LIABILITY OF THE SMART CONTRACT DEVELOPER

A Comparative Analysis in the light of US and EU Law

by

Dimitrios Roumpos

Master Thesis

LL.M. International Business Law

Tilburg Law School

Supervision: Omololu Bajulaiye

Second reader: Dr. Jing Li

Tilburg, July 2020

Snr. 2040587

ACKNOWLEDGEMENTS

This thesis marks the end of my journey as a student in International Business Law (LL.M.) at Tilburg University. The path towards the completion of this paper has been challenging especially due to the outbreak of the COVID-19 pandemic. Fortunately, thanks to the help and support of special people, any obstacles were overcome, and the present thesis was successfully completed.

Firstly, I would like to express my sincere gratitude to my supervisor Omololu Bajulaiye for the guidance he provided me throughout this research and writing process. Further, I want to thank my lecturers, Prof. Dr. Erik Vermeulen, Prof. Dr. Joseph McCahery, and Prof. Dr. Christoph van der Elst who enabled me to see the Law differently and triggered my creativity. I am also grateful to the rest of the IBL members and teachers for their valuable tutoring and helpful advice.

Last but certainly not least, I want to thank my loved ones without whom this would not have been possible; my parents and siblings for having faith in me and Konstantina for her constant encouragement and unconditional support.

Dimitrios Roumpos

PREFACE

Abstract:

The widespread adoption of smart contracts in many types of transactions has created a plethora of legal concerns, including the attribution of liability. The usage of blockchain services in many cases involves a number of legal risks that can be distributed beyond the contractual parties to third parties, such as the authors of the smart contract code. The focus of this thesis is to highlight these possible risks and to discuss whether software developers are able to guarantee the security of the smart contract and manage the relevant operational and cyber-security risks. While smart contracts have the potential to disrupt the current legal and transactional status quo, notorious events such as attacks on Ethereum or Bitcoin platforms demonstrate the need to fill any gaps in relevant legislation. This thesis explores the nature and key features of blockchain-based smart contracts and examines whether and to what extent the code developer can be held liable to other network participants.

Keywords: *Blockchain, DLT, smart contracts, cyber-security, liability.*

TABLE OF CONTENTS

ACKNOWLEDGEMENTS ..... **iii**
PREFACE ..... **iv**
LIST OF ABBREVIATIONS & ACRONYMS ..... **vii**
INTRODUCTION **1**
1. Background 1
2. Literature Review 3
3. Purpose and Research Questions 5
4. Methodology Employed 6
5. Significance 6
6. Outline 7
CHAPTER 1: Smart Contracts **7**
1.1 Introduction 7
1.2 Blockchain Technology 8
1.3 Defining Smart Contracts 14
1.4 The Key Features 18
1.4.1 Conditional nature 18
1.4.2 Self-enforceability 19
1.4.3 Increased precision 19
1.4.4 Time-efficiency 20
1.5 How do Smart Contracts work? 21
1.6 Applicability of Smart Contracts: The E-commerce scenario 23
CHAPTER 2: **25**
The legal regime of smart contracts under the US & EU law **25**
2.1 Introduction 25
2.2 US state legislation on smart contracts 26
2.3 EU legislation on smart contracts 32
CHAPTER 3: Legal challenges surrounding smart contracts **35**
3.1 Introduction 35
3.2 Coding errors and security risks 36
3.3 Privacy issues and the right to be forgotten 39
3.4 Illegal activity 40

3.5 Other legal concerns 41
3.5.1 Contract Law 41
3.5.2 Consumer protection 42
3.5.3 Discrepancies between the parties' intent and the content of smart contracts 43
CHAPTER 4: 44
The distributed liability of smart contract developers 44
4.1 Introduction 44
4.2 The key role of the smart contract developer 45
4.3 Different liability types 45
a. Contractual liability 46
b. Non-contractual liability 47
4.4. Liability risks of the smart contract developer in major legal systems 49
4.4.1 The United States 49
4.4.2 The European Union 54
4.5 Mandatory insurance for smart contract development 57
CONCLUDING REMARKS 59
BIBLIOGRAPHY 62

LIST OF ABBREVIATIONS & ACRONYMS

DApps	Decentralized Applications
EBA	European Bank Authority
KYC	Know Your Customer
AML	Anti-Money Laundering
CFTC	Commodity Futures Trading Commission
SEC	Securities Exchange Commission
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technology
ISP	Internet Service Provider
TTP	Trust Third Parties
PoW	Proof of Work
PKI	Public Key Infrastructure
P2P	Peer-to-Peer
GDP	Gross Domestic Product
IoT	Internet of Things
EVM	Ethereum Virtual Machine
ESIGN Act	Electronic Signatures in Global and National Commerce Act
UETA	Uniform Electronic Transactions Act
AETA	Arizona Electronic Transactions Act
BBLLC	Blockchain-based Limited Liability Company
BTA	Blockchain Technology Act
NETA	Nevada Electronic Transactions Act
eIDAS	Identification, Authentication and Trust Services regulation
ETH	Ethers
GDPR	General Data Protection Regulation, (EU) 2016/679
CSCs	Criminal Smart Contracts
B2B	Business-to-Business
B2C	Business-to-Consumer

INTRODUCTION

1. Background

Imagine a venture capital fund operating through self-executing contracts, without managers, employees, or executives. This is the Decentralized Autonomous Organization, known as "The DAO." By buying digital tokens in the immutable and transparent DAO universe, investors from all over the world, aim to have voting rights on potential projects and enjoy returns if these plans make a profit. However, in June 2016, the most notorious cyber-attack had as a target the Ethereum DAO, a set of smart contracts running on Ethereum blockchain.[1] This DAO was funded via tokens, the "Ethers."[2] A hacker exploiting a vulnerability in the DAO stole about 3.6 million Ethers ($70 million) in a couple of hours. The attacker using a coding loophole of the blockchain platform managed to grow the Ethereum's block size by doing multiple transactions with zero value and got back lots of Ethers before the blockchain platform could update its balance.

The incident mentioned above is not the only bad precedent that raises doubts about the immutability of blockchain technology. Ethereum was attacked again in July 2017, when cyber-criminals who took advantage of technical mistakes in the Parity multi-signature wallets introduced a bug in the algorithms.[3] As a result, the hackers had access to three massive wallets and stole Ethers worth more than $31 million worth of Ether. Unfortunately, the history of cyber-attacks is not limited to these two heists, with more recent attacks in Ethereum, Bitcoin, and other blockchain platforms.[4]

---

[1] Samuel Falkon, *"The Story of the DAO - Its History and Consequences"* (Medium.com, 24 Dec 2017). Available at: <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee> accessed 28 Feb 2020.

[2] Ether currency has two functions, as a "gas" used to pay the cost of smart contract transactions and as a means of exchange, exactly like the Bitcoin.

[3] Haseeb Qureshi, *"A hacker stole $31M of Ether — how it happened, and what it means for Ethereum"* (freecodecamp.org/news/, 20 Jul 2017). Available at: <https://www.freecodecamp.org/news/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce/> accessed 28 Feb 2020.

[4] Jeff Hu, *"Learn Blockchain's Top 25 Hacks in History"*, (Hackernoon.com, 7 Feb 2019). Available at:

All these events teach the significance of establishing more secure smart contracts and raise once again the liability issues when something goes wrong. It is clear that the shielding of the blockchain-based platforms and smart contracts is primarily the responsibility of their designers. In fact, the potential liability of founders-developers must be examined carefully in case of attacks, malfunctions, or other illegal activities on the network. However, the number of participants, the anonymity, and the complex function of smart contracts make the distribution of liability difficult work. The nature of blockchain-based contracts can be an additional obstacle to allocate the risks and the legal responsibility in the event of compensation to the injured parties.

The concept behind the smart contract is to shift the need for trust. The parties don't need to really trust each other because the algorithms of the smart contracts are programmed to execute automatically exactly what has been agreed upon. Thus, these contracts contain the intention of the parties and are binding for this reason. But why do the parties enter into a "smart designed" contract? The nature and the main characteristics of smart contracts (disintermediation, decentralization, security, and immutability)[5] introduce a new era in legal theory and practice. A plethora of papers has been written explaining the challenges and the legal issues that the smart contracts present towards the interpretation, the applicable law, the dispute resolution, and of course, the risk allocation.[6]

Smart contracts are based on software architecture and -maybe-[7] this is the reason they are called "smart." However, in many cases, they cannot ensure a perfect performance free of errors and security risks, since the smart contract code may contain significant backdoors or technical flaws. The decentralized character of blockchain technology also makes it very difficult to control smart contracts in cases of unlawful activity. Thus, from their very nature,

---

<https://hackernoon.com/tech-explained-top-24-blockchain-hacks-in-history-first-half-40c390dc4a96> accessed 28 Feb 2020.

[5] Primavera De Filippi and Aaron Wright, Blockchain and the Law (HUP 2018) 33-57; Michèle Finck, Blockchain Regulation and Governance in Europe (CUP 2019) 10-33.

[6] Some of these academic articles and reports are mentioned in the next section.

[7] See notably Grimmelmann, James. *"All Smart Contracts Are Ambiguous."* Penn Journal of Law and Innovation (Forthcoming) (Oct. 2019). Available online at: <https://www.law.upenn.edu/live/files/9789-jli-volume-2> accessed 28 Feb 2020.

smart contracts are vulnerable to failures and mistakes, and for this reason, the need for new laws to address these liability issues effectively is as urgent as ever.

2. Literature Review

Firstly, Dr. Mik,[8] de Graaf,[9] Raskin[10] Maher, and Van Moorsel[11] focus on the definition, the main features, and the penetration of smart contracts in the real world. Already since the early 1990s, Szabo[12] had defined for the very first time the term of a smart contract as *"a computerized transaction protocol that executes the terms of a contract."*

Giancaspro (2017)[13] explains the blockchain and distributed ledger technology behind the smart contracts by demonstrating the principal advantages of using them. He also proceeds to outline the main legal issues derived from smart contracts and place possible conflicts with the traditional contract law of several jurisdictions, namely France and the US. The article analyses the liability and remedial issues in case of error or malfunction occurred by a third party. In the same way, Zetzsche, Ross, and Douglas (2018)[14] describe the main characteristics of the Distributed Ledger Technology (DLT) and analyses the risks associated with the use of DLT.

---

[8] Mik, Eliza. *"Smart contracts: terminology, technical limitations and real world complexity."* Law, Innovation and Technology 9.2 (2017): 269-300. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038406> accessed 28 Feb 2020.

[9] de Graaf, T. J. *"From old to new: From internet to smart contracts and from people to smart contracts."* Computer Law & Security Review 35.5 (2019): 105322. Available on ScienceDirect at: < https://www.sciencedirect.com/science/article/pii/S0267364919300147> accessed 28 Feb 2020.

[10] Raskin, Max. *"The law and legality of smart contracts."* (2016). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166> accessed 11 April 2020.

[11] Alharby, Maher, and Aad Van Moorsel. *"Blockchain-based smart contracts: A systematic mapping study."* (2017).
Available online at:
<https://www.researchgate.net/publication/319603816_Blockchain_Based_Smart_Contracts_A_Systematic_Mapping_Study> accessed 7 April 2020.

[12] Szabo Nick. "Smart contracts: building blocks for digital markets." (1996) Available online at: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 28 Feb 2020.

[13] Giancaspro, Mark. "Is a 'smart contract' really a smart idea? Insights from a legal perspective." *Computer law & security review* 33.6 (2017). Available on Researchgate.com at: <https://www.researchgate.net/publication/317354410_Is_a_'smart_contract'_really_a_smart_idea_Insights_from_a_legal_perspective> accessed 28 Feb 2020.

[14] Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner. *"The distributed liability of distributed ledgers: Legal risks of blockchain." U. Ill. L. Rev.* (2018). Available on SSRN at: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214> accessed 28 Feb 2020.

The authors focus on the potential liability of DTL participants in the event of a cyber-attack or an operational mistake.

The Report of The EU Blockchain Observatory and Forum (2019)[15] asses the legal challenges that the blockchain technology presents at the EU level. The decentralized blockchain-based platforms can be tough from a legal perspective. Legal problems such as who is responsible for the security and its smooth operation, or the governing law that is applicable in different cases, are underlined in the particular paper. The liability of the core software developers is also analyzed by the authors, who point out serious concerns for the process of the liability allocation. As an implication of the blockchain technology networks, smart contracts are becoming more and more popular. The authors canvass different types of smart legal contracts investigating the legal risks and threats that can be raised by their use. This thematic report emphasizes the need for a clearer and more effective regulatory framework for blockchain cases, and it concludes with several recommendations to EU lawmakers.

Further, Buonanno (2019)[16] analyses the civil liability of the decentralized platform operator under the EU law. The author explains why the decentralized nature of blockchain technology makes it extremely easy to be used for illegal activities. The paper also discusses the operational risks of using blockchain technology and how the EU legislation faces the liability distribution in case of damage caused to end-users.

On the other side of the Atlantic, Madir's paper (2018)[17] intends to explain whether the new and fast-evolving area of smart contracts fits under the existing laws of the US. The author refers to the efficiency and accuracy gains from smart contracts, but she explains that their immutable and unchangeable nature may raise serious questions about security and legal

---

[15] Tom Lyons, Ludovic Courcelas, Ken Timsit, "Legal and Regulatory Framework of Blockchains and Smart Contracts". The European Union Blockchain Observatory and Forum (2019). Available online at: < https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> accessed 28 Feb 2020.

[16] Buonanno, Luigi. *"Civil Liability in the Era of New Technology: The Influence of Blockchain*." *Bocconi Legal Studies Research Paper Forthcoming* (2019). Available online at: <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/YLA_Award/Submission_ELI_Young_Lawyers_Award_Luigi_Buonanno_ELI_2019.pdf> accessed 28 Feb 2020.

[17] Madir, Jelena. *"Smart Contracts:(How) Do They Fit Under Existing Legal Frameworks?."* (2018). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301463> accessed 28 Feb 2020.

responsibility. Focusing on liability issues, the article highlights the complex relationships between the participants to the smart contracts. From core software developers to end-users or to third parties that can be affected by the decentralized systems, the legal responsibility varies. The allocation of liability also depends on the type of loss or damage, its nature as contractual or non-contractual, and the existence or not of an error.

Finally, The Chamber of Digital Commerce (2018)[18] looks into the applicability and enforceability of smart contracts under the existing laws in the US and abroad. The main legal challenges in relation to the automated contracts are also analyzed in detail: the formation, the validity, the governing law, the judicial enforcement, and the potential scope of liability of self-executed contracts are examined in the context of common and civil law. Apart from the potential liabilities that derive from a contractual breach, the law should codify the cases of non-contractual liabilities. Further, the blockchain platform itself may raise additional liabilities, regarding data privacy, cyber-security, or operational flaws. Both common law and civil law systems taxonomize this kind of liability in the tort law for negligence, fraud, or breach of fiduciary duty.

3. Purpose and Research Questions

The purpose of this paper is to investigate the potential liability allocation of smart contract developers in the EU and US context. The study aims to outline the main legal responsibility issues that arise from blockchain-based platforms in case of an undesirable outcome. By examining the applicability of the existing EU and US regulatory framework to this fast-evolving technology, the author's objective is to answer the following central research question and propose relevant solutions:

"How and to what extent can smart contract code developers be held liable under the EU and US legislation?"

[18] Smart Contract Alliance, "Smart Contracts: Is the Law Ready?", Chambre of Digital Commerce (2018).

In order to find a comprehensive answer to this question, it is useful to analyze the following sub-questions:

- *"What is the nature and the main features of smart contracts and blockchain technology?"*
- *"Who are the participants to smart contracts, and what is the role of a software developer?"*
- *"To what extent are developers responsible for the weaknesses of codes to prevent illegal activities and unexpected events such as technical errors or cyber-attacks?"*
- *"How do the EU and US regulation address the smart contract coders liability?"*

4. Methodology Employed

The concept behind this research is to discuss the legal regime under which the smart contract developer can be found liable. By explaining smart contracts and the blockchain technology and comparing the EU and US legislation, the author aims to give the reader a more comprehensive view of the subject. The approach of the research questions is based on different types of legal sources, not only the letter of the law but also on doctrines, case law, and examples from everyday life. To this purpose, the author employs a comparative legal methodology in the light of the two major legal systems. More specifically, the main sources of the thesis are the EU and US legislation on smart contracts and developer's liability, academic books, scientific articles, thematic reports, online blogs, and websites.

5. Significance

The widespread adoption of smart contracts in many types of transactions, and especially in the online commerce industry, has raised a plethora of legal concerns between which and the attribution of liability. In fact, the usage of blockchain services in many cases involves a series of legal risks that may be distributed beyond the contractual parties to third parties, including the authors of the smart contract code. The contribution of this analysis is to highlight these possible risks and examine whether software developers are in a position to guarantee the security of the smart contract and manage the relevant operational and cyber-security risks. The notorious events such as the attacks on Ethereum or Bitcoin platforms demonstrate the

need to fill any gaps in the relevant legislation that could ensure full compensation to the injured parties and prevent any future damage or losses.

6. Outline

The thesis begins, in Chapter 1, by explaining the blockchain technology and describing the functions of smart contracts. It also explores the main industries in which the automated contracts are applicable and their main features. Chapter 2 looks at the existing US and EU regulatory framework related to blockchain-based smart contracts, and it examines whether it is required to introduce new laws that sufficiently address them. Chapter 3 discusses the legal issues that this type of contracting can raise in common and civil law. Some types of risks behind the use of smart contracts and the possible allocation of liabilities that may arise are further considered. Finally, in Chapter 4, the role of smart contract code developers and their interaction with the remaining involved parties is analyzed. Small mistakes or technical glitches in the code may result in big problems and make smart contract developers legally responsible to the end-users. The research also emphasizes the possible liability of developers in cases where their own codes are used for unlawful purposes. In conclusion, the need for a more effective legal framework that can address these emerging liability issues is underlined.

CHAPTER 1: Smart Contracts

1.1 Introduction

With the rise of the Internet, the vision of online transactions has come one step closer to reality. In the early 2000s, the World Wide Web allowed several businesses in the US and Western EU to provide their goods around the world. The suppliers were able to sell products and services over the Internet to customers with whom they did not have a pre-existing business relationship. The electronic contracts do not present significant differences from the traditional ones.

However, online contracting requires a special type of intermediary, such as the Internet Service Provider (ISP), in order to exist.

Over the years, the US and the EU legal systems tried to regulate the online transaction environment. This governmental intervention was a natural result as the open and unreliable nature of the Internet does not make it a perfect place for trading. Trust has always been requested. The increased online activity and the development of e-commerce lead central authorities to establish confidence between transactional parties. The laws of online electronic contracts aim primarily to regulate the information provided by the suppliers and protect the consumers.[19] Legislators placed a great emphasis on the intermediation of trusted third parties (TTP)[20] to safeguard the security of the transactions.[21]

Nowadays, the emergence of blockchain technology changes the picture and takes contracting to the next phase. In contrast to online contracts, smart contracts are not focused on the centralization, middlemen, and trusted third parties, but on algorithms and decentralization. They bring a "shift from trusting people to trusting math".[22] The new generation of Web 3.0, unlike the centralized nature of the Web 2.0 server, introduces through smart contracts the automatable execution without the involvement of a central control system.

1.2 Blockchain Technology

Before giving a brief definition of blockchains, it is useful to mention the common misconception between the Distributed Ledger Technology and Blockchain Technology. The two terms are not synonyms, as the blockchain represents only one form of the DTL. Although they may have a lot of similarities, such as the decentralized nature, the former does not require

---

[19] See articles 5 and 10 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

[20] The Certification Service Provider (CSP) is an example of the centralized trust mechanism of e-contracting. CSP as trusted third party (TTP) provides digital certificates to addressee to validate electronic signatures. See article 2 under 11 Electronic Signature Directive and article 3 under 19 eIDAS Regulation (with the term of "qualified Trust Service Provider" (TSP)

[21] de Graaf, T. J. *"From old to new: From internet to smart contracts and from people to smart contracts."* Computer Law & Security Review 35.5 (2019): 105322. Available on ScienceDirect at: < https://www.sciencedirect.com/science/article/pii/S0267364919300147> accessed 28 Feb 2020.

[22] Andreas Antonopoulos, "*Bitcoin security model: trust by computation"* (radar.oreilly.com, 20 Feb 2014) <http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html> accessed 12 April 2020.

a structure based on interconnected blocks of data. Here, blockchain is analyzed as the most popular type of DLT and the one that underlies smart contracts.

The birth of blockchain dates back to 1991 when Stuart Haber and W. Scott Stornetta[23], for the first time, explained a new technology of time-stamping data without the need for the traditional record-keeping procedure. However, it was only until 2008 that the blockchain idea implemented and become more popular by Satoshi Nakamoto's Bitcoin paper.[24]

Blockchain is a shared distributed database that keeps records of all the transactions occurred by the participants of the network. More technically, blockchain consists of sets of data packages (blocks) where a block stores digital pieces of information about multiple transactions.[25] The stored data inside the block depends on the sort of blockchain. A Bitcoin block, for instance, records data about the amount of transfer and the persons who send and receive the bitcoins. Each block except for the data on the stored transactions contains a cryptography hash, which identifies the block and all of its contents. Once the block is formed, its hash is calculated automatically by an algorithm function that turns data into a code of numbers and letters.[26]

Further, blocks have an additional component, the hash of the previous block ("parent"), which is to ensure the origin of the block and the integrity of the entire blockchain through to the first block ("genesis block").[27] Hash codes are just like fingerprints; that means that they are unique,

---

[23] Haber Stuart, and W. Scott Stornetta. *"How to time-stamp a digital document."* Conference on the Theory and Application of Cryptography. Springer, Berlin, Heidelberg, 1990.
[24] Nakamoto, Satoshi. *"Bitcoin: A peer-to-peer electronic cash system."* (2008). Available online at: <https://bitcoin.org/bitcoin.pdf> accessed 30 Feb 2020.
[25] See Fenwick Mark, Wulf A. Kaal, and Erik PM Vermeulen. *"Why'Blockchain'Will Disrupt Corporate Organizations."* Lex Research Topics in Corporate Law & Economics Working Paper 2018-3 (2018): 18-17. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3227933> accessed 30 Feb 2020. See also, Erik PM Vermeulen, "3 Reasons Why the Blockchain Revolution Is (Finally) Becoming a Reality!" (Medium.com, May 5, 2017). Available at: <https://medium.com/startup-grind/3-reasons-why-the-blockchain-revolutionis-finally-becoming-a-reality-63bdd90c89e2> accessed 30 Feb 2020.
[26] Isaac Simpson *"To Understand Blockchains, You Should Understand Cryptographic Hashes First - Bitcoin is first and foremost a child of cryptography*" (Medium.com, 19 Sep 2017). Available at: https://medium.com/vandal-press/to-understand-blockchains-you-should-understand-cryptographic-hashes-first-for-normies-93bc7645e816> accessed 10 June 2020.
[27] Nofer Michael, Peter Gomber, Oliver Hinz, and Dirk Schiereck. *"Blockchain."* Business & Information Systems Engineering 59, no. 3 (2017): 183-187. Available online at: <https://www.researchgate.net/publication/315462390_Blockchain> accessed 30 Feb 2020.

and if they change, the block is no longer the same.[28] Say that a hacker edits your transaction details from an e-commerce platform so that he charges you twice for the purchased product. With this modification in payment information, the block's hash will change as well, and the next block in the chain will remain with the old reference hash code and will become invalid because the chain will be broken. Consequently, these changes will make invalid the following blocks as well, and the attacker would need to update the new hashes to follow the blocks' tracks of the entire blockchain. The task of reforming all these hashes requires gigantic computing power, and so once a block is created, its stored data is very difficult to be changed or deleted.[29]

However, with the development of computing technologies, it is not impossible for a hacker to recalculate hundreds of thousands of hashes in some minutes. In order to maintain a secure place of transactions, blockchain aims to create a uniform common state – a consensus.[30] Before anyone tries to add new data to the blockchain, it is necessary to be accepted and validated by the remaining users. Validating the information is done through cryptography and the consent of the 50% + 1 of the participants to the blockchain. In this direction, the blockchain-based networks use the Proof-of-Work (PoW) mechanism to produce the needed decentralized consensus. PoW is a costly and consuming-time function that generates new blocks and, at the same time, a tool to confirm the data inserted in the network efficiently.[31] Through PoW, the creation of new blocks slows down -the bitcoin blockchain needs 10 minutes for each new block- making the tamper a challenging task for someone intending to change all the chained blocks. The PoW system is an extra measure that secures the integrity of blockchains and generates a consensus between the participants, who don't need to rely on a centralized authority but only on the provided technology.

---

[28] Kareem, Amer, R. B. Sulaiman, and M. U. Farooq. *"Algorithms and Security Concern in Blockchain Technology: A Brief Review."* (2018). Available on the Social Science Research Network (hereinafter reffered to as "SSRN") at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3227933 > accessed 30 Feb 2020.
[29] See Nathan Reiff, *"Blockchain Explained"* (invetstopedia.com, 1 Feb 2020). Available online at: <https://www.investopedia.com/terms/b/blockchain.asp> accessed 30 Feb 2020.
[30] Cong, Lin William, and Zhiguo He. *"Blockchain disruption and smart contracts."* The Review of Financial Studies 32.5 (2019): 1754-1797
[31] Andrew Tar, *"Proof-of-Work, Explained"* (cointelegraph.com, 17 Jan 2018) Available online at: <https://cointelegraph.com/explained/proof-of-work-explained> accessed 30 Feb 2020.

Another core component of blockchain technology is the authentication of users' identities. Identity authentication plays a pivotal role in preventing fraudulent transactions, where an attacker interacts in the name of someone else. By using the public key infrastructure (PKI), blockchains make it possible for parties to securely access the network and check the correctness of their digital signatures. More specifically, through public key infrastructure,[32] the participants obtain two keys, a public and private one, and it is only the latter that can decrypt the data that was encrypted by the public key and vice versa. The fact that a piece of information can be decrypted with a public key, automatically means that it came from a private key owner. This dual key mechanism also enables the creation of digital signatures, which establish that the transaction originates from a validated user and increases the accuracy of verification between the parties.

With the widespread of digital currencies, blockchain technology became an essential tool for preventing the risk of double-spending.[33] Bitcoins, Ethers, and other cryptocurrencies are now a hype because of the need for their players to invest in the secure and trustworthy place of blockchain systems. As explained above, the public distributed ledgers allow the participants to detect tampering and verify the content of the network. Blockchain is making use of a peer-to-peer (P2P) system, where users are free to join it and create new blocks. Once the information is verified and stored, it cannot be altered or deleted. It is so from its nature, blockchain, an immutable and safe environment for transactions that ensures a high degree of transparency between the transactional parties protecting at the same time their privacy via cryptography.

The absence of a central authority controlling the interaction between the peers makes blockchain networks ideal for direct transacting. In contrast to centralized systems, blockchain provides a high level of autonomy and a room of "doing businesses" without the need for

---

[32] Bacon, Jean, et al. *"Blockchain demystified."* Queen Mary School of Law Legal Studies Research Paper 268 (2017) p.8. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218> accessed 30 Feb 2020.

[33] The "double-spending" problem first emerged with online payments when digital currencies can be spent more than once. For more information about "double-spending" issue please see: Bisade Asolo, *"Double-Spending Explained"* (mycryptopedia.com December 21, 2018). Available at: https://www.mycryptopedia.com/double-spending-explained/ accessed on 7 April 2020.

middlemen and gatekeepers. A central bank is no longer needed in blockchain-supported money transfers, as the P2P technology empowers the owner to send digital assets whenever and to whoever he wants via his cryptographic key. The decentralized governance shifts the trust from banks, multinational companies, and governments and allow the peers to keep control of their own data and transactions. Blockchain introduces a faster, safer, and cheaper cross-border transactional technique and increases the efficiency gains in comparison to the traditional services, which are highly centralized and based on the involvement of intermediaries.

In this context, public ledgers may benefit their users, bringing massive changes in the way that they are used to make transactions. First of all, since blockchain technology does not need the intermediation of third parties for its function, it is able to eliminate the security risks associated with them. The common practice of third parties to collect and control personal data implies, in many cases, risks for privacy breaches.[34] Still, in P2P networks, they are only the users that manage their own personal information. Additional risks in transactions such as prolonged delays, bureaucratic inefficiency, political corruption, or excessive fees are good reasons for someone not to rely on a central governance or an intermediary. It is clear that blockchain promotes fairness and effectiveness in transactions, covering a big gap of uncertainty that often derives from the third trusted parties' involvement.

Among the benefits that distributed blockchain ledgers offer is that they are considered one of the best ways to protect stored data from cyber-attacks.[35] Since they do not have a central administrator (as they are distributed), blockchain ledgers are very difficult to be hacked. They are spread across multiple devices around the world, and it would be almost impossible for someone to interfere with all the computers of the network. The decentralized nature of blockchain also supports the authenticity and integrity of its content. Hundreds of thousands or millions of computers are connected in the same network to confirm the validity of the

[34] Zyskind, Guy, and Oz Nathan. *"Decentralizing privacy: Using blockchain to protect personal data."* 2015 IEEE Security and Privacy Workshops. IEEE, 2015.
[35] As a matter of fact, there is no blockchain platform that can be regarded as 100% attack-resistant, since the technology and the methods utilized by the cybercriminals are developing rapidly.

transaction recorded, ensuring that the data is correct, complete, time-stamped, and publicly viewable[36].

Speaking about blockchains is crucial to distinguish between the private (or permissioned) and the public (or permissionless), as it is only the latter that deemed as fully open and decentralized.[37] The most common examples to describe the public blockchains are Bitcoin and Ethereum,[38] where the access to the ledgers is entirely open to anyone who wants to use the network anonymously. Any user is free to make transactions, add and verify data only by hooking up his computer to the decentralized network and downloading a blockchain program. Conversely, in private blockchains, the access is controlled, and the participants can use it only after specific permission is granted. Most of the time, entities are responsible for permitting joining the network, something that makes this type of blockchain inherently more centralized. Companies and groups of companies, like financial institutions, are usually behind this type of blockchain.[39] Ripple and Hyperledger[40] constitute well known examples of the private blockchain network.

Although blockchains are widely associated with cryptocurrencies, especially with bitcoin, the possibilities of this technology go a lot further, and almost any industry related to transactions can use it. Blockchain is very quickly gaining ground and has found applications in a large scale of services[41] such as supply chain management, online payments, banking, or the

---

[36] According to prominent Bitcoin Core Developer Luke Dashjr, Bitcoin blockchain network has nearly 100,000 nodes see: David Canellis, *"Bitcoin has nearly 100,000 nodes, but over 50% run vulnerable code*". Available online at: < https://thenextweb.com/hardfork/2019/05/06/bitcoin-100000-nodes-vulnerable-cryptocurrency/> accessed 10 June 2020. See also the Bitcoin blockchain size in megabytes from 2010 to 2020. Available on Statistica.com at: < https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/> accessed 10 June 2020.

[37] Swanson, Tim. *"Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems."* Report (2015). Available online at: <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf> accessed 7 April 2020.

[38] For a comparison between Bitcoin and Ethereum platform See: Brown, Richard Gendal, et al. "Corda: an introduction." R3 CEV, August 1 (2016): 15.

[39] Four of the biggest banks in the world including UBS developed a private blockchain to facilitate payments and settle transactions. See more at: <https://www.reuters.com/article/us-banks-blockchain-ubs-idUSKCN10Z147> accessed 7 April 2020.

[40] See more: *"Understanding Public vs. Private Blockchain"* (selfkey.com, 4 Jan 2020). Available at: <https://selfkey.org/understanding-public-vs-private-blockchain/> accessed 7 April 2020.

[41] Lakhani Karim R., and M. Iansiti. *"The truth about blockchain."* Harvard Business Review 95 (2017): 118-127. Available online at: <https://hbr.org/2017/01/the-truth-about-blockchain> accessed 7 April 2020. The report explains the wide blockchain adoption especially by the financial services.

healthcare system. Any type of transaction can be recorded on the blockchain, from rental car agreements and exchanges of digital assets to music royalty payments and health insurance contracts. Not surprisingly, the World Economic Forum reported that by 2027, 10% of the global gross domestic product (GDP) will be stored in blockchain-supported technologies.[42]

Cryptocurrencies only represent the "first generation" of blockchains based on basic cryptographic technologies and P2P networks.[43] These types of ledgers, for example, like Bitcoin, have usually limited programming capabilities and are unable to execute complicated transactions and "build" demanding applications. On the other side, blockchains such as Ethereum have been considered as "the second generation" of blockchain, being able to support complex applications that go beyond the cryptocurrency transactions. Smart contracts, which will be analyzed below, are the ultimate paradigm of this new generation introducing a new era in contracting.

1.3 Defining Smart Contracts

There is no consensus on the definition of smart contracts, which is not surprising due to their new and disputable nature. The term "smart contract" was first introduced by cryptographer and computer scientist Nick Szabo in 1994. According to Szabo:[44]

> *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*

---

[42] Espinel, Victoria, et al. *"Survey report:"Deep shift: Technology tipping points and societal impact"."* World Economic Forum, September. 2015, p.24.
Available online at:<http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf> accessed 7 April 2020.

[43] Alharby, Maher, and Aad Van Moorsel. *"Blockchain-based smart contracts: A systematic mapping study."* (2017).
Available online at:
<https://www.researchgate.net/publication/319603816_Blockchain_Based_Smart_Contracts_A_Systematic_Mapping_Study> accessed 7 April 2020.

[44] Szabo Nick, *"Smart Contracts"* (1994). Available online at:
<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> accessed 4 April 2020.

enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.

With a newer report,[45] Szabo defines smart contracts as *"a set of promises, specified in digital form, including protocols within which the parties perform on these promises."*

One of the commonly used metaphors to explain smart contracts is vending machines.[46] Vending machines can be described as automatic machines that provide goods or services after the displayed price has paid in cash or by card. The idea behind the vending machine is pretty old. Indeed, the earliest known reference to it goes back to the first century AD of the Roman Empire years. The dispenser of holy water was a work of Greek engineer and mathematician Hero of Alexandria (also known as Heron). Heron presents the invention in his book "Pneumatika"[47] published in 62 AD. The vessel was usually positioned out of the temples, and it functioned as follows: when a coin of five drachmas inserted, then dispensed holy water for the faithful people. Pilgrims threw a coin, which falls from the tip of a sensitive lever. So it lifts the other end of the lever and opens the valve. The coin continued to push the lever until it fell from there into a piggy bank, and a little water ran to wash their hands and face. The lever then returns to its original position and closes the valve. So both the concept and the technology of automated machines are based on a model counting two thousand years old reminding us that "there is nothing new under the sun."

Nevertheless, the example of the vending machine to define smart contracts cannot efficiently demonstrate their capabilities and highlight the aspects of the technology behind them. The definition provided by Gideon Greenspan that a smart contract is *"a piece of code which is stored on a Blockchain, triggered by Blockchain transactions, and which reads and writes data*

---

[45] Szabo Nick, *"Smart contracts: building blocks for digital markets"* (1996). Available online at: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 28 Feb 2020.

[46] Szabo Nick, *"The idea of smart contracts."* (1997). Available online at: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html> accessed 7 April 2020.

[47] Hero of Alexandria, *"The Pneumatics"* translated from Greek and edited by Bennet Woodcroft, available online at: <https://web.archive.org/web/20101208040820/http://www.history.rochester.edu/steam/hero/index.html> accessed 7 April 2020. The mechanism of the "Sacrificial Vessel" is described by Heron in the Section 21 of the book.

in that blockchain's database"[48] seems to be more relevant, as it places emphasis on the technology of smart contracts. In fact, the concept of smart contracts was not very popular until the emergence of blockchain technology, which enables them.

Today, smart contracts are considered to be self-executable agreements that are converted into computer codes and stored on decentralized blockchain infrastructure. Their underlying technology guarantees that they cannot be altered or stop to exist and that neither party can change their programmed performance.[49] Hence, smart contracts are able to mitigate informational asymmetries[50] and create trust in so-called no-trust contracting environments.

The public distributed ledgers supporting the creation of smart contracts (like Ethereum) provide a great transacting environment. The huge computing capacity of these platforms allows the users to interact in a peer-to-peer network by using cryptocurrencies and preserving their anonymity. In these ecosystems, the execution of the contract relies on a tamper-proof consensus that facilitates and gives a safer character to the transactions. Their software structure also ensures the autonomy of their terms, which are capable of performing automatically when the predefined conditions are met.

The capabilities of smart contracts allow them to be used in many interesting situations. They can be used, for example, in the process of exchanging digital assets or to create a DAO community. For this reason, legal scholars divide smart contracts into two major categories: smart legal contracts and smart contracts with legal implications.[51]

Smart legal contracts constitute blockchain-based smart contracts that reflect the legal relationship between the contractual parties and, therefore, the legal issues that may arise from this agreement. In other words, a "smart legal contract" is synonymous with a formal legal

---

[48] Greenspan Gideon 'Beware of the Impossible Smart Contract' (Multicain.com, 12 April 2016) <https://www.multichain.com/blog/2016/04/beware-impossible-smart-contract/> accessed 4 April 2020.
[49] Mik, Eliza. *"Smart contracts: terminology, technical limitations and real world complexity."* (2017). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038406> accessed 7 April 2020.
[50] Cong Lin William, and Zhiguo He. *"Blockchain disruption and smart contracts."* The Review of Financial Studies 32.5 (2019): 1754-1797.Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764> accessed 7 April 2020.
[51] Notably see Tom Lyons, Ludovic Courcelas, Ken Timsit, *"Legal and Regulatory Framework of Blockchains and Smart Contracts"*. The European Union Blockchain Observatory and Forum (2019). Available online at: < https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> accessed 28 Feb 2020.

agreement, and according to Smart Contract Alliance is "capable of self-executing, on a legally-enforceable basis, the terms of an agreement between two or more parties."[52]

However, when it comes to the legal taxonomy of smart contracts, issues concerning the validity, legal formation, and enforceability of the legal contract may reveal. More specifically, under some legal systems, a contract must be on paper or not, or even be certified by a notary public. Greek law, for instance, in some cases accepts oral agreements, while real estate agreements must be in writing. At the same time, under Greek contract law, the use of notaries is also required when it comes to property transactions.[53]

Besides the formal requirements, legal contracts need to have some specific elements in order to be valid. Two or more parties are essential for a contract to be concluded, and, in most jurisdictions, legal agreements contain an offer, acceptance, an intention to be binding, and a consideration. In this context, the large body of the literature suggests that traditional principles of contract law may apply perfectly in the case of smart contracts.[54] It has also been stressed that smart contracts can revolutionize the corporate and commercial transactions and bring more clarity, predictability, and speed to agreements.[55]

On the other hand, some smart contracts may not simply reflect a legally binding agreement. These can be used for more than just the agreement between the parties and therefore be "smart contracts with legal implications." Smart contracts with legal implications are considered to be constructions based on blockchain technology. One of the most popular uses of smart contracts is for representing digital assets, such as cryptocurrencies, physical assets, or even intangible assets like IP rights. Another common use of smart contracts is the creation of a DAO. In this

---

[52] Smart Contract Alliance, *Smart Contracts: Is the Law Ready?*, Chamber of Digital Commerce (2018).
[53] See Art. 1033 Greek Civil Code
[54] Raskin, Max. *"The law and legality of smart contracts."* 1 Georgetown Law Technology Review 304 (2017) Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166> accessed 20 May.
[55] Josh Stark, *"How Close Are Smart Contracts to Impacting Real-World Law?"*, (Coindesk.com, Apr. 11, 2016). Available online at: <https://www.coindesk.com/snake-oil-and-overpriced-junk-why-blockchain-doesnt-fix-online-voting> accessed 26 June 2020.

case, smart contracts are interconnected and function as the primary source of governance for the DAO community.[56]

1.4 The Key Features

1.4.1 Conditional nature

Smart contracts are designed in a conditional way ("If X, then Y"). This means that they store their terms on decentralized networks, ensuring that if the "X" is met, then the "Y" will automatically be executed. In other words, a smart contract consists of a set of instructions that are placed on blockchain, and it contains predetermined rules. When these conditionals are satisfied, then the agreed clauses are executed by themselves. So now, computer protocols are in charge of verifying and enforce the contractual conditions which are programmed by the smart contract developer according to the parties' intention.

Thanks to the nature of smart contracts, the parties can ensure performance ex-ante by merely making "If-this,then-that" sentences. To illustrate, in a "smart" car rental agreement, *if* the specific amount of money is not received on time, *then* the vehicle cannot be started. In this context, it could be said that "the enforcement of the contract is nothing more than running of a circumstance through a conditional statement."[57] Conditional statements are fundamental to create smart contracts because the computer 0codes are based on this event-driven structure.

Sometimes, the use of an input (the so-called "Oracle") outside the blockchain is essential in order to be identified whether the conditions for the execution of a smart contract have been really met. Data, for instance, on flight delays, deaths that have been insured, or even the results of sports events for gambling can be easily determined and used as external sources for the distributed ledgers. The primary purpose of oracles is to provide information about off-chain events which can be relevant to execution or the efficient breach of the smart contract. Oracles feed smart contracts with external factual information serving as the bridge between the "deaf

---

[56] De Filippi, Primavera De Filippi. "*Blockchain and the law: The rule of code*." Harvard University Press, 2018. Available on

[57] Raskin, Max. *"The law and legality of smart contracts."* (2016). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166> accessed 11 April 2020.

and blind" decentralized network and "real world."[58] Behind these third-party sources could be authorized agencies, a trusted database, or Internet of Things (IoT) devices.[59]

1.4.2 Self-enforceability

Unlike the classic contracts where the performance depends on the parties' will, smart contracts can self-execute through the aid of computers not requiring any human intervention.[60] The Latin phrase "pacta sunt servanda[61]" cannot apply in the smart contract case. The agreement completion is no longer based on contractual promises, but on the programmed codes in which the agreed clauses are recorded. The obligations and the rights concerning the execution are already implemented in smart contracts, so there is no room for errors or willful breaches of contract.

Further, the self-enforcing character allows smart contracts to be autonomous. They have no need for enforcement agencies that may increase the litigation costs or the expenses associated with the involvement of intermediaries necessary for contract performance (e.g., financial institutions or insurance companies). Their functionality and capacity make smart contracts more cheap, fast, and more independent than the regular ones.

1.4.3 Increased precision

Due to the software architecture of smart contracts, their content is developed on a programming language that ensures an explicitly defined and detailed form. This accuracy provided by computer codes can minimize concerns related to the creation or the interpretation of the agreement by the involved parties. Errors or misunderstandings are almost out of the picture, because of the strictly defined terms of the deal. Smart contracts are considered stand-

---

[58] Stefan Thomas and Evan Schwartz, *"Smart Oracles: A Simple, Powerful Approach to Smart Contracts"* (19 July 2018) Available online at: <https://github.com/codius/codius-wiki/wiki/White-Paper#overview> accessed 10 April 2020.

[59] IoT devices are capable of connecting to other smart devices via the Internet and are remotely accessible to a user.

[60] A report of Clifford Chance, *"Are Smart Contracts Contracts?"*, December 2017. Available online at: <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2017/08/are-smart-contracts-contracts.pdf> accessed 7 April 2020.

[61] In English version: "The agreements must be kept".

alone and are not subject to external misjudgment since the code is defined as the sole arbiter of the agreement it represents.[62]

However, in many cases, the gap between the intent and the development of the contract may raise the risk of misconstruction. The different backgrounds between the person creating a smart contract and the one who uses it are capable of bringing undesirable outputs. It is also possible, as it discusses in the next sections, a smart contract to be subject to mistakes in drafting. This means that it is potentially vulnerable to flaws or outside threats like cyber-security attacks.

1.4.4 Time-efficiency

Ordinarily, when someone desires to make a contract, he needs to go to a lawyer, a broker, or a notary public and pay for their services. However, smart contract technology makes possible almost all the agreement stages -from drafting to execution- without the participation of traditional intermediaries. Both parties are able to manage the execution of their own agreement, which is easily viewable on the blockchain network. Thus, self-enforceable contracts can reduce the costs as well as the potential risk of fraud, error, or manipulation coming from the involved third parties.[63]

Making contracts may be a time-consuming process. Significant delays in completing agreements are due to the unnecessary steps[64] taken and the involvement of middlemen. The digital nature of smart contracts advantage them to the traditional ones because they are run online; there is no need for spending time on paperwork. The contribution of software codes allows smart contracts to facilitate transactions making them more fast and efficient. Smart contracts can be time-saving since their execution is automated. Many stages of a deal, from signing to the closing, take less or no time; because with smart contracts, financial transactions,

---

[62] Savelyev, Alexander. *"Contract law 2.0:'"Smart" contracts as the beginning of the end of classic contract law."* Information & Communications Technology Law 26.2 (2017): 116-134. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241> accessed 10 April 2020.

[63] Ameer Rosic, *"Smart Contracts: The Blockchain Technology That Will Replace Lawyers"* (blogeeks.com, 2017) Available at: <https://blockgeeks.com/guides/smart-contracts/> accessed 6 April 2020.

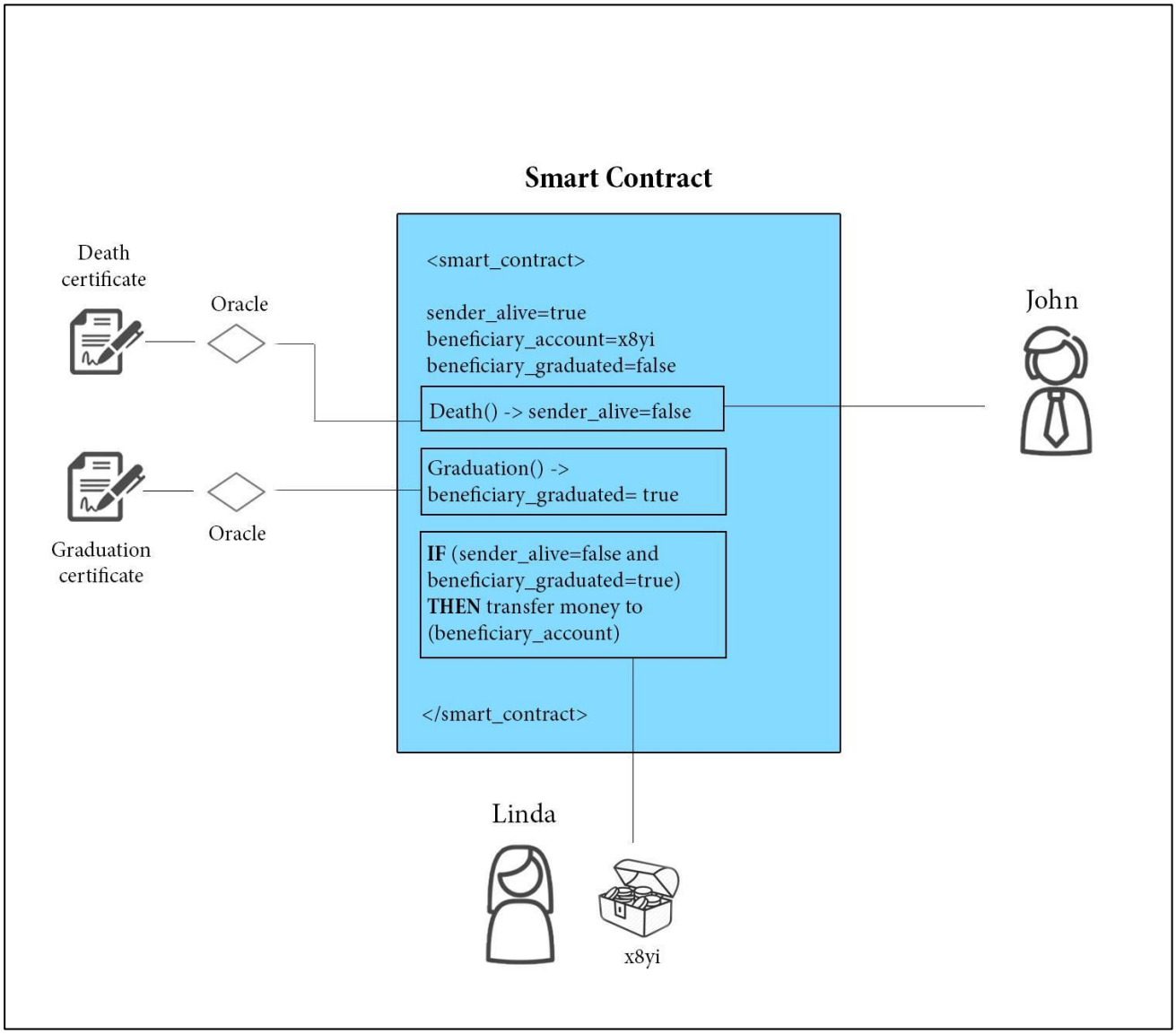
[64] A contract needs traditionally to go through a number of stages in order to complete. Due diligence, contract preparation, approval and filing could automate thanks to smart contract technology.

such as payments or settlements, can only be triggered if each party has fulfilled its obligations under the agreement.[65]

1.5 How do Smart Contracts work?

As previously mentioned, blockchain was initially adopted by financial services. However, the limited computing capabilities of Bitcoin do not address the need for developing contracts with more complex logic. Ethereum constitutes the first public blockchain platform that is able to support advanced self- enforceable contracts. Smart contracts are saved and organized within the Ethereum virtual machine (EVM), which enables the design of complicated sets of instructions executed specific tasks. This function is based on "IF-this-THEN-that" statements that can form contractual legal concepts and express the parties' intent.

[65] For more information on how smart contracts and blockchain technology can affect the M&A process, see the report of Clairfield International, *"The potential of blockchain and smart contracts in M&A"* (March 2019). Available online at: <http://www.clairfield.com/wp-content/uploads/Blockchain-and-Smart-Contracts-in-MA-2019.03.12.pdf> accessed 7 April 2020.



(Figure 1 – Example of a Smart Contract)

To make it more clear with an example: say that John, Linda's grandfather, wants to create a smart contract in order to code his last will (Figure 1). According to his will, John states that all the digital coins will be transferred to his beloved grandchild when he is no longer alive.

Further, John can define additional conditions, such as that the money can only be transferred after Linda graduates from high school.

Technically, smart contracts store variables, which are storages of digital information and their paired codes. Here, John formed his "smart" will by setting three stored variables as follows: 1. the "sender_alive," which shows whether John has passed away or not, 2. the "beneficiary_account," which represents the address of Linda's wallet and indicates where the money will be sent after the death of John and 3. the "beneficiary_graduated" indicating Linda's graduation.

Since smart contracts are not able to be fed from events outside the blockchain, so John's smart contract needs external data sources (oracles). In our case, John decided to rely on two oracles. The first aims to inspect the death records, and if it finds any certificate related to John's death, then it will activate the function of Death (). The second is about Linda's graduation. Once Linda graduates and the oracle finds the graduation certificate, it will trigger the Graduation () function.[66]

The above is a simple example of a smart contract that can be written. The capabilities of high-level programming languages go beyond the creation of a "smart" will and allow the development of more complicated smart contracts and decentralized applications (DApps).[67]

1.6 Applicability of Smart Contracts: The E-commerce scenario

Throughout the years, a number of possible smart contract applications have been introduced in various areas. All these proposals use blockchain technology to store different types of information and transactions: from notary public services (like the example of John's last will), money transfers and mortgage loans to real estate deals, employment contracts, and personal data management. E-commerce also constitutes a potential application of smart contracts.

---

[66]Valentina Gatteschi, Fabrizio Lamberti, and Claudio Demartini, Chapter 3: "Technology of Smart Contracts" *"The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms."* Vol. 1. Cambridge University Press, (2020), p. 43.

[67] DApps consider to be digital applications that run on a decentralised blockchain networks instead of a centralized server controlled by a single entity.

The open and unsafe nature of the Internet didn't manage to solve the perpetual problem of trading between untrusted parties.[68] Online platforms such as eBay and Amazon, providing the needed trust, creates secured but fully controlled transacting environments, and as a result, e-commerce became heavily mediated. On the other hand, blockchain replaces the need to trust third parties, even in environments that almost no-one can be trusted. The promise for disintermediation of online commerce lies at the ability of the blockchain technology to be trusted itself, without middlemen and central authorities.

For e-commerce, smart contracts can prove a high level of trust and transparency in transactions between sellers and buyers. These programmed retail agreements can only be executed when the two parties have fulfilled their obligations. The amounts paid by the shopper could be released to the merchant's wallet only if the latter has transferred ownership and shipped the product. Further, the immutable character of smart contracts prevents potential fraud and guarantees that the customers' personal data cannot be stolen or hacked.

In the decentralized online marketplace, users are able to manage their transactions and interact directly with each other.[69] As the blockchain removes intermediaries, trading becomes easier, faster, and more secure. Despite the existing payment services such as PayPal, which may charge high transactional fees,[70] smart contracts allow immediate payment by cryptocurrencies with low or even zero cost.[71]

Today more and more blockchain-powered platforms emerge in the online marketplace giving producers, sellers, and buyers the opportunity to transact directly. Origami Network[72] is an example of these peer-to-peer applications that support the execution of smart contracts in online commerce and promises an entirely decentralized online marketplace. Origami Network

---

[68] Blumenthal, Marjory S., and David D. Clark. *"Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world."* ACM Transactions on Internet Technology (TOIT) 1.1 (2001): 70-109.
[69] Tania H., *"Why Should You Consider Implementing Blockchain Technology in Your Marketplace?"* (rubygarage.org, 27 Jan 2020) Available at: <https://rubygarage.org/blog/how-blockchain-impacts-marketplace> accessed on 12 April 2020.
[70] PayPal currently charges a 2.9% + $0.30 per transaction within the US and 4.4% transaction fee for international sales. See more about the PayPal fees at: <https://www.paypal.com/us/webapps/mpp/paypal-fees>.
[71] The Ethereum transaction fees are significantly lower compared to the traditional payment systems of Visa, Mastercard and PayPal. According to BitInfoCharts (https://bitinfocharts.com/ethereum/) Ethereum have an average transaction fee of $0.79 USD and a median transaction fee of $0.27.
[72] See more online at: <https://ori.network/>.

attempts to solve the problems related to the e-commerce transactions such as the escrow payments and the review process. So it is based on three complementary platforms: Origami Marketplace, Origami Payment[73] powered by the Ethereum blockchain, and Origami Review[74] that guarantees a high level of trust with reliable and authenticated user's reviews. This open-source project provides a fully decentralized solution for businesses and consumers as well. It constitutes a new form of a marketplace that will possibly disrupt the traditional centralized e-commerce platform in the near future.[75]

CHAPTER 2:

The legal regime of smart contracts under the US & EU law

2.1 Introduction

As a matter of fact, an international legal regime specifically provided for blockchain networks, and smart contracts does not exist.[76] However, some legal systems, particularly at a state level, in the United States have already adopted regulations on blockchain technologies and applications, while others such as in the European Union are on the way to do so.

[73] See more online at: <https://payment.ori.network/>.
[74] Origami Review is connected to Oracles and ensures that the consumers reviews are validated. See more online at: <https://review.ori.network/>.
[75] See "*Disruption by Blockchain Part 4: Alexandre Duquenoy – Origami Network"* (disruptordaily.com, 15 Feb 2018) Available at: <https://www.disruptordaily.com/disruption-blockchain-part-4-alexandre-duquenoy-origami-network/> accessed 20 May 2020.
[76] Riccardo de Caria, *"A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities"*, United Nations Commission on International Trade Law (UNCITRAL) 7 (June 9, 2016), Available at: <http://www.uncitral.org/pdf/english/congress/Papers_for_Programme/5-DE_CARIA-A_Digital_Revolution_in_International_Trade.pdf> accessed 18 April 2020.

Outside the US and EU, the National Public Registry of Georgia[77] and Ukraine's e-Governance Agency[78] have been taking steps on supporting the use of smart contracts in real estate transactions and creating a decentralized Land Registry. Further, in 2017 Belarus became the first-ever country to legally recognize the "smart contract," defining it in the Decree of the President.[79]

Legislators lack sufficient understanding of blockchain infrastructure, and so they cannot take decisive steps towards smart contract legislation. Moreover, the speed with which this technology is evolving inevitably increases the inability of legal systems around the world to follow and regulate smart contracts. As it has been noted: "Today is all about blockchain brainstorming,"[80] and in this direction, the US and EU have created blockchain task forces, observatories, and fora to produce a comprehensive source of blockchain knowledge for lawmakers as well as the general public.

This chapter examines the current US and EU regulatory framework related to smart contracts. It also discusses whether it is required to introduce new laws that sufficiently address blockchain-based smart contracts.

2.2 US state legislation on smart contracts

In the United States, both lawmakers and courts have been flexible and receptive to accept electronic contracts.[81] The adoption of the Electronic Signatures in Global and National

---

[77] Laura Shin, *"The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project"* (Forbes.com, 7 Feb 2017). Available at: <https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#22a05c64dcdc> accessed 18 April 2020.

[78] Douglas Heaven, *"A house has been bought on the blockchain for the first time"* (newscientist.com, 11 Oct 2017). Available at: <https://www.newscientist.com/article/mg23631474-500-a-house-has-been-bought-on-the-blockchain-for-the-first-time/> accessed 18 April 2020.

[79] Iryna Chelyshava, *"Belarus' Cryptocurrency Experiment: Why the World Should Take Notice"* (Jurist.org, 12 Jan 2018). Available at: <https://www.jurist.org/commentary/2018/01/iryna-chelyshava-belarus-cryptocurrency/> accessed 18 April 2020.

[80] Matt Hancock Minister for Cabinet Office, Speech on *"Digital transformation in government and blockchain technology",* delivered at Digital Catapult, Kings Cross, London on 26 April 2016. Available at: <www.gov.uk/government/speeches/digital-transformation-in-government-and-blockchain-technology> accessed 22 April 2020.

[81] Dell'Erba Marco, *"Demystifying Technology. Do Smart Contracts Require a New Legal Framework? Regulatory Fragmentation, Self-Regulation, Public Regulation."* (2018) p.28. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228445> accessed 22 April 2020.

Commerce Act (ESIGN Act) and the Uniform Electronic Transactions Act (UETA) laid the foundations for the development of e-commerce regulation.

The ESIGN Act and UETA give quite broad definitions of the notions of electronic records and electronic signatures, supporting in this way the concept of blockchains and smart contracts. In both Acts, an electronic record means "a record created, generated, sent, communicated, received, or stored by electronic means."[82] An electronic signature may include any "electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[83] Further, under UETA, "a digital signature using public key encryption technology would qualify as an electronic signature."[84]

In addition, even though ESIGN Act is a federal statute, the states may individually "modify, limit, or supersede"[85] the Act, but only if such states have adopted the UETA or "alternative procedures or requirements."[86] UETA has been adopted by 47 states. Illinois, New York, and Washington have each adopted their own e-signature laws.[87]

Over the last few years, a multitude of states has amended their laws to be tailored to the emerging smart contract technology. In fact, many states in order to build a blockchain-friendly visage and to attract blockchain-based companies, are adopting specific legislation applicable to smart contracts.

In 2017, Arizona became the first state that attempted to provide specific regulation for blockchain, smart contracts, and electronic signature. Approving the "Blockchain Bill,"[88] Arizona amended its Electronic Transactions Act (AETA)[89] in order to address the emerging

---

[82] See UETA § 2(6) and 15 U.S. Code § 7006(4).
[83] See 15 U.S. Code § 7006(5)
[84] See UETA § 2(7)
[85] See 15 U.S. Code § 7002(a) – "Exemption to preemption".
[86] *Id.* § 7002(a)(2)(A)
[87] For Illinois State see the Electronic Commerce Security Act (5 Ill. Comp. Stat. 175/5-110New York), New York State adopted the Electronic Signatures and Records Act (N.Y. State Tech. 304) and for Washington State, see, Washington Revised Code 19-360.
[88] See Arizona Revised Stat. Ann. § 44-7061. *"Signatures and records secured through blockchain technology; smart contracts; ownership of information; definitions"*
[89] See <https://perma.cc/FHR8-JTD2> and the full text of law online at:

blockchain technology. The Act now introduces the key notions of blockchain and smart contracts[90] and recognizes that "smart contracts may exist in commerce" and that "may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term."[91]

Similar to Arizona, in Tennessee, its amended version of UETA, recognizes legal authority to use distributed ledger technology and smart contracts. The Law gives a complete definition of DLT[92] and adopts the blockchain technology description used by Arizona. The smart contract is also described in the statute as "an event-driven computer program that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions."[93]

In Vermont, Bill 205 passed into law in May 2018,[94] creating a special type of business entity: the "blockchain-based limited liability company" (BBLLC). A company which is organized "for the purpose of operating a business that utilizes blockchain technology for a material portion of its business activities"[95] may elect to be this new class of limited liability company. The law allows the BBLLCs to use the blockchain technology for all or some aspects of its corporate governance, including smart contract.[96]

The state of Illinois embraced smart contracts with a new legislation. In January 2020, the Illinois Blockchain Technology Act (BTA) went into effect, determining the legal status of smart contracts and blockchain technology. Illinois BTA is considered one of the most comprehensive laws on smart contracts, as it provides certainty on legal definition and several potential uses of the blockchain-powered contracts.[97]

< https://www.lawserver.com/law/state/arizona/az-laws/arizona_laws_title_44_chapter_26>

[90] *Id. ""Smart Contract" means an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger".*

[91] *Id.*

[92] See Tenn. Code Ann. § 47-10-201(1).

[93] *Id.* § 47-10-201(2).

[94] See Bill No. 205 VT S0269 | 2017-18 "An act relating to blockchain business development".

[95] See VT S0269 | 2017-18 § 4172.

[96] See VT S0269 | 2017-18 § 4173 (C).

[97] See Sections 5 and 10 of (205 ILCS 730/) Blockchain Technology Act.

Lastly, Nevada in 2017 and Ohio in 2018, amended their version of UETA defining the electronic record and blockchain. The Electronic Transactions Act of Nevada (NETA) states that blockchain means:[98]

> *an electronic record of transactions or other data which is: (a) uniformly ordered, (b) processed using a decentralized method by which one or more computers or machines verify the recorded transactions or other data, (c)redundantly maintained or processed by one or more computers or machines to guarantee the consistency or nonrepudiation of the recorded transactions or other data, and (d) validated by the use of cryptography.*

Further, with a newer amendment, the definition of blockchain also covers public blockchains.[99] However, smart contracts are not directly determined in the Act.[100]

Under Ohio amended version of UETA, "a record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record."[101] The statute also states that "a signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature" and that "a record or signature may not be denied legal effect or enforceability solely because […] the contract contains a smart contract term."[102]

In addition to the statutes above, other states are seeking to pass laws in order to recognize and regulate the use of smart contracts. More recently, a bill accepting the use of blockchain technology and smart contracts in commerce is pending before the New York legislature.[103] Several states are also establishing task forces or exploratory committees, as the first step in passing smart contract legislation. For example, California, Texas, New Jersey, and New York

---

[98] See Nevada Revised Stat. Ann. § 719.090, as amended by 2019 Nev. S.B. 162.
[99] See 2019 Nev. S.B. 162 that went into effect on October 1, 2019.
[100] See 2019 Nev. S.B. 163.
[101] See Ohio Revised Code Ann. § 1306.01(G)
[102] *Id.* § 1306.01(H)
[103] See Senate Bill S4142. Available at: <https://www.nysenate.gov/legislation/bills/2019/s4142> accessed 22 April 2020.

have already formed committees to explore possible applications of smart contracts and blockchain technologies.[104]

On the other hand, it has been argued[105] that there is no need for regulation at the state level because the existing federal frameworks for legal contracts can be a sufficient legal basis for smart contracts. According to the Chamber of Digital Commerce,[106] the US common law, namely the ESIGN Act and the UETA, can be applied in addition to the traditional commercial transactions, to transactions based on smart contract technology.

All in all, either with the state or the federal law, smart contract legal recognition continues to gain growth in a number of states in America. The rapid response of the US legal system to the DLTs and smart contracts may raise concerns as to whether the legislative attempts introduce problematic or deficient legal definitions and cause interpretational confusion.[107,108] However, this wide adoption of the technology in law could definitely boost automated transactions among different industries and open the door to the digitization of the economy.

---

[104] Christopher Adcock, *"An Update on State Smart Contract Legislation"* (The National Law Review, 15 April 2020) Available at: <https://www.natlawreview.com/article/update-state-smart-contract-legislation> accessed 18 April 2020.

[105] Aaron Stanley, in his article, *"Can Code Really Be Law? New Report Clarifies Smart Contract Misconceptions"* (Forbes.com, 27 Sep 2018) quoted lawyer Miren Aparicio's phrase: "The law is ready - we do not need specific legislation for the smart contracts by state law, under e-commerce laws". Available at: <https://www.forbes.com/sites/astanley/2018/09/27/can-code-really-be-law-new-report-clarifies-smart-contract-misconceptions/#4f6a955834e2> accessed 18 April 2020.

[106] Chamber of Digital Commerce, *""Smart Contracts" Legal Primer: Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable"* (January 2018). Available at: <https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf> accessed 22 April 2020.

[107] See Walch Angela, *"The path of the blockchain lexicon (and the law)."* Rev. Banking & Fin. L. 36 (2016): 713. Available on SSRN at: <https://ssrn.com/abstract=2940335> accessed 22 April 2020.

[108] See Cardozo Blockchain Project, *'Smart Contract and Legal enforceability'*, second Research Report (2018). Available at: <https://larc.cardozo.yu.edu/cgi/viewcontent.cgi?article=1001&context=blockchain-project-reports> accessed 22 April 2020.

Table 1 – US state legislation on smart contracts

Arizona	Ariz. Rev. Stat. Ann. § 44-7061	Allows the use of smart contracts in commerce and states that they may not be denied legal effect solely because they contain a smart contract term. It also recognizes electronic records and signatures secured through blockchain as valid.
Tennessee	Tenn. Code Ann. § 47-10-201(1) and (2)	The use of smart contracts and the DLT is legally recognized. The statute also defines the DLT and adopts the blockchain technology description used by Arizona.
Vermont	Bill No. 205 VT S0269 | 2017-18 § 4172-3 (C) Passed on 30 May 2018	The "blockchain-based limited liability company" (BBLLC) is introduced as a special type of business. These BBLLCs can utilize blockchain technology for a material portion of their business activities and corporate governance. The law allows the BBLLCs to use smart contracts.
Illinois	Sections 5 and 10 of (205 ILCS 730/) Blockchain Technology Act	Relates to allowing blockchain-powered smart contracts and provides several potential uses of them.
Nevada	Nev. Rev. Stat. Ann. § 719.090, as amended by 2019 Nev. SB 162	Gives a complete definition of electronic records and blockchains. But there is no express reference to smart contracts.
Ohio	Ohio Rev. Code Ann. § 1306.01(A), (G) and (H)	The law defines the electronic record and signature secured through blockchain and states that they may not be denied legal effect. It also determines the DLT and the public and private blockchains.
New York	Senate Bill S4142 Still pending	Recognizes the electronic signatures, records, and contracts secured through blockchain technology and allows smart contracts to exist in commerce.

2.3 EU legislation on smart contracts

In comparison to the United States, the smart contract legislation trend is not observed in the remaining jurisdictions around the world. The lack of specific regulatory frameworks related to smart contracts is mainly due to the complexity of the underlying technologies and the inability of legislative systems to understand and follow the fast-evolving blockchain area. The European Union is an example of a jurisdiction that closely monitors the rapid developments in smart contracts but proceeds cautiously into their legislation.

Under the electronic Identification, Authentication, and Trust Services regulation (eIDAS) electronic documents cannot be denied legal force solely because they have a digital form.[109] This means that data contained in these e-documents, including smart contracts running on the blockchain, can also produce legal effects. Further, the E-Commerce Directive[110] provides that the Member States are required to allow the conclusion of contracts by electronic means, in both Business-to-Business and Business-to-Consumer transactions, supporting the potential for legal standing for smart contracts.

Even though almost all Member States do not expressly determine the legal status of smart contracts, they recognize the principle of freedom of contract, which in many cases, allows the use of electronically executed contracts. The digital nature of smart contracts does not constitute a severe problem, as most jurisdictions let the parties free to choose the form of their agreement. Given these, it can be stressed that smart contracts can usually be caught by national legislation regarding electronic contracts.[111]

---

[109] Article 46 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[110] Article 9 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

[111] European Commission Study on Blockchains - Legal, governance and interoperability aspects (SMART 2018/0038), Feb 2020. Available at: <https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038> accessed 22 April 2020.

The French Civil Code explicitly recognizes the possibility of entering into a contract by electronic means.[112] Especially in B2B transactions, the law does not put any restrictions on the use of electronic means to conclude a contract. French contract law, therefore, supports the formation of smart contracts and allows the parties to express their intent by using electronic means, such as cryptographic keys. Dealing with the digital signature, France has adopted the concept of e-signatures issued with asymmetric cryptography two decades ago[113], which facilitates the smart contracts' use.

In Spain, the Electronic Commerce Law 34/2002 (article 23) provides that the parties are not required to enter into a prior agreement to use electronic means. It also establishes that the legally required written form of the contract can also be fulfilled electronically.[114] Similarly, the German Civil Code provides the digital conclusion of an agreement with the use of a qualified electronic signature.[115]

As noted, in many cases, the current domestic laws governing electronic contracts and e-signatures can cover smart contracts as well. However, over the last few years, the EU made significant steps to "legalize" blockchain-powered smart contracts.

In 2018, the Renewable Energy Directive defining the "peer-to-peer trading" mechanism indirectly recognized the smart contract technology. Under Article 2(18) the P2P trading of renewable energy is

> *the sale of renewable energy between market participants by means of a contract with pre-determined conditions governing the automated execution and settlement of the transaction, either directly between market participants or indirectly through a certified third-party market participant, such as an*

---

[112] Articles 1125 – 1127-4 and 1174-1177 of the French Civil Code as amended by Article 2 of Ordinance No. 2016-131 of February 10, 2016. Available in French at: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032004939&categorieLien=id> accessed 22 April 2020.

[113] Campbell Dennis, *"E-Commerce: Law and Jurisdiction: Comparative Law Yearbook of International Business-Special".* No. 2002. Kluwer Law International BV, 2003. p.210.

[114] Law 34/2002 of 11 July, Services Of The Society Of Information And Electronic Commerce, as amended by Law No. 7/2010. Available in English at: <https://www.global-regulation.com/translation/spain/1450967/law-34-2002%252c-of-11-july%252c-services-of-the-society-of-information-and-electronic-commerce.html> accessed 22 April 2020.

[115] Article 126a of the German Civil Code (BGB). Available in English at: <https://www.gesetze-im-internet.de/englisch_bgb/> accessed 22 April 2020.

> *aggregator. The right to conduct peer-to-peer trading shall be without prejudice to the rights and obligations of the parties involved as final customers, producers, suppliers or aggregators.*[116]

Recently, Malta recognized smart contracts as

> *a form of innovative technology arrangement consisting of: (a) a computer protocol; and, or (b) an agreement concluded wholly or partly in an electronic form, which is automatable and enforceable by execution of computer code, although some parts may require human input and control and which may be also enforceable by ordinary legal methods or by a mixture of both.*[117]

With the Law no. 12/2019 Italy affirmed the legal validity of DTL and smart contracts. More specifically, the statute introduces smart contracts as "computer programs that operate on distributed registers-based technologies and whose execution automatically binds two or more parties according to the effects predefined by said parties." It also states that this type of contract can satisfy the legal requirement of the written form.[118]

Table 2 – EU legislation on smart contracts

France	Art.1125 – 1127-4 and 1174-1177 of the French Civil Code	Recognizes the possibility of concluding contracts by electronic means such as cryptographic keys. The use of digital signature issued with asymmetric cryptography is also established under the French contract law.
Spain	Art. 23 of Electronic Commerce Law 34/2002	The use of smart contracts and the DLT is legally recognized. The statute also defines the DLT and adopts the blockchain technology description used by Arizona.

[116] Article 2(18) of Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources.
[117] Malta Digital Innovation Authority Act of 2018, Part I § 2(1). Available at: <https://parlament.mt/media/95199/act-xxxi-malta-digital-innovation-authority-act.pdf> accessed 22 April 2020.
[118] European Commission Study on Blockchains - Legal, governance and interoperability aspects (SMART 2018/0038) p.68, Feb 2020. Available at: <https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038> accessed 22 April 2020.

Germany	Art. 126a of the German Civil Code (BGB)	Allows the conclusion of contracts with the aid of digital means such as the use of a qualified electronic signature.
Malta	Malta Digital Innovation Authority Act of 2018, Part I § 2(1)	Directly defines and addresses smart contracts as a computer protocol, or agreement concluded wholly or partly in digital form and executed automatically.
Italy	Law no. 12/2019	Recognizes DTL and smart contracts and address them as valid and legally binding contracts.

CHAPTER 3: Legal challenges surrounding smart contracts

3.1 Introduction

As discussed in the first chapter, the use of smart contracts can deliver numerous benefits to commercial transactions. The possibility of contractual breaches and human errors or the risk of non-performance is greatly reduced by utilizing smart contracts. However, this novel type of contracting may introduce significant challenges for participants and raise legal questions on potential liability allocations.

Smart contracts are considered problematic for a list of reasons. A large body of literature[119] highlights concerns, such as cyber-security, privacy, and criminal activity related to smart contracts. In addition, it is observed that due to the fact that smart contracts are written in a

[119] For instance, see: Savelyev, Alexander. *"Contract law 2.0: 'Smart Contracts as the beginning of the end of classic contract law."* Information & Communications Technology Law 26.2 (2017): 116-134, and O'Shields, Reggie. *"Smart contracts: Legal agreements for the Blockchain."* NC Banking Inst. 21 (2017): 177.

programming language,[120] many of them are technically vulnerable to malfunctions, programming errors, or other cyber risks.[121]

This chapter looks at the main drawbacks of smart contracts and how these can affect commercial transactions. It is particularly focused on the efficiency losses that blockchain-based contracts may present regarding their enforceability, security, and legality. The technical or legal problems associated with smart contracts are closely intertwined with their key features discussed in previous sections.

3.2 Coding errors and security risks

One of the major issues surrounding smart contracts is the possible operational flaws contained in the contract. Unlike traditional contracts, smart contracts are formed and run in a computer-driven world, so they are exposed to technical mistakes that cause malfunctions and deficiencies in their operation. Particularly, due to their architecture, they represent technical issues similar to the software. According to the experts, the software is always prone to computing errors ("bugs") that may adversely affect its performance or make it vulnerable towards potential cyber-attacks.[122]

Smart contracts, however, present an additional difficulty because their execution is automated by computer protocols, and they cannot be modified or stopped. While the immutable element of smart contracts ensures the efficiency and the speed of transactions, it has the problem that once something is written into them and after they have been deployed, it cannot be altered or deleted. So, any flaws in the code remain permanent too. In such a case, the self-enforcing agreements are in danger of being executed incorrectly not because of a partial breach but due to technical glitches.

---

[120] Ethereum smart contracts are usually written in programming language "Solidity" <https://solidity.readthedocs.io/en/v0.6.7/>.
[121] Atzei Nicola, Massimo Bartoletti, and Tiziana Cimoli. *"A survey of attacks on ethereum smart contracts (sok)."* International conference on principles of security and trust. Springer, Berlin, Heidelberg, 2017.
[122] Walch Angela. *"The bitcoin blockchain as financial market infrastructure: A consideration of operational risk."* NYUJ Legis. & Pub. Pol'y 18 (2015): 837. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579482> accessed 1 May 2020.

Further, the vulnerabilities in the code may leave an open window for attacks or malicious manipulation of the smart contracts' content. Recent incidents, especially form the financial sector, such as the cyber-attacks of "Mt. Gox" and "Bitstamp" Bitcoin exchanges,[123] show that smart contracts can be hacked and prove that cyber-security is an additional issue facing blockchain-based contracts.

The attack to Ethereum DAO in 2016, is maybe the most famous case, where the cyber-criminals exploited critical bugs in code and stole 3.6 million ETH - nearly $70 million at the time - from the common fund. The computing error allowed malicious users to increase the block's size with numerous zero-valued transactions and gain Ethers because of the inability of the system to update the balances.[124] The solution came finally from the DAO's developers who decided to split ("fork") the Ethereum community and create a completely new version of DAO with the bugs fixed. As a result, there were two Ethereum DAOs: the "Ethereum Classic" with the stolen money and the "Ethereum" running on the forked code.[125]

The existence of loopholes in smart contract technology is not rare. The same is true for incidents where their integrity is at stake, as has already happened several times. The paper of Morshed et al. shows that between 2011 and 2019, 65 cyber-security incidents took place, having a total impact of more than $3 billion.[126] Among the cases, hacking frauds outmatch

---

[123] The hack of Mt. Gox, a Japanese Bitcoin exchange from 2011 to 2014. The attack relied on a hot-wallet bug, resulted in losses equivalent to $620 million and led the company to bankruptcy. Emerging Technology from the arXivarchive page, *The Troubling Holes in Mt. Gox's Account of How It Lost $600 Million in Bitcoins*, (Apr. 4, 2014), Available online at: <https://www.technologyreview.com/2014/04/04/173475/the-troubling-holes-in-mtgoxs-account-of-how-it-lost-600-million-in-bitcoins/> accessed 15 June 2020. See also the hack of one of the biggest Bitcoin exchanges, the Bitstamp, in 2015 with a total loss of 19,000 Bitcoins ($5.1 million). Stan Higgins, *Details of $5 Million Bitstamp Hack Revealed* (coindesk.com, 1 Jul 2015). Available at: < https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange> accessed 15 June 2020.

[124] Samuel Falkon, *"The Story of the DAO - Its History and Consequences"* (Medium.com, 24 Dec. 2017) <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee> accessed 1 May 2020.

[125] For a critical analysis of Ethereum Classic (ETC) and Ethereum (ETH), see Alex Moskov, "*Ethereum Classic vs Ethereum (ETC vs ETH): What's the Difference?".* (coincentral.com, 20 March 2020). Available at: <https://coincentral.com/ethereum-classic-vs-ethereum/> accessed 1 May 2020.

[126] Morshed Mohammad Jabed, and Paul A. Watters. *"An Empirical Analysis of Blockchain Cybersecurity Incidents." (2019).* Available online at: <https://www.researchgate.net/profile/Alex_Ng14/publication/337647279_An_empirical_analysis_of_blockchain_cybersecurity_incidents/links/5e087691a6fdcc2837460279/An-empirical-analysis-of-blockchain-cybersecurity-incidents.pdf> accessed 13 May 2020.

with 48 known attacks and a total loss of $1.6 billion, while Ethereum smart contract coding flaws number 7 cases with a total amount loss of $289 million.

Smart contracts usually contain coding errors and backdoors that make them vulnerable to cyber-attacks and unauthorized access to data. A recent report stated that one in twenty smart contracts running on the Ethereum blockchain network is vulnerable to be hacked,[127] while another concluded that a quarter of all smart contracts audited contain some kind of coding error.[128] Considering that these figures only refer to bugs contained in the contract by mistake, cyber-security is becoming perhaps the most discussed aspect of blockchain-based contracts.

Technical mistakes in smart contracts may be introduced in a plethora of ways, such as the developer's incapacity to understand the complex programming language and properly create secured algorithms; the inaction, negligence, or haste of the coder; and other reasons why the software products may be found defective.

Either with more or less vulnerable smart contracts, their failure is becoming more significant as the value committed to them grows. Looking at the numbers, in February 2020, assets locked up in smart contracts reached $1 billion, increasing worth from $700 million in December 2019.[129] In fact, the rapidly evolving dynamics of smart contracts enable them to gain considerable strength in the modern economy. But only if the probability of technical mistakes affecting their operation is eliminated, is it possible that smart contracts guarantee a flawless self-performance.

---

[127] Nikolić Ivica, Aashish Kolluri, Ilya Sergey, Prateek Saxena, and Aquinas Hobor. *"Finding the greedy, prodigal, and suicidal contracts at scale."* In Proceedings of the 34th Annual Computer Security Applications Conference, pp. 653-663. (2018). Available at: <https://arxiv.org/pdf/1802.06038.pdf> accessed 26 April 2020.
[128] Kai Sedgwick, *"25% of All Smart Contracts Contain Critical Bugs"* (Bitcoin.com, 29 Aug 2018). Available at: <https://news.bitcoin.com/25-of-all-smart-contracts-contain-critical-bugs/> accessed 26 April 2020.
[129] Brady Dale, *"Why DeFi's Billion-Dollar Milestone Matters"* (Coindesk.com, 7 Feb 2020). Available at: <https://www.coindesk.com/why-defis-billion-dollar-milestone-matters> accessed 26 April 2020.

3.3 Privacy issues and the right to be forgotten

Although the cryptography preserves the anonymity (more accurately, pseudonymity) of the users, it has been claimed that the technology underlying smart contracts may not be compatible with EU and US privacy laws.[130]

As mentioned above, in permissionless blockchains, the transactions and the balances of the peers are publicly visible. This practically means that every participant in the network may have access to the stored data. Consequently, this unlimited transactional transparency in P2P platforms may minimize the use of smart contracts as many of the users consider the data of financial and commercial transactions confidential. Privacy concerns may also arise when smart contracts need data feeds.[131] The contract sending a special request to the party that provides the external information makes its identity available to the public.

Further, with regard to the personal data stored in smart contracts, there is a contradiction between an individual's right to be forgotten (Article 17 of the GDPR) and the immutable character of the DTL. While personal data, like the user's name or address, may be cryptographically "sealed", it has been stressed that such encryption can only ensure pseudonymity and not fully anonymity.[132] According to this view, the pseudonymized personal data will continue to be subject to the GDPR. Having said that, a solution that excludes the data containing personal details outside the ledger could not address the problem sufficiently, as it comes with drawbacks of possible tampering of the off-ledger database.

---

[130] For more about data and privacy issues of blockchain technology at EU level, see: Salmon, John, and Gordon Myers. *"Blockchain and associated legal issues for emerging markets."* (2019). Available at: <http://documents.vsemirnyjbank.org/curated/ru/658041547845804080/pdf/133877-EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf> accessed 29 April 2020.
at US level, see: Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). *"Hawk: The blockchain model of cryptography and privacy-preserving smart contracts".* In 2016 IEEE symposium on security and privacy (SP) (pp. 839-858). IEEE.

[131] See Zhang Fan, et al. *"Town crier: An authenticated data feed for smart contracts."* Proceedings of the 2016 aCM sIGSAC conference on computer and communications security. 2016.

[132] Clifford Chance and European Bank for Reconstruction and Development, "*Smart Contracts – Legal Framework and Proposed Guidelines for Lawmakers"* (September 2018) p.47. Available online at: <www.ebrd.com/documents/pdf-smart-contracts-legal-framework-and-proposed-guidelines-for-lawmakers.pdf> accessed 13 May 2020.

3.4 Illegal activity

The pseudonymity and the absence of trusted third parties ensured by DLT may create room for criminal activity implemented through smart contracts. The rise of cryptocurrencies, in recent years, has attracted cyber-criminals to use blockchain-powered contracts as a means for illegal purposes. Money laundering, private key thefts, illicit transactions, or other physical world crimes can be facilitated by the conclusion of criminal smart contracts (CSCs).

Silk Road was a notorious paradigm of an ungovernable black market. In this online marketplace powered by bitcoin, the users were able to buy and sell illegal products and services, namely drugs, weapons, child pornography, and others. Similar to the legitimate online platforms, Silk Road allowed the shopper to rate the supplier and enabled the conclusion of criminal smart contracts between the parties.[133] In October 2013, Silk Road came to a bitter end when the Federal Bureau of Investigation (FBI) shut down the illegal marketplace and arrested its founder.

The report of Juels et al. emphasizes on three possible types of crimes in ecosystems that use smart contracts; the illegal sale of confidential documents, the theft of cryptographic keys and the so-called "calling-card" crimes, which are referred to the illegal activities committed in the real world such as murders, blackmailing or terrorist acts.[134] According to the authors, the aforementioned crimes can be efficiently supported by the current Ethereum programming languages. Cyber-criminals may utilize the cryptographic primitives provided in order to achieve their goals. However, no sufficient solution to this problem is currently in place.

While normally the courts would not enforce an illegal contract, in our case, it is almost impossible to stop the programmed execution of smart contracts. To that end, legal literature highlights the absence of safeguards against the criminal smart contract and gives weight on

---

[133] For more information about the Silk Road marketplace see: Andrew Norry, *"The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin",* (blockonomi.com, 11 Oct 2017). Available at: <https://blockonomi.com/history-of-silk-road/> accessed 2 May 2020.

[134] Juels Ari, Ahmed Kosba, and Elaine Shi. *"The ring of gyges: Using smart contracts for crime."* aries 40 (2015): 54. Available online at: <http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf> accessed 2 May 2020.

the significance of constructing mechanisms capable of blocking unlawful transactions and mitigating the legality risks.[135]

3.5 Other legal concerns

3.5.1 Contract Law

The idea of smart contracts in commercial transactions may create a number of problems when the principles of existing contract law are applied. The self-performing nature of smart contracts raises the question of whether they are "contracts" under the traditional requirements of contract formation.

The legal literature shows that smart contracts may not challenge the basic elements of contract law.[136] The capacity of the parties, the offer, and acceptance, the consideration or the mutual assent imposed by the law are all compatible with the blockchain-powered smart contract, and they allow them to be legally valid contracts.

However, there may be conflict areas between smart contracts and the applicable contract law rules. In case of mistake, fraud, duress, or incapacity, the smart contract will prove problematic, because it will be impossible to cancel. Even the courts cannot stop the execution of a smart contract when they consider the agreement void.

As has been stressed, smart contracts are usually not flexible and, therefore, cannot be adapted to changing circumstances or parties' preferences[137]. The ex-ante automated character of smart is incompatible with the flexibility of regular legal contracts. So, there is no room for variation and efficient breaches.

---

[135] See, for example: Werbach Kevin, and Nicolas Cornell. *"Contracts ex machina."* Duke Law Journal 67 313 (2017): p. 373. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2936294> accessed 2 May 2020.

[136] See: DiMatteo LA, Cannarsa M and Poncibò C (eds), "Contract Law and Smart Contracts" in, The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (Cambridge University Press 2019) and O'Shields, Reggie. *"Smart contracts: Legal agreements for the Blockchain.*" NC Banking Inst. 21 (2017): 177.

[137] Hsiao, Jerry IH. *"Smart Contract on the Blockchain-Paradigm Shift for Contract Law."* US-China L. Rev. 14 (2017). p.691. Available on Hein online at: <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/uschinalrw14&id=687&men_tab=srchresults> accessed 19 May 2020.

3.5.2 Consumer protection

Several scholars have raised questions in connection with the negative impact of smart contracts on consumer rights protection.[138] Since, in the vast majority of the situations, smart contracts are set up by the most powerful party (i.e., businesses), consumers are placed at a disadvantage. In B2C relationships, it is practically impossible for consumers to have the choice of negotiating and concluding smart contracts.[139] The terms and conditions of the contract are predefined, and usually, the weaker party is not able firstly to understand and then to modify them.

Currently, the contractual safeguards protecting consumers cannot be applied to smart contracts. Due to their predetermined nature, smart contracts are not able to become void or stop in the event of unconscionability, informational asymmetries, and lack of legal capacity. Thus, in practice, it becomes very difficult - if not impossible - to integrate consumer protection laws into transactions supported by smart contracts.

Nevertheless, it is argued that, in the near future, the "smart" contractual terms may have the potential to be implied to consumer protection laws.[140] The idea of smart contracts that allow consumers to lay down their own provisions in the agreement will definitely bring more fairness in commercial B2C transactions. Thanks to their architecture, smart contracts can self-enforce potential contractual disputes and incorporate pro-consumer terms (e.g., cancelation rights and claims for compensation). A smart contract code may, for instance, embody the European passenger rights and automatically refund money to consumers in the event of a delay

---

[138] See, for example: Wright, Aaron, and Primavera De Filippi. *"Decentralized blockchain technology and the rise of lex cryptographia."* (2015) p.26. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> accessed 2 May 2020, and Athanassiou Phoebus. *"Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks."* (2017) Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3067222> accessed 2 May 2020.

[139] Borgogno Oscar, *"Usefulness and Dangers of Smart Contracts in Consumer Transactions"* in Larry A DiMatteo, Michel Cannarsa and Cristina Poncibò (eds), The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (Cambridge University Press 2019). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350128> accessed 3 May 2020.

[140] Fairfield Joshua AT. *"Smart contracts, Bitcoin bots, and consumer protection."* Wash. & Lee L. Rev. Online 71 (2014): 35. Available online at: <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1003&context=wlulr-online> accessed 3 May 2020.

of the train.[141] The German government has already announced its intention to legislate smart contracts related to consumer commerce.[142]

3.5.3 Discrepancies between the parties' intent and the content of smart contracts

Another challenge with smart contracts is whether and to what extent the code correctly reflects the original intent of the parties. In most of the cases, people entering into blockchain-based smart contracts are unable to create them due to the complex programming language they require. To that end, the participation of a coder who "writes" the contract is essential.

Nevertheless, if the counterparties use a smart contract implemented by a third party, there may be a mismatch between their real will and the actual content of the agreement. A smart contract developer may fail to properly design a contract that will be executed as agreed upon. This can be due to several reasons, namely misunderstanding of the agreement, lack of adequate communication, incapacity, or even the malicious attitude of the creator.[143]

In addition, the inability of the parties to understand computer languages and tools can maximize the problem. Since the person using the smart contract is not able to read and recognize any errors or misconstructions in the code, he cannot confirm the accuracy of its content. The parties are, therefore, unable to verify whether the smart contract will do what it promised to do or not.

The involvement of an experienced technical expert (individual or entity) who designs a smart contract can create problems. The contracting parties do not have the technical expertise to create it, so in most cases they are unable to identify possible discrepancies between their intent

---

[141] Martin Fries, *'Smart consumer contracts - The end of civil procedure?'*, Oxford Business Law Blog - Law and Autonomous Systems Series (2018). Available at: <https://www.law.ox.ac.uk/business-law-blog/blog/2018/03/smart-consumer-contracts-end-civil-procedure> accessed 3 May 2020.
[142] Finck, Michèle. *"Blockchain regulation and governance in Europe"*. Cambridge University Press, 2018. p.76.
[143] See Mik Eliza. *"Smart contracts: terminology, technical limitations and real world complexity."* Law, Innovation and Technology 9.2 (2017): 269-300. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038406> accessed 12 May 2020.

and the content of the smart contract. For this reason, the continuous and regular communication of the parties with the smart contract author is particularly important.

CHAPTER 4:

The distributed liability of smart contract developers

4.1 Introduction

Usually, the parties entered into a smart contract do not have the technical ability to draft and deploy it. So, they rely on a smart contract model provided by a third party, i.e., the individual or the group of people developing the smart contract code. However, coding errors and resulting cyber-attacks are likely to occur, and all these may expose the smart contract developer(s) to legal responsibility towards the parties.

Indeed, blockchain-powered smart contracts introduce an additional risk that does not exist in traditional paper contracts; the possibility of being hacked or containing programming errors. In most of the cases, cyber-attacks against DLT ecosystems are simply exploitation of a technical mistake into the smart contract protocol.

It is highly important for all participants to consider how the liability risks for unintended coding backdoors and resulting security breaches are distributed. Smart contract code developers should keep in mind that the legal responsibility may extend beyond the contracted parties, and to the individuals or the entities developing and deploying smart contracts.[144] However, developers may be located all over the world, and thus it is difficult to be founded and treated in a single jurisdiction.

---

[144] Notably See: Giancaspro, Mark. "Is a 'smart contract' really a smart idea? Insights from a legal perspective." *Computer law & security review* 33.6 (2017). Available on Researchgate.com at: <https://www.researchgate.net/publication/317354410_Is_a_'smart_contract'_really_a_smart_idea_Insights_from_a_legal_perspective> accessed 28 Feb 2020. See also: Madir, Jelena. *"Smart Contracts:(How) Do They Fit Under Existing Legal Frameworks?."* (2018). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301463> accessed 28 Feb 2020.

This chapter discusses the significant role of smart contract code developers and the leading decision-making position in open, decentralized systems. It further looks into the different types of liability that may arise in the smart contract development and examines the relevant liability issues in the light of the US and EU legal system. The chapter concludes with a proposed insurance scheme against any potential smart contract failure.

4.2 The key role of the smart contract developer

In the open-source decentralized systems like the permissionless blockchains, not all the participants are considered equal. The key role of "core developer" is very important as to lead the code development process and make the main decisions about the policy to be embedded in the smart contract code. In the Bitcoin example, the small team of core developers is allowed to notify all users in the network with emergency messages. They also have "commit access" to the software code, enabling them to make decisive changes to the underlying bitcoin code.[145]

The term "smart contract developer" in this thesis is intended to include those not only drafting the smart contract software code but also have a decision-making position on the main technical choices. The power of core developers is most visible in times where the decentralized system is at stake. The hard forks in Bitcoin and Ethereum are examples of the exercised power of developers. As a matter of fact, these decisions have affected many smart contract users, and the more widely used open blockchain is, the larger the user base relies on developers' choices.

4.3 Different liability types

In spite of the tamper-proof and immutable nature of smart contract technology, which is mainly ensured by blockchain operators, developers, and a considerable part of literature, technical and legal risks may arise. As noted in the above section, the characteristics of smart contracts could result in issues related to their operation and cyber-security. All these possible

---

[145] Andreas M. Antonopoulos, “Mastering Bitcoin: Unlocking Digital Cryptocurrencies” (2017) 157. The emergency messages power “allow the core developer team to notify all bitcoin users of a serious problem in the bitcoin network, such as a critical bug that require[s] user action” and was held “by a few select members of the core development team.” See also, Gervais, Arthur, et al. *"Is bitcoin a decentralized currency?."* IEEE security & privacy 12.3 (2014): 54-60.,‘ Available online at: <http://eprint.iacr.org/2013/829.pdf> accessed 21 May 2020 (arguing that giving the emergency alert power only to the core developers “gives these entities privileged powers to reach out to users and urge them to adopt a given Bitcoin release”).

defaults lead, as a matter of fact, to questions about who is legally responsible and to what extent.

To begin with, the liability of smart contract code developers may be assigned in two different ways: as contractual or as non-contractual.[146]

a. Contractual liability

In contract law, the parties are liable under the terms of the agreement. Many jurisdictions require a contractual breach in order to determine liability. So, for those who argue that smart contracts can include the contractual liability,[147] a contractual relation, and a breach of this by one of the parties are necessary.

Notably, in order for a legal agreement to be valid, the following are required: two (or more) parties, an offer and acceptance, the mutual consideration, and the parties' intention that the contract is binding. In the Ethereum example, participants and the group of core developers are the parties to the "distributed ledger contract." The offer, acceptance, and mutual assent are also satisfied: individuals who desire to join the blockchain network, download the software and enable their devices to run Ethereum decentralized ledgers. The consideration may be in different ways, such as additional virtual assets or extra fees in payments.[148] As for the intent to establish a legal relationship, even if the developers may not wish to conclude a legally binding contract, their awareness that this contractual relationship may affect third parties makes their participation legally considerable conduct.[149]

---

[146] See for instance: Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner. *"The distributed liability of distributed ledgers: Legal risks of blockchain." U. Ill. L. Rev. (2018): 1393*. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214> accessed 22 May 2020.

[147] See for instance: Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner. *"The distributed liability of distributed ledgers: Legal risks of blockchain." U. Ill. L. Rev. (2018): 1393*. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214> accessed 22 May 2020.

[148] *Ibid. 1392*.

[149] In the US legal system, an implied-in-fact agreement could be found to exist. See: Baltimore & Ohio R.R. v. United States, 261 U.S. 592, 597 58 Ct. Cl. 709, 43S. Ct. 425, 67 L. Ed. 816 (1923). ("*an agreement...although not embodied in an express contract, is inferred, as a fact, from conduct of the parties showing, in the light of the surrounding circumstances, their tacit understanding".)*

On the other side, a number of legal scholars suggest that a contractual agreement is incompatible within the distributed ledgers networks.[150] Their core argument is that network's participants usually don't pursuit to grant contractual rights to the other users.[151] Indeed, it would be said that In such a complex ecosystem, where the user base is pseudonymized and unstable, it is extremely difficult to establish a contractual relationship between the participants. Thus, it can be no express contractual relationship between the parties using DL-based smart contracts and the developer in open source software platforms.

b. Non-contractual liability

The applicable law of torts is very important where contractual liability cannot be established. Specifically, in smart contracts, tort claims against core developers may arise in the absence of a contractual relation between the end-users and the formers. The academic literature argues in favor of the coder's responsibility instead of the other participants to the distributed ledgers.[152] It would be unfair for the user lacking knowledge and control over the smart contract function to be responsible for the damages incurred. Conversely, the smart contract creator is considered to be in charge because he is the only one that can understand and improve the underlying technology and, ultimately, the one who can prevent present or future risks.

If the programmer or the group of programmers developing the smart contract act or omit negligently resulting damage, then they are likely liable under tort law. The particular harmful effect may include loss caused by technical malfunctions, security breaches, or other illegal activities. Further to this, the existence of liability depends on whether with their negligent act

---

[150] *See* Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner. *"The distributed liability of distributed ledgers: Legal risks of blockchain." U. Ill. L. Rev. (2018) p. 1395*. (the authors state that it is almost impossible to prove that a software program was written negligently). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214> accessed 22 May 2020.

[151] Bayern, Shawn. *"Dynamic common law and technological change: the classification of Bitcoin."* Wash. & Lee L. Rev. Online 71 (2014): 22. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2554747> accessed 22 May 2020.

[152] See, for instance: Wright, Aaron, and Primavera De Filippi. *"Decentralized blockchain technology and the rise of lex cryptographia."* (2015). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> accessed 24 May 2020 (the authors adopt the nearest person theory and show that code founders should be held jointly liable in any undesirable event subject to the product liability law), and see: Francesca Musiani, Cécile Méadel et Alexandre Mallard, Chapter 6: Bitcoin in "Abécédaire des architectures distribuées" (2015) p.45-46 (the authors stress the tortious liability of core developers and exclude it towards the miners and the nodes).

or omission, such coders owe and breach a reasonable "duty of care". In order to prove the specific harm, a causal link between the breach of the fiduciary duty and the caused loss is also required.

More precisely, under tort law, the breach of duty of care may be found where the wrongdoer fails to act in a way that met the standard of care required in certain circumstances. Putting differently, the defendant can be held liable if she was not acting as a "reasonable person" would have acted, considering, of course, that the given situations may vary. Once the plaintiff has proven that the tortfeasor owes him a duty of care, and this duty has been breached, the causation between the tortfeasor's actions and the occurred damage must also be established.[153]

But how is a breach of the reasonable duty of care translated into smart contracts? The duty of care is linked to the basic obligations and liability risks that developers may face during the operation blockchain-based contract. For instance, the smart contract developer must exercise the expected care of a skilled person and provide a secure code free of errors and deficiencies. This means that any coder may be found liable in failing to prevent operational or security issues and take adequate precautions against a foreseeable risk of harm. However, the existence of a breached duty of care is extremely difficult to prove particularly in the case of smart contracts, where the terms -and any potential failure into them- are written in a programming language.[154]

The tests to identify the developer's duty of care vary across the legal systems. Several American states have adopted the foreseeability test, where solely the proof that the defendant's harmful action against the plaintiff was foreseeable, is sufficient to determine the reasonable duty of care.[155] Other state jurisdictions use multi-factor judicial tests for finding the duty of

---

[153] See David Pogue, Elizabeth Clifford and Alan L. Schwartz, "*Understanding New York Law"*, 2013-14, Chapter 8 "GENERAL LAW OF TORTS". Available online at: < https://courses.lumenlearning.com/suny-monroe-law101/chapter/general-law-of-torts/> accessed 23 June 2020.

[154] *See* Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner. *"The distributed liability of distributed ledgers: Legal risks of blockchain." U. Ill. L. Rev. (2018): 1373-1380*. (the authors state that it is almost impossible to prove that a software program was written negligently). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214> accessed 22 May 2020.

[155] See for instance the *McCain v. Florida Power Corporation*, 593 So. 2d 500 (Fla. 1992) in the State of Florida. Available online at: < https://law.justia.com/cases/florida/supreme-court/1992/75637-0.html> accessed 24 June 2020 and the *Jupin v. Kask*, 447 Mass. 141, 849 N.E.2d 829 (2006) in the State of Massachusetts. Available online at: <http://masscases.com/cases/sjc/447/447mass141.html> accessed 24 June 2020.

care.[156] Factors such as the proximity between the wrongdoer and the injured party, the foreseeability of the harm, or the feasibility of alternative conduct are taken into account to justify the duty of care. However, even if the liability is proven, it is practically very difficult to identify the programmer who is responsible for the occurred damage or loss. Whether individually or as a group of people, smart contract developers can be anywhere in the world and, in most cases, do not have enough resources to compensate the injured parties.

Regardless of the liability stems from the law of torts, other types of non-contractual liabilities may arise in relation to the design and the use of smart contracts. Such claims might include fraud, theft, unfair trade practices, or other illicit conduct. Additionally, issues associated with the increased transparency of distributed ledgers such as data privacy violations and insider trading might constitute legal grounds for claims against the smart contract code developers.

Finally, with respect to product liability, certain jurisdictions may potentially apply "strict liability" in the case of a smart contract. The product strict liability may be easily established, since it does not require the traditional elements of the tortious one. In this context, the plaintiff needs to prove only the defect of the product, the harmful effect, and the causality between the defect and the alleged damage. The main objective of product strict liability is to protect consumer' interests in situations of physical harm or damage to property caused by defective products.

4.4. Liability risks of the smart contract developer in major legal systems

4.4.1 The United States

In regards to software contracts, it is possible that the existing US legal system and courts will have laws and tools to adequately address the distribution of liability in the event of contractual

---

[156] See for instance the multi-factor approach of *Adams v. City of Fremont*, 80 Cal. Rptr. 2d 196, 68 Cal. App. 4th 243, 68 Cal. 4th 243 (Ct. App. 1998). Available online at: <https://law.justia.com/cases/california/court-of-appeal/4th/68/243.html> accessed 24 June 2020. (In this case *"the foreseeability and certainty of harm suffered are factors which favor imposing a duty"*. Further, *"the absence of moral blame, the remoteness of the connection between the conduct of appellants and the harm suffered, the policy of preventing future harm, consequences to the community, the role of law enforcement in society, and the potential detriment to the public in imposing judicial allocation of resources all heavily favor shielding law enforcement personnel from tort liability in instances such as this"*.)

deficiencies or technical mistakes. However, it has been noted that the current US legal regime regulating negligent actions, intentional misconduct, or strict liability is struggling to involve the modern automated marketplaces that use smart contracts.[157] More specifically, according to Polin*:*

> *the law of software liability seems to be strangely undeveloped, considering the size of the software industry and the infiltration of software into virtually every aspect our lives […] And though legal commentators have been predicting a great expansion of liability for defective software since the 1980's […] it has not occurred.*[158]

Both common and civil law jurisdictions have adopted tort liability in cases dealing with negligence. The main purpose of tort law is to recover any personal or property damage of individual caused by the wrongful behavior of the tortfeasor. It would be futile to list each type of actions or omissions that may hold someone legally responsible, but mainly the liability arises out of negligence, intentional conduct, or defect in the product sold.

General speaking under the US common law, a "tort" is a *"private or civil wrong or injury, including action for bad faith breach of contract, for which the court will provide a remedy in the form of an action for damages."*[159]

In the US context, the body of law of torts is settled on at the state level, and it may vary across the states. However, in many states, the tort law reflects principles found in the "Restatement of Torts", a treatise written by the American Law Institutes[160]. Under the Restatement of Torts (Second), the negligence is "conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm, and it does not include conduct recklessly disregardful of interest of others."[161] Further, section 402A discusses the strict

---

[157] Yadav Yesha. *"The Failure of Liability in Modern Markets."* Va. L. Rev. 102 (2016): 1031. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652893> accessed 26 May 2020.
[158] Polin David, *"Proof of Manufacturer's Liability for Defective Software"*, 68 Am." Jur. Proof of Facts - 3d edition (2015).
[159] Black Henry Campbell, et al. *"Black's law dictionary"* - 6th edition (1991) p. 1036.
[160] The Restatement of Torts issued by the American Law Institute (ALI) has been broadly adopted as state law by many courts in the US. The Restatement of Law, Torts, Second vol. 1,2 (1965), 3 (1977) and 4 (1979) summarizes the general principles of US tort law and covers many types of liability in tort, applicable defenses and remedies. The Restatement of Law, Torts, Third (1997) looks at strict liability for defective products.
[161] Restatement (Second) of Law of Torts § 282 (1965).

liability of a product's seller for physical harm to the user or consumer and defines when a product should be deemed defective.

According to professor Walch, the fiduciary construct is applicable to the public blockchains, and so smart contract developers can be treated as fiduciaries towards the participants to the peer-to-peer network.[162] The concept of the fiduciary is quite old and reflects one's obligation to act solely in the best interests of the other and before his/her own. Tamar Frankel, who is considered to be one of the leading legal scholars on fiduciary law, summarizes the common characteristics of fiduciaries as follows:

> *First, [fiduciaries] offer mainly services (in contrast to products) [...]. Second, in order to perform these services effectively, fiduciaries must be entrusted with property or power. Third, entrustment poses to entrustors the risks that the fiduciaries will not be trustworthy. They may misappropriate the entrusted property or misuse the entrusted power or they will not perform the promised services adequately. Fourth, there is likelihood that [1] the entrustor will fail to protect itself from the risks involved in fiduciary relationships; [2] the markets may fail to protect entrustors from these risks; and that [3] the costs for the fiduciaries of establishing their trustworthiness may be higher than their benefits from the relationships.*[163]

The fiduciary factors identified by professor Frankel can be applied to the developers of smart contracts utilized in open blockchain platforms. As for the first requirement, it has been argued that the software code is a "product",[164] but it is arguable that what the developers provide is more than just a product, while maintaining and upgrading the code. Further, smart contract coders have the discretion to configure the decentralized platform function like in the Bitcoin (2013) and Ethereum hard forks (2016), where key developers by themselves decide to release

---

[162] See: Walch Angela, *"In Code (rs) We Trust: Software Developers as Fiduciaries in Public Blockchains."* eds. Georgios Dimitropoulos, Stefan Eich, Philipp Hacker, Ioannis Lianos Oxford University Press, Forthcoming 2018. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198> accessed 26 May 2020.

[163] Frankel, Tamar T. Fiduciary law. Oxford University Press, 2010.

[164] See: Berke, David. "Products liability in the sharing economy." Yale J. on Reg. 33 (2016): 603. Available on Heinonline at: <https://heinonline.org/HOL/Page?handle=hein.journals/yjor33&id=605&collection=journals&index=> accessed 26 May 2020.

a new version of the code. Individuals or entities that owned tokens and used smart contracts were not part of these decisions.

As with any power position, key software developers could fail to act diligently, thus harming the people who rely on the blockchain network. Examples of coding flaws resulting in cyber-attacks, token thefts, and data manipulations, all can seriously damage the end-users of blockchain-based smart contracts. However, it should be considered extremely unlikely that "entrustors" will be able to protect themselves from the risks involved in the fiduciary relationship. The lack of know-how and specific tools makes participants unable to evaluate the smart contract code themselves and thus safeguard their interests against the actions of any developer.

One the other hand, it is true that a fiduciary characterization of developers can be considered unrealistic in the smart contract realm.[165] As noted above, establishing a breach of duty would be very demanding compared to the traditional tort cases, and this is because it is extremely difficult to be identified in which line of code is located the problem and then to pin the developer who designed the particular code.

Over and above the errors or other malfunctions in code, developers might be held liable for creating DTL-based smart contracts that facilitate illicit conduct. Indeed, it is arguable whether smart contract developers can be held liable in cases where a smart contract is used for unlawful purposes. While the legal responsibility of coders is quite clear in cases where they are part of illegal activities (like in the Silk Road marketplace), there is a lot of discussions to which extend smart contract code developers could be responsible for the acts or omissions of the network participants.

Recently, efforts have been made to bring more clarity in terms of the potential liability of developers who design smart contracts. On October 16, 2018, in his speech, Commissioner of the Commodity Futures Trading Commission (CFTC), Brian Quintenz explained the need to

---

[165] McKinney, Scott A., Rachel Landy, and Rachel Wilka. "Smart contracts, blockchain, and the next frontier of transactional law." Wash. JL Tech. & Arts 13 (2017): 313. Available on Heinonline at: <https://heinonline.org/HOL/Page?handle=hein.journals/washjolta13&id=321&collection=journals&index=> accessed 26 May 2020.

determine who is responsible in cases where smart contract use violates CFTC regulations for ensuring that multiple transactions on blockchain systems are compatible with the existing laws.[166] And he suggested that smart contract coders could be held liable for aiding and abetting CFTC violations if they could reasonably foresee, that US persons would likely use the smart contract they created to violate CFTC rules.

In November 2018, the Securities Exchange Commission (SEC) settled charges of operating an unregistered securities exchange against Zachary Coburn, the founder, and developer of Ether Delta, a decentralized digital assets trading platform.[167] The SEC's order pointed out that Coburn caused EtherDelta to violate the Securities Exchange Act of 1934 because he "wrote and deployed the EtherDelta smart contract to the Ethereum Blockchain" and exercised sole control over the platform's operations.

Beyond the CFTC legislation, the judicial precedent on the developer's liability in the DLT context may provide adequate guidance on balancing the protection of developers and the remedies award to the injured parties by the unlawful use of smart contracts. In the *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*[168] became clear that smart contract developers should not only avoid coding smart contracts with the potential to be used for illegal purposes but also to make actual efforts to prevent any unlawful use. Under this case, the respondent developers of a file-sharing peer-to-peer software, are not liable for the user's acts resulting infringements, if: (a) they don't distribute the software "with the object of promoting its use to infringe" the laws, (b) they have "no actual knowledge" of the specific infringements and even if they do have actual knowledge, they are not able to prevent the infringing conduct, and (c) the software is "capable of substantial noninfringing uses".

---

[166] Brian Quintenz, Commissioner of the U.S. Commodity Futures Trading Commission, Remarks of at the 38th Annual GITEX Technology Week Conference, Oct. 16, 2018. Available online at: <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16> accessed 26 May 2020.
[167] See the Securities Act of 1934, Release No. 84553 / November 8, 2018. Available online at: <https://www.sec.gov/litigation/admin/2018/34-84553.pdf> accessed 31 May 2020.
[168] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). Available online at: <https://supreme.justia.com/cases/federal/us/545/913/> accessed 26 May 2020.

4.4.2 The European Union

Similar to the US legal system, one of the primary blockchain-related concerns that face the European Union is to identify who is responsible for either insufficient coding and resulting security risks causing damage to end-users of smart contracts.[169] Indeed, the European Banking Authority has repeatedly criticized the lack of an appropriate legal regime that would efficiently govern the rights and obligations among the participants to the blockchain, as well as the allocation of potential liability[170]. Moreover, recent events of cyber-attacks against Ethereum and Bitcoin decentralized platforms revealed the vulnerable nature of smart contracts. They reminded the need for a legal scheme governing the "algorithmic" civil liability.[171]

Smart contracts rely on sophisticated computer protocols written by experts who know their potential and weaknesses in depth. Their use also involves a series of risks allocated among their users and third parties. Hence, the legal responsibility of smart contract developers has been quite a concern for legal theory and practice. In this context, it is stressed that two types of liability may arise in distributed ledgers applications, including smart contracts: the liability derives from the reasonable-care of smart contract developers and the strict liability for defective products.[172]

As noted in the US case, smart contract developers can be found liable if their actions are negligent. This means that the plaintiff should establish a duty of care owed by the coder and

---

[169] See: para 49 of European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

[170] See The EBA's opinions on virtual currencies in 2013, 2014 and 2016 Available online at: <http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies> (2013) <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> (2014) and <https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD> (2016) accessed on 29 May 2020.

[171] See Infantino, Marta, and Weiwei Wang. "Algorithmic Torts: A Prospective Comparative Overview." Transnational Law & Contemporary Problems 29.1 (2018). Available on Heinonline at: <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/tlcp28&id=335&men_tab=srchresults> accessed 27 May 2020. And Buonanno, Luigi. *"Civil Liability in the Era of New Technology: The Influence of Blockchain*." *Bocconi Legal Studies Research Paper Forthcoming* (2019). Available online at: <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/YLA_Award/Submission_ELI_Young_Lawyers_Award_Luigi_Buonanno_ELI_2019.pdf> accessed 28 Feb 2020.

[172] See European Commission Study on Blockchains - Legal, governance and interoperability aspects (SMART 2018/0038), Feb 2020. p.48. Available at: <https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038> accessed 28 May 2020.

further prove that this obligation to act or omit has been breached, causing the particular damage or loss. Although these tort law principles are well established in English and German-law-based civil law jurisdictions, under French law, there is no necessity to prove the existence of a duty of care towards the injured party. In other words, every plaintiff does not necessarily need to establish the defendant's duty of care - the proof of fault, harm, and the causation between them is sufficient for a claim for compensation.[173]

Further, it is of high importance whether the smart contract authors have excluded or limited the liability for any type of loss or damage. The broad disclaimers or liability limitation clauses are of dubious validity as they exempt developers from basic liability risks. It is fair and reasonable that the smart contract developer is borne with the risks of any potential liability. From their position, smart contract founders are obligated to provide flawless smart contract codes and ensure maximum security. The attacks and the followed decisions surrounding Ethereum and Bitcoin platforms showed that smart contract founders and operators are relevant to manage the risks, block further damage, and possibly compensate the users who suffered the occurred losses.

However, it must be stressed that if developers of smart contracts utilized in open distributed ledgers were not allowed to disclaim liability, the costs of code development would increase significantly because they would have to take into account possible legal costs. And since developers are afraid to take on any liability risks; this can disincentivize them from developing innovative smart contract codes.[174]

In addition, the alternative standard of the "strict product liability" can be established at the national level even without the proof of fault. From a European perspective, if the smart contract characterized as a product, the relevant Member State's Acts implementing the

---

[173] See the “Introduction to French tort law” written by the British Institute of International and Comparative Law. Available online at: <https://www.biicl.org/files/730_introduction_to_french_tort_law.pdf> accessed 29 May 2020.

[174] Notably see: Kirk St Amant and Brian Still, ‘Research Handbook on Open Source Software: Technological, Economic and Social Perspectives’, Hershey, 2007, page 333-334. Available online at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.8272&rep=rep1&type=pdf> accessed 29 May 2020.

European Directive on Product Liability (1985) will be applied.[175] However, it seems unclear whether and how strict product liability would align with smart contract technology. Recently, the European Commission launched an assessment to evaluate the relevance of the Directive with the emerging digital technologies, including IoT devices or autonomous systems, and examine whether it continues to provide adequate protection to businesses and consumers.[176]

In Spain, for instance, the product liability might be distributed to the manufacturers, the importers of the product as well as the remaining middlemen across the supply chain.[177] The Spanish Civil Code does not provide a clear definition of what a defective product is. However, under Article 1484, the seller is liable for the latent or hidden damages of the product in case they deem it worthless for its main use or the damages have deteriorated to such extent that had the purchaser known them before had never bought it.[178]

In general, under strict product liability, coders would be legally responsible for any flaws in the code. Although the perfection of the smart contract execution is always the major priority for the parties entering into it, this expectation may not come true, because of undesirable technical glitches or hacking events. But the high-rate of risks and potential costs may discourage developers and slow down the blockchain development. To that end, a limited liability approach for smart contract developers could be applied. Some authors argue in favor of a legal framework similar to the limited liability of the companies.[179] Liability standards that

---

[175] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.
[176] See the final report of the European Commission *"Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products"* (2018). Available online at: <https://op.europa.eu/en/publication-detail/-/publication/d4e3e1f5-526c-11e8-be1d-01aa75ed71a1/language-en> accessed 27 May 2020.
[177] Spanish Product Liability Act (Ley 22/94 de responsabilidad civil por daños causados por productos defectuosos) amended by Ley 14/2000 of 19 December.
[178] See the overview of Spanish product liability regime translated in english at: <https://www.biicl.org/files/1120_overview_spain.pdf> accessed 27 May 2020.
[179] Notably see: European Commission Study on Blockchains - Legal, governance and interoperability aspects (SMART 2018/0038), Feb 2020. p.48. Available at: <https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038> accessed 28 May 2020.

include best efforts and reasonableness may motivate coders to take risks and boost innovation.[180]

As discussed, smart contracts have been used in highly regulated industries, like financial services and data transfers. For this reason, coders must be aware of applicable sectoral legislation when drafting smart contracts. The EU's GDPR and the "right to be forgotten" should be applied in cases of data transfers.[181] Further data retention rules such as "Know Your Customer" (KYC) and "Anti-Money Laundering" (AML) regulations are considered to be very important in order to prevent money laundering and terrorist financing activities. The compliance with the AML and KYC contexts should include the obligation of developers to take appropriate measures that can prevent criminal conduct, especially in permissionless blockchain networks, where participants could be concluding contracts, knowingly or unknowingly, with entities prohibited by law.[182]

4.5 Mandatory insurance for smart contract development

Among the arguments against the characterization of smart contracts developers as fiduciaries is that they are not compensated at a sufficient level.[183] Therefore, they don't have adequate resources to compensate the injured parties if something goes wrong such as in case of theft of digital assets or other security breaches.

Recently, about $530 million worth of the NEM cryptocurrency was stolen from the Coincheck exchange platform.[184] This cyber-heist has been considered one of the biggest ever affecting

---

[180] Paul Rosenzweig, *"Bad Code Is Already a Problem. Soon, Companies Will Be Liable"* (foreignpolicy.com, 28 July 2018). Available at: <https://foreignpolicy.com/2017/07/28/bad-code-is-already-a-problem-soon-companies-will-be-liable/> accessed 29 May 2020.

[181] See: Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12) 2014.

[182] See European Commission Study on Blockchains - Legal, governance and interoperability aspects (SMART 2018/0038), Feb 2020. p.49-50. Available at: <https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038> accessed 28 May 2020.

[183] See: Walch Angela, *"In Code (rs) We Trust: Software Developers as Fiduciaries in Public Blockchains."* eds. Georgios Dimitropoulos, Stefan Eich, Philipp Hacker, Ioannis Lianos Oxford University Press, Forthcoming 2018. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198> accessed 26 May 2020.

[184] Jake Adelstein, *"Japan Cracks Down On Cryptocurrency Exchanges After $534M Heist; Police Begin Investigation" (Forbes.com, 30 Jan 2018). Available at:* <https://www.forbes.com/sites/adelsteinjake/2018/01/30/japan-cracks-down-on-cryptocurrency-exchanges-after-534m-heist-police-begin-investigation/#c5adac55031e> accessed 28 May 2020.

nearly 260.000 users. In public conferences, the Coincheck management could not give a clear answer on whether and how the investors will be fully compensated. Even today, the platform has not found a way to cover all lost cryptocurrencies and refund the customers.[185] This event demonstrates, once again, the urgency to prudently consider the introduction of mandatory insurance for developers against the smart contract failure.

Traditionally, banks have a pool of funds to recover damage to their customers due to possible insolvency and insurance companies maintain a reserved capital for paying compensation to individuals injured in accidents where the liable person has not been identified or properly insured. In the case of blockchain-powered smart contracts, similar solutions may be implemented.

An insurance system that covers the creation and use of smart contracts can protect developers as well as other participants. This solution can have many benefits in developing smart contracts and building more trust in their use. First of all, it can ensure that in the event of cyber-crime, the injured parties will be fully compensated. Recent events have shown that blockchain users invest a lot of money in blockchains and DAO platforms. This increases the risk of a possible attack, making it extremely difficult to compensate those who have suffered losses and damages.

In addition, this protection against smart contract failure will not only safeguard investors from losing their money but also develop a smart contract with greater confidence. The importance of a safer and more reliable smart contract is to encourage users to invest money and get economic incentives by transacting via smart contract technology. Thus, a solution ensuring that developers will be able to compensate those affected by any damage or incidents of attack primarily aims to make smart contracts a secure and trustworthy way to trade.

Given the possible failure of smart contracts, further questions arise as to who could be able to evaluate their insurable risks and assist in a successful insurance provision.[186] Auditors will

---

[185] Daniel Shane, *"$530 million cryptocurrency heist may be biggest ever"* (Cnn.com, 29 Jan 2018). *Available at:* <https://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html> accessed 28 May 2020.

[186] Luke Duncan, *"Insuring against smart contract failure"* (Medium.com, 26 April 2018). Available at: <https://medium.com/@lkngtn/insuring-against-smart-contract-failure-86d0d9206d90> accessed 4 June 2020.

play this role. In particular, auditing companies should evaluate code vulnerability and review the probability of being hacked. The insurance premium of each smart contract will be determined based on the experts' assessment and on whether it represents a viable risk of exposure to the insurance pool. This analysis by the auditing company is extremely significant for both the developers and individual users as they confirm whether a smart contract is safe to be used or not.

CONCLUDING REMARKS

Nowadays, while blockchain applications are gaining ground and smart contracts becoming more and more popular in the transactional landscape, a plethora of legal concerns between which and the attribution of liability have emerged. The design and use of smart contracts, in many cases, involve a series of legal risks that may be distributed among the smart contract code developers.

In this thesis, the blockchain technology underlying smart contracts is explained. Its main elements and mode of operations are also examined. The distributed ledgers may facilitate a wide range of transactions, namely money transfers and online commerce. In particular, a decentralized blockchain network provides a high level of autonomy and a room of "doing businesses" without the need for intermediaries and gatekeepers. Further, this thesis introduces the reader to the concept of smart contracts and canvases their key features. The immutable and self-enforcing nature of smart contracts allows them to intervene vigorously in the real world and be widely adopted in recent years.

The dissertation provides a comparative analysis of the EU and US legal regime surrounding the blockchain-based smart contracts. With this approach, it takes a closer look at the regulatory framework related to blockchain technology and smart contracts in the two major legal systems. In particular, while US state legislation on automated smart contracts seems well-developed, on the other side of the Atlantic, the vast majority of EU Member States proceed cautiously into their legislation. In this context, although some jurisdictions are receptive to accept the

new concept of smart contracts, electronic signatures, and documents, the existing laws surrounding the blockchain applications and smart contracts need to expand to accommodate the legal issues surrounding smart contracts.

In most of the cases, the parties who conclude a smart contract do not have the technical expertise to create it. So, there is a factual need of a trusted and experienced technical expert (individual or entity), which will draft blockchain algorithms. Small or bigger coding errors and malfunctions may result in cyber-attacks that expose the smart contract developer(s) to legal responsibility towards the parties. The notorious cyber-attacks against DLT networks like Bitcoin and Ethereum demonstrate the need to fill any gaps in the relevant legislation that could ensure full compensation to the injured parties and prevent any future damage or losses.

The contribution of this analysis is to highlight these possible risks and examine whether software developers are able to guarantee the security of the smart contract and manage the relevant operating and security risks in cyberspace. The significant role of smart contract code developers and the leading decision-making position in open, decentralized systems points in favor of the coder's responsibility instead of the other participants. The smart contract maker is considered responsible because he is the only one who can understand and improve the underlying technology and, ultimately, the one who can prevent the present or future risks.

Whether under the contractual or non-contractual liability of smart contract developers, the legal standards differ between American and European legal systems. In the US, it is highly recommended that smart contract code developers may constitute a new type of fiduciary given their prominent position in the network.[187] While at the EU level, this liability can be extended to the product liability. The research also emphasizes the potential liability of developers in cases where their own codes are used for illegal purposes.

---

[187] See: Walch Angela, *"In Code (rs) We Trust: Software Developers as Fiduciaries in Public Blockchains."* eds. Georgios Dimitropoulos, Stefan Eich, Philipp Hacker, Ioannis Lianos Oxford University Press, Forthcoming 2018. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198> accessed 26 May 2020.

To conclude, although smart contracts will possibly disrupt the traditional commercial and legal transactional environment, it is very important that the legal framework is expanded to address the fast-evolving legal issues of smart contracts. It can be observed that the current legal framework regulating the developer's liability is in infancy. This means that there are steps that can be taken to adequately deal with the liability issues of smart contracts. The existing rules need to adapt to the smart contract context, and for this reason, a mandatory insurance system is proposed. With this measure, all participants in the blockchain ecosystem, as well as the developers, will be insured against any possible smart contract failure.

BIBLIOGRAPHY

BOOKS:

Amant, K. S., *'Research Handbook on Open Source Software: Technological, Economic and Social Perspectives',* (Hershey, 2007)Available online at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.8272&rep=rep1&type=pdf> accessed 29 May 2020.

Black, H. C., et al., *"Black's law dictionary"* - 6th edition (1991).

Blumenthal, Marjory S. & Clark D., *"Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world."* ACM Transactions on Internet Technology (TOIT) 1.1 (2001): 70-109.

Borgogno O., *"Usefulness and Dangers of Smart Contracts in Consumer Transactions"* in DiMatteo L.A., Cannarsa M. and Poncibò C. (eds), The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (Cambridge University Press 2019). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350128> accessed 3 May 2020.

Campbell D., *"E-Commerce: Law and Jurisdiction: Comparative Law Yearbook of International Business-Special".* No. 2002. Kluwer Law International BV, 2003.

De Filippi, P. D. F., "*Blockchain and the law: The rule of code*." Harvard University Press, (2018).

DiMatteo L.A., Cannarsa M. and Poncibò C. (eds), *"Contract Law and Smart Contracts"* in, The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (Cambridge University Press 2019)

Finck M., *"Blockchain regulation and governance in Europe."* Cambridge University Press (2018).

Frankel T.T., *"Fiduciary law".* Oxford University Press, 2010.

Gatteschi, V., Lamberti, F., & Demartini, Chapter 3: *"Technology of Smart Contracts"* in DiMatteo L.A., Cannarsa M. and Poncibò C. (eds), The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (Cambridge University Press 2019)

Musiani F., Méadel C. et Mallard A., Chapter 6: BITCOIN in *"Abécédaire des architectures distribuées"* (2015).

Pogue D., Clifford E. & Schwartz A., "*Understanding New York Law"*, 2013-14, Chapter 8 "GENERAL LAW OF TORTS". Available online at: < https://courses.lumenlearning.com/suny-monroe-law101/chapter/general-law-of-torts/> accessed 23 June 2020.

ACADEMIC PAPERS:

Alharby, M., & Van Moorsel, A., *"Blockchain-based smart contracts: A systematic mapping study."* (2017).

Antonopoulos A., "Mastering Bitcoin: Unlocking Digital Cryptocurrencies" (2017) 157.

Athanassiou P., *"Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks."* (2017) Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3067222> accessed 2 May 2020.

Bacon, J., Michels, J. D., Millard, C., & Singh, J., *"Blockchain demystified."* Queen Mary School of Law Legal Studies Research Paper 268 (2017). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218> accessed 30 Feb 2020.

Bayern S., *"Dynamic common law and technological change: the classification of Bitcoin."* Wash. & Lee L. Rev. Online 71 (2014): 22. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2554747> accessed 22 May 2020.

Berke D., "Products liability in the sharing economy." Yale J. on Reg. 33 (2016): 603. Available on Heinonline at: <https://heinonline.org/HOL/Page?handle=hein.journals/yjor33&id=605&collection=journals&index=> accessed 26 May 2020.

Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M., *"Corda: an introduction."* R3 CEV, August 1 (2016): 15.

Buonanno L., *"Civil Liability in the Era of New Technology: The Influence of Blockchain*." *Bocconi Legal Studies Research Paper Forthcoming* (2019). Available online at: <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/YLA_Award/Submission_ELI_Young_Lawyers_Award_Luigi_Buonanno_ELI_2019.pdf> accessed 28 Feb 2020.

Chamber of Digital Commerce, *"'Smart Contracts" Legal Primer: Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable"* (January 2018). Available at: <https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf> accessed 22 April 2020.

Cong, L. W., & He, Z., *"Blockchain disruption and smart contracts."* The Review of Financial Studies 32.5 (2019): 1754-1797.Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764> accessed 7 April 2020.

De Caria R., *"A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities"*, United Nations Commission on International Trade Law (UNCITRAL) 7 (June 9, 2016), Available at: <http://www.uncitral.org/pdf/english/congress/Papers_for_Programme/5-DE_CARIA-A_Digital_Revolution_in_International_Trade.pdf> accessed 18 April 2020.

De Graaf, T. J., *"From old to new: From internet to smart contracts and from people to smart contracts."* Computer Law & Security Review 35.5 (2019): 105322. Available on ScienceDirect at: <https://www.sciencedirect.com/science/article/pii/S0267364919300147> accessed 28 Feb 2020.

Dell'Erba M., *"Demystifying Technology. Do Smart Contracts Require a New Legal Framework? Regulatory Fragmentation, Self-Regulation, Public Regulation."* (2018). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228445> accessed 22 April 2020.

Fairfield, J. A., *"Smart contracts, Bitcoin bots, and consumer protection."* Wash. & Lee L. Rev. Online 71 (2014). Available online at: <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1003&context=wlulr-online> accessed 3 May 2020.

Fries M., *'Smart consumer contracts - The end of civil procedure?'*, Oxford Business Law Blog - Law and Autonomous Systems Series (2018). Available at: <https://www.law.ox.ac.uk/business-law-blog/blog/2018/03/smart-consumer-contracts-end-civil-procedure> accessed 3 May 2020.

Gervais A. et al., *"Is bitcoin a decentralized currency?"* IEEE security & privacy 12.3 (2014): 54-60.,' Available online at: <http://eprint.iacr.org/2013/829.pdf> accessed 21 May 2020

Giancaspro M., *"Is a 'smart contract' really a smart idea? Insights from a legal perspective."* Computer law & security review 33.6 (2017). Available on Researchgate.com at: <https://www.researchgate.net/publication/317354410_Is_a_'smart_contract'_really_a_smart_idea_Insights_from_a_legal_perspective> accessed 28 Feb 2020.

Grimmelmann J., *"All Smart Contracts Are Ambiguous."* Penn Journal of Law and Innovation (Forthcoming) (Oct. 2019). Available online at: <https://www.law.upenn.edu/live/files/9789-jli-volume-2> accessed 28 Feb 2020.

Hsiao, J. I., *"Smart Contract on the Blockchain-Paradigm Shift for Contract Law."* US-China L. Rev. 14 (2017). Available on Hein online at: <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/uschinalrw14&id=687&men_tab=srchresults> accessed 19 May 2020.

Infantino, M., & Wang, W., *"Algorithmic Torts: A Prospective Comparative Overview."* Transnational Law & Contemporary Problems 29.1 (2018). Available on Hein online at: <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/tlcp28&id=335&men_tab=srchresults> accessed 27 May 2020.

Juels, A., Kosba, A., & Shi, E., *"The ring of gyges: Using smart contracts for crime."* aries 40 (2015): 54. Available online at: <http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf> accessed 2 May 2020.

Kareem, A., Sulaiman, R. B., & Farooq, M. U., *"Algorithms and Security Concern in Blockchain Technology: A Brief Review."* (2018). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3227933 > accessed 30 Feb 2020.

Madir J., *"Smart Contracts:(How) Do They Fit Under Existing Legal Frameworks?"* (2018). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301463> accessed 28 Feb 2020.

McKinney, S. A., Landy, R., & Wilka, R., *"Smart contracts, blockchain, and the next frontier of transactional law."* Wash. JL Tech. & Arts 13 (2017): 313. Available on Heinonline at: <https://heinonline.org/HOL/Page?handle=hein.journals/washjolta13&id=321&collection=journals&index=> accessed 26 May 2020.

Mik E., *"Smart contracts: terminology, technical limitations and real world complexity."* Law, Innovation and Technology 9.2 (2017): 269-300. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038406> accessed 12 May 2020.

Morshed, M. J., & Watters, P. A., *"An Empirical Analysis of Blockchain Cybersecurity Incidents." (2019).* Available online at: <https://www.researchgate.net/profile/Alex_Ng14/publication/337647279_An_empirical_analysis_of_blockchain_cybersecurity_incidents/links/5e087691a6fdcc2837460279/An-empirical-analysis-of-blockchain-cybersecurity-incidents.pdf> accessed 13 May 2020.

Nakamoto S., *"Bitcoin: A peer-to-peer electronic cash system."* (2008). Available online at: <https://bitcoin.org/bitcoin.pdf> accessed 30 Feb 2020.

Nikolić, I., Kolluri, A., Sergey, I., Saxena, P., & Hobor, A., *"Finding the greedy, prodigal, and suicidal contracts at scale."* In Proceedings of the 34th Annual Computer Security Applications Conference, pp. 653-663. (2018). Available at: <https://arxiv.org/pdf/1802.06038.pdf> accessed 26 April 2020.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D., "*Blockchain."* Business & Information Systems Engineering 59, no. 3 (2017): 183-187. Available online at: <https://www.researchgate.net/publication/315462390_Blockchain> accessed 30 Feb 2020.

O'Shields, R., *"Smart contracts: Legal agreements for the Blockchain.*" NC Banking Inst. 21 (2017). Available on Hein online at: <https://heinonline.org/HOL/Page?handle=hein.journals/ncbj21&div=12&g_sent=1&casa_token=jOKoTOP54wcAAAAA:js94Os1fKHPTtVTr31PwKXMgDj0NFJDLjDVr_6AwIiN-VSx1iybIgJ99OR4PhNann5Ywjc0&collection=journals> accessed 11 April 2020.

Polin D., *"Proof of Manufacturer's Liability for Defective Software"*, 68 Am." Jur. Proof of Facts - 3d edition (2015).

Primavera De Filippi and Aaron Wright, Blockchain and the Law (HUP 2018) 33-57;

Raskin M., *"The law and legality of smart contracts."* (2016). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166> accessed 11 April 2020.

Salmon, J., & Myers, G.,*"Blockchain and associated legal issues for emerging markets."* (2019). Available at: <http://documents.vsemirnyjbank.org/curated/ru/658041547845804080/pdf/133877-EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf> accessed 29 April 2020.

Savelyev A.,*"Contract law 2.0:'"Smart" contracts as the beginning of the end of classic contract law."* Information & Communications Technology Law 26.2 (2017): 116-134. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241> accessed 10 April 2020.

Smart Contract Alliance, "Smart Contracts: Is the Law Ready?", Chambre of Digital Commerce (2018).

Szabo N., *"Smart contracts: building blocks for digital markets."* (1996) Available online at: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 28 Feb 2020.

Szabo N., *"The idea of smart contracts."* (1997). Available online at: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html> accessed 7 April 2020.

Szabo N., *"Smart Contracts"* (1994). Available online at: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> accessed 4 April 2020.

Thomas, S., & Schwartz, E., *"Smart Oracles: A Simple, Powerful Approach to Smart Contracts"* (19 July 2018) Available online at: <https://github.com/codius/codius-wiki/wiki/White-Paper#overview> accessed 10 April 2020.

Vermeulen, E., Fenwick, M., & Kaal, W., *"Why'Blockchain'Will Disrupt Corporate Organizations."* Lex Research Topics in Corporate Law & Economics Working Paper 2018-3 (2018): 18-17. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3227933> accessed 30 Feb 2020.

Walch A., *"In Code (rs) We Trust: Software Developers as Fiduciaries in Public Blockchains."* eds. Georgios Dimitropoulos, Stefan Eich, Philipp Hacker, Ioannis Lianos Oxford University Press, Forthcoming 2018. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198> accessed 26 May 2020.

Walch A., *"The bitcoin blockchain as financial market infrastructure: A consideration of operational risk."* NYUJ Legis. & Pub. Pol'y 18 (2015): 837. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579482> accessed 1 May 2020.

Walch A., *"The path of the blockchain lexicon (and the law)."* Rev. Banking & Fin. L. 36 (2016): 713. Available on SSRN at: <https://ssrn.com/abstract=2940335> accessed 22 April 2020.

Werbach, K., & Cornell, N. *"Contracts ex machina."* Duke Law Journal 67 313 (2017). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2936294> accessed 2 May 2020.

Wright, A., & De Filippi, P., *"Decentralized blockchain technology and the rise of lex cryptographia."* (2015). Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> accessed 2 May 2020.

Yadav Y.,*"The Failure of Liability in Modern Markets."* Va. L. Rev. 102 (2016): 1031. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652893> accessed 26 May 2020.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W., *"The distributed liability of distributed ledgers: Legal risks of blockchain." U. Ill. L. Rev. (2018): 1393*. Available on SSRN at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214> accessed 22 May 2020.

Zyskind, G., & Nathan, O., *"Decentralizing privacy: Using blockchain to protect personal data."* 2015 IEEE Security and Privacy Workshops. IEEE, 2015.

ONLINE ARTICLES & BLOGS:

Adcock C., *"An Update on State Smart Contract Legislation"* (The National Law Review, 15 April 2020) Available at: <https://www.natlawreview.com/article/update-state-smart-contract-legislation> accessed 18 April 2020.

Adelstein J., *"Japan Cracks Down On Cryptocurrency Exchanges After $534M Heist; Police Begin Investigation" (Forbes.com, 30 Jan 2018).* Available at: <https://www.forbes.com/sites/adelsteinjake/2018/01/30/japan-cracks-down-on-cryptocurrency-exchanges-after-534m-heist-police-begin-investigation/#c5adac55031e> accessed 28 May 2020.

Antonopoulos A., "*Bitcoin security model: trust by computation"* (radar.oreilly.com, 20 Feb 2014) <http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html> accessed 12 April 2020.

Asolo B., *"Double-Spending Explained"* (mycryptopedia.com December 21, 2018). Available at: https://www.mycryptopedia.com/double-spending-explained/ accessed on 7 April 2020.

Chelyshava I., *"Belarus' Cryptocurrency Experiment: Why the World Should Take Notice"* (Jurist.org, 12 Jan 2018). Available at: <https://www.jurist.org/commentary/2018/01/iryna-chelyshava-belarus-cryptocurrency/> accessed 18 April 2020.

Dale B., *"Why DeFi's Billion-Dollar Milestone Matters"* (Coindesk.com, 7 Feb 2020). Available at: <https://www.coindesk.com/why-defis-billion-dollar-milestone-matters> accessed 26 April 2020.

Duncan L., *"Insuring against smart contract failure"* (Medium.com, 26 April 2018). Available at: <https://medium.com/@lkngtn/insuring-against-smart-contract-failure-86d0d9206d90> accessed 4 June 2020.

Falkon S., *"The Story of the DAO - Its History and Consequences"* (Medium.com, 24 Dec. 2017) <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee> accessed 1 May 2020.

Greenspan G., *'Beware of the Impossible Smart Contract'* (Multicain.com, 12 April 2016) <https://www.multichain.com/blog/2016/04/beware-impossible-smart-contract/> accessed 4 April 2020.

Heaven D., *"A house has been bought on the blockchain for the first time"* (newscientist.com, 11 Oct 2017). Available at: <https://www.newscientist.com/article/mg23631474-500-a-house-has-been-bought-on-the-blockchain-for-the-first-time/> accessed 18 April 2020.

Higgins S., "*Details of $5 Million Bitstamp Hack Revealed"* (coindesk.com, 1 Jul 2015). Available at: < https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange> accessed 15 June 2020.

Hu J., *"Learn Blockchain's Top 25 Hacks in History"*, (Hackernoon.com, 7 Feb 2019). Available at: < https://hackernoon.com/tech-explained-top-24-blockchain-hacks-in-history-first-half-40c390dc4a96> accessed 28 May 2020.

Moskov A., "*Ethereum Classic vs Ethereum (ETC vs ETH): What's the Difference?".* (coincentral.com, 20 March 2020). Available at: <https://coincentral.com/ethereum-classic-vs-ethereum/> accessed 1 May 2020.

Norry A., *"The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin",* (blockonomi.com, 11 Oct 2017). Available at: <https://blockonomi.com/history-of-silk-road/> accessed 2 May 2020.

Qureshi H,, *"A hacker stole $31M of Ether — how it happened, and what it means for Ethereum"* (freecodecamp.org/news/, 20 Jul 2017). Available at: <https://www.freecodecamp.org/news/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce/> accessed 28 Feb 2020.

Reiff N., *"Blockchain Explained"* (invetstopedia.com, 1 Feb 2020). Available online at: <https://www.investopedia.com/terms/b/blockchain.asp> accessed 30 Feb 2020.

Rosenzweig P., *"Bad Code Is Already a Problem. Soon, Companies Will Be Liable"* (foreignpolicy.com, 28 July 2018). Available at: <https://foreignpolicy.com/2017/07/28/bad-code-is-already-a-problem-soon-companies-will-be-liable/> accessed 29 May 2020.

Rosic A., *"Smart Contracts: The Blockchain Technology That Will Replace Lawyers"* (blogeeks.com, 2017) Available at: <https://blockgeeks.com/guides/smart-contracts/> accessed 6 April 2020.

Sedgwick K., *"25% of All Smart Contracts Contain Critical Bugs"* (Bitcoin.com, 29 Aug 2018). Available at: <https://news.bitcoin.com/25-of-all-smart-contracts-contain-critical-bugs/> accessed 26 April 2020.

Shane D., *"$530 million cryptocurrency heist may be biggest ever"* (Cnn.com, 29 Jan 2018). *Available at:* <https://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html> accessed 28 May 2020.

Shin L., *"The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project"* (Forbes.com, 7 Feb 2017). Available at: <https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#22a05c64dcdc> accessed 18 April 2020.

Simpson I., *"To Understand Blockchains, You Should Understand Cryptographic Hashes First - Bitcoin is first and foremost a child of cryptography*" (Medium.com, 19 Sep 2017). Available at: https://medium.com/vandal-press/to-understand-blockchains-you-should-understand-cryptographic-hashes-first-for-normies-93bc7645e816> accessed 10 June 2020.

Stanley A., *"Can Code Really Be Law? New Report Clarifies Smart Contract Misconceptions"* (Forbes.com, 27 Sep 2018). Available at: <https://www.forbes.com/sites/astanley/2018/09/27/can-code-really-be-law-new-report-clarifies-smart-contract-misconceptions/#4f6a955834e2> accessed 18 April 2020.

Stark J., *"How Close Are Smart Contracts to Impacting Real-World Law?"*, (Coindesk.com, Apr. 11, 2016). Available online at: <https://www.coindesk.com/snake-oil-and-overpriced-junk-why-blockchain-doesnt-fix-online-voting> accessed 26 June 2020.

Tania H., *"Why Should You Consider Implementing Blockchain Technology in Your Marketplace?"* (rubygarage.org, 27 Jan 2020) Available at: <https://rubygarage.org/blog/how-blockchain-impacts-marketplace> accessed on 12 April 2020.

Tar A., *"Proof-of-Work, Explained"* (cointelegraph.com, 17 Jan 2018) Available online at: <https://cointelegraph.com/explained/proof-of-work-explained> accessed 30 Feb 2020.

Vermeulen E., *"3 Reasons Why the Blockchain Revolution Is (Finally) Becoming a Reality!"* (Medium.com, May 5, 2017). Available at: <https://medium.com/startup-grind/3-reasons-why-the-blockchain-revolutionis-finally-becoming-a-reality-63bdd90c89e2> accessed 30 Feb 2020.

OTHER MATERIAL:

Atzei N., Bartoletti M., and Cimoli T., *"A survey of attacks on ethereum smart contracts (sok)."* International conference on principles of security and trust. Springer, Berlin, Heidelberg, 2017.

British Institute of International and Comparative Law, *"Introduction to French tort law".* Available online at:

<https://www.biicl.org/files/730_introduction_to_french_tort_law.pdf> accessed 29 May 2020.

Cardozo Blockchain Project, *'Smart Contract and Legal enforceability'*, second Research Report (2018). Available at: <https://larc.cardozo.yu.edu/cgi/viewcontent.cgi?article=1001&context=blockchain-project-reports> accessed 22 April 2020.

Clairfield International, *"The potential of blockchain and smart contracts in M&A"* (March 2019).

Clifford Chance and European Bank for Reconstruction and Development, "*Smart Contracts – Legal Framework and Proposed Guidelines for Lawmakers"* (September 2018) p.47. Available online at: <www.ebrd.com/documents/pdf-smart-contracts-legal-framework-and-proposed-guidelines-for-lawmakers.pdf> accessed 13 May 2020.

Clifford Chance, *"Are Smart Contracts Contracts?"*, December 2017. Available online at: <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2017/08/are-smart-contracts-contracts.pdf> accessed 7 April 2020.

Espinel V., et al., *"Survey report:"Deep shift: Technology tipping points and societal impact"."* World Economic Forum, (September 2015).

European Commission Study on Blockchains - Legal, governance and interoperability aspects (SMART 2018/0038), Feb 2020. Available at: <https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038> accessed 22 April 2020.

European Commission, *"Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products"* (2018). Available online at: <https://op.europa.eu/en/publication-detail/-/publication/d4e3e1f5-526c-11e8-be1d-01aa75ed71a1/language-en> accessed 27 May 2020.

Haber, S., & Stornetta, W. S. *"How to time-stamp a digital document."* Conference on the Theory and Application of Cryptography. Springer, Berlin, Heidelberg, 1990.

Hancock M., Minister for Cabinet Office, Speech on *"Digital transformation in government and blockchain technology",* delivered at Digital Catapult, Kings Cross, London on 26 April 2016.

Hero of Alexandria, *"The Pneumatics"* translated from Greek and edited by Bennet Woodcroft, available online at: <https://web.archive.org/web/20101208040820/http://www.history.rochester.edu/steam/hero/index.html> accessed 7 April 2020.

Iansiti, M., & Lakhani, K. R., *"The truth about blockchain."* Harvard Business Review 95 (2017): 118-127. Available online at: <https://hbr.org/2017/01/the-truth-about-blockchain> accessed 7 April 2020.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C., (2016, May). *"Hawk: The blockchain model of cryptography and privacy-preserving smart contracts".* In 2016 IEEE symposium on security and privacy (SP) (pp. 839-858). IEEE.

Lyons T., Courcelas L., Timsit K., *"Legal and Regulatory Framework of Blockchains and Smart Contracts".* The European Union Blockchain Observatory and Forum (2019). Available online at: <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> accessed 28 Feb 2020.

Quintenz B., Remarks of at the 38th Annual GITEX Technology Week Conference, Oct. 16, 2018. Available online at: <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16> accessed 26 May 2020.

Swanson T., *"Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems."* Report (2015). Available online at: <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf> accessed 7 April 2020.

Zhang, F., Cecchetti, E., Croman, K., Juels, A., & Shi, E.,*"Town crier: An authenticated data feed for smart contracts."* Proceedings of the 2016 aCM sIGSAC conference on computer and communications security. (2016).

LEGISLATION:

European Union

- Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.
- Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources.
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
- European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).
- French Civil Code as amended by Article 2 of Ordinance No. 2016-131 of February 10, 2016. Available in French at:

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032004939&categorieLien=id> accessed 22 April 2020.

- German Civil Code (BGB). Available in English at: <https://www.gesetze-im-internet.de/englisch_bgb/> accessed 22 April 2020.
- Greek Civil Code
- Malta Digital Innovation Authority Act of 2018, Part I § 2(1). Available at: <https://parlament.mt/media/95199/act-xxxi-malta-digital-innovation-authority-act.pdf> accessed 22 April 2020.
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- Spanish Product Liability Act (Ley 22/94 de responsabilidad civil por daños causados por productos defectuosos) amended by Ley 14/2000 of 19 December.

United States

- 15 U.S. Code
- 2019 Nev. S.B. 162 and 163.
- Arizona Revised Stat. Ann. § 44-7061.
- Bill No. 205 VT S0269 | 2017-18 "An act relating to blockchain business development".
- Illinois Blockchain Technology Act (205 ILCS 730/)
- Illinois State Electronic Commerce Security Act (5 Ill. Comp. Stat. 175/5-110)
- Law 34/2002 of 11 July, Services Of The Society Of Information And Electronic Commerce, as amended by Law No. 7/2010. Available in English at: <https://www.global-regulation.com/translation/spain/1450967/law-34-2002%252c-of-11-july%252c-services-of-the-society-of-information-and-electronic-commerce.html> accessed 22 April 2020.
- Nevada Revised Stat. Ann. § 719.090, as amended by 2019 Nev. S.B. 162.
- New York State Tech. 304
- Ohio Revised Code Ann.

- Securities Act of 1934, Release No. 84553 / November 8, 2018. Available online at: <https://www.sec.gov/litigation/admin/2018/34-84553.pdf> accessed 31 May 2020.
- Senate Bill S4142. Available at: <https://www.nysenate.gov/legislation/bills/2019/s4142> accessed 22 April 2020.
- Tennessee Code Ann. § 47-10-201(1).
- The Restatement of Law, Torts, Second vol. 1,2 (1965), 3 (1977) and 4 (1979). The Restatement of Law, Torts, Third (1997) looks at strict liability for defective products.
- UETA § 2(6), (7)
- VT S0269 | 2017-18 § 4172, 4173 (C).
- Washington Revised Code 19-360.

CASES:

- *Adams v. City of Fremont*, 80 Cal. Rptr. 2d 196, 68 Cal. App. 4th 243, 68 Cal. 4th 243 (Ct. App. 1998). Available online at: <https://law.justia.com/cases/california/court-of-appeal/4th/68/243.html> accessed 24 June 2020.
- *Baltimore & Ohio R.R. v. United States*, 261 U.S. 592, 597 58 Ct. Cl. 709, 43S. Ct. 425, 67 L. Ed. 816 (1923).
- *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (C-131/12) 2014.
- *Jupin v. Kask*, 447 Mass. 141, 849 N.E.2d 829 (2006) in the State of Massachusetts. Available online at: <http://masscases.com/cases/sjc/447/447mass141.html> accessed 24 June 2020.
- *McCain v. Florida Power Corporation*, 593 So. 2d 500 (Fla. 1992) in the State of Florida. Available online at: < https://law.justia.com/cases/florida/supreme-court/1992/75637-0.html> accessed 24 June 2020
- *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).* Available online at: <https://supreme.justia.com/cases/federal/us/545/913/> accessed 26 May 2020.