3) what they're doing."¹⁴⁴ Yet, the blockchain is and will remain regulatable.¹⁴⁵ In the following paragraphs, we analyze how jurisdictions may identify, localize and govern a permissioned blockchain-based money remittance application at the level its nodes, the distributed ledger as an entity itself and the transactions it processes. While the first two targets are to be subject to public laws of a regulatory nature, *e.g.* minimum capital requirements, reporting duties and a reliable internal organization; the third category comprises provisions of private law relating to the validity and enforceability of transactions executed on the ledger.

a. Individual nodes

38. The nodes in an interbank money remittance network are to be existing banks and financial institutions, hence, these actors are already regulated and both governing and supervising them is nothing new. A payment ledger that relies on a cooperation of authorized payment service providers should not pose great regulatory problems.¹⁴⁶ It is possible that the network also contains non-bank nodes with the only purpose of validating new transactions.¹⁴⁷ While KYC, AML, tax laws and minimum capital requirements are irrelevant for these participants with a purely auxiliary role, it might make sense to subject their activities and internal organization to some sort of prudential regulation and supervision, according to the services they provide.¹⁴⁸ Helpers of this kind are responsible for bringing the blockchain's consensus algorithm into practice and after all, this mechanism is the backbone of the payment network's reliability and security. Regarding the nodes that take up an active financial role in the network, the single element demanding some attention is the requirement to adequately guard the access gates to the network – that is, only financial institutions that are indeed properly authorized to unfold banking activities can be allowed

¹⁴⁴ See L. LESSIG, *Code version 2.0*, New York, Basic Books, 2006, 23. Available at <http://codev2.cc/download+remix/Lessig-Codev2.pdf>, last accessed 3 February 2018.

¹⁴⁵ A. WRIGHT and P. DE FILIPPI, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015, 51. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

¹⁴⁶ P. PAECH, "The Governance of Blockchain Financial Networks", *Mod. L. Rev.* 2017, 1103.

¹⁴⁷ D. MILLS, K. WANG *et al.*, "Distributed ledger technology in payments, clearing, and settlement", *Finance and Economics Discussion Series* 2016, 12. Available at <https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf>, last accessed 17 April 2018.

¹⁴⁸ *Ibid.*, 29; and, E. KARAINDROU, "Distributed ledger technology and the future of payment services", 2017, 20. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078523, last accessed 10 March 2018.

to participate.¹⁴⁹ This can only be achieved with a permissioned, private blockchain administered by a platform supervisor that has a good communication line with the competent regulator or regulators. Note that every node can, regardless of its geographic location, potentially access and impact any transaction executed over the ledger – be it, in accordance with the rules set forth by the consensus algorithm; hence the necessity of a tailor-made and performant mechanism to validate transactions. The shared control among all nodes explains why every state where a participating bank is located has an actual interest in regulating the entire network including all of its nodes. Yet, the resultant conflicts of laws between nodes in different states render doing so practically unfeasible.¹⁵⁰ A solution hinged on one focal point and on some degree of mutual recognition makes more sense.¹⁵¹ For instance, the home jurisdiction of a bank could make the legitimacy of participating in a certain blockchain network subject to the existence of adequate regulation and supervision by the jurisdiction appointed to govern the blockchain.¹⁵² Countries may want to create a harmonized level playing field to ensure a common quality standard for this particular regulatory task.¹⁵³ Along these lines, we arrive at the question of how to regulate the network as an entity.

b. Blockchain as an entity

39. The issue of governing the distributed ledger itself boils down to finding the right anchor point to connect law with regulated substance. While it is almost impossible to identify the person or persons controlling the software in a public, permissionless virtual currency scheme like *Bitcoin*, this problem would not exist in relation to a modern interbank money remittance blockchain.¹⁵⁴ At this stage, well-established financial institutions and even central banks are openly launching proof of concepts for this kind of application.

¹⁴⁹ Or, in the EU context, institutions that enjoy a single license since the adoption of the Second Council Directive 89/646/EEC of 15 December 1989 on the coordination of laws, regulations and administrative provisions relating to the taking up and pursuit of the business of credit institutions (no longer in force).

¹⁵⁰ E. KARAINDOU, “Distributed ledger technology and the future of payment services”, 2017, 20. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078523, last accessed 10 March 2018.

¹⁵¹ *Ibid.*, 20.

¹⁵² Alternatively, absent a uniform solution, countries can still enforce their AML, KYC and tax laws on nodes under their jurisdiction by imposing full transparency of transactions and identification of transaction parties. See A. WRIGHT and P. DE FILIPPI, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia”, 2015, 22. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

¹⁵³ P. PAECH, “The Governance of Blockchain Financial Networks”, *Mod. L. Rev.* 2017, 1104.

¹⁵⁴ *Ibid.*, 1093.

PAECH calls the entity behind the development of the technology the ‘platform provider’.¹⁵⁵ Contrastingly, according to a working paper published by the US Federal Reserve Board, this entity has ‘ownership rights’ over the distributed platform.¹⁵⁶ Both wordings have a different connotation and it seems that PAECH’s term better complies with the underlying philosophy of a blockchain application, regardless of its permissioned setup.¹⁵⁷ Nevertheless, both authors agree that this entity is the single appropriate addressee for regulation. It bears the responsibility for complying with financial regulation, supervision and reporting obligations and it should oversee that the network does not allow for transactions with non-regulated entrants or other ledgers lacking governance standards of a comparable level.^{158, 159} Implementation requires policymakers and financial regulators to tailor the existing regulatory framework accordingly in order to bring these new actors within their scope in an adequate manner.¹⁶⁰ From the perspective of the regulated entity, efforts could be made to align the decentralized nature of the blockchain’s architecture with, and to extend it to the responsibilities originating from the legal reality. Hence, the individual financial institutions engaging to participate in the network as a node may want to share the regulatory burden by engaging to equitably support the platform provider in its governance tasks – this is where we believe that the term ‘platform owner’ fails to convey this spirit of mutuality. Such collaboration arrangement is justified by the fact that, in the event this blockchain application is successfully operationalized among the partnering banks, it is expected to save them a substantial amount of operational costs; and, these institutions will likely benefit from simplified compliance processes within their own organization.¹⁶¹ Besides having a compliant internal organization put in place, the platform provider should also ensure that its digital environment only allows for the execution of

¹⁵⁵ *Ibid.*, 1093 and 1101.

¹⁵⁶ D. MILLS, K. WANG *et al.*, “Distributed ledger technology in payments, clearing, and settlement”, *Finance and Economics Discussion Series* 2016, 31. Available at <https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf>, last accessed 17 April 2018.

¹⁵⁷ A relationship of ownership is appropriate vis-à-vis a traditional database, whereas a solution based on distributed ledger technology is unique in its decentralized governance.

¹⁵⁸ E. KARAINDRU, “Distributed ledger technology and the future of payment services”, 2017, 20. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078523, last accessed 10 March 2018.

¹⁵⁹ Acting in the capacity of the permissioned network’s preselected central authority, *supra*, 13.

¹⁶⁰ P. ATHANASSIOU, “Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks”, *ECB Legal Working Paper Series* 2017, 32. Available at <https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf?344b9327fec917bd7a8fd70864a94f6e>, last accessed 15 April 2018.

¹⁶¹ Santander bank estimates that the adoption of blockchain technology may reduce transaction and compliance costs for banks by up to 20 billion USD a year. See SANTANDER, INNOVENTURES *et al.*, “The Fintech 2.0 Paper: rebooting financial services”, 2016, 8. Available at <http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf>, last accessed 17 April 2018.

transactions that are pursuant to the applicable rules of private law, in order to guarantee the enforceability of the network participants' rights.¹⁶² This consideration leads us to the final and most challenging regulatory mystery: which law applies to cross-border payment transactions registered on the ledger?

c. Transactions

40. The adoption of an interbank decentralized money remittance ledger as described in paragraph 36 is particularly economically advantageous in the context of cross-border transactions, executed and validated by nodes that are located in more than one jurisdiction. Absent any adequate contractual arrangements, such transaction would potentially be governed by the laws of every jurisdiction where a network node is located.¹⁶³ A similar analysis can be made regarding court jurisdiction: in the event a dispute arises, for instance regarding a fraudulent or erroneously executed transaction; courts in every jurisdiction where a node exists may simultaneously claim jurisdiction over the dispute.¹⁶⁴ A clear connecting factor between a transaction and a given territory does not exist due to the lack of a single account or register where the funds involved are held.¹⁶⁵ In the contemporary legal landscape, the nodes in an interbank blockchain-based payment network would transact under legally uncertain conditions.¹⁶⁶ Hence, the network participants would incur higher costs to mitigate this risk, partially defeating the advantage of decreased total transaction cost.¹⁶⁷ Such level of uncertainty is incompatible with the profoundly coordinated blockchain application proposed in these paragraphs. The applicable law should instead be defined from the outset, for all transactions occurring on the network. It may be linked to the jurisdiction governing the platform provider as well as the network itself, as presented in the previous paragraph; or it can be derived from a choice of law made by the platform provider, or by the collaborating financial institutions setting up the network and

¹⁶² E. KARAINDROU, "Distributed ledger technology and the future of payment services", 2017, 20. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078523, last accessed 10 March 2018.

¹⁶³ P. ATHANASSIOU, "Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks", *ECB Legal Working Paper Series* 2017, 30. Available at <https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf?344b9327fec917bd7a8fd70864a94f6e>, last accessed 15 April 2018.

¹⁶⁴ *Ibid.*, 31.

¹⁶⁵ *Ibid.*, 31, see also P. PAECH, "The Governance of Blockchain Financial Networks", *Mod. L. Rev.* 2017, 1106.

¹⁶⁶ P. PAECH, "Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?", *Unif. L. Rev.* 2016, 21, 622.

¹⁶⁷ P. PAECH, "The Governance of Blockchain Financial Networks", *Mod. L. Rev.* 2017, 1107.

thus establish the provider.¹⁶⁸ This choice of law should however be restricted to exclude forum shopping, which would possibly weigh on the trustworthiness of distributed ledger solutions from the perspective of the end-users.¹⁶⁹ In the EU legal context, the Settlement Finality Directive (SFD) limits this choice to the Member States where at least one of the network participants has its head office.¹⁷⁰

The blockchain-based configuration of the money remittance network should entail near to real-time settlements. This quality may be weakened by erroneous implementations of the technology or, in an early stage of development, by an inadequate linkage between the accounts presented in the application's master-ledger on the one hand and the concrete financial situation of a bank on the other hand. In this situation, the law applicable to the transactions is particularly relevant in the event one of the nodes should become insolvent and other nodes seek to enforce their rights vis-à-vis the insolvent network participant.¹⁷¹ This enforceability is usually determined by the laws of the state where the debtor's main interests are located. This is also the approach followed by the EU Insolvency Regulation, which in principal connects both the issue of international jurisdiction and applicable law to this location-based factor, insofar it is situated within an EU Member State.¹⁷² Given the multitude of potentially applicable insolvency laws this rule entails, it would once again be very costly to achieve legal certainty for the participating banks.¹⁷³ We suggest that an analogous solution as presented above may resolve this obstacle, *i.e.* the countries involved should simultaneously link the law applicable to any eventual insolvency dispute to the qualified jurisdiction governing the platform provider itself.

C. CONCLUSION

41. We have identified several configurations for how DLT innovations may affect money as we know it and the operation of the financial institutions underpinning our payment systems. The pure, highly decentralized cryptocurrencies in their current form fail

¹⁶⁸ *Ibid.*, 1106.

¹⁶⁹ *Ibid.*, 1106.

¹⁷⁰ Article 2 (a) Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (SFD).

¹⁷¹ P. PAECH, "The Governance of Blockchain Financial Networks", *Modern Law Review*, 2017, 1107.

¹⁷² Articles 3 and 7 Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings.

¹⁷³ P. PAECH, "The Governance of Blockchain Financial Networks", *Modern Law Review*, 2017, 1107.

to meet the conditions set forth in economic and legal definitions of money, their use for payment purposes is still very limited and therefore, extensive regulation is not yet present nor is it urgent. While these initiatives further develop, cryptosecurity holders and users should be conscious about the differences with the money held in bank accounts; of which the most important difference pertains to the lack of a legal claim vis-à-vis the blockchain entity.

42. Alongside the further development of pure cryptocurrencies, it is likely that established financial institutions will adopt DLT to a certain degree to improve the efficient administration and resilience of bank accounts and payment systems. Such innovation may take place on the level of the existing interbank financial communication network or it may even have the ambition to entirely replace the contemporary mechanisms by putting in place a detailed and reliable master-record for all accounts held by the financial institutions in the permissioned network. The second option will indeed bring about the greatest leaps of increased efficiency, but it will require an enormous effort to convince and unite enough participants to match the size of for instance the SWIFT systems and thus to create a relevant global master-ledger; as well as to guarantee its interoperability with the existing computer programs of all banks involved. Consequentially, the initiative undertaken by SWIFT to enhance the legacy financial communication network is a more feasible scenario in the nearer future, thanks to SWIFT's established participation level in the financial industry and its experience and standardization.

The deployment of an interbank DLT platform gives rise to a number of important policy considerations as to the governance of the participating financial institutions, the interbank platform itself and the law applicable to the transactions potentially effectuated thereon. In the most workable approach to handle these three distinct legal questions, an important role is reserved for the platform provider at the basis of the relevant DLT application. We expect the platform provider to be a new and specialized actor established by the cooperating financial institutions, responsible for a specific range of tasks regarding access control as well as governance and compliance of the platform, its nodes and its users. In the context of the appropriate international regulation, the platform provider can also serve as a reference point to hinge applicable law and international jurisdiction on, with regard to the legal relationships on the DLT.

CHAPTER 2. CRYPTOSECURITIES

43. While blockchain technology may considerably improve efficiency in disintermediated peer-to-peer payments as well as in interbank payment mechanisms, such improvement may be even greater if blockchain innovation is applied to the practice of issuing, holding and transferring securities. Likewise, the legal challenges this transition entails are also considerably greater, given the tremendously complex set of rules surrounding these particular financial activities. We will highlight several aspects of the current market infrastructure at the outset of this part, followed by an exploration of various potential blockchain modernizations in this field.

A. THE MODERN SECURITIES MARKET – *intermediaries, origins and problems*

44. The contemporary organization of holding and trading securities has become a prime example of ultimate intermediation, especially after the implementation of some global and EU responses to the 2008-2009 financial crisis. The following paragraphs explain the functions and origins of the current framework, followed by some adverse effects of this densely intermediated system.

1. Trade lifecycle

45. The lifecycle of a trade transaction involves numerous actors who all have their specific tasks and responsibilities regarding the trading, clearing or settlement of the securities. The number of relevant actors is determined by the complexity and risk innate to the financial instrument at hand. The following brief overview of a transaction aims to provide a general image of the industry, thereby revealing all steps and actors that possibly play a role in a given trade.¹⁷⁴

¹⁷⁴ G.W. PETERS and E. PANAYI, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money” in P. TASCA, T. ASTE *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016, 270-272.

Trading – Investors place their orders to buy or sell a financial instrument with a trading member, which is either a bank who centralizes these orders among a group of banks in an order driven market, or a broker who internalizes these trades by determining an individual buy or sell price for a certain financial instrument, in a quote driven market. The first situation prevails in continental Europe whereas brokerage is typical in the US and UK trading infrastructure. The banks or brokers will rely on an exchange that is responsible to match the accumulated buy and sell orders. Hence, their task is to find counterparties for the investors willing to buy or sell financial instruments.

Post-trading: clearing and settlement – After the banks or brokers establish a purchase agreement between a buyer and a seller through the exchange, the clearing process is initiated, which involves updating the accounts and arranging for the transfer of the securities and money. Parties will clear the transaction, either bilaterally or through a third party. If bilateral clearing is allowed by law, the contracting parties can engage in a direct contractual relationship with each other. Given the considerable risks this entails, the use of risk mitigation techniques like collateralization is essential. Alternatively, parties can seek intermediation by a clearing house, whose role is to facilitate the settlement of the agreement. Not all trading members have direct access to a clearing house, some need to take an additional step through transacting with a clearing member. Clearing houses receive the details on matched orders from their members. They standardize all steps leading up to a net settlement of the aggregated orders; thereby reducing costs and the operational risk of clearing and settling the transactions among multiple parties.

Central clearing – In the EU financial markets, the clearing of certain financial assets is subject to a central clearing obligation.¹⁷⁵ Central clearing serves as an additional layer of risk insulation, built on the intermediation by a clearing house which operates as a Central Counterparty (CCP). The CCP steps in between the original buyer and seller, thereby becoming the buyer to the seller and the seller to the buyer of the original transaction. Hence, through novation, it internalizes and virtually eliminates the counterparty risk the original parties would otherwise incur vis-à-vis each other. Since CCPs have the important role to guarantee the execution of the transactions, these entities are strongly regulated. The

¹⁷⁵ *E.g.* certain classes of over-the-counter derivatives, determined in accordance with article 5 Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (EMIR).

intervention of central counterparties causes a shift of systemic risk from the trading banks to the CCPs; hence, it is imperative for these entities to be robust enough to manage this risk concentration. Therefore, CCPs in the EU are subject to prior authorization (or recognition, for non-EU CCPs) and supervision by the ESMA and by national supervision bodies.

Settlement – The financial assets are held by custodian banks that ensure the safekeeping of the investor’s securities and cash to mitigate risk of loss or theft. These banks hold their clients’ assets in centralized custody at a national or international Central Securities Depository (CSD or ICSD). This entity serves as a first point of entry into the market for newly issued financial instruments, and usually all securities in circulation are deposited at the same CSD at issuance. The custodian banks will send the trade details to the CSD, who then validates and executes the transfer. While the custodian banks of buyer and seller are not necessarily the same entity, the responsible CSD remains unchanged in the context of a trade. For CSDs located within the EU, the CSDR and SFD establish a set of common requirements.¹⁷⁶ The CSDR aims at creating harmonized regulatory and operational conditions for EU CSDs in order to enhance cross-border settlements. On the other hand, the SFD plays an important role in mitigating the systemic risk related to settlement systems in general, therefore it also applies to CSDs. Its goal is to guarantee the enforceability of the transaction, even in the event of a participant’s insolvency.

2. Origins

46. The intermediated handling of transactions in the financial industry as displayed above results from a number of historical efforts to increase transferability and thus liquidity in financial markets; complemented by more recent initiatives to bolster their stability.

From a historical perspective, both shares and bonds have evolved from being nothing more than a bundle of mutual personal obligations between issuer and investor. These primitive financial instruments were difficult to transfer to a second acquirer because of three reasons: the object of the relevant transfer was difficult to assess, given the personal nature of the obligation; it was hard to ascertain whether or not the seller was empowered to dispose over

¹⁷⁶ Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories (CSDR) and the SFD.

the instruments and; lastly, the method to transfer these elementary shares and bonds, *i.e.* assignment, was inadequate, given the fact that obligations (unlike rights) cannot be assigned without the consent of the other party to the obligation.¹⁷⁷ To resolve these limitations, the market was in need of standardization – reducing various personal rights and obligations to straightforward and fungible financial assets is the solution to avoid the excess due diligence needs caused by the uncertainties in the initial situation.

To allow for smoother transferability, the market developed two new concepts: transfer of financial assets by delivery of a certificate and transfer through entries in a registry.¹⁷⁸ Rights and obligations were incorporated in standardized paper, resulting in the certificate being the security, allowing for transfer by delivery of a clearly identifiable asset – certificated securities were treated as negotiable instruments, protecting the subsequent acquirer.¹⁷⁹ Transfer through entry in a register by the issuer also promoted clarity and standardization; and, additionally, it allowed for the issuer to, by changing the register, expressly accept the transfer of obligations represented by the security, thus consenting to novation.¹⁸⁰

While these solutions sufficiently addressed the lack of transferability, they were not future-proof. The continuously growing financial markets in the industrialized world required more liquidity and transfers of certificates or manual entries in registers did not support a high frequency of transactions. This is where intermediation stepped in, along with two innovations for increased liquidity: immobilization and dematerialization of the assets.¹⁸¹ Immobilized physical certificated securities were safely put in central securities depositories and the financial institutions set up an infrastructure of interlinked accounts among them, allowing them to keep record of all investors' security holdings and transactions.¹⁸² Over time, both physical certificates and changing the issuer's registers became irrelevant and the cascade of accounts set up by the financial industry replaced their functions.¹⁸³ The issuance

¹⁷⁷ P. PAECH, "Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?", *Unif. L. Rev.* 2016, 21, 615.

¹⁷⁸ *Ibid.*, 616.

¹⁷⁹ L. THÉVENOZ, "Intermediated Securities, Legal Risk, and the International Harmonisation of Commercial Law", *Stan. J.L. Bus. & Fin.* 2008, 13, 2.

¹⁸⁰ P. PAECH, "Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?", *Unif. L. Rev.* 2016, 21, 617.

¹⁸¹ L. THÉVENOZ, "Intermediated Securities, Legal Risk, and the International Harmonisation of Commercial Law", *Stan. J.L. Bus. & Fin.* 2008, 13, 3.

¹⁸² P. PAECH, "Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?", *Unif. L. Rev.* 2016, 21, 617.

¹⁸³ *Ibid.*, 618.

of securities had moved to the virtual, now computerized world, largely dominated by trading members, clearing members and clearing houses, CCPs and CSDs.¹⁸⁴

47. Among many other measures taken in the aftermath of the 2008 financial crisis, the G20 decided to pursue a safer, more transparent and responsible financial system by establishing a new and global financial policy. It instructed regulators to support effective regulation and supervision to mitigate potentially systemic risks and the ESMA helped implementing the G20 commitments in the EU.¹⁸⁵ Part of this plan focused on the role assigned to CCPs to centralize counterparty risk in the OTC derivatives trading business, as explained earlier. This policy change drastically increased the systemic importance of CCPs in the EU. While these entities are fundamentally different from banks in terms of their business model, ESMA chairman Steven MAIJOR estimates that the impact of a CCP failure could exceed the systemic impact of the failure of a large bank.¹⁸⁶ A similar systemic important role was attributed to CSDs and accordingly, their operation and structure was also harmonized and reinforced in the EU.¹⁸⁷ These efforts illustrate the continued and growing care dedicated to intermediaries that emerged from the immobilization and dematerialization of securities. Certain intermediaries, especially banks, CCPs and CSDs, have evolved from just necessary tools in meeting the need for more liquidity in the financial market, into systemic important entities at the focal point of global financial policy considerations attempting to decrease the risk of future market failures. Hence, their functions in the modern day financial system have diversified and fulfilling these functions adequately remains more relevant than ever before.

3. Deficiencies of the intermediated infrastructure

48. According to PAECH, the emergence of intermediation also entailed major drawbacks, especially from the perspective of the investor.¹⁸⁸ The dematerialization of securities undermined the evidencing function of bearer securities and investors are not even

¹⁸⁴ L. THÉVENOZ, “Intermediated Securities, Legal Risk, and the International Harmonisation of Commercial Law”, *Stan. J.L. Bus. & Fin.* 2008, 13, 3.

¹⁸⁵ S. MAIJOR, “Regulatory measures to prevent another crisis”, transcript, 19 November 2014, 2. Available at <https://www.esma.europa.eu/sites/default/files/library/2015/11/2014-1382.pdf>, last accessed 22 April 2018.

¹⁸⁶ *Ibid.*, 9.

¹⁸⁷ Recitals 1-5 CSDR.

¹⁸⁸ P. PAECH, “Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?”, *Unif. L. Rev.* 2016, 21, 617-619.

registered by their own name in the records that replace the certificates – only the intermediaries are identified, and they hold the aggregate of the securities in bulk, pursuant to the sequence of legal relations in the holding cascade. The former *erga omnes* claim held by the investor vis-à-vis the issuer is reduced to a chain of stacked contractual relations, mirroring each other from intermediary to intermediary.¹⁸⁹ It is argued that the modern transactional framework has weakened the position of the individual investor, especially in the event one of the intermediaries becomes insolvent.¹⁹⁰ The risks involved are enlarged given the considerable amount of time it takes to complete the traditional settlement process.¹⁹¹ The lack of harmonized legal approaches to determine the rights and duties in the global intermediated financial infrastructure has worsened the problem.¹⁹²

4. The blockchain alternatives

49. Various DLT-based solutions have been suggested to resolve the inefficiencies and risks inherent to the modern infrastructure. These ideas differ in their degree of promoted disintermediation, similar to the classification of the different strategies regarding the implementation of blockchain technology in payment transactions. Some authors advocate a *Bitcoinization* of the securities market.¹⁹³ They propose complete disintermediation through the establishment of a public distributed ledger serving as an independent cryptosecurity record, where trades are concluded on a peer-to-peer stock exchange. The issuance of these native cryptosecurities is called an Initial Coin Offering (ICO), *i.e.* the blockchain version of an IPO.¹⁹⁴ The cryptosecurities exist separately from the intermediated securities market; however, in an alternative version of the native cryptosecurity scenario, pre-existing intermediated securities would also be moved to the

¹⁸⁹ *Ibid.*, 619.

¹⁹⁰ E. MICHELER and L. VON DER HEYDE, “Holding, clearing and settling securities through blockchain/distributed ledger technology: creating an efficient system by empowering investors”, *Journal of International Banking & Financial Law* 2016, 653.

¹⁹¹ The EU financial market has moved to a two days settlement cycle; in the US, this takes three days. See also G.W. PETERS and E. PANAYI, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money” in P. TASCA, T. ASTE *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016, 270.

¹⁹² P. PAECH, “Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?”, *Unif. L. Rev.* 2016, 21, 619-624.

¹⁹³ *E.g.* LEE, PAECH and, to some extent, HACKER and THOMALE.

¹⁹⁴ Note that an ICO should be distinguished from the hypothesis where pre-existing traditional securities are moved to a blockchain environment.

blockchain environment, thereby gradually phasing out the current infrastructure.¹⁹⁵ Others envision a back-office adoption of blockchain technology to enhance the existing intermediated approach.¹⁹⁶ As is the case for cryptocurrencies, both tracks for blockchain innovation are not mutually exclusive, yet they require a distinct regulatory approach and a different focus.

B. HIGHLY DECENTRALIZED AND PUBLIC – *token sales, ICOs and ...*

1. vs. cryptocurrencies?

50. We already established that practice shows that the majority of cryptocurrency holders is driven by speculative objectives rather than by an ambition to use the coins in their account for day-to-day payments.¹⁹⁷ Speculative investors of this kind anticipate an appreciation of the cryptocurrency's value, purely based on their artificial, coded scarcity combined with an expected widespread adoption as a means of payment in the future.¹⁹⁸ Besides this form of pseudo-investment, other blockchain-based assets have emerged that bear a closer resemblance to traditional financial investment assets, for instance by incorporating a dividend or interest rights, based on the expectation of future cash flows to be generated by the issuer. However, it is often difficult to make the distinction between cryptocurrencies and cryptosecurities since many crypto-assets exhibit specific characteristics of both categories.¹⁹⁹ Yet, the exact qualification of the tokens is important in order to identify the potentially relevant legal framework.²⁰⁰ HACKER and THOMALE have suggested a litmus test in case of doubt. According to these authors, a crypto-asset is to be

¹⁹⁵ So-called trans-cryptocurrencies. See P. PAECH, "Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?", *Unif. L. Rev.* 2016, 21, 634.

¹⁹⁶ E.g. PETERS and PANAYI, MICHELER and VON DER HEYDE, ESMA.

¹⁹⁷ *Supra*, 27.

¹⁹⁸ For instance, the number of newly supplied *Bitcoins* decreases ensuring a final total of slightly less than 21 million coins in circulation. This upper limit will be reached around 2040, depending on the evolution of the mining power in the network. See ECB, "Virtual currency schemes", report, 2012, 25. Available at <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, last accessed 15 April 2018; see also: J.L. VERHELST, "Zijn cryptomunten muntten? Een analyse van Bitcoin" in M.E. STORME and F. HELSEN (eds), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia, 2017, 34.

¹⁹⁹ P. HACKER and C. THOMALE, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law", 2017, 36. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, last accessed 12 February 2018.

²⁰⁰ *Infra*, 54-57.

considered a cryptosecurity if at least one of the following circumstances applies: the issuers raised significant expectations of profits through their communication, or, the given crypto-asset is mostly bought with the intention to resell it with profit while the issuers are aware of this incentive.²⁰¹ Determining the nature of the crypto-assets based on the motifs of the average token investor moreover corresponds with the scope of EU and US securities rules, respectively embodied in the Prospectus Regulation and the US *Howey*-test.²⁰² Besides the specific underlying objectives of investor and issuer, it is difficult to differentiate cryptocurrencies from cryptosecurities.

51. Indeed, the technical setup of the fully disintermediated cryptosecurities strongly resembles the construction of cryptocurrencies. In the context of the broader ‘tokenization of assets’, companies have started issuing tokenized securities, thereby using public blockchain platforms like *Ethereum* or *Ripple*.²⁰³ Just like cryptocurrency coins, these securities exist only by entry in a public distributed ledger and ownership as well as all transactions are recorded in this ledger; hence, the cryptosecurities are native crypto-assets.²⁰⁴ Trading occurs on a public blockchain to prevent double-spending, the tokenized assets are freely transferable upon initiative of the holder of the associated private key. Given its public nature, a performant and future-proof consensus mechanism is indispensable for a trustworthy cryptosecurities market. Tokens can be accurately designed to represent any type of debt or equity financial instrument, possibly implementing smart contracts to facilitate the execution of rights by the asset holder, *e.g.* automated dividend distribution to shareholders.²⁰⁵

52. Similar to how publicly transferable native cryptocurrencies may compete with traditional money, one could say that cryptosecurities compete with traditional means of

²⁰¹ P. HACKER and C. THOMALE, “Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law”, 2017, 37. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, last accessed 12 February 2018.

²⁰² *Ibid.*, 18-19 & 34.

²⁰³ In this regard, cryptocurrencies can also be seen as a specific kind of tokenized assets. See for example the clarification published by the MONETARY AUTHORITY OF SINGAPORE (MAS), “MAS clarifies regulatory position on the offer of digital tokens in Singapore”, press release, 1 August 2017. Available at <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx>, last accessed 16 April 2018.

²⁰⁴ C. VAN DER ELST and A. LAFARRE, “Blockchain and the 21st Century Annual General Meeting”, *European Company Law Journal* 2017, 4, 173.

²⁰⁵ Smart contracts, *infra*, 64 *sqq.*

issuing and trading financial assets.²⁰⁶ The blockchain solution has its strengths: it increases stock market stability by, among others, banning the practice of spoofing and naked short selling; and it allows for more transparency, fast settlement, twenty-four hours of trading per day and reduced transaction costs.²⁰⁷ Peer-to-peer transactions or direct trading through the exchange renders intermediation by a broker unnecessary and since the rights of all investors are recorded in the distributed ledger, transfer agents or registrars are completely obviated.²⁰⁸ Furthermore, these native cryptocurrencies are also well-positioned to both meet the needs for higher liquidity in the financial markets without bringing along the drawbacks caused by a chain of mirrored rights between numerous intermediaries.²⁰⁹ The realization of the underlying objectives of dematerialization is preserved – tokenization allows for even greater transferability and thus liquidity – while the cumbersome cascade of contractual relations is eliminated along with the risks and uncertainty it caused. The blockchain-based settlement system aims at increasing the direct relationship between investors and the issuer, reducing the degree of dependency on intermediating actors.²¹⁰

53. A specific aspect of native cryptosecurities is their initial emission to the market. Unless they are meant to replace pre-existing traditional shares, new cryptosecurities are distributed through an ICO. Note that an ICO can also be launched to create a new cryptocurrency or any other kind of innovative blockchain platform. Many ICOs however concern coins that serve an investment objective, for instance to raise money for a specific and possibly lucrative project. For the time being, most established issuers of financial instruments seek funding through the traditional infrastructure as described above, in order to ensure legal certainty while the industry awaits regulatory changes to support blockchain alternatives. For startups and young companies however, native cryptosecurities are regarded an attractive and accessible new way of financing; hence, the startup environment is currently the most important source of native cryptosecurities. They potentially offer higher returns for the investors and, for the issuing company, it is a less burdensome way to obtain financing than the venture capitalist alternative. Some even refer to ICOs as

²⁰⁶ *Supra*, 28 *sqq.*

²⁰⁷ L. LEE, “New Kids on the Blockchain: How Bitcoin’s Technology Could Reinvent the Stock Market”, *Hastings Business Law Journal* 2016, 12(2), 119-122.

²⁰⁸ *Ibid.*, 123.

²⁰⁹ P. PAECH, “Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?”, *Unif. L. Rev.* 2016, 21, 631.

²¹⁰ Consequentially, it may fulfill the role of ‘future innovations’ as envisioned by Charles MOONEY, see C.W. MOONEY, “Beyond negotiability: a new model for transfer and pledge of interests in securities controlled by intermediaries”, *Cardozo L. Rev.* 1990, 12, 414.

“unregulated issuances of crypto coins”, implying that cryptosecurity issuers avoid the entirety of regulation surrounding a financing undertaking on the capital markets.²¹¹ The statement is a misconception based on the finding that, currently, almost no regulation exists that specifically addresses ICOs and other blockchain-based solutions for holding financial assets. It must be noted that, depending on the governing jurisdiction, general financial regulations possibly apply to these schemes, regardless of their underlying technology.²¹²

2. Regulation?

a. Issuance and market infrastructure

54. Before assessing whether any legal provisions with a general scope may apply to the issuance, trading and the (minimal) infrastructure surrounding cryptosecurities, we need to establish how to appoint the jurisdiction that governs the issuer and the blockchain platform it operates through. In the first place, concerning laws that create obligations for the issuer, it is logical that an issuer will have to obey the rules that exist in the market where the financial instruments are sold. As the platform will be accessible for investors through a website, the issuer can be expected to use this layer to control in which countries the relevant webpage is accessible, by blocking IP-addresses located elsewhere. Consequentially, the issuer will, for instance, be responsible to obey prospectus rules that apply in the market or markets where he offers the cryptosecurities through the blockchain platform’s website.²¹³ Secondly, the general rules that apply to the blockchain application itself are more difficult to enforce or to hold the issuer accountable for. However, while pure cryptocurrencies – in contrast to their permissioned, private counterparts – lack any reference point for enforcement, it might be more feasible to find a highly decentralized cryptosecurities blockchain platform (or, its establishers) willing to actively comply with the relevant laws.²¹⁴ Indeed, a securities issuer seeking investments will likely choose a platform that is trusted in the investor’s market. A platform that complies with financial regulations

²¹¹ See for example the wording used in I. KAMINSKA and P. MURPHY, “Bitcoin’s surge fuels fears of asset bubble”, *Financial Times*, 14 May 2017. Available at <https://www.ft.com/content/ce3ef54e-371b-11e7-bce4-9023f8c0fd2e>, last accessed 20 April 2018.

²¹² P. HACKER and C. THOMALE, “Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law”, 2017, 5. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, last accessed 12 February 2018.

²¹³ *Ibid.*, 17.

²¹⁴ See the preliminary question raised concerning the applications of payment service laws, *supra*, 31.

presumably bears such a ‘trusted’ seal. Moreover, a rational issuer will minimize its own risk and ensure the reliability of the investment capital by choosing a trusted blockchain platform. Accordingly, the success of this type of blockchain platform is to be contingent on its compliance with the laws of a country that has a solid financial legal framework in place, *e.g.* an EU member state; which is why it is in their interest to take such rules into account.

55. In the event the spatial scope of EU or US security regulations would be established to extend to a certain issuance of cryptosecurities and the market they are traded on, different general sets of rules can be identified that do not take into account the technical particularities of a given financial instrument. Consequentially, these laws contain provisions that potentially apply to the activities on a market that is built on a highly decentralized, public blockchain platform; and to the operation of such platform.²¹⁵

Regarding the applicability of the general existing EU financial laws, the ESMA has already stressed that the Prospectus Regulation, MiFID II, the AIFM Directive and the AML Directive should be complied with by organizations issuing cryptosecurities.^{216, 217} Other relevant EU legal instruments generally applicable to securities, thus potentially applicable

²¹⁵ *Financial Times* also recognized this reality after the misleading wording used medio 2017. See H. MURPHY and B. THOMPSON, “Law firms look to capitalise on initial coin offering boom”, *Financial Times*, 26 March 2018. Available at <https://www.ft.com/content/2ae9154c-1d56-11e8-aaca-4574d7dabfb6>, last accessed 20 April 2018.

²¹⁶ Article 1 (1) Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market (Prospectus Regulation) (in force, but not yet entirely applicable); and, Article 4 (1) (15) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (MiFID II); and, Article (4) (1) (n) Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers (AIFM Directive); and, Article 3 (2) and article 2 (1) (2) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AML Directive).

²¹⁷ ESMA, “ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements”, statement, 13 November 2017. Available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf, last accessed 7 April 2018.

to certain cryptosecurities, are the MAR, the UCITS Directive as well as the EMIR.^{218, 219} Note that rules on prospectus obligations and the rules regarding the trading and market infrastructure are only applicable to securities, thereby explicitly excluding instruments of payment such as pure cryptocurrencies.²²⁰ Determining the degree of this legal framework's applicability to ICOs and other tokenized financial instruments is however beyond the scope of our current research. An in-depth analysis concerning the impact of notably the new European Prospectus Regulation on ICOs is presented in the cited article by HACKER and THOMALE.²²¹ This research specifically addresses the subject of public blockchain applications for registering and transferring financial assets in the EU legal context.

Similarly, in the US, Larissa LEE expects that most of the existing financial legal framework will remain the same with a public cryptosecurities market. In a recent research paper, she analyses the implications of the development of a cryptosecurities market, for the legal status of traditional financial market actors under the Securities and Exchange Act. LEE concludes that, while some intermediaries partially or wholly lose their relevance, the individual responsibilities of issuers, purchasers and platforms that serve as an exchange would not change.²²²

b. Transactions

56. Another question relates to determining the law applicable to the nature of the rights associated with the cryptosecurity and the enforceability of their acquisition and disposition. In the contemporary intermediated context, measures have been taken to promote the Place

²¹⁸ Article 2 (1) Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (MAR); and,

Article 1 (2) Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS Directive); and,

Article 1 (3) EMIR.

²¹⁹ P. HACKER and C. THOMALE, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law", 2017, 19. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, last accessed 12 February 2018.

²²⁰ Article 4 (1) (44) MiFID II and article 2 (a) Prospectus Regulation.

²²¹ P. HACKER and C. THOMALE, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law", 2017. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, last accessed 12 February 2018.

²²² L. LEE, "New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market", *Hastings Business Law Journal* 2016, 12(2), 123-127.

of Relevant Intermediary Approach (PRIMA) in this regard.²²³ It is the answer to the conflict of laws problems that emerged from the dematerialization and pooling of financial instruments and it presupposes the existence of accounts held with intermediary actors. However, excluding such intervention happens to be the very purpose of setting up a blockchain for the issuance and trading of cryptosecurities. A possible alternative is to determine the applicable law based on the location of the issuer, *i.e.* the *lex societatis*.²²⁴ This solution would lead to a situation where an investor with an internationally diverse portfolio has to consider the rules of all countries where an issuer is incorporated.

57. Instead, it would be more manageable if all cryptosecurities issued through the same blockchain platform were governed by one and the same jurisdiction, the *lex systematis*.²²⁵ This choice of law would have to coincide with the jurisdiction the platform itself complies with for the sake of clarity. Thus, this mechanism once again implies the willingness of the individuals or organization behind the blockchain platform to be governed by the laws of a certain country, but as described above, this undoubtedly is in the interest of the issuers of financial instruments.²²⁶

3. Conclusion

58. It is clear that the emergence of pure cryptosecurities has opened a door for issuers to attract investments more fluently and in a less burdensome way. The investment component of these tokenized assets means an important difference with cryptocurrencies, arising from the fact that pure means of payment are exempt from many sets of rules that do apply to financial instruments, as well as to their issuance and the infrastructure they are traded on. As the relevant legal instruments are underdeveloped and only apply in general terms, legal uncertainty still prevails at this experimental stage of cryptosecurities. This explains why ICOs are, for the time being, mainly embraced by startups and smaller

²²³ See for example the aforementioned SFD and the Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary (The Hague Securities Convention).

²²⁴ P. PAECH, “Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?”, *Unif. L. Rev.* 2016, 21, 636.

²²⁵ *Ibid.*, 636.

²²⁶ *Supra*, 54.

innovative companies.²²⁷ Certain countries are willing to promote the pure cryptosecurity emergence by taking some first steps towards the legal recognition of this innovation. France recently passed a law that accommodates ICOs in the existing legal framework, by explicitly allowing the use of DLT for the issuance and transmission of unlisted securities.²²⁸ The issuer can choose to register the securities to a blockchain platform instead of to a CSD. The French legislator ascertained that the targeted financial instruments are out of the scope of EU rules regarding listed companies, regulated markets and organized trading facilities, thereby avoiding a collision with mandatory EU rules. Similarly, the Monetary Authority in Singapore invites fintech firms that develop blockchain platforms for financial services to experiment with their innovations in the controlled environment of a proverbial ‘regulatory sandbox’.²²⁹ This measure is in sharp contrast with efforts in China and South Korea to ban ICOs.²³⁰

It is unlikely that the legal framework surrounding the established intermediated financial markets would change overnight, especially not on the matters of heavily regulated subjects such as listed companies and organized trading facilities. The ICOs and token trades will not entirely replace the intermediated financial landscape anytime soon, however, there is a tendency to grant the ICOs the room to further develop independently from the traditional financial markets; while controlling potential risks. It is mainly important for investors to receive information and education on the practical and legal differences between holding shares through the intermediated market or by means of a blockchain-based issuance. LEE compares the finding that both models for financial markets can exist next to each other to the advent of the email and continued relevance of traditional post services.²³¹ However, while the modern market infrastructure must not necessarily be replaced, that does not mean

²²⁷ H. MURPHY and P. STAFFORD, “Blockchain explainer: a revolution in its infancy”, *Financial Times* (2 February 2018). Available at <https://www.ft.com/content/6c707162-ffb1-11e7-9650-9c0ad2d7c5b5>, last accessed 20 April 2018.

²²⁸ Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers. Available at <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036171908>, last accessed 1 May 2018.

²²⁹ MAS, “Fintech Regulatory Sandbox Guidelines”, 2016. Available at <http://www.mas.gov.sg/~/-/media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines.pdf>, last accessed 20 April 2018.

²³⁰ D. WEINLAND and L. LUCAS, “Asian investors flock to initial coin offerings despite bans”, *Financial Times*, 14 November 2017. Available at <https://www.ft.com/content/05b2748c-c903-11e7-aa33-c63fdc9b8c6c>, last accessed 20 April 2018.

²³¹ L. LEE, “New Kids on the Blockchain: How Bitcoin’s Technology Could Reinvent the Stock Market”, *Hastings Business Law Journal* 2016, 12(2), 127.

that DLT may not impact its back-end transaction mechanisms. The following paragraphs will discuss how blockchain-technology may improve the efficiency and coordination across all actors currently involved in the securities trade cycle.

C. PERMISSIONED AND PRIVATE – *blockchain-based interbank securities clearing and settlement*

59. Financial institutions in the regulated securities market industry are actively investing in the development of DLT-based solutions.²³² Their incentive is two-fold: in the first place, established actors likely want to guarantee the continuity of their own business in the future; and additionally, the adoption of DLT can drastically increase the efficiency of the infrastructure that currently underpins the financial markets. Pursuing the first ambition demands innovative changes to keep offering competitive services – therefore, both incentives go hand in hand. Likewise, the ESMA stipulated in a report to the industry that DLT in financial markets should be of the permissioned, private kind.²³³ Policy and governance arguments relating to the regulatability aspect of the technology explain this stance. Analogous to the reasoning presented in paragraphs 37 to 40, it is manageable to adequately subject emergent permissioned, private blockchain networks to a large part of existing financial regulation and supervision; while highly decentralized ledgers need tailor-made regulation to a greater extent.

60. DLT is capable of simplifying the contemporary regulated trade lifecycle in various ways. It is suggested to adopt blockchain technology for each step of the trade settlement process separately, so-called ‘consortium blockchains’.²³⁴ The existing actors situated at every level of the cycle will then benefit from moving on to DLT. Consequentially, the enhanced trade lifecycle works as follows. A securities transaction, once established by the

²³² For example, the projects launched by clearing houses like the Australian Securities Exchange (ASX) and the US Depository Trust & Clearing Corporation (DTCC). See M. ARNOLD, “Five ways banks are using blockchain”, *Financial Times*, 16 October 2017. Available at <https://www.ft.com/content/615b3bd8-97a9-11e7-a652-cde3f882dd7b>, last accessed 20 April 2018.

²³³ ESMA, “The distributed ledger technology applied to securities markets”, report, 2017, 4. Available at https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf, last accessed 7 April 2018.

²³⁴ G.W. PETERS and E. PANAYI, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money” in P. TASCA, T. ASTE *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016, 272.

banks or brokers acting on behalf of the investors, is securely registered to and verified on the first blockchain network; to which access is permissioned to the banks or brokers. By doing so, validly recorded orders can easily be accumulated to facilitate communication with the entities at the clearing level in the chain. Secondly, clearing members can set up a distributed clearing house. They are the nodes in a blockchain to which the transaction is uploaded in the form of a smart contract that represents the bilateral relations between the buyer's and seller's end of the transactions. Consequentially, there is no need for an intermediary entity cutting the contractual relation in two halves. Risk mitigation mechanisms are to be built into the standardized smart contracts created at this level of the chain – while a securities settlement blockchain network still primarily serves to store the transfers of the financial asset, second generation innovations are introduced to expand its functionality. Once this smart contract is verified, the execution is carried out by transmitting the relevant information to the custodian or CSD level. Settlement entities, thirdly, replace the contemporary accounts by the blockchain substitute. The custodian banks are the nodes who are running this ledger. This innovation enhances the safety and permanence of the data kept by custodian entities, which, after all, is the core purpose of custodians. This account data can be complemented by smart contracts that support and automate other services offered to clients and investors. An example of such application is the tool for shareholder voting at an issuer's annual general meeting, as described by VAN DER ELST and LAFARRE.²³⁵ In a scenario of full DLT adoption at the settlement level, these accounts will represent the actual custody of all dematerialized financial assets in circulation. Upon issuance of these securities, they will be directly recorded to the settlement ledger. Consequentially, the assets registered on the blockchain application at this third and final stage of the settlement cycle are native crypto-assets, contrary to the intermediary transactions that only occur on the DLT systems established at phase one and two of the trade sequence.

The configuration described above is an example of how different DLTs can enhance the performance of all contemporary intermediaries in the settlement cycle, while these entities fulfill their individual purposes independently. Additionally, the advantages of reduced risk and costs would be shared among all actors on every level of the procedure, including the end-users and investors. Indeed, the interconnectedness of the three layers of the DLT and the streamlined processes within every level leads to a shorter settlement cycle, which, by

²³⁵ C. VAN DER ELST and A. LAFARRE, "Blockchain and the 21st Century Annual General Meeting", *European Company Law Journal* 2017, 4, 174.

definition, also brings about a lower level of credit and counterparty risk.²³⁶ Nevertheless, the effectuation of this adoption scheme must acknowledge various elements of legal reality and the crucial role of certain intermediaries, especially in scenarios where a central clearing obligation exists. In particular, in the EU, this process needs to be made compatible with the standards stipulated by the ESMA for emerging DLT solutions on the securities markets.²³⁷

61. In 2016, the ESMA has launched a discussion paper with the ambition to engage in a dialogue with the market of DLT fintech companies.²³⁸ The 2017 report is based on the findings from this dialogue and it serves as a set of guidelines for innovative financial players with the ambition to develop DLT solutions that are meant to operate within the boundaries of the regulated EU financial market. Given the premature stage of various projects, the ESMA chose to follow a general approach in the discussion of DLT opportunities and *caveats*, without detailed consideration of where the DLT role in the settlement cycle is envisioned. A plausible explanation is that the ESMA tries to avoid unnecessarily limiting the innovative creativity; additionally, the DLT potential should be accessible for the stakeholders at all levels of the current settlement cycle. Nevertheless, the report heavily focuses on post-trading processes and the ESMA authors promote the concept of a single ‘golden record’ blockchain which is shared across all market participants and which centralizes all information related to a given financial instrument. Such scheme would in fact allow for near to instantaneous clearing and settlement with a single step trade confirmation, affirmation, allocation and settlement.²³⁹ This disruptive vision is somewhat contrary to the ESMA’s conviction regarding the incessant relevance of regulated, pre-authorized and supervised entities, even in the context of DLT clearing. It also seems inconsistent with the concerns expressed in relation to a possible disturbance to the fair competition between market participants who are or are not granted access to the single distributed ledger. The blockchain is set up by private entities and as its success is largely

²³⁶ ESMA, “The distributed ledger technology applied to securities markets”, report, 2017, 7. Available at https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf, last accessed 7 April 2018.

²³⁷ *Ibid.*, 7-19.

²³⁸ ESMA, “ESMA Assesses usefulness of distributed ledger technologies”, press release, 2 June 2016. Available at <https://www.esma.europa.eu/press-news/esma-news/esma-assesses-usefulness-distributed-ledger-technologies>, last accessed 9 April 2018.

²³⁹ ESMA, “The distributed ledger technology applied to securities markets”, report, 2017, 7. Available at https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf, last accessed 7 April 2018.

determined by the network effects of its extensive adoption, the market configuration risks to be prone to monopolistic effects.²⁴⁰

62. The ESMA stresses that counterparty and credit risk cannot be excluded by decentralized ledgers in their current development stage; especially not in relation to financial instruments with a term structure. Accordingly, the execution of transactions that are in the scope of the EMIR and MiFIR clearing obligation should, if conducted on a blockchain, be compliant with the relevant provisions. More specifically, an authorized CCP must join this network or the application itself would have to meet the requirements and acquire authorization. An analogous reasoning pertains to the settlement level: if the settlement transactions fall within the scope of the CSDR, the risk mitigating mechanisms apply and hence a licensed CSD must be involved in the blockchain or it needs to obtain a CSD authorization itself. A scenario where clearing and settlement are transformed into a single, near to instantaneous transaction which is conducted on a single ‘golden record’, that accommodates any trade or financial asset regardless of its individual features and needs, leads to an undue consolidation of the specific features attributed to a CCP *c.q.* a CSD – that is, to the extent the activities are subject to a CCP clearing obligation. After all, a CCP entity centralizes and accepts risk whereas a CSD is meant to avoid risk.²⁴¹ On the other hand, the DLT will not be deployed across the entire securities market all at once. The first blockchain-based settlement systems that are designed to facilitate the existing intermediated procedure in the EU could target a more accessible market segment with straightforward financial products and lower risks; thereby steering away from the central clearing obligation and, possibly, other regulations.²⁴²

²⁴⁰ *Ibid.*, 11-15.

²⁴¹ The DLT platform *Corda*, launched by *R3*, would however allow for the implementation of CCP and CSD functions, and to meet the relevant legal requirements. See M. HEARN, “Corda: A distributed ledger”, whitepaper, 2016, 28. Available at https://docs.corda.net/_static/corda-technical-whitepaper.pdf, last accessed 5 May 2018.

²⁴² As also indicated by many of the respondents to the ESMA discussion paper, see ESMA, “The distributed ledger technology applied to securities markets”, report, 2017, 23. Available at https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf, last accessed 7 April 2018.

D. CONCLUSION

63. Regardless of how a blockchain that administers the issuance, holding and transactions of financial instruments relates to the contemporary, intermediated securities markets; users and developers should be aware of general financial regulations that may not have been created with DLT solutions in mind but that do apply to the activities this innovation is capable to facilitate. The most suitable path depends on a wide range of factors: the type of financial assets involved, the targeted average investor, the issuer's quality and strategy... Accordingly, interesting DLT applications will emerge both on a highly decentralized level and in permissionless setups; both to directly accommodate native crypto-assets and to facilitate the execution of an intermediary step through validating non-native transaction data. The great variety of blockchain arrangements is capable to meet an equal variety of market needs; while all different setups benefit from the core blockchain features regarding its immutability, resilience and transparency within the network.²⁴³ Hence, we find it beneficial to promote the co-existence of both the disintermediated scenarios (notably ICOs) and the traditional financial markets with DLT-based clearing and settlement. An enhanced legal framework should focus on advising both users and investors on the differences and on leading them to the most suitable scenario, especially where more considerable risks are involved. Establishing such clarity would be significantly more challenging if securities that pre-exist in the intermediated financial system are partly moved to the pure DLT environment, thereby creating a category of trans-cryptosecurities.²⁴⁴ Furthermore, lawmakers will closely have to monitor DLT while the technology further develops, and new regulatory action should bear the diversity of possible applications in mind. While some legal novelties may overlap for the different sorts of crypto-assets, *e.g.* regarding the law applicable to transactions involving native crypto-assets; other laws will need to be tailor-made for an individual scenario, *e.g.* a set of regulatory authorization conditions specifically meant for the activities of a DLT-based clearing solution. Given the fact that the global nature of securities markets will only extend further due to the advent of blockchain technology, EU and international cooperation and engagement will be crucial

²⁴³ G.W. PETERS and E. PANAYI, "Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money" in P. TASCIA, T. ASTE *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016, 259-260.

²⁴⁴ P. PAECH, "Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?", *Unif. L. Rev.* 2016, 21, 634.

for the development of an adequate legal framework that finds a balance between mitigating risks and promoting valuable innovation.²⁴⁵ DLT is expected to rapidly develop, hence, substantial efforts will be required to modify the legal reality accordingly. Or, as appropriately phrased by Joanna Diane CAYTAS, “the current speed of global constitutional, legislative, regulatory and adjudicatory systems not only should but must accelerate by quantum leaps commensurate to those of the underlying technologies they relate to.”²⁴⁶

²⁴⁵ ESMA, “The distributed ledger technology applied to securities markets”, report, 2017, 19. Available at https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf, last accessed 7 April 2018.

²⁴⁶ J.D. CAYTAS, “Developing Blockchain Real-Time Clearing and Settlement in the EU, U.S. and Globally”, *Columbia Journal of European Law: Preliminary Reference* 2016, 11.

TITLE 4. SMART CONTRACTS

*Le langage est source de malentendus.*²⁴⁷

– A. DE SAINT-EXUPÉRY, *Le Petit Prince*

CHAPTER 1. ORIGINS

64. In the previous chapters, we already came across several instances where the use of smart contracts is suggested to further enhance the functionality of a crypto-asset DLT application, e.g. for the implementation of shareholder voting rights.²⁴⁸ While the recent advent of blockchain technology provides the ideal platform to more efficiently operationalize the concept of a smart contract, a considerable lapse of time exists between the first appearance of both individual novelties. Nick SZABO first defined a smart contract back in 1994 as follows:

*A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.*²⁴⁹

According to this initial understanding, a smart contract is mainly characterized by the computer protocol that determines its effectuation. SZABO built his idea on the theory that many common contractual clauses are capable to be embedded in the hardware and software humans interact with.²⁵⁰ As such, the machine incorporates the actual realization of the meeting of the minds that precedes and constitutes the contract. For instance, the fulfillment

²⁴⁷ A. DE SAINT-EXUPÉRY, *Le Petit Prince*, Paris, Gallimard, 1943, 80.

²⁴⁸ *Supra*, 18 and 60.

²⁴⁹ N. SZABO, “Smart Contracts”, 1994. Available at <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>, last accessed 24 April 2018.

²⁵⁰ N. SZABO, “Formalizing and Securing Relationships on Public Networks”, *First Monday* 1997.

of a sales contract is translated into the design of a vending machine.²⁵¹ This primitive example only includes one standard contract but with the development of computers came the rise of a formal language to design more intricate and custom-made ‘vending machines’ and to operationalize specific financial contractual clauses that constitute collaterals, bonds, futures, derivatives...^{252, 253} The aggregate of formal computer language is deemed to be able to process data correctly in order to reach the outcome envisaged by the traditional contract counterpart. Correspondingly, a smart contract is an execution-focused tool. The result of embedding an agreement into hardware and software is that it becomes increasingly and sometimes prohibitively expensive for parties to breach the terms of the contract; or, more precisely, to breach the terms of the coded smart contract version of it.²⁵⁴ In conclusion, “a smart contract is an agreement whose execution is automated.”²⁵⁵

65. The emergent blockchain technology and the concept of smart contracting are different yet complementary. DLT extends the capacities of formal computer language, in a way that it allows to guarantee the effective completion of the smart contract script between individuals. It promotes the protocol in its ability to indeed achieve its execution through the terms and mechanisms of the contract on the DLT itself without recourse to third parties.²⁵⁶ By virtue of the employment of blockchain technology, both parties necessarily run the same ‘golden’ version of the contract code which is anchored in the distributed ledger; rather than both parties installing an individual instance of the program on their own computers and relying on each other’s willingness to the run the code agreed on.²⁵⁷

Likewise, the smart contract concept extends the functionality of the initial, first generation blockchain technology. It allows for the use of the consensus mechanism to process and validate computation rather than to just validate data; and to cement the running of a computer program in the blockchain rather than just adding blocks of plain transactional

²⁵¹ *Ibid.*

²⁵² *Ibid.*, and N. SZABO, “A Formal Language for Analyzing Contracts”, 2002. Available at <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/contractlanguage.html>, last accessed 24 April 2018.

²⁵³ For a practical example of an elaborated bond issuance smart contract, see R3 LIMITED, “Writing a contract”, 2018. Available at <https://docs.corda.net/tutorial-contract.html>, last accessed 26 April 2018.

²⁵⁴ N. SZABO, “Formalizing and Securing Relationships on Public Networks”, *First Monday* 1997.

²⁵⁵ M. RASKIN, “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 309.

²⁵⁶ *Ibid.*, 321.

²⁵⁷ ISDA and LINKLATERS, “Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective”, 2017, 9. Available at <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>, last accessed 24 April 2018.

data to the chain.²⁵⁸ The establishment of platforms that effectively host and execute smart contract formal language has brought the smart contract concept into the mainstream.²⁵⁹ One of the most successful DLT platforms supporting the use of smart contract language is *Ethereum*, which follows the model of *Bitcoin* – it is permissionless and it relies on an elaborate consensus mechanism – and it accommodates its own pure cryptocurrency to perform contractual payment obligations with, *ether*.²⁶⁰ This platform has its own programming language, designed specifically for the implementation in smart contracts: *Solidity*.²⁶¹

CHAPTER 2. CODERS' APPROACH – *code is law*

66. The currently prevailing view on smart contracts represents a mere technical-theoretical approach – what is the combination of smart contracting language and DLT capable of? It represents the viewpoint of the computer engineer rather than how a law professional examines it. While SZABO's definition highlights the automated execution aspect, little consideration is given to the establishment of a legally binding contract. By describing a self-executing transaction protocol that realizes the terms of a (legal) contract as a tool that, among others, decreases enforcement costs, it seems that execution and enforceability are near to confounded. The definition presented by CLACK *et al.* even puts both concepts on the same level:

*A smart contract is an agreement whose execution is both automatable and enforceable. Automatable by computer, although some parts may require human input and control. Enforceability by either legal enforcement of rights and obligations or tamper-proof execution.*²⁶² (emphasis added)

²⁵⁸ G.W. PETERS and E. PANAYI, "Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money" in P. TASCA, T. ASTE *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016, 246. See also: D. DRESCHER, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, New York: Springer Science+Business Media, 2017, 240.

²⁵⁹ ISDA and LINKLATERS, "Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective", 2017, 8. Available at <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>, last accessed 24 April 2018.

²⁶⁰ *Ethereum*, <https://www.ethereum.org/>, last accessed 7 April 2018.

²⁶¹ *Solidity*, <http://solidity.readthedocs.io/en/latest/>, last accessed 7 April 2018.

²⁶² C. D. CLACK, V. A. BAKSHI and L. BRAINE, "Smart Contract Templates: foundations, design landscape and research directions", position paper, 2016, 2. Available at <https://arxiv.org/pdf/1608.00771v2.pdf>, last accessed 24 April 2018.

Correspondingly, these authors differentiate between ‘traditional’ and ‘non-traditional’ means of enforcing an agreement. The traditional method comes down to enforcement by a body of law that is backed by the power of a government.²⁶³ The non-traditional method depends on the use of tamper-proof blockchain technology. This type of enforcement is based on the assumption that it is possible to create a perfect computer language implementation of an agreement which entirely excludes the possibilities of wrong-performance and non-performance of the agreement.²⁶⁴

67. In effect, the computer science approach assumes that the computer code’s automation of a transaction between parties, when embedded in the solid framework of a DLT network, is equivalent to the legally binding agreement between these parties; because the factual consequences they lead to are, or are expected to be, the same. The law *sensu lato*, being the underlying legal agreement and the broader context of the legislation it exists under, become irrelevant. This ideal considers that programs uploaded to a DLT exclusively govern the arrangements between parties; therefore, it does not have to operate under the shadow of the law.²⁶⁵ Lawrence LESSIG’S famous quote “code is law” corresponds with this modern viewpoint.²⁶⁶

CHAPTER 3. SMART LEGAL CONTRACT – *law is law, and code is code*²⁶⁷

68. A different way to look at smart contracts is by acknowledging the difference between the legal, enforceable obligations on the one hand and the tool to wholly or partially operationalize these obligations on the other hand.²⁶⁸ Indeed, for the purposes of a legal analysis, we cannot consider the non-traditional method of smart contract enforcement consistent with the legal notion of enforcement because this is inevitably linked to

²⁶³ *Ibid.*, 4.

²⁶⁴ *Ibid.*, 4.

²⁶⁵ E. TJONG TJIN TAI, “Smart contracts en het recht”, *NJB* 2017, 92(3), 179.

²⁶⁶ L. LESSIG, *Code version 2.0*, New York, Basic Books, 2006, 5. Available at <http://codev2.cc/download+remix/Lessig-Codev2.pdf>, last accessed 3 February 2018.

²⁶⁷ G. JACCARD, “Smart Contracts and the Role of Law”, *Justletter IT* 2017, 23, 9.

²⁶⁸ ISDA and LINKLATERS, “Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective”, 2017, 4. Available at <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>, last accessed 24 April 2018.

obligations recognized by law, and, therefore based on a valid agreement.²⁶⁹ The tamper-proof computer code merely imitates the law and the law remains the only source of the binding legal nature of the agreement.²⁷⁰ Generally speaking, the core condition for the establishment of a legally enforceable contract is the expressed and valid consent by parties, the consensus on the contents of an agreement with a valid object and *causa* – to put it in Belgian civil law terms. While the smart contract is a very straightforward product of human coding activity, the contents of the actual agreement are only to be found in the meeting of the minds of the parties involved.

Nevertheless, it cannot be denied that once a protocol has been executed through the above-mentioned non-traditional method, it is indeed ‘enforced’ in some sense. For the lawyer, a so executed contract does not equal or guarantee a legally enforceable contract.²⁷¹ Absent the fulfillment of the constituent conditions underpinning a valid contract, the costs arising from the ultimate enforcement of a potentially wrongfully executed contract may surpass the normal enforcement costs – thereby nullifying the desired cost reduction benefit of the technology.

69. This approach resonates the most with legal professionals and practitioners since it detaches the computer protocol from the traditional contract that precedes and justifies the implementation of the computer code.²⁷² The readjusted concept that resulted from this viewpoint was first labeled a ‘smart legal contract’ by Josh STARK.²⁷³ By distinguishing between the code and the agreement it imitates, we have the opportunity to zoom in on the interaction – or lack thereof – between both separate concepts. The next paragraphs will briefly discuss this interplay between law and code in relation to the operational nature of the contractual clauses, the degree of automatability of the rights and obligations they contain, the ability for a court body to intervene and the internal or external positioning of

²⁶⁹ *Ibid.*, 6.

²⁷⁰ G. JACCARD, “Smart Contracts and the Role of Law”, *Justletter IT* 2017, 23, 9.

²⁷¹ M. RASKIN, “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 309.

²⁷² As also presented by K. VERSLYPE during his lecture “Bitcoin, Blockchain & Smart Contracts – Inleiding voor juristen”, Ghent, 26 October 2017.

²⁷³ J. STARK, “Making Sense of Blockchain Smart Contracts”, 2016. Available at <https://www.coindesk.com/making-sense-smart-contracts/>, last accessed 22 April 2018. On the notion of smart legal contracts, see also: G. JACCARD, “Smart Contracts and the Role of Law”, *Justletter IT* 2017, 23, 21-24; and, S. BLEMUS, “Law and Blockchain: a legal perspective on current regulatory trends worldwide”, *RTDF* 2017, 4, 13.

the code vis-à-vis the legal agreement, the ‘dumb’ contract.²⁷⁴ While the third disparity concerns the relationship between code and courts, the others appertain to the ties between code and traditional contract.

A. RELEVANT DISTINCTIONS

1. Operational vs. non-operational contract clauses

70. Not all clauses in a traditional legal contract are capable of being expressed in a language that can be readily executed by a computer. Operational clauses are mainly concerned with the actual execution of the contract – although certain remedies can also be expressed in operational terms – while non-operational or denotational terms are important for the legal interpretation of the entire agreement.²⁷⁵ The operational clauses are characterized by their straightforward conditional logic: if X, then Y; therefore, it is possible to translate these provisions into pure Boolean logic.^{276, 277} For instance, *if* (when) a bond reaches its maturity date, *then* the issuer repays the initial investment increased with payable interests. Non-operational clauses do not embody such logic, they determine the wider relationship between parties.²⁷⁸ For instance, a clause that determines the law applicable to the contract does not have a conditional structure. This does not exclude the possibility that an advanced computer would be able to read the structure and understand its semantics to produce the desired result. For instance, such computer could recognize a standard representation stating that parties are “duly organized and validly existing under the laws of the jurisdiction of its organization or incorporation”, and automatically consult the electronic

²⁷⁴ As conceptually different from the ‘smart’ contract – I have borrowed this alternative term for the traditional, legal agreement from C. LIM, T.J. SAW and C. SARGEANT, “Smart Contracts: Bridging the Gap Between Expectations and Reality”, blog, 2016. Available at <https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality>, last accessed 2 May 2018.

²⁷⁵ C. D. CLACK, V. A. BAKSHI and L. BRAINE, “Smart Contract Templates: foundations, design landscape and research directions”, position paper, 2016, 5. Available at <https://arxiv.org/pdf/1608.00771v2.pdf>, last accessed 24 April 2018.

²⁷⁶ For an interesting proposal for a machine-readable format of legal semantics creating obligations, permissions and rights; see: H. LAM, M. HASHIMI and B. SCOFIELD, “Enabling Reasoning with LegalRuleML” in J. J. ALFERES, L. BERTOSSI *et al.* (eds), *Rule Technologies: Research, Tools, and Applications: 10th International Symposium*, proceedings, 6-9 July 2016, 241-257.

²⁷⁷ ISDA and LINKLATERS, “Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective”, 2017, 11. Available at <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>, last accessed 24 April 2018.

²⁷⁸ *Ibid.*, 11.

registers in order to determine whether the agreement can indeed be executed.²⁷⁹ Additionally, there is a growing interest for the subject of creating a dedicated legal computer language that also captures such non-operational statements.²⁸⁰

A specific category of clauses with an absent or low degree of operational character are provisions that contain a certain subjectivity, which is per definition incompatible with computer language.²⁸¹ The conditional logic in such clause is rendered ineffectual because of the ambiguous way it is expressed. This is for instance the case with all obligations to carry out a task “in good faith”, to “produce reasonable efforts”, or to be “liable for foreseeable damages only”; which are all circumstances to be assessed through human judgment.^{282, 283}

71. In some instances, the triggering factor that determines the outcome of an operational or non-operational clause relies on data which is not capable of being readily built into the contract itself. This is notably the case for events or values that are to be discovered in the world outside of the contract code, like interest rates, stock market data or party decisions. The smart contract can interface with this real-world information through determinations provided by so-called ‘oracles’, which are preselected trusted sources of data that remain available to the contract code while it is executing.²⁸⁴ We will further differentiate between objective oracles, *i.e.* trusted sources of objective data; and, subjective oracles, which serve as a point of entry for some sort of human judgment into the smart contract.

²⁷⁹ *Ibid.*, 12.

²⁸⁰ C. D. CLACK, V. A. BAKSHI and L. BRAINE, “Smart Contract Templates: foundations, design landscape and research directions”, position paper, 2016, 11. Available at "<https://arxiv.org/pdf/1608.00771v2.pdf>, last accessed 24 April 2018.

²⁸¹ M. RASKIN, “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 325.

²⁸² Also labelled “complex evaluative rules” by E. TJONG TJIN TAI, “Formalizing contract law for smart contracts”, *Tilburg private law working paper series* 2017, 5. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038800, last accessed 8 April 2018.

²⁸³ Alternatively, in a far future (*cf.* the aforementioned Gartner Hype Cycle), by an artificial intelligence application of which the design is based on machine learning technology and big data, by processing a collection of human decision-making and experience of how to deal with various potential problems during the life of a contract. See S. HASSAN and P. DE FILIPPI, “The expansion of algorithmic governance: from Code is Law to Law is Code” *Field Actions Science Reports* 2017, 90; also mentioned by K. VERSLYPE during his lecture “Bitcoin, Blockchain & Smart Contracts – Inleiding voor juristen”, Ghent, 26 October 2017.

²⁸⁴ C. D. CLACK, V. A. BAKSHI and L. BRAINE, “Smart Contract Templates: foundations, design landscape and research directions”, position paper, 2016, 9. Available at "<https://arxiv.org/pdf/1608.00771v2.pdf>, last accessed 24 April 2018; and, ISDA and LINKLATERS, “Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective”, 2017, 18. Available at <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>, last accessed 24 April 2018.

2. Automatable vs. non-automatable contractual rights and obligations

72. In order to allow the smart legal contract to imitate the content of a traditional contract, it is essential that at least some contents of it, mainly the obligations incorporated therein, are automatable in one way or another. Automatization is understood in a way that the execution of the contents can be achieved by means of one or more computers, or by any electronic means in general.²⁸⁵ For instance, a contractual obligation for a person to personally carry out a task of a physical nature, like painting a wall, will not be automatable; it may however become automatable in a future of advanced robotics and Internet of Things. However, the majority of common obligations in a contract of a financial nature are indeed automatable by a computer since many are already initiated by computer systems. Examples are netting transactions between banks or bilateral clearing in DLT-based security trade lifecycle, as presented earlier in this research.²⁸⁶

Even though certain contractual provisions might be automatable, it can be undesirable to automatically trigger the contractually provided consequences for a given, contractually specified event – this is especially relevant regarding certain rights emerging from the contract. For instance, the contract may provide for early termination in the event of default by any of the parties. However, the choice to actually execute this early termination should remain at the discretion of the non-defaulting party, whose decision may well be influenced by commercial or other considerations external to the agreement.²⁸⁷

3. Strong vs. weak smart contract code

73. A further important distinction was presented by Max RASKIN. It expresses the degree of rigidity affiliated with the contract's relevant enforcement method. The perfect implementation of the above-mentioned non-traditional enforcement through integral dependence on blockchain technology is regarded a strong smart contract because such a configuration brings about prohibitive costs for a court of law or arbitration institute to alter

²⁸⁵ C. D. CLACK, V. A. BAKSHI and L. BRAINE, "Smart Contract Templates: foundations, design landscape and research directions", position paper, 2016, 3. Available at "<https://arxiv.org/pdf/1608.00771v2.pdf>, last accessed 24 April 2018; and, E. TJONG TJIN TAI, "Smart contracts en het recht", *NJB* 2017, 92(3), 179.

²⁸⁶ *Supra*, 59-62.

²⁸⁷ ISDA and LINKLATERS, "Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective", 2017, 17. Available at <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>, last accessed 24 April 2018.

the contract *post factuum*.^{288, 289} A smart contract setup which somehow allows for a court to influence the contract with relative ease and without incurring disproportional costs, after it has been initiated, is labeled a weak smart contract.²⁹⁰ One way of constructing such state is by establishing a subjective oracle of which the source has a certain degree of discriminatory decision power; or which specifically enables for human judgment by an external party.²⁹¹ Likewise, all agreements that contain obligations regarding some sort of alterable, non-computable behavior fall within this category, *i.e.* all non-automatable obligations.²⁹²

4. External vs. internal smart contract models

74. Lastly, the smart legal contract approach allows us to discern two arrangements with a different degree of interconnectedness between both code and contract, represented by two distinct implementation schemes. These schemes are named the external model and the internal model in a recent whitepaper by the ISDA and LINKLATERS.²⁹³ Whereas in the internal model, the smart part of the contract is part of the legal agreement; it is kept outside the scope of the legal agreement in the external setup.²⁹⁴ External smart contract code is hierarchically secondary to the legal contract terms.²⁹⁵

B. IN PRACTICE

75. In the following paragraphs, we will examine some important aspects of the external and internal variety of the smart contract with greater detail in the context of a hypothetical example. We will thereby dedicate special attention to the obstacles posed by non-

²⁸⁸ M. RASKIN, “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 310.

²⁸⁹ Note that a strong smart contract setup requires that the assets involved in the transaction are crypto-assets in order to exclude real-world interference.

²⁹⁰ *Ibid.*, 310.

²⁹¹ A. WRIGHT and P. DE FILIPPI, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia”, 2015, 50. Available at "https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

²⁹² M. RASKIN, “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 311.

²⁹³ ISDA and LINKLATERS, “Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective”, 2017, 14. Available at "<https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>, last accessed 24 April 2018.

²⁹⁴ *Ibid.*, 14.

²⁹⁵ S. BLEMUS, “Law and Blockchain: a legal perspective on current regulatory trends worldwide”, *RTDF* 2017, 4, 14.

operational and non-automatable elements in the legal contract; as well as by potential disputes or erroneous coding.

Imagine a consumer loan agreement for the purchase of a car. At the creditor's side of the agreement, core common obligations are providing the funds and assessing the client's financial situation and creditworthiness, as well as adequately informing and advising the client. The main obligations that bear on the borrower, on the other side, consist of repaying the funds in monthly instalments, providing accurate and honest information to the creditor and, usually, providing some sort of collateral. The next parts will operationalize this agreement in an external and an internal setup in order to identify the strength and potential problems in both scenarios.

1. External smart legal contract

a. Setup and use

76. Parties may agree in the legal agreement to partially enhance the performance of specific contract obligations by embedding them in a piece of computer code uploaded to a DLT platform, specifying that the code is subordinated to the terms of the primary contract. For instance, the external smart contract may automate the release of funds by the creditor to the lender, or to his car dealership; and it may also automate the monthly repayments by the debtor, linked to an appointed (crypto-) bank account. Such constellation does not add a lot of certainty for the creditor since similar contemporary systems already allow for such automation and because it is still the lender's responsibility to keep the connected account sufficiently pre-funded to answer to the recurring payment obligations.²⁹⁶ In the hypothesis of rapidly maturing first generation blockchain technologies, however; the smart contract code may be able to prompt performance from the lender's account in the 'golden' crypto-asset ledger, on which the external smart contract imposes some sort of restrictions regarding the lender's right of free disposal. Additionally, the external smart contract may govern the handling of the collateral or the right to withhold performance in the event of breach; for instance, by embedding a function for the execution of some sort of charge on the debtor's

²⁹⁶ The solution to block the funds in such account comes at a cost of liquidity loss. See E. TJONG TJIN TAI, "Smart contracts en het recht", *NJB* 2017, 92(3), 179.

car.²⁹⁷ Eric TJONG TJIN TAI has thought out a simple program architecture to operationalize such mechanism.²⁹⁸ Note that, in the external smart contract setup, the actual loan agreement undergoes little change compared to modern loan agreements – it exists in a human language document that stipulates all rights and obligations but that provides for partial and specific execution by way of smart contract, subordinated to the main legal contract.

77. An external smart contract arrangement helps the creditor to streamline its processes and to decrease potential losses caused by operational risks, human mistakes or administrative delays. Given the fact that the piece of smart contract code is uploaded to a DLT, both parties can trust that the automatization of their performances is administered in a highly secure and resilient manner; and that all individual coded obligations are carried out in a necessarily conjunct manner. Borrowers may benefit from reduced loan costs due to the increased certainty, clarity and efficiency in the lender’s processes.

b. Non-operational and non-automatable distortions

78. The legal loan agreement may contain non-operational elements because of the lack of Boolean logic (“This agreement is governed by the laws of Belgium.”) or because they give expression to a certain ambiguity (“The lender has used reasonable efforts to recommend a loan arrangement that adequately matches the borrower’s financial situation, objectives and demands.”). The external smart contract is supplementary to the main legal contract; hence, non-operational clauses can just be kept in the ‘dumb’ part of the contract and the designer of the external smart component must ensure that the code corresponds with these provisions. A similar assessment is to be made for non-automatable elements; they can simply be kept outside the scope of the smart contract and remain executed in the contemporary way. Consequentially, computer code is reserved for solidly automating straightforward and fully operational processes; and non-operational as well as non-automatable distortions cause little to no problems for external smart contract setups.

²⁹⁷ M. RASKIN, “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 329-333.

²⁹⁸ E. TJONG TJIN TAI, “Formalizing contract law for smart contracts”, *Tilburg private law working paper series* 2017, 7. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038800, last accessed 8 April 2018.

c. Smart bugs: disputes and unwanted output

79. A number of issues may arise throughout the duration of the agreement; parties may want to renegotiate the contract terms based on changes in circumstances, parties may become involved in a dispute regarding the external smart contract's execution or parties may simply find themselves confronted with a buggy computer program of which the output does not at all reflect the meeting of the minds behind the traditional contract. Given the external organization of the smart component, and thus its hierarchically secondary status vis-à-vis the main legal contract; the code must be alterable at all times after the smart contract's launch, to align it with the authentic contract terms. Hence, external smart contract code must, by definition, adopt the structure of a weak smart legal contract – there must be a way to change the blockchain in exceptional circumstances.²⁹⁹

80. Implementing a weak smart contract setup requires adequate care not to undermine the smart contract's security. There are various functions that can be pre-programmed into a smart contract to allow for later changes or for complete rescission by the rightful actor or actors: (1) the code can contain certain variables that are designated to be changed (*e.g.* the interest rate), (2) the code can provide for the disabling of certain functions in the smart contract, even after they were uploaded to the DLT; as well as for the addition of new ones, and (3) the smart contract can contain an auto-destruct function.³⁰⁰ Such functions must be wrapped in a conditional statement that only grants access when called by the rightful exerciser.³⁰¹ The rightful exerciser is recognized and identified by its address or public key on the DLT, which is only accessible by means of its unique private key.³⁰² Consequentially, firm security measures need to be taken to safeguard the private key of an actor who can rescind or alter the contents of the smart contract.

In order to make a smart contract qualify as weak, the tools mentioned above, and particularly the third tool, need to be accessible for a state-backed judicial body. Indeed, courts should be assigned some sort of oracle-like status in the weak smart contracts

²⁹⁹ P. PAECH, "The Governance of Blockchain Financial Networks", *Mod. L. Rev.* 2017, 1085.

³⁰⁰ B. MARINO and A. JUELS, "Setting Standards for Altering and Undoing Smart Contracts" in J. J. ALFERES, L. BERTOSSI *et al.* (eds), *Rule Technologies: Research, Tools, and Applications: 10th International Symposium*, proceedings, 6-9 July 2016, 158-164.

³⁰¹ *Ibid.*, 158-159.

³⁰² *Supra*, 12 on the subject of cryptographic key pairs.

concluded under their jurisdiction.³⁰³ Such mechanism requires that (1) every jurisdiction runs a node on the relevant smart contract platform(s), which is controlled by the jurisdiction's judicial body; and, (2) the external and thus necessarily weak smart contract incorporates data on the competent jurisdiction for any technical or juridical issues with the smart contract, as established in the traditional legal contract it relates to. The relevant jurisdiction may be directly appointed by the statement of this node's public key or address; or the smart contract may rely on a trusted third-party oracle to obtain this data from, allowing for a higher degree of flexibility.³⁰⁴

81. Lastly, parties may want to expand the 'weak' nature of their external smart contract by appointing more private key holders besides the judicial nodes to be the rightful exerciser of specific tools to alter or terminate the smart contract. Hence, parties can provide for conditional modification or termination rights (e.g. the borrower can execute an early termination upon the repayment of the outstanding funds and an automatically calculated reinvestment fee); or for a possibility to modify or to terminate the smart contract upon mutual agreement.³⁰⁵ Accordingly, the wrapping around the relevant functions can identify certain preconditions for its execution, as well as multiple public key holders or addresses who must act jointly to trigger the function.

2. Internal smart legal contract

a. Setup and relevance

82. The consequences of an internal setup are more extensive and so are the questions raised concerning the smart contract's governance. In the internal smart contract version of our loan agreement example, the computer protocol is agreed to constitute an integral

³⁰³ G. JACCARD, "Smart Contracts and the Role of Law", *Justletter IT* 2017, 23, 24.

³⁰⁴ Additionally, states may want to engage in specific conflict of law treaties to expand and align the principles of governing law and competent jurisdiction to smart contracts; and, to create a commitment to, if necessary, alter the smart contract on each other's behalf in the event the competent jurisdiction does not match the in the (smart) contract nominated jurisdiction.

³⁰⁵ B. MARINO and A. JUELS, "Setting Standards for Altering and Undoing Smart Contracts" in J. J. ALFERES, L. BERTOSSI *et al.* (eds), *Rule Technologies: Research, Tools, and Applications: 10th International Symposium*, proceedings, 6-9 July 2016, 153-154 and 156-157.

component of the legal contract.³⁰⁶ Maintaining a natural language version of the clauses transferred to the smart contract is irrational since code and contract language have the same legal value.³⁰⁷

The internal version of the smart consumer loan agreement would therefore almost entirely exist of computer code, including the precontractual steps – a particular application will standardize the mandatory exchange of information between client and creditor, and it will automatically produce correct advice and judgment on the appropriate loan contract terms; thereby minimizing future conflicts over the validity of the loan agreement.³⁰⁸

83. Clearly, an internal smart contract generates the benefits mentioned above, along with an even higher degree of certainty since the auto-execution is expanded to the entire legal contract. To the contrary, it also makes it more challenging to deal with the issues of non-operational and non-automatable elements, as well as with code deficiencies or potential disputes.

b. Non-operational and non-automatable distortions

i. *General non-operational clauses*

84. We believe that most non-operational clauses will not pose any problems in the long run. Some of these clauses could be artificially transformed into a more operational phrasing – it is not because a typical governing law clause is not construed in a conditional manner, that it does not comprise any conditional logic. Other general non-operational clauses, *e.g.* an entire agreement clause, could be recognized and given effect to through the use of advanced semantic analysis; or captured by custom-made computer language.³⁰⁹

³⁰⁶ ISDA and LINKLATERS, “Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective”, 2017, 14. Available at <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>, last accessed 24 April 2018.

³⁰⁷ *Ibid.*, 16.

³⁰⁸ M. RASKIN, “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 324.

³⁰⁹ *Supra*, 70.

ii. *Ambiguous clauses*

85. Absent any futuristic artificial intelligence and machine learning innovations, the solution suggested above is not workable when the non-operational character of a contract clause exists in a certain subjectivity, therefore requiring human assessment. Some authors accept this feature as one of the smart contract's main strengths.³¹⁰ Contracting parties are obliged to construct their legal relation in a precise manner and by doing so, they ensure the agreement's effective execution. The accurate literalism inherent to computer code eliminates the potential, frustrating incapability of vague human linguistics and it decreases the need for *ex post* assessment.³¹¹ Others however call attention to the utility of somewhat subjective contract language and the flexibility it allows for.³¹² Ambiguity may be desirable from a pragmatic point of view: the nuance may make it easier for both sides of a negotiation to agree and sign a contract.³¹³ Moreover, the idea that it is possible to entirely strip a legal relation of all its ambiguity may be utopic, especially in the context of more complex business dealings.³¹⁴ Contracting parties will have to decide to either insert or ban ambiguous language by making the cost-benefit analysis based on the complexity and economic importance of the agreement they are concluding.

Parties who wish to take advantage of such flexibility however will likely have to accept a weak smart contract configuration. Indeed, to allow for the subjective evaluation of the adequate fulfillment of contractual clauses or conditions, the smart contract will somehow have to embed an oracle which obtains data from human judgment.³¹⁵ As a subjective oracle ultimately relies on alterable human behavior, any smart contract that contains such oracle

³¹⁰ S. HASSAN and P. DE FILIPPI, "The expansion of algorithmic governance: from Code is Law to Law is Code" *Field Actions Science Reports* 2017, 89. Available at <https://ssrn.com/abstract=3117630>, last accessed 3 May 2018.

³¹¹ M. RASKIN, "The Law and Legality of Smart Contracts", *Geo. L. Tech. Rev.* 2017, 326; and, A. WRIGHT and P. DE FILIPPI, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015, 24-25. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017

³¹² P. PAECH, "The Governance of Blockchain Financial Networks", *Mod. L. Rev.* 2017, 1097.

³¹³ A. WRIGHT and P. DE FILIPPI, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015, 25. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017; and, ISDA and LINKLATERS, "Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective", 2017 13. Available at <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>, last accessed 24 April 2018.

³¹⁴ *Ibid.*, 13.

³¹⁵ E. TJONG TJIN TAI, "Formalizing contract law for smart contracts", *Tilburg private law working paper series* 2017, 5. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038800, last accessed 8 April 2018.

is of the weak variety – that is, if the appointed individuals behind the oracle are identified to the court.^{316, 317}

iii. *Non-automatable elements*

The distinction between internal and external smart contracts is irrelevant for the issue of non-automatable rights and obligations – actions that are not somehow initiated by a computer preclude the implementation in a true internal smart contract. This does however not constitute a real impediment for applications in the scope of this research, as computer-based transactions are ubiquitous in the financial sector.

c. Smart bugs: disputes and unwanted output

86. Internal smart contracts, once uploaded to a DLT platform and launched, make it much more difficult to deal with the potential issues throughout the duration of the contract. Absent any hierarchical relation to the traditional agreement, the parties to an internal smart contract have to abide with the output of the computer program and both the track of a weak or a strong constellation is theoretically possible.

i. *Strong internal smart contract*

87. Parties may consent to have their contractual relations governed by an internal smart contract without any kind of built-in recourse mechanism. There are however multiple disincentives for this approach. In the first place, it is conceptually difficult to harmonize the principles of an internal smart contract on the one hand with the representation of the parties' intentions on the other hand. Unlike the external configuration, there is no entire, legally existing or recognized agreement to fall back on to prove the meaning of the contract in natural language. Given the freedom of the form, the legal issue exists in the alleged consensus between parties and not in the mere use of computer code as a form.³¹⁸ Indeed, the opacity of computer language – as it exists today – raises doubts about the validity of

³¹⁶ Even if judicial bodies would not have direct access to an internal smart contract; a court could issue an injunction vis-à-vis the identified subjective oracle in the event of dispute. *Supra*, 71.

³¹⁷ M. RASKIN, "The Law and Legality of Smart Contracts", *Geo. L. Tech. Rev.* 2017, 311.

³¹⁸ G. JACCARD, "Smart Contracts and the Role of Law", *Justletter IT* 2017, 23, 22.

the parties' consent to the terms of a smart contract, and it increases the risk of erroneous consent.³¹⁹ Especially in more complex and long-term arrangements, it is highly uncertain whether a contracting party can foresee, conceive and indeed intend all consequences of the many possible chains of commands an internal smart contract consists of.^{320, 321} Consequentially, internal, strong smart contracts are conceptually very close to the computer science approach of “code is law”, therefore outside the scope of the law. The obligations expressed therein risk to be grounded only on computer code; while the only authentic source of enforceable legal obligations is society and its legal normativity.³²²

A creative solution to bring the internal, strong smart contract within the scope of the law nevertheless, is by regarding the computer code as a third party ruling which bindingly shapes the contractual relations between parties; thereby transforming potentially unconceivable contractual obligations into determinable obligations, based on objective standards. The difference is solely artificial in nature and since the ‘third party’, being the computer program, is in fact built by the contracting parties, it seems indefensible to consider it an independent entity.

Additionally, even if parties would verifiably grasp the substance of the code, and therefore it would be possible to fit a choice for a strong, internal setup into the concept of a smart legal contract; it still seems inadvisable to enter in such protocol for meaningful transactions. The combination of the still relatively immature technology and equally undeveloped legal framework produces a perfect climate for scams and unexpected, destructive loopholes.³²³ The choice for a strong, internal smart contract would therefore put all contractually bound accounts of crypto-assets at risk, without any recourse in order to reverse harmful results.³²⁴

³¹⁹ M. GIANCASPRO, “Is a ‘smart contract’ really a smart idea? Insights from a legal perspective”, *Computer Law & Security Review* 2017, 33, 831; and, E. TJONG TJIN TAI, “Smart contracts en het recht”, *NJB* 2017, 92(3), 181.

³²⁰ JACCARD compares the consent to launch such computer protocol to consent in the context of general terms in click-wrap agreements, of which the validity is equally doubtful. See G. JACCARD, “Smart Contracts and the Role of Law”, *Justletter IT* 2017, 23, 22.

³²¹ C. D. CLACK, V. A. BAKSHI and L. BRAINE, “Smart Contract Templates: foundations, design landscape and research directions”, position paper, 2016, 11. Available at <https://arxiv.org/pdf/1608.00771v2.pdf>, last accessed 24 April 2018.

³²² G. JACCARD, “Smart Contracts and the Role of Law”, *Justletter IT* 2017, 23, 9.

³²³ See for instance A. SAMSON, “SEC accuses crypto-bank of fraud, halts \$1bn initial coin offering”, *Financial Times*, 30 January 2018. Available at <https://www.ft.com/content/678a75dc-05cc-11e8-9650-9c0ad2d7c5b5>, last accessed 5 May 2018; and, the aforementioned hack of The DAO, *supra*, 16.

³²⁴ P. PAECH, “The Governance of Blockchain Financial Networks”, *Mod. L. Rev.* 2017, 1087.

ii. *Weak internal smart contract*

88. Parties who are concerned about safeguarding the continuous congruence between the authentic content and meaning of their agreement and the implementation in an internal smart contract, will likely wish to embed a tool that allows for judicial recourse by providing backstop functions to an individually nominated node.³²⁵ By doing so, parties benefit from the full certainty of execution offered by the DLT platform and they can rest assured that the object of their actual consent will prevail in the event of manifest fraud, clear technical defaults or proven illegalities. Note that judicial intervention will likely be limited to marginal review of the contract's legitimacy, given the freedom of contract and taken in consideration the fact that the competent authority will have to rely on only the obvious general principles of the internal smart contract to understand the parties' intentions.

Parties may also wish to equip the weak internal smart contract with the necessary tools to allow for modifications by mutual agreement, as described earlier.³²⁶

C. CONCLUSION

89. Based on all previous considerations, we can display the various possible smart legal contract configurations in the following schematic overview:

³²⁵ As explained earlier, *supra*, 79-80. Alternatively, parties may opt to allow for subjective remedies without resorting to a weak smart contract by creating some sort of *ad hoc* arbitration tool, which summons and incentivizes arbitrators from around the internet to assess the situation; however, this idea ultimately also relies on the perfection of the contract code and no such system has been successfully implemented so far. Nonetheless, it may be a pragmatic solution for a first instance review of non-urgent internal smart contract problems, supplementing and narrowing down the role of the state-backed judicial body, which would then serve as an appeal forum. See A. WRIGHT and P. DE FILIPPI, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015, 50. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017; and, I. KAMINSKA, "Decentralized courts and blockchains", *Financial Times*, 29 April 2016. Available at <https://ftalphaville.ft.com/2016/04/29/2160502/decentralised-courts-and-blockchains/>, last accessed 5 May 2018.

³²⁶ *Supra*, 81.

	Strong	Weak
Internal	<ul style="list-style-type: none"> - Potentially difficult to understand. - Questionable status as a smart legal contract; possibly unlawful. - Incapable of accommodating ambiguous and non-automatable elements. - High risks in the event of undesirable consequences. 	<ul style="list-style-type: none"> - Potentially difficult to understand. - High degree of total execution certainty. - Incapable of accommodating non-automatable elements; ambiguities may be assessed by a subjective oracle. - Backstop judicial recourse against manifest fraud, legally invalid contract formation or clear bugs.
External	<ul style="list-style-type: none"> - Logical fallacy. 	<ul style="list-style-type: none"> - Natural language document as basis. - High degree of flexibility regarding the automated execution. - Flexibility to provide for non-operational and non-automatable elements in the ('dumb') legal contract. - Broader judicial recourse against irregularities and against all non-conformities with the ('dumb') legal contract.

90. It is clear that the strong internal smart contract is conceptually the closest to the archetypical “code is law” philosophy of breach-resistant coded agreements between individuals, without any need for recourse to third parties. By building a scheme which is immune for third party interference, it is also in principle immune for the adequate application of the law. Such configuration entails considerable risks since many agreements inevitably need some sort of mechanism to correct mistakes that may arise during the life of a contract, including obvious matters such as erroneous consent, fraud other illegalities.³²⁷ The strong approach seems to overlook that it is precisely these issues that contract law has created solutions for, over centuries of aggregated knowledge and practical experience.³²⁸

³²⁷ *Supra*, 87.

³²⁸ E. TJONG TJIN TAI, “Formalizing contract law for smart contracts”, *Tilburg private law working paper series* 2017, 2 and 4. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038800, last accessed 8 April 2018.

Therefore, a strong internal smart contract can arguably be considered a smart legal contract; and, if transactions in crypto-assets become more widely adopted, it is possible that states want to protect their citizens against these contracts by resorting to drastic measures aimed at banning strong smart contracts; by pressurizing internet service providers, human-run online entities like search machines or DLT platforms, software developers and hardware manufacturers.³²⁹ The potential risk of course depends on the complexity and duration of the agreement, the (crypto-)expertise of the contracting parties and the quantity of crypto-asset funds potentially involved.

As mentioned earlier, strong external contracts cannot exist since the external arrangement necessitates the possibility to enforce the prevailing ‘dumb’ agreement and thus to influence the contract code. Hence, a strong external contract is a *contradictio in terminis*.³³⁰

91. The weak varieties, on the other hand, combine the unique characteristics of a DLT smart contract with the protection offered by the law; to a larger or lesser extent depending on the choice for an internal or external arrangement of the smart contract. Parties benefit from the resilient auto-execution and durability offered by blockchain technology, as long as it is consistent with the actual legal agreement they wish to automate and as long as it is not somehow legally invalid – indeed, the intention to also execute the contract outside of these circumstances would likely not constitute ‘acting in good faith’.

Whereas the code is fully scrutinized against the entire content of the ‘dumb’ contract in the external setup, the internal smart contract solely allows for judicial review of the validity of the contract formation and manifest technical defects – *i.e.*, could both parties have intended and foreseen the contract code to produce this output?

92. In conclusion, by launching an internal or external weak smart legal contract, parties agree to rely on the code in the first place and to shift any potential enforcement of the law to an *ex post* phase.³³¹ It is the pinnacle of freedom of contracting regarding the execution modality, but at the same time, it is insulated against situations where a traditional contract

³²⁹ A. WRIGHT and P. DE FILIPPI, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia”, 2015, 51-52 and 56. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

³³⁰ *Supra*, 79.

³³¹ M. RASKIN, “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 329.

would also be legally unenforceable. In the event of future mass adoption of crypto-assets and smart contract modalities, states may want to facilitate the *ex post* enforceability of existing contract law by adopting specific rules on the setup of a weak smart contract on the one hand and by providing template blocks of smart contract code on the other hand.

93. Jurisdictions may adopt a regulatory framework which guides the arrangement of an individual smart contract, depending on the contracting parties and on the nature and value of the smart contract at hand. For instance, a weak setup could be compulsory for a contract with a converted maximum value over €300 at its conclusion, or with a term surpassing one year. Additionally, consumer smart contracts could be restricted to an external arrangement to ascertain the understandability and informed consent by consumers. Such rules could be enforced through civil or even criminal liability provisions targeting identified contracting parties and software developers.³³²

Such laws would favorably be complemented by a state-backed and publicly available database of template computer protocols, compatible with the major DLT platform programming languages or in pseudocode form. These templates should specifically address the structure of the weak contract setup, including access for a designated node or nodes. It may also go further in promoting the relevance of contract law in smart legal contracts by formalizing pertinent legal provisions into code which is to be adopted in the smart contracts in an unaltered way.³³³ Direct connection to the database would also support automated updates with changes in the law.³³⁴

94. Based on these considerations, we conclude that the weak internal or external smart contract, when complemented by the necessary state-backed measures, is the only convincing configuration of a valid smart legal contract; which respects the source of legal

³³² A. WRIGHT and P. DE FILIPPI, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia”, 2015, 56. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

³³³ As suggested by Kristof VERLSYPE and firstly undertaken by TJONG TJIN TAI, with a template of pseudocode for withholding performance, see E. TJONG TJIN TAI, “Formalizing contract law for smart contracts”, *Tilburg private law working paper series*, 2017, 6-7. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038800, last accessed 8 April 2018.

³³⁴ M. RASKIN, “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 327.

obligations and the difference between law and code, and, at the same time, embraces and optimizes the efficiency and trust benefits promoted by the use of DLT.³³⁵

³³⁵ Partially concurring with the position taken by Kristof VERSLYPE; albeit that VERSLYPE only considers external smart legal contract setups during his lecture “Bitcoin, Blockchain & Smart Contracts – Inleiding voor juristen”, Ghent, 26 October 2017.

TITLE 5. CONCLUDING CONSIDERATIONS

95. After a deeper analysis of the various implementation schemes for financial DLT applications, we can establish that there are many ways for this new technology to reshape the contemporary financial landscape. The most nearby innovations appertain to how various financial assets are held and transacted with, including currencies; and to the relation between, or the consolidation of, traditional legal contracts and their smart, coded counterparts.

Disruption is a popularly used term in relation to the emergent blockchain technology, and it primarily refers to the highly decentralized applications that pursue the complete disintermediation of the targeted sector. However, it is now clear that the technology can become equally relevant in the context of the modernization of pre-existing infrastructures and legal concepts, through permissioned platform configurations and weak smart contract setups. This approach combines and reconciles existing trust, regulation and experience with the main unique capabilities of DLT applications. Indeed, regardless of the question whether a certain blockchain is highly decentralized and independent, or instead permissioned and administered to a certain degree; all innovations of this kind still materialize in a context where the society and its legal normativity prevail – especially in a densely regulated environment like the financial sector.³³⁶ Blockchain is and will remain a regulatable technology, by one way or another; if necessary, through the use of draconian measures on the edge of government control abuse.³³⁷ As Max RASKIN puts it, “It is a good rule of thumb that the entity with more guns wins”, and, “governments generally have more guns.”³³⁸

96. A more desirable scenario undoubtedly comprises supportive regulation that aims to maximally turn the implementation of DTL platforms to the advantage of the entire financial industry, and, by extension, society as a whole. To achieve this objective, regulatory adaptations specifically addressing this new technology will need to show up on the horizon in the near future. Many private DLT initiatives come on stage on a daily basis and some of

³³⁶ G. JACCARD, “Smart contracts and the Role of Law”, *Justletter IT* 2017, 23, 9.

³³⁷ A. WRIGHT and P. DE FILIPPI, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia”, 2015, 51-53. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

³³⁸ M. RASKIN, “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 328.

them are based on the false assumption of a legal vacuum. The proposed adjustments will be built on the present-day legal framework and need not to amount to a whole new domain of law.³³⁹

At the outset of this endeavor, policy makers worldwide, especially in dominant financial markets, should bear the following key points in mind. Supportive new DLT laws should ...

- ... appreciate the diversity of possible blockchain configurations and the consequential differences in their governance and in the suitable regulatory approach; and,
- ... provide for regular re-evaluations as this diversity is continuously growing, especially with the advent of consensus mechanisms that may drastically extend the blockchain's capacities; and,
- ... be pragmatic, strict and active where necessary, to deal with outright scams and manifestly irresponsible decentralized network platforms; and,³⁴⁰
- ... also recognize the importance of the protection of individuals with an information deficit (*e.g.* consumers), regarding the concrete differences between highly decentralized crypto-assets and their contemporary counterparts as well as in the context of strong internal smart contracts; and,
- ... be established on international cooperation and harmonized regulatory standards; and,³⁴¹
- ... leave a certain degree of freedom for ongoing technological creativity, possibly in a controlled environment to limit risk exposure, depending on the scale of the project.³⁴²

97. Undoubtedly, intriguing times are ahead of us as both the technology and the law mature together, until maybe, finally a point is reached where both are sufficiently developed and reliable for the financial sector and for society to abandon or drastically review the legacy systems and concepts. For the time being, however, whether and when this vision will materialize is an open question.

³³⁹ A new domain called the *Lex Cryptographia*, *supra*, 4.

³⁴⁰ *E.g.* by means of the more drastic measures mentioned *supra*, 90.

³⁴¹ With regard to supervision, authentication, applicable law and jurisdiction. See *supra*, 38; and P. PAECH, "The Governance of Blockchain Financial Networks", *Mod. L. Rev.* 2017, 1110.

³⁴² See for instance the regulatory sandbox approach, *supra*, 58.

BIBLIOGRAPHY

Legislation and legislative documents

European Union

Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories.

Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms.

Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse.

Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories.

Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings.

Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market.

Second Council Directive 89/646/EEC of 15 December 1989 on the coordination of laws, regulations and administrative provisions relating to the taking up and pursuit of the business of credit institutions.

Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems.

Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities.

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers.

Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms.

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

Conventions

Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary.

France

Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers. Available at <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036171908>, last accessed 1 May 2018.

Guidance papers and statements

ECB, “Virtual currency schemes”, report, 2012. Available at <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, last accessed 15 April 2018.

ECB, “Virtual currency schemes – a further analysis”, report, 2015. Available at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, last accessed 15 April 2018.

ESMA, “ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements”, statement, 13 November 2017. Available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf, last accessed 7 April 2018.

ESMA, “The distributed ledger technology applied to securities markets”, report, 2017. Available at https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf, last accessed 7 April 2018.

ESMA, “ESMA Assesses usefulness of distributed ledger technologies”, press release, 2 June 2016. Available at <https://www.esma.europa.eu/press-news/esma-news/esma-assesses-usefulness-distributed-ledger-technologies>, last accessed 9 April 2018.

MONETARY AUTHORITY OF SINGAPORE, “Fintech Regulatory Sandbox Guidelines”, 2016. Available at <http://www.mas.gov.sg/~media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines.pdf>, last accessed 20 April 2018.

MONETARY AUTHORITY OF SINGAPORE, “MAS clarifies regulatory position on the offer of digital tokens in Singapore”, press release, 1 August 2017. Available at <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx>, last accessed 16 April 2018.

Case law

ECJ 22 October 2015, *Skatteverket v David Hedqvist*, C-264/14, EU:C:2015:718.

Literature

Books and contributions

DRESCHER, D., *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, New York, Springer Science+Business Media, 2017.

HAUBEN, C., “Bitcoin en EU-recht: de virtuele vreemde eend in de bijt” in STORME, M.E. and HELSEN, F. (eds), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia, 2017.

LAM, H., HASHIMI, M. and SCOFIELD, B., “Enabling Reasoning with LegalRuleML” in ALFERES, J.J., BERTOSSI, L. *et al.* (eds), *Rule Technologies: Research, Tools, and Applications: 10th International Symposium*, proceedings, 6-9 July 2016.

LESSIG, L., *Code version 2.0*, New York, Basic Books, 2006. Available at <http://codev2.cc/download+remix/Lessig-Codev2.pdf>, last accessed 3 February 2018.

MARINO, B. and JUELS, A., “Setting Standards for Altering and Undoing Smart Contracts” in ALFERES, J.J., BERTOSSI, L. *et al.* (eds), *Rule Technologies: Research, Tools, and Applications: 10th International Symposium*, proceedings, 6-9 July 2016.

PETERS, G.W. and PANAYI, E., “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money” in TASCA, P, ASTE, T. *et al.* (eds), *Banking Beyond Banks and Money. New Economic Windows*, Cham, Springer, 2016.

PROCTOR, C., *Mann on the Legal aspects of money*, Oxford, Oxford University Press, 2012, 10.

VERHAERT, R., *Blockchain, de overheid aan of in de ketting?*, Brugge, Vanden Broele, 2016.

VERHELST, J.L., “Zijn cryptomunten munten? Een analyse van Bitcoin” in STORME, M.E. and HELSEN, F. (eds), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia, 2017.

Journals and online research papers

ATHANASSIOU, P., “Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks”, *ECB Legal Working Paper Series* 2017. Available at <https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf?344b9327fec917bd7a8fd70864a94f6e>, last accessed 15 April 2018.

ATHEY, S., PARASHKEVOV, I., SARUKKAI V. and J. XIA, “Bitcoin Pricing, Adoption, and Usage: Theory and Evidence”, working paper, 2016. Available at <https://www.gsb.stanford.edu/faculty-research/working-papers/bitcoin-pricing-adoption-usage-theory-evidence>, last accessed 14 April 2018.

BLEMUS, S., “Law and Blockchain: a legal perspective on current regulatory trends worldwide”, *RTDF* 2017, 4.

CAYTAS, J.D., “Developing Blockchain Real-Time Clearing and Settlement in the EU, U.S. and Globally”, *Columbia Journal of European Law: Preliminary Reference* 2016.

CLACK, C.D., BAKSHI, V.A. and BRAINE, L., “Smart Contract Templates: foundations, design landscape and research directions”, position paper, 2016. Available at <https://arxiv.org/pdf/1608.00771v2.pdf>, last accessed 24 April 2018.

CLAESSENS, S. and KODRES, L., “The Regulatory Responses to the Global Financial Crisis: Some Uncomfortable Questions”, *IMF Working Paper* 2014. Available at <https://www.imf.org/external/pubs/ft/wp/2014/wp1446.pdf>, last accessed 16 April 2018.

GIANCASPRO, M., “Is a ‘smart contract’ really a smart idea? Insights from a legal perspective”, *Computer Law & Security Review* 2017, 33, 825-835.

GIKAY, A.A., “Regulating decentralized cryptocurrencies under payment services law: lessons from European Union law”, *Journal of Law, Technology & the Internet* 2018, 9.

HACKER, P. and THOMALE, C., “Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law”, 2017. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, last accessed 12 February 2018.

HASSAN, S. and DE FILIPPI, P., “The expansion of algorithmic governance: from Code is Law to Law is Code” *Field Actions Science Reports* 2017.

JACCARD, G., “Smart Contracts and the Role of Law”, *Justletter IT* 2017, 23, 7.

JENSEN, M. and MECKLING, W., “Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure”, *Journal of Financial economics* 1976, 3(4), 305-360.

KARAINDROU, E., “Distributed ledger technology and the future of payment services”, 2017. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078523, last accessed 10 March 2018.

LEE, L., “New Kids on the Blockchain: How Bitcoin’s Technology Could Reinvent the Stock Market”, *Hastings Business Law Journal* 2016, 12(2), 81-132.

MANDENG, O. J., “Cryptocurrencies, monetary stability and regulation: Germany’s nineteenth century private banks of issue”, *LSE Institute of Global Affairs* 2018. Available at <http://www.lse.ac.uk/iga/assets/documents/research-and-publications/LSE-IGA-WP-5-2018-Ousmene-Mandeng.pdf>, last accessed 11 March 2018.

MICHELER E. and VON DER HEYDE, L., “Holding, clearing and settling securities through blockchain/distributed ledger technology: creating an efficient system by empowering investors”, *Journal of International Banking & Financial Law* 2016, 652-656.

MILLS, D., WANG, K. *et al.*, “Distributed ledger technology in payments, clearing, and settlement”, *Finance and Economics Discussion Series* 2016. Available at <https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf>, last accessed 17 April 2018.

MOONEY, C.W., “Beyond negotiability: a new model for transfer and pledge of interests in securities controlled by intermediaries”, *Cardozo L. Rev.* 1990, 12.

NABILOU, H. and PRÜM, A., “Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies”, 2018. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3121918, last accessed 11 April 2018.

PAECH, P., “Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?”, *Unif. L. Rev.* 2016, 21, 612-639.

PAECH, P., “The Governance of Blockchain Financial Networks”, *Mod. L. Rev.* 2017, 1073-1110.

RASKIN, M., “The Law and Legality of Smart Contracts”, *Geo. L. Tech. Rev.* 2017, 305-341.

SZABO, N., “Formalizing and Securing Relationships on Public Networks”, *First Monday* 1997.

THÉVENOZ, L., “Intermediated Securities, Legal Risk, and the International Harmonisation of Commercial Law”, *Stan. J.L. Bus. & Fin.* 2008, 3.

TJONG TJIN TAI, E., “Formalizing contract law for smart contracts”, *Tilburg private law working paper series* 2017. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038800, last accessed 8 April 2018.

TJONG TJIN TAI, E., “Smart contracts en het recht”, *NJB* 2017, 92(3), 176-183.

VAN DER ELST, C. and LAFARRE, A., “Blockchain and the 21st Century Annual General Meeting”, *European Company Law Journal* 2017, 4, 167-176.

WRIGHT, A. and DE FILIPPI, P., “Decentralized Blockchain Technology and the Rise of Lex Cryptographia”, 2015. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 7 March 2017.

YERMACK, D., “Is Bitcoin a real currency? An economic appraisal”, working paper, *National Bureau of Economic Research Working Paper Series* 2013. Available at <http://www.nber.org/papers/w19747>, last accessed 14 March 2018.

Whitepapers, blog articles and various electronic sources

DUTCHCHAIN, “The real value of bitcoin and crypto currency technology - The Blockchain explained”, video, 2014. Available at <https://www.youtube.com/watch?v=YIVAluSL9SU>, last accessed 6 March 2017.

FRIEDL, S., “An Illustrated Guide to Cryptographic Hashes”, 2005. Available at <http://www.unixwiz.net/techtips/iguide-crypto-hashes.html>, last accessed 15 April 2018.

HEARN, M., “Corda: A distributed ledger”, whitepaper, 2016. Available at https://docs.corda.net/_static/corda-technical-whitepaper.pdf, last accessed 5 May 2018.

ISDA and LINKLATERS, “Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective”, 2017. Available at <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>, last accessed 24 April 2018.

LANTMÄTERIET *et al.*, “The Land Registry in the blockchain – testbed”, report, 2017. Available at https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf, last accessed 9 April 2017.

LIM, C., SAW, T.J., and SARGEANT, C., “Smart Contracts: Bridging the Gap Between Expectations and Reality”, blog, 2016. Available at <https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality>, last accessed 2 May 2018.

NAKAMOTO, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. Available at <https://bitcoin.org/bitcoin.pdf>, last accessed 6 March 2017.

R3 LIMITED, “Writing a contract”, 2018. Available at <https://docs.corda.net/tutorial-contract.html>, last accessed 26 April 2018.

SANTANDER, INNOVENTURES *et al.*, “The Fintech 2.0 Paper: rebooting financial services”, 2016. Available at <http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf>, last accessed 17 April 2018.

SCHWARTZ, D., YOUNGS, N. and BRITTO, A., “The Ripple Protocol Consensus Algorithm”, *Ripple Labs Inc* 2014. Available at https://ripple.com/files/ripple_consensus_whitepaper.pdf, last accessed 15 April 2018.

STARK, J., “Making Sense of Blockchain Smart Contracts”, 2016. Available at <https://www.coindesk.com/making-sense-smart-contracts/>, last accessed 22 April 2018.

SWANSON, T., “Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems”, 2015. Available at <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>, last accessed 7 April 2018.

SWIFT, “gpi Nostro Proof of Concept”, interim report, 2017. Available at <https://www.swift.com/news-events/press-releases/swift-tests-show-blockchain-has-potential-for-global-liquidity-optimisation>, last accessed 15 April 2018.

SWIFT, “SWIFT on distributed ledger technologies”, position paper, 2016. Available at <https://www.swift.com/resource/swift-distributed-ledger-technologies>, last accessed 15 April 2018.

SZABO, N., “A Formal Language for Analyzing Contracts”, 2002. Available at <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/contractlanguage.html>, last accessed 24 April 2018.

SZABO, N., “Smart Contracts”, 1994. Available at <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>, last accessed 24 April 2018.

WESTPAC BANKING, “Blockchain Demystified”, video, 2016. Available at <https://youtu.be/LdOcXXB48fI>, last accessed 6 March 2017.

X., “Gartner Hype Cycle for Emerging Technologies”, 2017. Available at https://blogs.gartner.com/smarterwithgartner/files/2017/08/Emerging-Technology-Hype-Cycle-for-2017_Infographic_R6A.jpg, last accessed 20 February 2018.

Colloquia

MAIJOOR, S., “Regulatory measures to prevent another crisis”, transcript, 19 November 2014. Available at <https://www.esma.europa.eu/sites/default/files/library/2015/11/2014-1382.pdf>, last accessed 22 April 2018.

MARCKX, T., “Blockchain: disrupting markets & governments”, Ghent, 25 October 2017.
MUYLDERMANS, C., ZHANG, J. and WAUTERS, N., “Becon Blockchain Conference”, Brussels, 8 March 2017.

RICHELLE, J. and BERGER, P., “Studiedagen Instituut Financieel Recht: Fintech”, Brussels, 16 January 2018.

VERSLYPE, K., “Bitcoin, Blockchain & Smart Contracts – Inleiding voor juristen”, Ghent, 26 October 2017.

Newspaper articles

ARNOLD, M., “Five ways banks are using blockchain”, *Financial Times*, 16 October 2017. Available at <https://www.ft.com/content/615b3bd8-97a9-11e7-a652-cde3f882dd7b>, last accessed 20 April 2018.

CHAVEZ-DREYFUSS, G., “Sweden tests blockchain technology for registry”, *Reuters*, 16 June 2016. Available at <http://www.reuters.com/article/us-sweden-blockchain-idUSKCN0Z22KV>, last accessed 10 March 2017.

HERN, A., “Bitcoin mining consumes more electricity a year than Ireland”, *The Guardian*, 27 November 2017. Available at <https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland>, last accessed 8 March 2018.

JEMIMA, K., “Blockchain insiders tell us why we don’t need blockchain”, *Financial Times*, 2 May 2018. Available at <https://ftalphaville.ft.com/2018/05/02/1525253799000/Blockchain-insiders-tell-us-why-we-don-t-need-blockchain/>, last accessed 2 May 2018.

KAMINSKA, I. and MURPHY, P., “Bitcoin’s surge fuels fears of asset bubble”, *Financial Times*, 14 May 2017. Available at <https://www.ft.com/content/ce3ef54e-371b-11e7-bce4-9023f8c0fd2e>, last accessed 20 April 2018.

KAMINSKA, I., “Decentralized courts and blockchains”, *Financial Times*, 29 April 2016. Available at <https://ftalphaville.ft.com/2016/04/29/2160502/decentralised-courts-and-blockchains/>, last accessed 5 May 2018.

MURPHY, H. and STAFFORD, P., “Blockchain explainer: a revolution in its infancy”, *Financial Times*, 2 February 2018. Available at <https://www.ft.com/content/6c707162-ffb1-11e7-9650-9c0ad2d7c5b5>, last accessed 20 April 2018.

MURPHY, H. and THOMPSON, B., “Law firms look to capitalise on initial coin offering boom”, *Financial Times*, 26 March 2018. Available at <https://www.ft.com/content/2ae9154c-1d56-11e8-aaca-4574d7dabfb6>, last accessed 20 April 2018.

SAMSON, A., “SEC accuses crypto-bank of fraud, halts \$1bn initial coin offering”, *Financial Times*, 30 January 2018. Available at <https://www.ft.com/content/678a75dc-05cc-11e8-9650-9c0ad2d7c5b5>, last accessed 5 May 2018.

SKINNER, C., “Will the blockchain replace SWIFT?”, *American Banker*, 8 March 2016. Available at <https://www.americanbanker.com/opinion/will-the-blockchain-replace-swift>, last accessed 16 April 2018.

WEINLAND, D. and LUCAS, L., “Asian investors flock to initial coin offerings despite bans”, *Financial Times*, 14 November 2017. Available at <https://www.ft.com/content/05b2748c-c903-11e7-aa33-c63fdc9b8c6c>, last accessed 20 April 2018.