İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

THE REGULATION OF SMART CONTRACTS: LAW, GOVERNANCE AND PRACTICE

Ezgi Elife Pilavcı
116692021

Dr. Öğr. Üyesi Mehmet Bedii KAYA

İSTANBUL
2019

TABLE OF CONTENTS

ABBREVIATIONS

AETA	Arizona Electronics Transactions Act.
ACK/NACK	Acknowledged and Non-acknowledged
AI	Artificial Intelligence.
API	Application Programming Interface.
B2B	Business-to-Business.
B2C	Business-to-Consumer.
BKM	Bankalararasi Kart Merkezi.
CPU	Central Processing Unit.
CISG	United Nations Convention on Contracts for the International Sale of Goods.
DAO	Decentralized Autonomous Organization.
EC Directive	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.
EDI	Electronic Data Interchange.
EMRB	Energy Market Regulatory Board
ESIGN	Electronic Signatures in Global and National Commerce Act.
EU	The European Union.
EVM	Ethereum Virtual Machine.
GPS	Global Positioning System.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
GLBA	Glamm-Leach-Bliley Act.
HIPAA	Health Insurance Portability and Accountability Act.
ISO	International Organization for Standardization.
KVKK	Turkish Data Protection Law (*Kişisel Verileri Koruma Kanunu*).
PCI-DSS	Payment Card Industry Data Security Standards
P	Page.

PIL	Private International Law and Procedural Law.
POS	Point of Sale.
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCO	Turkish Code of Obligations.
TCC	Turkish Civil Code.
UETA	Uniform Electronic Transactions Act.
UCC	Uniform Commercial Code
UK	The United Kingdom.
US	The United States of America.
USD	United States of America Dollars.
WAP	Wireless Application Protocol.
QEC	Qualified Electronic Certificate.

LIST OF FIGURES

ABSTRACT

This research aims to examine smart contracts and its legal situation together with the promises, advantages and disadvantages of smart contract technology. In this context, smart contract is evaluated as a contract and legal requirements for contract conclusion and reflection of contracting rules to the smart contracts are examined in detail.

This research concludes with four main sections, first section includes the evaluations of backbone technology in smart contracts, distributed ledger, and decentralized feature, verification procedure in smart contract systems. The second section presents the evaluation of contract conclusion principles, digital contracts and governance of smart contracts in that context. In the third section, technical and practical obstacles in smart contract systems, smart contract use cases, potential advantages and disadvantages are reviewed. In the forth section, affects in legal practice realm evaluated and potential issues in information security, data protection compliance are discussed.

Keywords: Smart Contracts, Blockchain, Distributed Ledger, Decentralized System, Digital Contracting, Governance

ÖZET

Bu araştırma ile amaçlanan akıllı sözleşmelerin hukuku durumunun incelenmesi ve akıllı sözleşme teknolojisinin pratik hayatta vaat ettikleri, avantaj ve dezavantajlarının değerlendirilmesidir. Bu kapsamda, akıllı sözleşmelerin mevcut bilinen anlamda sözleşmesel niteliği incelenmiş, fiziksel sözleşmelerin kurulması için aranan şartlarının akıllı sözleşmelerde ne şekilde bulunabileceği hususu ayrıntılı bir şekilde ele alınmıştır.

Araştırma dört ana kısımdan oluşmaktadır. Birinci bölümde akıllı sözleşme sisteminin altında yatan teknoloji incelenmiş, bu kapsamda dağıtık defter teknolojisi, merkezi olmayan sistem özellikleri ve akıllı sözleşmelerdeki verifikasyon, onay prosedürü mercek altına alınmıştır. İkinci bölümde sözleşmelerin kurulması kuralları, dijital sözleşmeler ve akıllı sözleşmelerin yönetişimi incelenmiştir. Üçüncü bölümde akıllı sözleşme teknoloji kullanılırken karşılaşılabilecek teknik ve uygulamaya yönelik engeller, pratik hayatta akıllı sözleşme uygulama örnekleri muhtemel avantaj ve dezavantajları incelenmiştir. Dördüncü bölümde hukuk uygulaması alanındaki etkileri ve bilgi güvenliği, kişisel verilerin korunması bakımından karşılaşılabilecek sorunlar tartışılmıştır.

Anahtar Kelimeler: Akıllı Sözleşmeler, Blokzinciri, Dağıtık Defter, Merkezi Olmayan Sistem, Digital Sözleşme Kurulması, Yönetişim

INTRODUCTION

The recent attention paid to cryptocurrencies has aroused people's interest in blockchain technology. Bitcoin, in particular, has created the momentum for such interest[1]. Thanks to the attention Bitcoin has attracted, people are learning about the benefits of using blockchain technology and its future potential. Blockchain has the potential of renovating different business models, mainly in the finance realm. Not only digital currency transactions but also different operations, such as keeping (storing) huge volumes of data, funding transactions, and creating smart contracts, are the promises of the system.

In the Nordic countries, around 95% of the people are no longer using cash in their daily, nor in their business transactions. Moreover, this cashless society approach is spreading around the globe. This requires more practical and more secure systems that can work with a fast-paced evolving digital society. Financial technologies have been seen as a remedy for the demands of society. Together with the technology itself, there are fundamental components that need to be developed simultaneously: legal regulations, investments, incentives, and evaluation of the demands, digital substructure, and education.

The Internet is a rapidly growing phenomenon, thus society is keener than ever to use new technologies that work via the Internet. This being the case, regulating the Internet is not easy since it does not have territorial boundaries. This creates problems in determining the jurisdiction on the cases which arise from activities taking place in cyberspace. Smart contracts also share this space and can move from jurisdiction to jurisdiction freely. As they are being operated on online platforms (the Internet), smart

[1] Chris Reed, Umamahesh Sathyanarayan, Shuhui Ruan, Justine Collins. Beyond Bitcoin – Legal Impurities and Off-Chain Assets. Queen Mary School of Law Legal Studies Research Paper No. 260/2017. p2. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3058945.[30April2019].

contracts also have a tendency to be used illegally, leading to activities such as gambling (for some countries) or selling drugs[2].

In this thesis, smart contract technology is analysed together with its underlying blockchain technology; how it works technically, its components, as well as its existing current and promising practices. Moreover, future potential use cases of the smart contract are discussed. Concerning the legal aspect, the smart contract's definition as a contract is investigated via analyses of existing contracting principles and how they can be applied in terms of smart contracts.

This thesis aims to explain the idea behind smart contracts and understand their benefits and, most importantly, how to make them work in practice. Therefore, the analyses herein are shaped around those important questions;

1. What is a smart contract? How does it work technically?
2. What is required to make smart contracts?
3. Where do smart contracts stand in relation to existing contracting rules? Can existing digital contracts help us to understand smart contracts?
4. What are the potential benefits of smart contracts? What are their real-life uses and future promises?
5. What are the reasons that stand in the way of adapting this technology? How and when can smart contracts find real practise?
6. What are the downsides or risks of smart contracts in the technical and legal sense?

This thesis is divided into four sections (besides the Introduction and Conclusion) in order to analyse in detail smart contracts in the light of the above-mentioned questions.

In the first section, an attempt has been made to describe smart contracts together with blockchain technology. This includes an analysis of their public, distributed ledger, and decentralized features, together with their relationship with centralized bodies, as well as

[2] Finck, M. (2018). Blockchain Regulation and Governance in Europe. Cambridge: Cambridge University Press. p20.

intermediary bodies and the new phenomenon of oracles. Bitcoin is also reviewed in this section as the most common use case of blockchain technology. Moreover, digital identity is covered, together with electronic signatures and finally, the verification scheme of blockchain technology.

The second section concludes with an analysis of contract conclusion rules, including certain main principles of contracting under Turkish law. Existing digital contracts that are being used in practice and their legal acceptance is investigated. In this section, smart contract acceptance as a legal contract is analysed and, finally, how current contract rules interact with smart contracts is examined.

The third section covers the practical and technical challenges of smart contracts and blockchain technology, together with their advantages and disadvantages. Also, practical cases studies regarding this technology are included in this section.

The fourth section looks into the review mechanism; lawyers practises and the legal position and the information security and data protection principles are visited and their appearances in blockchain systems are analysed.

Eventually, in the concluding analysis of this thesis, the potential and main issues of smart contract is put in a nutshell and areas that need further research are mentioned.

SECTION I

1. What is a Smart Contract?

Smart contract as a term which was first used by Nick Szabo[3] in 1997. In this term, he basically addressed the use of a distributed ledger to store contracts. Smart contract describes self-executing legal contracts created in digital platforms. In other words, the terms and conditions of the contracts are embedded into the codes of a smart contract program. Smart contracts are operated as computer programs located within the blockchain. This concept was discovered by computer scientists and cryptographers who combined many new and interesting algorithms to create a wide variety of new protocols[4].

In 2014, the first smart contract system was established by a company called Ethereum. In this system, which is basically a decentralized computing platform[5], smart contracts work using the Turing-complete program principles that are mined by participants called miners who are encouraged with rewards for completing transactions in Ether form. Further information regarding Ethereum and mining procedures will be provided in section 1.3 and 1.4 of this thesis. Miners can be the nodes[6] that participate in a consensus even though they are not entirely the same. Miners gather transaction information, add it to the blocks, and transmit them to the nodes[7]. Nodes keep the copy or copies of the data in the blockchain system and verify the new block that they have received from other

[3] Wikipedia. (2015) Available at: https://en.wikipedia.org/wiki/Nick_Szabo. [March 2018].

[4] Singh, R. (2017). Computing Platforms for Distributed Energy Resources and Transactive Energy: Case Studies Using Volttron and Smart Contracts. Washington State University.

[5] Cardozo Blockchain Project. (2018). Smart Contracts & Legal Enforceability. Research Report#2. P5.

[6] Alex 'Sandy' Pentland, Oz Nathan, Guy Zyskind. Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE CS Security and Privacy Workshops. p2. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163223.[27March2019].

[7] Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh. (2018). Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers. *Richmond Journal of Law & Technology*, Volume25(1). P6. Available at: https://jolt.richmond.edu/files/2018/11/Michelsetal-Final-1.pdf. [24 April2019].

nodes in the P2P network[8]. Especially in permissionless systems, this activity is not restricted to a node; everyone can be a node by downloading the system. However, it is not easy technically to do that since downloading and storing the system needs a great deal of bandwidth and storage capacity: around approximately 145GB of free space[9]. Users, on the other hand, people who enter the system in order to trade digital assets like Bitcoin and Ether, need to join the system by running the open source code on their hardware[10].

It is critical to understand the nature of the smart contracts as a first step; smart contracts do not look like contracts people use in real life. From a technical point of view, a smart contract is created as a computer code stored on a decentralized Ethereum blockchain. This system is executed by a network over the blockchain with the functions of: reading other contracts, transferring ether to other contracts in the distributed ledger or through a node, doing computations, and performing various decisions based on people's evaluations[11]. Ethereum is the most popular platform which has been created to support smart contracts since it is the first one, but it is not the only one. Smart contracts can be set up over a range of protocols or platforms, which can be listed as follows: Codius, BitHalo & BlackHalo, BurstCoin, Ethereum, and Counterparty[12]. Of these, Ethereum is still today the most famous platform for creating smart contracts. Below is a view of a text written in a smart contract on the Ethereum platform[13].

[8] (Bacon, Michels, Millard & Singh 2018). p21.

[9] (Bacon, Michels, Millard & Singh 2018).p20.

[10] (Bacon, Michels, Millard & Singh 2018). p18.

[11] Nikolic, I. Kolluri, A. Sergey, I. Saxena, P. and Hobor, A. 2018. Finding The Greedy, Prodigal, and Suicidal Contracts at Scale. Available from: https://ui.adsabs.harvard.edu/#abs/arXiv:1802.06038. [15 March 2019].

[12] Walsh, D. 2015. CRYPTORIALS. *A Beginner's Guide to Smart Contracts*. Available from: http://cryptorials.io/a-beginnersguide-to-smart-contracts/. [20 April 2017].

[13] Savelyev, A. (2016) Contract Law 2.0: Smart Contracts As the Beginning of the End of Classic Contract Law. *Higher School of Economics Research Paper*. WPBRP71/LAW/2016. Available at: SSRN: https://ssrn.com/abstract=2885241.[19AMrch2019].

Figure 1: Sample Smart Contract Code Text

```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

  /* Initializes contract with initial supply tokens to the creator of the contract */
  function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

  /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```

This clarifies how smart contracts are basically the computer codes created using blockchain technology. They, per se, are merely a computer code, and as such, they may not give the sense of being a physical contract. From the technical point of view, this is true; more specifically, the contract terms and conditions cannot be seen as in a hard copy contract since they are embedded in the code. However, people can track the process when the system is executing in accordance with the smart contract terms as agreed. In smart contracts, contract terms and conditions are not likely to be listed in detail as in physical contracts. Contractual obligations, such as covenants, obligations and sanctions (penalties, compensation, service suspensions, etc.) are deemed to be under the control of the system rather than being subject to parties' actions, demands and claims. For instance, in the case of a failure to perform the payment obligation on time, the system automatically takes the necessary action in response according to the smart contract terms, without being subject to human intervention[14]. Despite this is being the case, human interaction may be needed in some cases, and such circumstances will be re-visited in Section II in more detail.

[14] Schulpen, R. (2018). *Smart contracts in the Netherlands A legal research regarding the use of smart contracts within Dutch contract law and legal framework*. Master. Tilburg University. 16-17. Available at: http://arno.uvt.nl/show.cgi?fid=146860. [20April2019].

Smart contracts, in a technical sense, require actual contract terms to be embedded in the system. This may sound slightly confusing and maybe excessive from a legal aspect. However, given the extreme growing speed of technology, it is not hard to imagine and make it real. Contracts including acutely chaotic terms and amounting to 250 pages are not ideal for the smart contracts system. At least, in the beginning, parties might need to write down terms and conditions before implementing the smart contract system, and those details will eventually be embedded into the system. Detailed liability allocations might be needed, but the system's existing position does not really answer to this at the moment[15]. Although not all contractual obligations can be easily translated into smart contract language, obligations that are binary per se[16] (e.g. asset transfers) can be executed easily by smart contracts. However, the system cannot measure abstract requirements, for instance acting in good faith or as a prudent merchant[17]. Conflicts arising from these kinds of abstract notions will be subject to the relevant legal principles. The following figure illustrates an example of a smart contract-driven transaction and helps to explain the binary nature in obligations[18].

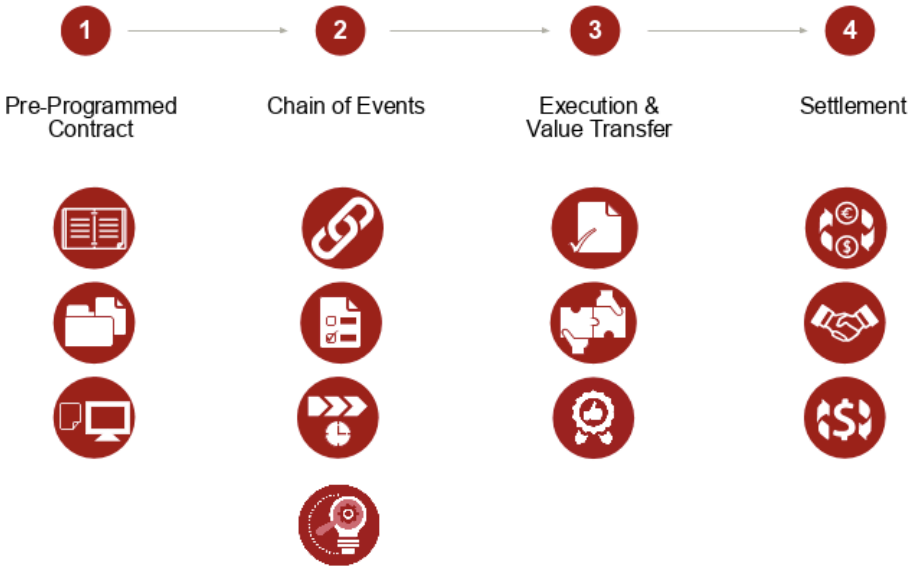
[15] (Finck 2018). p20.

[16] De Filippi, P. and Wright, A. 2018, *Blockchain and the Law The Rule of Code*. Cambridge, Massachusetts: Harvard University Press. p77.

[17] (De Filippi & Wright 2018). p77.

[18] Bacon, L. Clyde & Co. (2019). Legal implications of blockchain technology and how it will shape the work of future lawyers. *Blockchain and the Law Conference King's College London.*

Figure 2: Smart Contracts Basic Working Structure



- **Pre-Contract, Programming Phase;** as a first step, parties get together and set up the terms and condition of the transaction. Once they are settled and approved by all the parties of the transaction, those terms will be translated into code.
- **Action Chains;** in this phase, the obligations agreed in the first phase commence to be implemented by the code.
- **If-this-then-that phase;** once the system executes the necessary actions for the transaction, the smart contract takes the counter actions; this might be transferring the value (e.g. digital money, crypto currency, ether etc.).
- **Settlement;** in this phase, contractual obligations are performed and stored on the blockchain.

In the smart contracts system, the contract terms can be written in programming languages and embedded in a code, as in Ethereum Solidity[19], but basically not in legal

[19] (De Filippi & Wright 2018). p74-75.

prose as people are used to. There are different programming languages, such as C++, Go, Python, and Java. In most cases, smart contracts are developed with the help of these programming tools. The codes (executed in the distributed ledger system) are used to create the necessary environment for smart contracts. This also aims to set the structure of a smart contract, covering the obligations of the contracting parties, compensations, and penalties as in physical contracts. The freedom of contract principle under Turkish law, which is analysed in Section II of this thesis, can constitute an approach adopted in terms of physical contracts and has the potential to ease the understanding process of the smart contract, especially in terms of the application of the existing legal rules.

1.1. Trusted Public Ledger

The Trusted Public Ledger (also known as the Distributed Ledger) is not so new as a decentralized phenomenon; this system has been in use for quite some time. A distributed ledger is not the same in decentralized systems. A distributed network or distributed system does not have to be decentralized; the most common distributed systems are Dropbox, Google Drive, Onedrive, etc. Basically, cloud systems are based on distributed ledger systems. This means there are multiple copies at various different locations. The distributed approach is not new, and people rely heavily on them in practice. Smart contracts will use this system as well; however, the main difference is in using Blockchain instead of having a single party (such as Google, Facebook, etc.). In the blockchain system, the controllers will be the users. This is where the decentralized approach features: the idea of removing central control.

A distributed ledger is a ledger that is kept and distributed in a P2P network; a blockchain constitutes a distributed ledger in a decentralized format[20]. If a blockchain is centralized, it cannot be a distributed ledger since it is not distributed and controlled centrally.

In smart contract systems, distributed ledgers enable people to transfer digital assets of value (digital data) such as digital money (e.g., bitcoin and ether) without any need of an

[20] (Bacon, Michels, Millard & Singh 2018).

intermediary institution, and also store them, using the Internet[21]. In other words, it contains the data record of transactions between individuals in the system. In other words, *distributed* means everybody has a copy of the data.

In public ledger systems, individuals are not allowed to amend the system for their benefit. This is the reason why it is deemed *trusted*. For instance, Bitcoin technology is created based on the trusted public ledger mechanism in which everyone can access and download the software system; therefore, it is public. Bitcoin can be used without the requirement of an identification procedure. Everyone can start to use the software system after installing it.

The system has its wallet application which enables people to operate transactions with Bitcoin and which comes with the instalment of the system. The wallet works with a public and private key (that can be created through a public key infrastructure ("PKI")) and the private key is used for the transfer of bitcoin. The personal data of the owner is not shown to the other users, but the transactions can be seen publicly. As the name infers, the private key is kept strictly private and the public is public since it represents the person owning the private key[22]. The most important feature of the public key is that it is being used by the bitcoin network for verification of transactions[23]. Users can decrypt the blocks (that are encrypted with the public key) by using their private key, or the other way around and, most importantly, the decryption of the data in the block through using the public key shows that it was encrypted in the beginning; this means this data was sent by a reliable person owning a private key[24].

[21] Morrison, S. (2019). Smart contracts for enforcement of Islamic finance deals. *Journal of International Banking Law and Regulation*. Volume34(4). p145-151.

[22] (Bacon, Michels, Millard & Singh 2018). p14.

[23] (Savelyev 2016).

[24] (Bacon, Michels, Millard & Singh 2018). p14.

Mathematical principles that make the system work also make it very difficult to change. Unilaterally, people cannot amend it[25]. This will be demonstrated in section 1.4 below, with examples in detail. There is a further way used in key cryptography to prove the authenticity of a message which existed before crypto currency. It seems possible to place random messages within the private key. This is an example[26] written on Ethereum;

Figure 3: Private Key Code Text

```
web3.eth.sign(web3.utils.sha3("Thanks for reading the article.
Cheers Axel"),
"0x38588822Bea476d5e1D56cFC9CE9781Fe5262196").then(console.log)
> 0x027d1dd45ab0eeee5803079086679a70d444a2d4ea7e8db221894977eabf8bfc
7486d6a9413e4a9aeddccf851ba7c2ea81835576b0afabbcfd62493ff0924ff400
```

The ledger provides better storage opportunities for the users; contracts that are recorded in the ledger have long-lasting storage and log events[27]. This feature has huge potential in saving companies from archiving expenses and creating a risk-free environment against the potential breaches that might occur in archiving companies[28].

[25] Fairfield, J. (2014). Smart Contracts, Bitcoin Bots, and Consumer Protection. *Washington & Lee Law Review Online.* Volume 71(2) p.36. Available at: http://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3. [26 Jan. 2019].

[26] Axel Hodler. (2017). Proving ownership of a cryptocurrency. Medium. Available at: https://medium.com/yopiter/proving-ownership-of-a-cryptocurrency-86a96f2c52b. [10 March 2019].

[27] Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., HAL archives-ouvertes.fr. (2016). Formal Verification of Smart Contracts: Short Paper. ACM Workshop on Programming Languages and Analysis for Security. *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security*. Available at: https://hal.inria.fr/hal-01400469/document. [19 March 2019].

[28] There are other firms also providing services based on the distributed database technology, such as R3 consortium's Corda; R3 (R3CEV LLC). This firm is basically designing blockchain platforms for the business needs of the institution from a wide range of fields from finance, software firms.

1.2. How Does Blockchain Work?

In this thesis, blockchain will often be referred to when discussing technical aspects and case studies since it is the underpinning technology in smart contracts. Blockchain technology is the backbone of smart contracts and, in the majority of cases, therefore the working principles will be similar between smart contracts and blockchain. Blockchain is a relatively new concept and it still does not have a clear definition. Basically, it is a peer-to-peer operating platform that enables users to manage their transactions through the power of overseeing all the phases of a transaction[29]. This system has three main facets[30]: 1) data can be stored in blockchain; 2) technically, it is hard to amend the system after implementation; 3) data is approved and copied by the nodes in the ledger and stored in the system. These three components will be the main focus of this thesis.

First of all, blockchain can be essentially created in two different formats: private or public[31]. In private blockchain, although the system is created on a decentralised platform, the nodes comprise a limited group of people, as in Ripple. However, in public systems, that are also called "permissionless"[32], the nodes do not comprise any particular group of people or are not fixed in any particular location; the users can be from different parts of the world. Bitcoin and Ethereum are the biggest representatives of the public permissionless blockchain. These two systems will be analysed in sections 1.3 and 1.4 below. The permission-free feature enables anyone to join the Bitcoin as a miner[33]. However, since this requires a reliable and strong electricity supply and a powerful computer, in real life not everyone may easily participate in a blockchain system, even though they are permissionless and public.

---

[29] (Cardozo Blockchain Project 2018). P4.

[30] Christopher Kuner, Fred Cate, Orla Lynskey, Christopher Millard, Nora Ni Loideain and Dan Svantesson. (2018). *International Data Privacy Law*. Volume8(2). P103.

[31] David Meyer. (2017). Blockchain technology is on a collision course with EU privacy law. Iapp. Available at: https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/.[10 April2019].

[32] (Meyer 2017).

[33] (Kuner, Cate, Lynskey, Millard, Loideain & Svantesson. 2018).

In blockchain systems, the idea is to eliminate the third party verification step (I am still not talking about clearing off the banks from the transactions, which will be almost impossible in the near future), similar to the approach used in the Napster system. The similarity is primarily based on the idea of keeping data in the computer of the person who downloaded the system as a "peer-to-peer file sharing tool"[34]. This system allows users to seed and make the data available to be shared between the other users participating in the system. In the blockchain, each user keeps the data in their computer protected by a password, and these records are kept as a chain. These chains are sorted consecutively and accumulate into a block. This sortation and accumulation across the chains and block constitutes the verification of that block consecutively and amounts to the blockchain[35] (the verification process is examined in section 1.10 in detail.) Each piece of data has a specific free-from-interchange stance in the chain, and this is how a chain is validated and how the blocks are created.

The longer the chain, the more the valid the blocks. The length of the chain also demonstrates the admissibility of the block because if the chain amount is high, this basically means that more people are involved and the blocks become more rigorously verified. This also motivates users to be straight and reliable while creating the chain since admissibility of the system relies on them. As the chain becomes longer, its trustworthiness is guaranteed since the length of the chain proves that the consecutive transaction steps have been seen and approved by each user. The length of the chain also demonstrates proof that it is seen, approved and secure. In other words, the nodes are making system secure and this may lower the attacking attempts the network. The nodes eliminate the risk of cyber-attacks while creating a relatively long chain. This is the main feature that makes the Blockchain technology trustworthy and allow it to be labelled incorruptible[36].

[34] (Finck 2018).

[35] (Cardozo Blockchain Project 2018). P4.

[36] Maclean, F. (2017). Governing the Blockchain: How to Determine Applicable Law. *Butterworths Journal of International Banking & Financial Law*, Volume. 32(6), 359-361.

This whole process makes the system resistant to intervention. In other words, it is almost impossible to amend the data sitting in the blocks, and this is referred to in different terms such as 'tamper-proof' and 'immutable'. At the time the blocks are consecutively and connectively created (before and after the blocks are chained to each other) and the data is verified, each step is recorded in each user's computer with a time stamp. In practise, it is not easy to reach every miner/user in the system and change the data; that is why it is considered tamper-proof or immutable. As a result of being a public system, a great number of miners might be involved, and these miners cannot always be identified[37]. This might amount to legal problems in terms of contractual liability claims, and data protection compliance and liability as well. These matters will be analysed below in detail[38]. These concepts are reviewed in sections 2.9.3 and 3.6.1 respectively.

1.3. Ethereum

Since it is a widely used phenomenon, it will be useful to discuss Ethereum's working principles and why they were created in order to explain smart contracts more clearly. Ethereum provides a great practise tool to help people to understand and to explain the working mechanisms of smart contracts, especially to non-technical people. Ethereum has become famous for its technical feature of providing a substructure for smart contracts based on blockchain technology. This is the Ethereum Virtual Machine (EVM), which basically is a form of blockchain technology providing an open computing platform[39]. The EVM code was created to execute smart contracts via managing and transferring ethers. This also enables the system to work (especially advantageous for global transactions) based in one place with a local contract basis[40]. This means the system can adduce and notify the other contracting parties (contracts in the system, if it is

[37] (Kuner, Cate, Lynskey, Millard, Loideain & Svantesson 2018).

[38] *See* section 2.9.6 and section 6.8.5.

[39] (De Filippi & Wright 2018). P3.

[40] (Nikolic, Kolluri, Sergey, Saxena, Hobor 2018).

the case) while the transaction is running. Because smart contract-based transactions have been launched, the system runs automatically as the parties' representative[41]. In other technical prose, Ethereum works on a blockchain system that has a 'Turing complete contracting language', allowing the creation of complicated contracts automatically[42].

The digital currency in the Ethereum system, namely the Ether[43], is mainly created for the purpose of motivating developers and programmers to create smart contracts[44]. As in blockchain logic, for the system to work new blocks and chains need to be developed. The Ethereum system helps motivate developers to create these new blocks and chains. . In blockchain technology, the system basically originates in the idea of blocks that are mined at a permanent speed. Therefore, it is possible to create a myriad number of blocks quickly, which leads to people facing computational and electricity expenses for mining[45].

The reward system has been found to encourage people to continue mining despite the energy consumption that it requires. For example, Ethereum has been used in gas distribution transactions and, as in the blockchain system approach, individuals who create a block have the right to gain a reward, i.e., to gain Ether in alignment with a specified gas price[46]. In this example, the fees can be measured in gas units and the execution fee is usually paid by the system. The system relies on users continuing to create blocks, and with the each block they are able to claim their fee converted to Ether at a specified gas price. This price is not easily affected by market fluctuations. However,

[41] (Cardozo Blockchain Project 2018). P7.

[42] (De Filippi, & Wright 2018). P28-29.

[43] (De Filippi, & Wright 2018). P28-29.

[44] (Bhargavan, Delignat-Lavaud, Fournet, Gollamudi, Gonthier, Hal 2016).

[45] (De Filippi, & Wright 2018). P28-29.

[46] (Bhargavan, Delignat-Lavaud, Fournet, Gollamudi, Gonthier, Hal 2016).

even though the price is not fixed, miners are able to amend it subject to the market ether value[47].

Ethereum suggests executing even complicated contract procedures on smart contracts, especially concerning financial transactions or insurance contracts. Also, Ethereum can be used for transactions involving digital storage leasing, computational power, and communication bandwidth[48].

1.4. Bitcoin

While explaining how blockchain works, I must mention Bitcoin. It is a very well-known application in practice and, thanks to Bitcoin, society has become aware of the blockchain system and its potential, despite the fact that its history actually goes back to the late '70s[49].

The system is based on mining cryptocurrencies through blockchain, the record of this mining procedure being stored in the distributed ledger. Once having installed the software system, users are able to mine (this means *produce* in this structure) Bitcoin as a reward in response to solving a complex mathematical problem. This also helps in the verification of transactions performed with Bitcoins[50]. The verification method in Bitcoin is called 'hashing'[51], and it has a cost and this is where Satoshi Nakamoto[52] developed the idea of giving people coins. While creating Bitcoin, Satoshi Nakamoto wanted to

[47] (De Filippi, & Wright 2018). P29.

[48] Omohundro, S. (2014). Cryptocurrencies, Smart Contracts, and Artificial Intelligence. *Newsletter AI Matters,* Volume1(2), P19-21. Available at: https://dl.acm.org/citation.cfm?id=2685334. [10April 2019].

[49] (Omohundro 2014).

[50] (Savelyev 2016).

[51] "The network timestamps transactions by hashing them into an on-going chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work." *See* (Nakamoto 2008).

[52] *See* (Nakamoto 2008).

motivate people to generate blocks in the system by giving them digital money. In Bitcoin, creating blocks means mining coin in a blockchain system[53], and since mining Bitcoin consumes a great deal of electricity and CPU power, Nakamoto wanted to motivate miners by giving them Bitcoin for each block they created. "A single Bitcoin transaction requires an estimated 200kWh of energy compared to around 0.01kWh per Visa transaction"[54]. Blocks are produced continuously in a graduating manner; this is a challenging point of the blockchain system. In the case of a huge number of blocks being created too quickly, computational and electricity expenses rise.

As based on blockchain ledger technology, each time someone transfers Bitcoin to someone else, an encrypted record of the transaction is sent out to all the miners in the Bitcoin network for verification and notification. Every time a new block is confirmed valid (this is subject to the majority of the users' approval), it is added to the Blockchain database. Each block has to be arrayed consecutively; this allows the previous block's hash to be seen and confirmed. This verification is not always reliable; for instance, when the user number is low the majority will be low and it will not constitute a reliable verification. In the Bitcoin system, it is possible for everyone to join[55] the network by creating a public key. This key enables users to connect to the network with an identifying private key[56].

In order to transfer Bitcoin to another user, first of all the user sends an electronically signed notice to the network giving the information of the recipient's public key and the amount to be transferred. Next, the network checks and confirms the availability of the account for the requested transfer. The transfer order is recorded to the distributed ledger

[53] (Cardozo Blockchain Project 2018). P5.

[54] (Bacon, Michels, Millard & Singh 2018). P26.

[55] This is not very applicable in real life where not everyone has strong computers and power to mine.

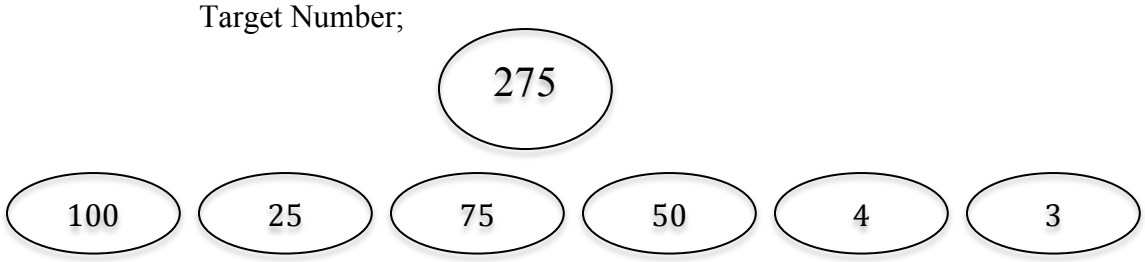
[56] (Nakamoto 2008).

installed on each user's device. This process is being seen by the others in the network and, therefore, the procedure is deemed fully public and, accordingly, incorruptible[57].

In the Bitcoin system, verification depends on the majority of the users; for instance, if amongst 50 users of a block, 26 of them is accept it as accurate, this block is considered valid; 51percent approval is needed. If that proportion cannot be reached, the network can break. To be more precise, miners participate in a consensus, which means when someone sends a transaction, everyone can verify whether it is correct or not, but no one can confirm that. So, there is the Proof-of-Work step; this involves solving a mathematical puzzle, and if a miner solves a puzzle that everyone can verify has been solved correctly, this means he has not cheated. A simple puzzle is demonstrated below in figure 5. This puzzle requires recreating the first number using any combination of the numbers listed on the second row. There are so many different solutions, everyone can verify different ways of solving that puzzle in any way.

The idea behind Proof-of-Work is also to make it as hard as possible to mine new blocks in order to lower the motivation to attack the system[58] This is because in permissionless systems, mining and joining the network is not restricted, and systems might end up with thousands of miners, which makes it difficult to protect the systems from ill-intentioned action.

Figure 4: Sample Proof of Work Puzzle



Direction; Use four standard operations (addition, subtraction, multiplication, division), using the numbers listed in the second row only once, to reach the Target Number.

[57] Mehta T. (2017). Smart Contracts. Dentons Articles. Available at: https://www.dentons.com/en/insights/articles/2017/june/29/smart-contracts.[20April2018].

[58] (Bacon, Michels, Millard & Singh 2018). P23.

Sample solution: 100+75+(4.25) = 275. Equals 12.5 Bitcoins.

This is just a demonstration; real puzzles are hard to solve and easy to verify. The verification system is generally based on solving a puzzle. Miners do not have to trust each other but they need to verify the blocks. And finally, the miners' motivation to solve these challenging puzzles is getting a reward at the end.

Clearly, the system works based on an incentivizing approach. However, miners might not always receive their reward: for instance, in the case where two miners create the same block as in two people answering the same puzzle at the same time. A distributed network is not under one person's control; therefore, there is no controlling party to decide what to do. In this case, miners need to create the next block that comes after the one that they first created as soon as they are aware of the situation. As the rule is that the longest chain wins - in other words, the longest chain with the most proof of work wins - users need to create the next block as soon as possible. The fastest one wins.

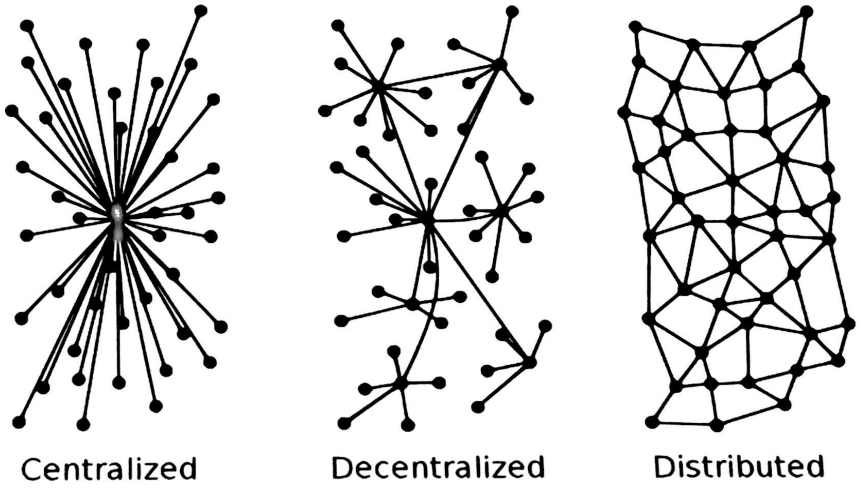
Even though Bitcoin has made blockchain technology very famous, there are now a number of replications of this system. There is a software program for smart contracting called BitHalo. It is combined with BlackHalo, and users can switch via this program to and fro between contracting with Bitcoin and contracting with Blackcoin, thus providing a multicoin smart contracting experience. The program also conveniently serves as a multicoin wallet. This service provided by BitHalo and BlackHalo has paved a new way in using cryptocurrency as a double deposit method. In the system, both parties have to deposit an amount of cryptocurrency before entering into a contract. The program sets an expiry period. If the parties do not want to proceed and agree on the transaction before the expiry time, the system blocks the account and makes the cryptocurrencies non-negotiable. The idea behind this is to make sure that the parties do not breach the contract because if one cheats, the system automatically burns the asset. In most cases, this is digital money, so cheating means risking the cryptocurrency and the potential gain[59].

[59] (Walsh 2015).

1.5. Decentralized Feature

Blockchain technology provides a system for people to be able to "codify, decentralize, secure and trade just about anything."[60]. In almost every study regarding this technology, the decentralized feature of blockchain is being encouraged. However, the concept of *decentralized* has not been fully clarified. Here is a very basic diagram[61] that the author considers helpful for beginners in comprehending the system, especially those beginners without a technical background.

Figure 5: Basic Diagram for Centralize, Decentralized and Distributed Systems



Decentralized is often confused with distributed ledger, which is a very understandable and fair mistake. A decentralized system is not far from a distributed ledger, conceptually. Decentralized protocols are created to enable asset transfers, manage interactions, and store data within blockchain systems[62]. It also makes it possible for

[60] Hertig, A. (2014). *How Bitcoin Could Decentralize the Courtroom*. Motherboard. Available At: https://motherboard.vice.com/en_us/article/vvb79d/code-as-law-how-bitcoin-could-decentralize-the-courtroom [10Jan 2018].

[61] (Clyde & Co 2019).

[62] (De Filippi & Wright 2018). p29.

people to control access to the data stored in smart contract systems. This concept promises 'zero down-time' and sustainability of the system in cases where the miners leave[63]. Developers believe that "pooling bandwidth and storage resources"[64] will have the power to take a place in online services where people choose decentralized systems as coordination and storage services instead of leasing spaces from internet giants such as Amazon, Microsoft, and IBM[65].

The decentralized feature has been questioned and it seems that it is not quite fully accepted. Most of the miners are thought to be located in China at the moment and this makes people naturally question how distributed and decentralized the system is (this is the case for Bitcoin)[66]. Having the majority of hash power puts them in charge of Bitcoin power and they can take down the Bitcoin system any time they want to. This seems likely to be the case for some time to come because a great deal of power is required to run such a system, almost equal to four times the power of what Google has at its disposal[67]. So, the decentralized aspect is not yet fully satisfactory in real life due to the level of technology available at the moment.

It is not easy for society to accept so quickly that they will not need any third party institution if they implement blockchain technology. This concept has many nuances, and although it promises an environment with no intermediary, this is not likely to happen in the near future. In almost every commercial transaction, a party is obliged to make a payment; regarding this, people mostly use banks to transfer money to the other party's account. Smart contracts do not force people to change this practice of money transfer via banks. However, it offers a system that is more transparent than banks. Nobody really knows what banks genuinely do with their money, so for those who are not comfortable

[63] (De Filippi & Wright 2018). p30.

[64] (De Filippi & Wright 2018). p30.

[65] (De Filippi & Wright 2018). p30.

[66] Volt P2P Blockchain Delivery Platfrom Presentation. Blockchain and Smart Contracts in General. King's College London Legal Tech and Emerging Technologies Conference 2019.

[67] (Volt 2019).

with this system, blockchain can be an alternative. The parties can still enter into a blockchain-driven smart contract and agree on transferring the money via banks or other payment systems; for instance, in terms of a supply chain transaction, once the goods are delivered in accordance with the contract terms, the system can automatically notify the bank to transfer the money. For this kind of system to work, the notification system with the banks may be re-regulated for clearance. I also believe that banks and payment system service organizations will work more to cope with this system rather than against it in the future.

In practice, banks transfer money from one account to another with a written and signed order, either electronically or physically signed. The concept is not very far from the approach used today in our daily transfers; for example, people make their rent payments through bank applications, as well as official payments such as taxes, electricity bills, phone internet service fees, etc. In smart contract-driven transactions, the money transfers can be monitored via banks or other payment systems that have been approved by the parties; in a bank transfer scenario, once the delivery of the goods is done, the system might automatically create a payment order with an electronic signature on it and notify the bank. In most jurisdictions, internal and external money transfers are generated based on a valid order from the account owner. This process can be written into the smart contracts' software code. In this kind of ecosystem, parties can choose how they wish to operate the transactions. Parties can designate a concept 'consensus by authority' that can be an outsourced third party[68].

For instance, if a transaction is set up based on transferring crypto currency (or even a stock share[69]) instead of using a bank or another payment system, in this scheme, parties will not need an intermediary body, such as a bank, to oversee this transfer. If parties would like to send crypto currency to each other, they are free from intermediaries such

[68] (Kuner, Cate, Lynskey, Millard, Loideain & Svantesson 2018).

[69] (De Filippi & Wright 2018). p30.

as banks and payment institutions. In blockchain-driven projects, the parties are able to customize the system in accordance with their business needs.

1.6. What Does Centralized Mean?

Within this part of the study, I would like to mention the *centralized* concept, which is the common practice in current money transfers. The consumers and business owners are the fundamental stakeholders of the daily transactions. Every day, innumerable transactions are being carried out between different parties and in almost every one of them, those stakeholders and different parties use banks or payment systems. In payment systems, the consumers are able to choose and use their authorized banks or payment institutions to carry out online shopping. In terms of an online transaction, when the seller receives an order from the consumer, it notifies the related bank or payment institution to make the payment for the designated consumer. This basically is the centralized structure widely accepted in practise[70].

In the existing money transfer systems, especially those executed in various bank transactions, banks have to verify the information of the sender, or the recipient's records at the other bank, before completing the transaction. The banks of both parties need a third party institution to confirm the information that the banks have in their records. This verification mechanism usually costs large sums of money since it requires the involvement of different parties, even for just one small transaction[71]. In the UK and the EU, the banking approach is different to that in Turkey. For example, there is an open banking approach in the UK that is based on the standards defined in a more detailed approach aimed at avoiding system risk and creating a more secure environment[72].

[70] (De Filippi & Wright 2018). p62.

[71] (Nakamoto 2008).

[72] Brazell, L. (2018). *Electronic Signatures and Identities: Law and Regulation.* Sweet & Maxwell, 2nd ed.

In the EU, during banking transactions, a password is given to the third party for verification. This is considered highly risky. In the UK, consumers complete the verification with the related third party, and this party goes to the banking system without using any individual's password or username information[73]. However, in China, there is a completely different approach. Basically, the government has power over technology companies to be able to track its citizens.

In China, the state is getting ready to enter into a national reputation system to evaluate the economic and social reputation of the citizens and companies; this is called the social credit system[74]. This system has been developed by the Chinese Government based on mass surveillance forms. These use big data analysis technology and are intended to be fully implemented by 2020. It is still not quite clear who will run the system; it has been suggested it could be run partially by city councils and partially by private technology companies holding personal data. The working principle of this system is being kept highly confidential. However, the first examples of what might cause bad scoring are listed as bad driving, smoking in non-smoking zones and posting fake news online.

This system is already being experienced in China, and people are facing sanctions as a result of their bad scores; for instance, almost nine million citizens are banned from purchasing internal flights due to their low scores[75]. Some other critical sanctions are listed as follows: throttling the internet speed due to spreading fake news, specifically about terrorist attacks or airport security; refusing to do military service, leading to a ban on higher education and some hotel and holiday services; not showing gratitude, leading

[73] "In the UK, the Key EID scheme is GOV.UK Verify, which is currently in public beta testing. When a citizen goes online to carry out a number of beta services on a gov.uk website, they are directed to verify their identity. 4 certified identity providers Verizon, The Post Office, Digidentity and Experian, carry out the identification procedure." (Brazell 2018).

[74] Bernard Marr. Enterprise&Cloud. (2019). Chinese Social Credit Score: Utopian Big Data Bliss Or Black Mirror On Steroids?. Forbes. Available at: https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#209767f048b8.[5April2019].

[75] Ma, A. (2018). China Ranks Citizens with a social Credit System-here's what you can do wrong and how you can be punished. *Independent*. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/china-social-credit-system-punishments-rewards-explained-a8297486.html.

to a ban on filling state body management positions. On the other hand, people with good scores get discounts on energy bills, rent deposits, and better interest rates at banks. This application can also be executed in the blockchain system. The author considers this a highly sensitive subject, touching on aspects of data protection and requiring the balancing of fundamental human rights. Therefore, the effect of this system must be evaluated and analysed with due care in terms of human rights and the government must be very careful and sensitive regarding these aspects.

1.7. Intermediary Parties

One of the most important questions that arises with the decentralized concept is: Where do the Intermediary Parties Stand in Blockchain Driven Transactions? It has been widely discussed that blockchain technology will eliminate intermediary parties from most of the transactions, even though the author considers that it is not likely to happen (especially for the banks) soon, as has been discussed in section 1.7 above. Briefly since the best-known version of a blockchain system (Bitcoin) clearly says that their aim is to remove intermediary parties from money transfer transactions, this leads to those questions. What intermediary parties do is basically assure parties that their monetary transactions are being taken care of securely; as the most common intermediary, banks have been doing this job for a long time. Bitcoin claims to provide this trust without the need for a bank or other intermediaries.

Intermediaries are not only banks or payment institutions. Notaries and lawyers are intermediaries, as well as big companies that provide central platforms for digital business, such as Apple, Facebook, Amazon, Microsoft, Tencent, Alibaba, Samsung, and SAP[76]. Intermediaries are the trust factor in business transactions for the parties. Blockchain technology provides a system where users trust each other instead of those

[76] Stev Heinert. (2018). Blockchain does not destroy intermediaries. It just changes their role. Medium Article. Available at: https://medium.com/evan-network/blockchain-does-not-destroy-intermediaries-it-just-changes-its-role-8c4691a60c78 [17 april2019].

intermediaries[77]. In other words, the trust is transferred from centralized bodies to the nodes that created the system.

There are various examples of technology companies using their own payment systems, especially in China where tech companies are well beyond banks in terms of personal banking and daily financial transactions. This does not mean the end of banks in the whole ecosystem since the most part of their transactions involve loans rather than regular personal banking transaction, such as daily money transfers. There are initiatives to try to operate loan transactions without banks too; for example, an online lending company[78] preparing to implement smart contract technology on Ethereum and engage their business of loan evaluations over this system[79].

The reason that the banks might lose power in terms of payment systems to the tech companies is because of the old and complicated systems they still (have to) use. For this reason, in most countries around the world, there is legislation that allows companies to create payment systems[80]. However, this is not the same for current loan and credit issuance procedures since this is a highly regulated and complicated procedure with a lot of hurdles involved.

The loan issuance process is incredibly delicate for banks; it requires management with high levels of punctiliousness and expertise. Many of the major financial crises have originated in poorly evaluated loan applications. Therefore, society, in general, does not tend to leave the loans process in inexperienced hands or to machines. On the other hand, creating payment systems is not an expensive process for the big tech companies; in fact,

[77] (Finck 2018). p10.

[78] WishFinance, a Singapore-based online lending company. https://wishfinance.com/.

[79] Wish Finance Platform. (2017). *How do Blockchain and Smart Contracts Revamp SME Lending*. Available at:https://medium.com/wish-finance/how-do-blockchain-and-smart-contracts-revamp-sme-lending-5497e2121fc5. [Jan 2019].

[80] Details of establishing a payments institutions and services are regulated under the Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions with No. 6493 and Date 20/6/2013.

some of the banks have adopted this approach since transitioning their old systems into new technology is extremely complicated. They prefer to create new banks called challenger banks[81]. This way, it is quite cheap and less exhausting than transmitting their existing systems into a technical scheme. This helps us to understand the position of intermediary parties, such as banks and payment institutions, regarding the use of blockchain-based technologies.

Moreover, the intermediary parties have already started to study the creation of blockchain-driven projects to make the best practise out of it for their businesses. Areas of interest include how to benefit from blockchain technology; the criteria for artificial intelligence being considered in the loan evaluation process; how artificial intelligence can help to examine the risks and create a report for determination of the credit limits for loans with small credit limits. An example of the move towards high tech solutions is The Interbank Card Center (*Bankalararası Kart Merkezi* "BKM")[82], who has created a product called digital identity which basically works on hyper ledger technology.

In smart contract systems, intermediaries might be needed yet in a different and new form called oracles[83], which is a third party that helps in the execution of the contract terms. They may also collaborate with the parties and traditional intermediaries as well. This concept will be examined in the following section.

1.8. Oracles

Smart contracts will be merely computer programs per se, and will not have smartness at the level of Artificial Intelligence ("AI"). They cannot connect and interact with the real world. Oracles have been suggested[84] as a means of clearing this hurdle and of helping

[81] Markos Zachariadis & Pinar Ozcan. (2017). The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. SWIFT Institute Working Paper No. 2016-001. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199.[20Jan2019].

[82] Bankalararası Kart Merkezi A.S. https://bkm.com.tr/en/about-bkm/bkm/history/.

[83] (Finck 2018). p19.

[84] (Walsh 2015).

the system to interact beyond the limits of its own ecosystem[85]. Oracles can conduct the performance of contractual obligations. Oracles are trusted third parties that can be real people, most likely developers or computer programmers[86]. Oracles basically help to transfer information and communicate with the world outside of smart contract transactions. For instance, flight information is generally open and easily accessed by people. This information amounts to empirical data, and computer programs, which can be called oracles in technical terminology, commonly manage such data[87]. They run in accordance with the conditions set forth in advance and are able to adjust according to the changing conditions in practice.

In smart contracts, parties in the system can regulate the oracle's position in advance, and allow it to take actions necessary for any transactions, such as adjusting payments or amending embedded obligations in the smart contract code. Parties can also rely on oracles to take the most beneficial action and embed it into the system without asking the parties every time this is required because they are generally designated human developers[88].

In smart contract transactions, it is important that contract terms and conditions[89] between the parties are written and implemented clearly [90]. However, the immutable nature of the transactions may create unwanted situations. These will be examined in section 3.6.1 below.

[85] (Finck 2018). p25.

[86] (De Filippi & Wright 2018). p75.

[87] (Morrison 2019). p145-151.

[88] (Cardozo Blockchain Project 2018). p8.

[89] (Cardozo Blockchain Project 2018). p6.

[90] (De Filippi & Wright 2018). p74.

1.9. Digital Identity

Online transactions have been conducted in various sectors, not only in developed, economically strong countries but also in the developing world[91]. Businesses based on distant online interaction are growing amongst various private sector actors, as well as in governmental services[92]. In these kinds of services, a fundamental principle is the creation of an identity on online platforms. This digital identity can differ from one's physical identity, or part of it, depending on the scope of the services. While these services are evolving, identity fraud and theft have become an important issue. Obscurity on trusting online identities has created an insecure environment, especially in terms of the e-commerce sector. Therefore, the market actors are searching for tools to meet this challenge. As an identification tool, the electronic signature is accepted in most jurisdictions; agreements require signatures and electronic signatures are the accepted legal equivalent of handwritten signatures[93].

Concerning means of identity - name, last name, age, birthplace, nationality, etc. - basically all the information written on official ID documents, passports are considered valid. However, the most important point of the information on official IDs is that each piece of information does not mean anything as and of itself. The name cannot solely identify a person, nor the age or nationality. It requires the accumulation of all that information regarding a person to constitute an identity. In the online realm, this includes the characteristics and interactions of a person: the "collection of attributes relating to a particular physical person"[94].

The general aspects of identity are personality and attributes (age, qualifications, location). All of these aspects may not always be of interest to a service provider in an e-commerce transaction but partial identity, consisting of aspects which are important in

[91] In Turkey e-government system is being used daily for instance hospital appointments, also in legal correspondences sent online.

[92] (Brazell 2018). p43-44.

[93] Except for the certain transactions requiring specific forms; handwritten signature or notarization.

[94] (Brazell 2018). *p37-38.*

the given context, is required. In the e-commerce sector generally, partial identity is used to provide personalized experience to the users. In this approach, service providers do not need all of the details of a user's personal information or all of the attributes of their identity, they just need to know the parts of the identity related to their scope of services, mostly behaviour on the web site, to create and send related services and discount ads to them.

Digital identity is basically information about people, legal entities and organizations which is kept in electronic platforms. This digital entity concept can be a useful tool, enabling parties to know each other and track down any processes in which they are participating in the smart contract system. It must be added that it is not just in smart contract transaction that the parties should be known to each other. Digital identification could be used for any transaction where the contracting parties would like to know more about each other for contractual claims.

Digital identity has different aspects, and the use of information varies according to the kind of transactions involved; personal information is not mandatory for creating a digital identity. In the current system in Turkey (as in most countries in Europe), people still have to go the banks to open a bank account, and they need to submit their official identification card with an identification number on it. However, opening a bank account online is possible with a well-placed, trusted digital identification system. This system has already been implemented in some countries following adoption of the Basel Criteria proposed by the Basel Banking Oversight Committee[95]. The aim of the Basel Criteria is to provide financial stability in the markets and reduce risks. This Committee has suggested the adoption of the 'know your customer' concept in transactions for banks around the world. These procedures have been created for the purposes of establishing integrity in banking systems, fighting money laundering and the maintenance of effective

[95] Yildirim, O. (2015). Basel Criteria in the Turkish Banking System. *Finance, Politics and Economic Comments,* Volume 52/6092015, p9-19. Available at: https://docplayer.biz.tr/38975405-Basel-criteria-in-the-turkish-banking-system-abstract-oguz-yildirim-1.html. [10June 2018].

risk management[96]. Naturally, face-to-face account-opening practice is based on these criteria.

Latterly, cameras on smartphones or computers have been used for the encryption of devices, and this process can be developed and used in the opening of bank accounts instead of physical presence in the bank. Blockchain technology can also be used for the verification of identities. This might become possible with the cooperation of the Government since they keep all the data. In such a scheme, the Government would enable the banks in certain circumstances (for verification purposes in transactions) to access the government database.

"On blockchains, asymmetric cryptography is used as a means to generate digital signatures"[97]. In the case of smart contracts, digital identity is important in order to claim contractual obligation; basically, parties need to know whom their counterparties are and where they based to make legal claims. The public key and hashing are two substantial features of blockchain technology that could help parties in this regard. As mentioned earlier, the public key function, which can be pseudonymous, is used for identity authentication[98].

1.10. Electronic Signature

In documents, mostly contracts, signatures are the tools used to identify the parties. An admissible signature proves the identity of the person, an intention to sign and to accept the document content[99]. It is believed that a physical signature is specific to each

[96] MASAK. (2001). *Customer Due Diligence for Banks Review.* Available at: http://www.masak.gov.tr/media/portals/masak2/files/mevzuat/sucgelirlerinin_aklanmasi/uluslararas%C4%B1_mevzuat/BaselKomite/2.htm [5April 2019].

[97] (Finck 2018). p91.

[98] (Finck 2018). p28.

[99] Reed, C. (2000). What is a signature?. *Journal of Information, Law and Technology,* Volume2000/3. Available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/. [9Feb 2019].

individual and that it provides evidence of identity[100]. As in most jurisdictions, under English law, admissibility of a signature relies on its satisfying its function as a signature rather than its legal recognition[101]. Lawyers generally concentrate on this function: to identify a person and his approval, and to confirm its reliability and that it is compatible with its purpose[102].

In the online identification concept, the e-signature is the most famous tool. In this case, the identification function is quite separate from the question of signature validity[103]. Therefore, companies and governments are more interested in developing different identification schemes rather than e-signatures[104]. An e-signature is accepted as a hand-written signature in most jurisdictions; however, there are certain transactions that require a hand-written signature. They are generally being used in public services in many other countries.

In Switzerland, the state planned to enable the use of electronic identity not only for public services but also for online transactions[105]. Public key cryptography has been suggested as a means of creating digital signatures (a form of electronic signature). This is not a brand new concept; Ericsson launched the first digital signature for secure mobile e-commerce. It worked by wireless application protocol ("WAP") on phones in October 1999[106]. The system required a technical substructure that might have challenged

[100] Even though an e-signature is not 100% secure, it is still much more secure than a handwritten signature. E-signatures are issued by a third party (government approved authorities), are not quite affordable since signing a document is not something we all do every day. Estonia created a great system for e-signature usage; even though people do not use it every day, 98% of Estonian citizens have an e-signature.

[101] Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions* (Advice From the Law Commission 2001) p.18. Available at: https://www.lawcom.gov.uk/project/electronic-commerce-formal-requirements-in-commercial-transactions/ [30April2019].

[102] (Law Commission 2001) p18.

[103] Reed, C. (2004). *Internet Law: Text and Materials,* 2nd ed. Cambridge: Cambridge University Press. p143.

[104] (Reed 2000). What is a signature?

[105] Hess, M., Hess R. (2018). Electronic Identity (e-ID). Available at: https://www.swissbanking.org/en/topics/digitalisation/electronic-identity-e-id. [10Jan2019].

[106] (Brazell 2018). p2.

individual users. However, an electronic signature is not an adequate identification tool that works in all situations; bank account opening is still not possible online using an e-signature anywhere except in Estonia. Most importantly, e-commerce companies cannot expect every user to have an e-signature to shop online because the e-signature system is not practical or cheap enough to be implemented. Furthermore, international acceptance is another hurdle for the e-commerce sector; whereas the use of e-signatures in governmental services seems more accepted. In e-commerce, service providers rely on identification schemes created by credit card companies since they cannot rely on electronic signature yet[107]; they are unable to authenticate another party's identity on e-commerce transactions other than through e-mails.

Viviane Reding[108] said 'a reliable system of electronic signatures that works across intra-EU borders was not fully satisfied with the take-up of EU signatures'. This paved the way to work on electronic identification and trust services for electronic transactions in the international market[109]. International acceptance of electronic signatures is still ambiguous. There is no uniform legal instrument, as in an apostil[110]. Every country that has regulated e-documents and e-signatures has its own way of applying apostil, and this can challenge international transactions. The author considers that the application of apostil can be achieved in different ways. One option can be to have a uniform act as an apostil regulation, but this may take a long time to implement. Since a convention is already active, it may be possible for electronic signature regulations to take the place of the apostil convention (the Hague Convention)[111]. This would be quicker than creating a new convention. Another, and more feasible, option could be bilateral agreements between countries involving the reciprocal acceptance of the e-signature.

[107] (Reed 2000). What is a signature?

[108] Former Commissioner for Information Society and Media.

[109] Murray, A. (2016). *Information Technology Law: The Law and Society*. 3rd ed. Oxford: OUP Oxford. p512.

[110] Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents. Available at: https://www.hcch.net/en/instruments/conventions/full-text/?cid=41.[30March2019]

[111] (Brazell 2018). p3.

This approach will also be needed in regulating smart contracts. In order to be successful, this has to be considered at an international level[112]. Turkey lunched an electronic Apostil system as of 1 January 2019. The system now allows people to have criminal records and reach out-of-court decisions; such documents will be admissible in signatory countries of the Hague Convention. Turkey is expanding the scope of the documents covered by the system to include identity registers, birth certificates, death certificates, marriage certificates, diplomas and transcripts, and company formation documents[113].

The author believes electronic signatures can contribute to smart contract technology as a concept that is accepted by society. Electronic signatures are regulated by European legislation and are widely used in transactions[114]. Electronic signatures are used in various transactions in practice since they have an equal legal standing as handwritten signatures, in most cases. Even court case decisions are signed electronically in Turkey[115]. Other areas where electronic signatures figure most prominently include insurance contracts, electronic commerce transaction documents, online banking, as well as administrative documentation such as declarations, residence permits, birth certificates and passports.

In the blockchain system, users verify electronic signatures generally by creating a public and private key over PKI for signing data[116]. PKI also enables users to generate their digital signatures. A digital signature ensures that the transaction has been generated by an identifiable, and thus reliable, person. Users may sign the data in the block by

[112] Schönfeld, C. (2018). Smart Contracts under Swiss Law. *FintechHub London*. p29.

[113] Electronic Apostil System. 2018. Announcement of PTT. Available at: https://www.ptt.gov.tr/Sayfalar/Kurumsal/DuyuruDetay.aspx?DetayId=26. [30March2019]

[114] European Commission. Trust Services and Electronic identification (eID). Available at: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid [30March2019].

[115] Under Turkish Law, an electronic signature is described as an item of electronic data that is used for authentication purposes, having a logical link to another item of data or being inserted into another item of electronic data (Article 3 of the Code of Electronic Signature dated 15 January 2015 and law No. 5070)[115].

[116] (Bacon, Michels, Millard & Singh 2018). p5.

encrypting it with his/her private key[117]. A private key is basically the users' way into the system; it helps to authenticate the users' identity. In cases where a private key is lost, the user may not re-enter the system[118].

1.11. Verification

As analysed in detail within the scope of this study, blockchain technology basically works as a distributed ledger, helping to keep a single record over different databases. In terms of an asset transfer, the initiating company first registers this asset transfer on the blockchain system with its own electronic signature. The data that is recorded onto a block in the blockchain system has its own ID, transaction time and has a record of the previous data created before itself. In other words, the data groups are defined in the system consecutively. This alignment verifies the validity of the chain.

Blockchain works over uninterrupted blocks that are basically datasets; these blocks are connected to each other sequentially and are recorded with a time stamp in each phase, which makes the data in this ecosystem tamper-proof[119]. Each user verifies each transaction in the whole system, repeating the same every time. The verification procedure basically relies on a timestamp since it helps to hash a block and shows that the data exists. Each data includes the previous data in its hash, together with the timestamp[120]. This record of the block is later broadcast to the other users and they record this block. This is where the consensus mechanism starts to process.

The underlying technology of this whole system requires an electronic verification scheme to run transactions over the blockchain systems. The designation of the transaction time with a timestamp resembles the existing system used to run registered

[117] (Bacon, Michels, Millard & Singh 2018). p15.

[118] (Bacon, Michels, Millard & Singh 2018). p15.

[119] (Maclean 2017).

[120] (Nakamoto 2008).

electronic signature mechanisms. In the electronic signature procedure, the verification scheme is usually taken care of by a third party (an authorized body) and this allows people to trust the signature. This concept may help people, especially legal decision-makers, to understand blockchain technology more easily while creating regulations needed to mitigate the adaptation process for wider society.

In the blockchain account, a secret code is placed for authentication purposes. Moreover, as explained above, the other users witness the transmission process and they validate the accuracy of the chains. The nature of the blockchain system allows the users to control the accounts and to check to see if the user is legitimate regarding completing the transaction. Hence, the users who are logged in to the system verify the smart contracts.

An electronic signature bears the same legal consequences as a physical signature in most jurisdictions. However, there are legal transactions that are subject to formal procedures. For example, guarantee contracts, with the exception of bank letters of guarantee, cannot be considered valid unless they are executed with a physical signature. Electronic signatures provide a unique system for authentication, privacy, and protection against fraudulent action. For the identification of the signatory, a Qualified Electronic Certificate ("QEC") is used. This consists of data files electronically used for the identification of the signatory. In other words, the QEC can be described as a digital identity card. The QEC can only be provided by authorized companies in Turkey[121] using a smartcard. A smartcard software program (such as Java) is used for the verification of the QEC. This structure can be used in smart contract-driven projects.

[121] Electronic Certificate Service Provider as described in Article 8 of the Code; state institutions and organizations that provide services related to electronic certificates, timestamp and electronic signatures.

SECTION II

2. Physical Contracts and Smart Contracts

After looking into technical components and working principles per se, in this chapter I will analyse the legal aspects of smart contracts. As a major concern of this study, it is very important for people in practice to understand the legal position regarding this new technology.

2.1. Contract Conclusion

In contract formation, the critical points are: whether the parties are bound or not; what the contract terms actually say; and whether it is possible to identify the contract execution time and place. Contract formation principles are quite similar in most jurisdictions. Turkey adopted the Swiss concept. Briefly, to make a contract there must be an expression of intent, an offer and its acceptance. Parties must express their mutual and consentaneous intents to fulfil these.

Basically, in physical contracts, the formation is considered done when the acceptance is received (communicated) by the offeror. With the offer, the offeror declares an intention to be bound by the conditions and terms (of the proposed contract) included in the offer, subject to the acceptance of the addressee. Mainly, an offer is considered binding unless the offeror reserves the right of withdraw in the offer. However, there are situations where an explicit acceptance is not necessary for contract formation (due to the nature of the law or business or the situation) unless the offer is rejected within a reasonable length of time.

The validity of a contract does not rely on a specific form unless it is otherwise specifically required in the law[122]. For instance, some contracts may be subject to certain

[122] Bainbridge, D. (2004). *Introduction to Computer Law*. 5th ed. Longman. p303.

formal requirements, e.g., deeds or real estate sale agreements[123]. Parties can also form a contract by agreeing on the terms and conditions verbally unless they are required to make it in writing by law. Thereby, general contracting rules are applicable to electronic contracts.

In terms of contracting, the key lies in the determination of the consensus, the "meeting of the minds"[124], and whether the communication between the parties constitutes an offer and an acceptance. It is easy to determine this in face-to-face communication[125]. Although, even if it is face-to-face communication, it can be challenging to determine if the offer is valid or the acceptance has been properly received to enable a contract to be formed.

Under Turkish law, for the formation of a contract, there must be an expression of intent, an offer, and an acceptance. This is similar to the United Nations Convention on Contracts for the International Sale of Goods[126] ("CISG") and the Swiss Code of Obligations[127], "Article 1: *(1) The conclusion of a contract requires a mutual expression of intent by the parties. (2) The expression of intent may be express or implied. Art. 2: (1) Where the parties have agreed on all the essential terms, it is presumed that the contract will be binding notwithstanding any reservation on secondary terms. (2) In the event of failure to reach agreement on such secondary terms, the court must determine them with due regard to the* nature of the transaction. *(3) The foregoing is subject to the provisions governing the form of contracts."*

[123] These documents have to be signed before a notary under Turkish Law.

[124] (De Filippi & Wright 2018). p74.

[125] Face-to-face communication includes direct online communication on a website.

[126] United Nations Convention on Contracts for the International Sale of Goods. https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf

[127] Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of 30 March 1911 (Status as of 1 April 2017).

According to Article 1 of the Turkish Code of Obligations[128] ("TCO"), for the formation of a contract, the parties must express their mutual and consentaneous (*karşılıklı*) intents to form said contract. The expression of intent is called *consensus ad idem* in Roman Law. The general rules applied to the formation of a contract have their basis in the legal theory adopted in the seventeenth and eighteenth centuries and are mostly based on the philosophy of the "Enlightenment". Roman Law tradition is adopted; specific rules are regulated to apply in terms of problems according to their specific situations[129].

An expression of intent can be explicit or implied. Intents must be mutual and consentaneous (*karşılıklı*); unilateral intent is not enough to enter into a contract. This principle is applicable to all kinds of contracts, whether created on online platforms or in a vending machine. An offer basically means the expression of interest in entering into the negotiations process of a contract. In this phase, the parties generally bargain over the contract terms. According to Articles 4 and 5 of the TCO, an offer can be made in the presence or absence of the parties. In terms of electronic transactions, there is an exception: an offer made over a communication device, such as a telephone or a computer, even though the parties are not physically present, is deemed to have been taken in the presence of the parties.

2.2. Written Form Requirement

According to Article 15 of the TCO, in terms of a signature on a contract, the signature has to be written in the parties' own handwriting. Parties can use a handwritten signature since it is legally recognised. However, in the e-commerce realm, the question of what constitutes writing has become a point of consideration. People want to understand what constitutes writing; more importantly, they want to know whether digital texts amount to writing and how signature schemes will look.

[128] Turkish Code of Obligations, no 6098, date 4/2/2011.

[129] Eugen Bucher. Introduction to Swiss Law; 3rd Ed. Chapter 8 Law of Contracts. Available at: http://www.eugenbucher.ch/pdf_files/86.pdf [30April2019].

In the UK, writing is defined as any form which "includes typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form, and expressions referring to writing are construed accordingly"[130]. Although this seems to be a comprehensive definition, the expression 'words in a visible form' restricts the scope of writing[131].

Further to this, the writing requirements vary in different jurisdictions; for instance, French law requires contracts over the value of 1,500 Euro to be in a traditional written form and signed physically. In the US, the party that the claim has been made to must physically sign sales contracts over the value of 500 USD[132]. However, in the US, writing requirements are not so strict; they do not have to be "thorough or complete"[133] if they conclude the main components of the contract. It is also possible to have them on electronic platforms, not in legal language entirely (but consisting of formulas) so they can be proved as evidence of a contract.

In Turkey, as in some other jurisdictions, parties can also form a contract by agreeing on the terms and conditions verbally unless they are required to make it in writing by law. The validity of a contract does not rely on a specific form unless it is otherwise specifically required by law[134]; certain contracting transactions can be subject to certain formal requirements:[135] e.g., deeds or real estate sale agreements[136].

---

[130] (Law Commission 2001). p7.

[131] Riefa, C. (2009). The Reform of Electronic Consumer Contracts in Europe: Towards An Effective Legal Framework?. *Lex Electronica*, Volume14(2). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1679673. [10 March 2019].

[132] (Brazell 2018). p3.

[133] (Cardozo Blockchain Project 2018). P10.

[134] Article 12 of the Turkish Commercial Code, no. 6098, dated 11/1/2011.

[135] Bainbridge, D., (2004). *Introduction to Computer Law*. p303.

[136] These documents have to be signed before a notary under Turkish Law.

2.3. Digital Contracts

Contracts that work on electronic platforms started in around 1970, and have been, technically, a form of Electronic Data Interchange ("EDI") [137]. Before that, digital contracts were created to solve the food and other needs supply problem caused by the Soviet Union's sanctions against West Germany (and the division of Berlin) around the late 1940s[138]. At that time, a US sergeant (Guilbert) created a "manifestation system than can be transmitted by telex, radio-teletype, or telephone."[139] Sergeant Guilbert went on to develop this system, and in 1965 he created the EDI system. This system constitutes the base for electronic contracts; for almost 50 years, especially big companies have been using EDI in their transactions, including for invoicing, orders and keeping inventories[140]. The EDI system only shows the terms and does not take part in performing contractual obligations per se[141]; this autonomous feature was developed by Nick Szabo later on. Starting from the 1990s, the number of transactions running over the Internet started to increase, making contract-writing an important issue. Online operators also came up with contract formation formulas using standard contract terms, which later led to serious litigation problems[142].

In online contracting, making sure whether the communication between the parties constitutes an offer and its acceptance is a problem[143]. In most jurisdictions, it has been discussed whether a web site creates an offer or merely an invitation to treat. If it is considered an offer, then the order of the customer automatically creates acceptance and

[137] Deveci, H. (2007). Consent in online contracts: old wine in new bottles. *Computer and Telecommunications Law Review,* Volume13(8), p223-231.

[138] (De Filippi, & Wright 2018). p72.

[139] (De Filippi, & Wright 2018). p73.

[140] (Cardozo Blockchain Project 2018). P15.

[141] (De Filippi, & Wright 2018). P73.

[142] Ramberg, C. (2001). The Ecommerce Directive and formation of contract in a comparative perspective. *European Law Review*, Volume26(5), p429-450.

[143] Reed, C. (1996). *Digital information law: electronic documents and requirements of form*. London: University of London, CCLS. p270.

the service provider does not have any means of rejecting it[144]. This approach obviously does not serve as a practical solution regarding transactions and service providers. Therefore, to overcome the ambiguities, the 2000 EC Directive[145] states businesses have to explain their operation and contracting procedures clearly to any potential customers on their web site as the EC does not explicitly regulate online contracting. This has been criticized since it has been suggested by the Member States that the contract formation rules at the CISG could be applied[146].

I do not believe applying CISG to the electronic realm would make any sense since its scope only covers distance sale contracts. Every transaction is individual, and it is hard to give one answer that suits all businesses. Also, the technology changes rapidly and it is not easy for the legal realm to keep up with the technological developments at the same rate of change. Therefore, leaving this to the business (by providing frameworks) seems the practical thing to do. For instance, Amazon has adopted the structure[147] required by the EC Directive perfectly. Briefly, regarding Amazon orders, the contract is considered established once Amazon sends the message/mail of acknowledgement of such orders. The author considers this to be the best interpretation and application of general contract law in the online contract-making process.

It has been seen in different ways that the rapidly developing nature of technology has paved the way to online platforms of all sizes to expand their business exponentially. So, what was once a small online platform business can now become a digital giant. These actors of the online sector have not only operated online platforms but have also shaped legislation over the years. As it has been put forward by economist Douglass C. North:

---

[144] Rowland, D., Kohl, U. and Charlesworth, A. (2011). *Information Technology Law*. 4th ed. London: Routledge. p236.

[145] Directive 2000/31/EC, Article 10(1)(a).

[146] (Law Commission 2001). p7.

[147] Winn, J. (2016). The Secession of the Successful: the Rise of Amazon as Private Global Consumer Protection Regulator. *Arizona Law Review*, Volume58(193), p194-211. Available at: http://arizonalawreview.org/the-secession-of-the-successful-the-rise-of-amazon-as-private-global-consumer-protection-regulator/. [30March2019].

"Institutions are the rules of the game in a society, or more formally, are the humanly devised constraints that shape human interaction. In consequence, they structure incentives in human exchange, whether political, social, or economic. Institutional change shapes the way societies evolve through time and hence is the key to understanding historical change."[148] For instance, as a US-based company, Amazon's innovative implementation of the EC Directive's provision on explaining their operations and online contract-making structure on their website to the customers has been very influential.

In the online realm, click-wrap, browse-wrap and web-wrap agreements are the best-known forms that are used in transactions. These are subject to general contracting rules as well. In these kinds of forms, there are generally click buttons instead of ink signatures; these allow users to show their consent as accept or agree buttons. This is a good example of contract conclusion between computers[149]. Therefore, this concept of making contracts through an online platform or a system without negotiation is not quite new; smart contracts can resemble those agreements[150].

However, smart contracts are not merely one of those digital contracts; the most differentiating feature is automatic execution in smart contracts[151] and the "code is the law" approach[152]. The way that those contracts are governed, the author considers that this is a good pattern the governance of smart contracts. The documents that are used in online transactions, such as in online shopping, have been showing us for years how it is possible for two parties to establish a contractual relationship online and conduct business through online platforms without interacting with each other. There are now other areas

[148] (Winn 2016). p7.

[149] Riefa, C. (2009). The Reform of Electronic Consumer Contracts in Europe: Towards An Effective Legal Framework?

[150] Ieva, Giedrimaite. (2019). IPKat Blok. Smart Contracts: Pros and Cons of the New Shiny Thing. Available at: http://ipkitten.blogspot.com/2019/03/smart-contracts-pros-and-cons-of-new.html. [22March2019].

[151] (Finck 2018).

[152] (Schönfeld 2018). p19.

of business where the number of online or electronically created contracts is increasing. For instance, students are able to create online transactions by creating an electronic request through the university system and, having electronically signed, create valid documents proving their status at the school. These documents can be used in international applications.

2.4. Main Contracting Principles

In the previous sections, contract conclusion principles have been analysed in part rather than in contracting per se. Now, I will look into some of the important principles in contract law I consider are relevant to smart contract procedures. Those principles are freedom of contract, preliminary contract liability *(Pactum de Contrahendo)* and culpa in contrahendo.

2.4.1. Freedom of Contract Principle

Under Turkish Law, a general principle, called a freedom of contract, is accepted in contractual relationships as the main principal. The main idea lying behind this principle is the protection of free will that finds its basis in the Constitution of the Republic of Turkey[153]: "Everyone has the freedom to work and conclude contracts in the field of his/her choice. The establishment of private enterprises is free. The State shall take measures to ensure that private enterprises operate in accordance with national economic requirements and social objectives and in security and stability."[154] This principal is also indicated in the TCO in detail by the words: "the parties may determine the content of the contract within the limits set forth by law freely"[155].

The principle of freedom of contract provides latitude to the contracting parties on determining contractual obligations. Although they are not specifically regulated by law,

[153] Constitution of Republic of Turkey, no 2709, date 9/11/1982.

[154] Article 48 of the Constitution.

[155] Article 26 of the Code of Obligations.

I would like to mention the fundamental components of the freedom of contract principle which have been shaped in practice over the years and which are widely accepted in the doctrine: the freedom to make a contract, to choose the contracting party, the freedom to terminate and amend a contract, the freedom to determine the content of a contract and the freedom to determine the form of a contract. This principal gives the freedom to people to create a contract on a blockchain-based system. Basically, there is no legal hurdle to creating smart contracts.

Smart contracts are no more than a computer program. The author considers that in smart contract-driven projects (at least at first until people trust the system), the parties are likely to create a physical (pre-prepared) contract with the terms set forth in the system. At this point, the party who has created the system or has developed it has control over the determination of the obligations. Smart contracts seem to provide best practise and benefits in multiple party transactions. In smart contract transactions, the system allows the operator (for instance a chocolate producing business owner) to be able to create the system according to the needs of the business, upload the relevant data (production temperatures, etc.) and have control over the transaction.

In this example, the suppliers only agree with the terms; the data regarding milk temperature is a block in the system. So, a company running a chocolate business purchases milk from different suppliers around the world and requires the suppliers or milk producers to keep and deliver the milk at certain temperatures. Sensors can do this. Each supplier/producer can set up a sensor mechanism on the containers that are used to store and transport the milk. However, it is still hard to trust the multiple suppliers not to change the temperature, and there is almost no way to make sure of this in real life.

There are cases where the principle of freedom of contract can be limited in terms of protection of the personal rights under the Turkish Civil Code ("TCC")[156]: "*No person may waive his/her rights and capacity to act freely even if it is in the least degree. Neither a person may waive his/her freedom nor any one may impose restrictions on a person*

[156]Turkish Civil Code, No 4721, Date 22/11/2001.

contrary to the laws and ethics. The extraction, vaccination and transfer of biological substances of human origin is subject to the written consent of the concerned body. However, no claim may be raised against a person who undertakes to give biological substance persuading him to fulfil his/her obligations; also, no claim may be raised for compensation of physical and moral damages."[157] This article 23 can be applicable regarding the limitations of economic freedom. Therefore, in terms of a contractual relationship, the creditor cannot totally or largely block the economic future of the debtor against the general moral rules[158]. In practice, these kinds of contracts are called Handcuffing Contracts (*kelepçeleme sözleşmeleri*).

There are different fields where the principle of freedom of contract is limited naturally. Those fields can be listed as hazard responsibility situations, consumer protection, and leasing and employment law regulations where it is necessary to protect the economically deficient parties[159] - in other words, a natural person against a big corporation.

The principle of freedom of contract can also be limited by the courts considering the general provision of the TCO and acting on the in good faith principle: "*Every person has to comply with the good faith rules when exercising his/her rights and performing his/her obligations. Legal regulations do not protect explicit abuse of a right."*[160] The judges are authorized to consider and determine the content of contracts in cases where there is a party who is economically deficient and who has limited power to negotiate the terms of the contract and thus cannot protect his/her rights and benefits at the time of the contract negotiations[161]. The author considers that these regulations can make people feel comfortable when starting to use smart contract systems in their daily transactions since it may seem complicated to adopt the system in the beginning.

[157]Article 23 of the Turkish Civil Code.

[158] Okumus, S. (2018). *Elektrik-Doğal Gaz Piyasaları Abonelik Sözleşmeleri ve Bu Sözleşmelerde Yer Alan Genel İşlem Koşulları*. Ankara: Yetkin. p22.

[159] Ruhi, A.C. (2013). *Sözleşmeler Hukuku*, 2nd ed. Istanbul: Seckin. p35-36.

[160] Article 2 of the Turkish Civil Code.

[161] (Okumus 2018).

There are two types of exceptions to the freedom of contract principle; (i) exceptions which can be regulated by law or (ii) exceptions which can be brought by a legal transaction. These will be only briefly mentioned in this study. These exceptions provide the obligation to make a contract. Preliminary contracts are the only examples of exceptions which can be brought by a legal transaction.

2.4.2. Exceptions of Freedom of Contract

2.4.2.1.Preliminary Contract Liability (Pactum de Contrahendo)

A preliminary contract (*Pactum de Contrahendo*) implies the commitment of the parties to each other to enter into a contract or the commitment of one party to another to make a contract with a third party. A preliminary contract is made only for promissory (*taahhüt içeren*) transactions, not for acts of disposal (*tasarruf işlemi*). In the case where it is made for acts of disposal, it should be considered a real contract not a preliminary contract. This can be the case in many types of smart contract-driven transactions since they have the potential of having a promissory nature.

A preliminary contract creates obligations for the contracting parties; the main obligation is the obligation to make a real contract. In the case where a covenanter does not fulfil the obligation to make the contract, the other party can bring an action for specific performance according to Article 123 and 125 of the TCO. If one of the parties fails to perform his obligations, the other party can be granted a period of time for the debtor to perform his obligation or go to courts and ask for time to be granted. If the performance is not done within the time given, the creditor has alternative rights, such as claiming compensation for damages, or reneging on the contract and asking for compensation for the damages arising from this.

According to a common view in Turkey, the qualification of the decision given by the court shall stand for the declaration of intention for making the real contract of the covenanter. The decision is also interpreted as constituting the real contract directly, not

the declaration of intention of the covenanter. The first and second view, even though having a correct theoretical basis, give rise to the problem of the application of the decision and also standing in contrast to economic procedures and the rules adopted in practice. According to a High Court decision, the decision given by the court will create the right to demand the rights, which will arise from the formation of the real contract[162].

This view is repeated by the 14th Court No. 2008/587 of 18 February 2008 for a preliminary contract on the sale of a piece of real estate, although it is criticized for superseding the difference between a preliminary contract and a real contract.[163] In the case where the obligation to make a contract cannot be fulfilled, the party may also bring an action for compensation, according to Article 112 of the TCO. Especially in some cases where the performance of duty is no longer possible or it does not provide any benefit to the party, the party has right to take this action. But the party may only bring this action where the covenanter has culpa on the impossibility.

For the calculation of the compensation, according to Article 114 of the TCO, the provisions regarding tort (Articles 51 and 52 of the TCO) shall apply. This means that culpa, the damaged party's actions and joint mistakes of the parties, will be considered. In the case where the covenanter proves that he has no culpa on the impossibility afterwards, according to Article 117 of the TCO, the covenanter will not be liable for the compensation.

2.4.3. The Difference Between Culpa in Contrahendo and Preliminary Contract Liability

According to Article 2 of the TCC, during the negotiations of a contract, the parties constitute a legal relationship and they are obliged to act in compliance with the good faith principle during these negotiations. Culpa in Contrahendo is the obligation to act in compliance with the good faith principle. In a more specific manner, during the

[162] Assembly of Civil Chambers No 1977/6-535 of 6 July 1977.

[163] 14th Court No. 2008/587 of 18 February 2008.

establishment of a contract or during the determination of the conditions of a contract, the parties will avoid deceptive actions, inform the other party about any important issues and even warn the other part in the case of mistakes.

Although the Culpa in Contrahendo is not specifically regulated under the TCO, the general principle of good faith is the legal basis of the Culpa in Contrahendo concept. Also, in particular situations, there are sanctions to be applied in terms of Culpa in Contrahendo; for instance, Article 39 of the TCO sets forth the responsibility of the party who persuades the other party to form a contract based on deceptive statements; and Article 35 of the TCO sets forth the responsibility of the party who makes the contract invalid by culpa. The legal sanctions that can apply in Culpa in Contrahendo are based on Article 41 of the TCO; the liability is a tort, since in Culpa in Contrahendo there is no contract and so it is not possible to go to the provisions of violation of debt arising from a contract. However, according to another view in the international doctrine (Oser, Schönenberger), the liability is based on the provisions of violation of debt arising from a contract. The significant difference between Culpa in Contrahendo and preliminary contract liability is gathered around this base of liability. Since, in Culpa in Contrahendo, the liability is based on the provisions on tort, the party who has suffered damage from Culpa in Contrahendo should prove the culpa of the other party. Also, in this situation, the statute of limitations is one year from the day of recognition of damage and 10 years from the day of damage in any case. In contrast, for preliminary contract liability, the liability is based on the violation of debt arising from a contract, subject to Article 112 of the TCO. The result of that is that the covenanter must prove the non-existence of culpa and the statute of limitations will be 10 years from the date of violation. Therefore, according to the differences set out above, it is possible to say that it is more favourable to the damaged party to opt for the preliminary contract terms rather than Culpa in Contrahendo.

Also, in Culpa in Contrahendo, there is another unfavourable situation for the damaged party. According to the dominant view in the doctrine, which is set out by several lecturers (inc. M. Kemal Oguzman), in Culpa in Contrahendo, the liability of the

damaged party from the negotiations of the contract should remain in the background in the form of the contract because this liability is only applicable if there is no contract and damage has occurred during the contract negotiations. But, for preliminary contracts, since there is the existence of a contract, the covenanter will still be responsible for the damages occurred, even in the formation of the real contract.

Even though a smart contract is able to confirm whether money has been transferred or not, a smart contract is a computer code and it is not possible for the code to say anything about the delivery itself. Involvement is necessary for the transaction to be completed and for the handover of the sold product to be confirmed. For example, when someone buys a product online, say a computer, through a smart contract, that smart contract cannot automatically decide on behalf of the seller to send the computer once the payment has been made. Here, the parties can enter into an escrow agreement and agree on freezing some of the digital money of the buyer until the delivery of the computer is completed. Once the delivery has been made, the freeze on the money ceases and the seller receives the full payment[164]. Escrow contracts in a smart contract system can segregate the obligations and keep the funds on the distributed ledger and, once the verification message is received and confirmed by the system, the smart contract automatically performs the contractual obligation accordingly[165].

In a transaction as in the example above, the parties are always able to breach the agreement terms or cheat. A smart contract cannot prevent this, yet a smart contract can be programed to perform the sanctions immediately, without any notification by the parties. A smart contract can automatically cease a service or freeze a payment depending on the type of breach and the contract terms. However, the physical availability of the system is still limited. For example, the system cannot check and confirm if the delivery has been made properly, which tells us clearly that human intervention is necessary at

[164] Engheim, E. (2018). What is a Smart Contract and why do we need them? Medium. Available at: https://medium.com/@Jernfrost/what-is-a-smart-contract-and-why-do-we-need-them-7d92f2131f03. [10December 2018].

[165] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *Peer Review Journal On the Internet*. Available at: https://ojphi.org/ojs/index.php/fm/article/view/548/469. [15December 2018].

this stage. It is clear people still have to trust each other considering that a simple beach may jeopardize their reputation. In terms of a violation of the contractual obligations, the parties will have the right to claim compensation. I will be reviewing this option where I analyse the non-performance of obligations in section 2.5 below.

2.5. Non-Performance

Non-performance of the obligation can occur in three different ways: impossibility of performance, non-performing properly (as agreed), and default[166]. Article 136 of the TOC states: "*The obligation is extinguished in the case where it is impossible to perform the obligation because of the reasons that are not attributable to the obligor. In bilateral contracts, the obligor who has been released from obligations because of impossibility shall be liable to return payments he has received from the counterparty in accordance with the provisions governing unjust enrichment, and he forfeitures the claim to payment, which has not been made to him yet. This provision shall not apply to the cases where the law or contract provides for an undertaking by the creditor of the damages that occur before performance of the obligation. Unless the obligor duly and in a timely manner notifies the creditor on the impossibility of the performance of the obligation and takes necessary precautions to prevent the increase of loss, he will be responsible for the compensation of the resulting losses*."

In these cases, the debtor is required to compensate for the damage or loss of the creditor unless the debtor proves that he was not at fault. Article 114 of the TCO states: "*In general, the obligor is liable for any faults. The scope of liability of the obligor is determined by the characteristics of the business. Specifically, where the business does not provide an advantage for the obligor, the liability is determined more leniently. The provisions related to tort liability are applied to breach of contract mutatis mutandis.*"

[166] (Ruhi 2013). p59.

In order to be able to talk about default, the debt must not be impossible. In default cases, the debtor has the ability to perform the obligation. In other words, the debt is due and payable but the debtor does not perform his obligations, even though the creditor has notified the debtor. However, in the case where the parties determine the date of the performance, the creditor does not have to notify the other party. Article 117 of the TCO states: "*Where the debt is due, the obligor falls in default by the notification of the obligee. If the day of performance is agreed upon by the parties together or notified by one of the parties duly on the basis of a reserved right in the contract, the obligor is in default by the lapse of this time. In the case of tort, the obligor is in default from the moment the tort occurs, and in the case of unjust enrichment, from the date enrichment occurs. In conditions where the unjust enrichment is in good faith, the notification is required for default*."

In the case of non-performance of the obligation at all or as agreed in the contract, the creditor has alternative rights, such as: to ask for the performance of the obligation as agreed in the contract (if the performance of the debt is not impossible) and to delay compensation; to ask for the compensation of the damages or loss incurred due to the non-performance; and to terminate the contract with compensation.

According to the Article 125 of the TCO, in the case where the debtor is in fault and has not performed the obligation within the granted cure period, the creditor has the right to demand the performance of the debt and compensation for the delay. The creditor has the right to terminate the agreement by immediately notifying the other party and to ask for the compensation of damages or loss incurred due to the non-performance. However, termination may be problematic in smart contracts given the difficulties in amending the information after the chains have been created[167]. Since smart contracts run using blockchain technology, which is subject to multiple party control[168], it is not easy to stop the autonomously performing system.

[167] (Cardozo Blockchain Project 2018). P8.

[168] (De Filippi & Wright 2018). p75.

In smart contracts, the obligations based on the contract are performed automatically, and the performance of the contractual obligations is self-executing; therefore, the system basically performs the main obligations but cannot have control over the parties. For example, in a smart contract-driven supply chain project, the system could automatically create a payment order with an electronic signature on it and notify the bank (or make the payment in digital money, if agreed) upon the confirmation of the delivery of the goods. It would appear that there would be nobody to claim any damages or loss or even to talk about damages or loss since the performance of the obligations were executed automatically. This might be a problem in permissionless blockchain systems where nobody knows who is who and there are numerous miners involved. However, in more limited blockchain systems that have been created by a group of users who can be identified, it is easier to claim contractual claims. In the automated blockchain transaction, the system is not able to confirm itself whether the delivery has been made properly or not. It is not easy for a computer program to have control over natural people so there will need to be an intervention (by a natural person or legal entity) for the completion of the transaction. Oracles have been suggested as parties able to play this role, as mentioned in section 1.8. In a more limited smart contract environment, if a violation occurs, the creditor will have recourse to the abovementioned rights due to non-performance of the contractual obligations. This raises the issue of whether contractual claims for non-performance can also be filed against oracles. Therefore, liability schemes must be determined in advance.

2.6. Standardized Terms in Contracts

Standardized terms are based on the approach to limiting the freedom of contracts principle created in the nineteenth century. In a land-purchasing contract, the price of the land has been valued at less than its real value. The right of termination has been given, and this has been accepted as the first example of the limitation of the principle of freedom of contract in the Corpus Iuris period[169].

[169] (Okumus 2018). p20-21.

Nowadays, in such a fast-paced growing environment, companies are keen to use contracts with a full set of standardized terms. With these kinds of contracts, human intervention is minimum and the parties almost never have the chance to negotiate the terms. This accelerates the transactions but the fairness of the terms is left in doubt. In the digitalized world, diminishing human intervention seems more and more appealing, not only in the negotiation process of the contract terms but also in the implementation of the contract[170].

Under Turkish law, standardized terms are described in Article 20 of the TCO as "*provisions, which are drafted in advance by the draftsman of the contract in order to use in a large number of the future contracts previously drafted single-handedly and offered to the other side of the contract.*" According to Article 21 of the TOC, the drafting party shall inform the other party of the contract regarding the standardized terms; otherwise, such standardized terms will be deemed unwritten. The standardized terms constitute another exception to the freedom of contract principle. In order to consider a provision a standardized term, the provision should have been drafted single-handedly before the formation of the contract in order to be used in a large number of the contracts and without taking into consideration the will of the other party.

Standardized terms are mostly seen in Business-to-Consumer ("B2C") transactions in practice. In the case where smart contracts are used in e-commerce transactions or in electricity distribution schemes, parties, especially the service providers, must be very careful using this type of unilaterally set-up contract terms because, in smart contract technology, they do not have a chance to easily amend the system after its implementation. They must also know that the whole process (the contracting scheme) can be considered void and the customers have the right to object to these standardized terms since they are in the weaker position.

[170] (Savelyev 2016).

2.6.1. Objection to Standardized Terms

The standardized terms are the terms in contracts that are drafted by one party for the purposes of use in more than one transaction with different parties. Examples of these types of contracts can be seen in banking transactions. Banks generally use one contract type for millions of customers in credit card sales contracts, with only slight differences. In these kinds of contracts, banks often use statements such as "I have read, understood and negotiated the terms of this contract and accept, declare and undertake all the terms and obligations hereunder". Article 20/3 of the TOC explicitly states that such statements do not change the fact that contracts have standardized terms[171].

Regarding standardized terms, usually the customer is in an economically weaker position than the service provider or institution. Therefore, there are rights granted for the protection of economically deficient parties of the contracts regulated under the TOC. Article 21 of the TOC states: "*the validity of standardized terms that are contrary to the interests of the other party depends on the condition that the drafter provides the other side opportunity to learn the content of those terms, clearly releasing explicit information about the existence of those terms, and on the acceptance of those terms. Otherwise, those standardized terms are deemed unwritten. The standardized terms contrary to the character of the contract and business are also deemed unwritten*."

If the standardized terms are not explained clearly to the customer and the customer is not aware of the content of these terms before signing the contract, the standardized terms are deemed invalid. Moreover, in contracts including standardized terms, if the party who drafts the contract has a unilateral right to amend or re-arrange the contract terms against the favour of the other party, such terms are considered invalid; according to Article 24 of the TOC, in a contract consisting of standardized terms giving a unilateral right of amending the contract to the drafting party against the favour of the other party, those terms are deemed unwritten. These invalid terms will not affect the execution of the contract, and other terms of the contracts are deemed valid. This may not be a case of

[171] (Ruhi 2013). p28.

concern in the smart contracts system due to the system being tamper-proof[172]. However, the service provider party must still be careful about the clarity of the transaction for the customer. If the standardized terms are not clearly written and understandable, these terms are interpreted in favour of the economically deficient party and against the party who drafts the contract. This might be an issue in smart contract-driven transactions since contract terms will be embedded in the code (since the system, at the moment, is not enhanced enough to have detailed clauses embedded). The clarity of the terms in such transactions can be achieved using upfront terms and conditions. In other words, service providers might provide the terms and conditions to the customers in advance.

2.6.2. Consumer Protection Rules

In most consumer related transactions, people generally do not clearly understand what they have agreed to in a contract. The legal language used in this type of contract is mostly legal jargon or legal prose and is not easy to understand by lay people. Such language use is often criticized, although consumers' rights are mainly protected in terms of bilaterally prepared and signed contracts since the consumers rely on the service providers, who are generally giant corporations. Although people have rights to seek legal remedy in regulatory bodies or courts to object to the terms of such contracts, the legal procedures may become too complicated and vague for the consumers.

Under Turkish Consumer Protection Law[173] ("Consumer Code"), Article 4, contracts and notifications in electronic commerce websites have to be written in at least 12 points in character size, drafted in a comprehensible language, in a clear, simple and legible manner and a copy of these must be handed out to the consumer, either on paper or on any other media platform. The conditions set forth in the contract cannot be altered to the detriment of the consumer during the term of the contract. Smart contract technology's tamper-proof feature makes it hard to change the terms of transactions, but according to

[172] *see* section 2.9.3.

[173] Law on Protection of the Consumer, no 6502, date 7/11/2013.

the current position, it is not clear how smart contracts can overcome the writing requirements (character size, etc.).

In these kinds of contracts, information on fees and expenses that will be paid by the customer subject to the contract can be provided to the consumer in writing as an attachment to the contract. In contracts created via telecommunication technologies, information of fees and expenses has to be presented in an adducible manner. The party who has drafted the contract, most often the service provider, has the liability to prove this in situations of a conflict over such information.

In Article 6 of the Consumer Code, the refusal to sell (*satıştan kaçınma*) concept is regulated. This provision is deemed to be an example of the limitation of the principle of freedom of contract in Turkish legislation. In the text of Article 6, it is clearly stated that: "*Unless there is a sign indicating that it is not for sale, a sale of a good that is on display in a window, shelf, on an electronic medium or any other place that is in a clearly visible area cannot be refused*." The principle of freedom of contract tends to be changed by interpretation in favour of the consumer by the courts as well[174].

2.7. Formation of International Sales Contracts

The author considers that the supply chain sector will realise the greatest benefits from smart contracts. In this globally connected world, efficiency is also needed for international sales contracts. Smart contracts technology can ease the contracting and application procedures, especially for multilateral transactions.

The formation of contracts for the international sale of goods is regulated under the CISG, between Articles 14 and 24. In the CISG, the concept for the formation of physical contracts is accepted, requiring mutual and consentaneous (*karşılıklı*) intents of the parties to enter into a contract. There are two components; offer and acceptance. According to Article 14 of the CISG: "*(1) A proposal for concluding a contract*

[174] (Okumus 2018). p31.

addressed to one or more specific persons constitutes an offer if it is sufficiently definite and indicates the intention of the offeror to be bound in the case of acceptance. A proposal is sufficiently definite if it indicates the goods and expressly or implicitly fixes or makes provision for determining the quantity and the price. (2) A proposal other than one addressed to one or more specific persons is to be considered merely an invitation to make offers unless the contrary is clearly indicated by the person making the proposal."

According to the CISG, there are three main components for an offer to be considered valid: addressing the proposal to one or more specific persons; being definite; having the intention of being bound. Offers not addressed to a specific person or persons are not deemed as offers but invitations to offer (*invitationes ad offerendum*). For instance, price lists, flyers, catalogues, newspaper, TV and radio ads, and Internet ads are accepted as invitations to offer since they are not addressed to specific people[175].

The other component of the expression of intent to enter into a contract is acceptance. According to Article 18 of the CISG: *(1) A statement made by or other conduct of the offeree indicating assent to an offer is an acceptance. Silence or inactivity does not in itself amount to acceptance. (2) An acceptance of an offer becomes effective at the moment the indication of assent reaches the offeror. An acceptance is not effective if the indication of assent does not reach the offeror within the time he has fixed or, if no time is fixed, within a reasonable time, due account being taken of the circumstances of the transaction, including the rapidity of the means of communication employed by the offeror. An oral offer must be accepted immediately unless the circumstances indicate otherwise. (3) However, if, by virtue of the offer or as a result of practices which the parties have established between themselves or of usage, the offeree may indicate assent by performing an act, such as one relating to the dispatch of the goods or payment of the price, without notice to the offeror, the acceptance is effective at the moment the act is performed, provided that the act is performed within the period of time laid down in the preceding paragraph.*"

[175] (Oral 2014). *p*27.

2.7.1. Breach of Contract

According to Article 45 of the CISG: "*(1) If the seller fails to perform any of his obligations under the contract or this Convention, the buyer may: (a) exercise the rights provided in articles 46 to 52; (b) claim damages as provided in articles 74 to 77. (2) The buyer is not deprived of any right he may have to claim damages by exercising his right to other remedies. (3) No period of grace may be granted to the seller by a court or arbitral tribunal when the buyer resorts to a remedy for breach of contract.*"

In the CISG, breach of the contract is not explained as a term. As in general understanding, failure by the parties to perform contractual obligations constitutes a breach of the contract. The type of breach does not make any difference; it does not matter whether the breach has occurred as a result of a violation of major obligations or ancillary obligations or general transaction terms.[176]

The CISG can demonstrate a good pattern for commercial smart contract transactions; it is not applicable to consumer-related matters. However, in terms of contract conclusion, B2C and Business-to-Business ("B2B") are quite similar. In consumer-involved transactions, it is extremely important to clarify the sale conditions to the customer, and not put a heavily-regulated onus on the customer. Furthermore, the consumer should have the right to withdraw or cancel the transaction. In similar smart contract-driven transactions, the supplier must be sensitive to consumer regulations. In online contracting schemes, new regulations have not been needed in terms of consumer protection, but the actors are expected to be careful about consumer protection principles. In smart contracts, a similar approach might be considered.

2.7.2. Unfair Terms in Consumer Contracts

According to Article 5 of the Consumer Code, unfair terms are basically the contractual terms included in the contract without negotiating with the consumer. This practice tends

[176] Oral, T. (2014). *Formation of Sales Contracts in CISG*. Yetkin Yayınevi Ankara.

to create an unfair environment, which can also be contradictory to good faith in the rights and obligations of the parties arising from such a contract. Those unfair terms included in the contract signed with the consumer are considered absolutely invalid. This does not make the whole contract invalid; other provisions of the contract remain effective.

If a contract condition had been prepared previously, and if it did not affect the consumer content due to it being in the standard contract, it is deemed that such a contract term has not been negotiated with the consumer. If the party who is drafting the contract is arguing that a standard condition has been solely negotiated, such a party has the burden of proof. If it can be interpreted from the evaluation of the contract that the parties are agreed on a standard contract, the negotiation of certain elements of a condition or a sole provision in this contract does not prevent the implementation of this article to the rest of the contract. If the contract terms are in written form, the language of the contract must be clear and comprehensible for the consumer to understand. In the event of a provision included in the contract not being clear and comprehensible or it having multiple meanings, such a provision will be interpreted to be to the benefit of the consumer.

In the event of discretion of the unfairness of the contract terms, provided that such terms are written in a clear and comprehensible manner, an evaluation cannot be made between the balance of the fundamental performance obligations, the market value of the good or service, and the price determined in the contract. The Ministry of Customs and Trade takes the necessary precautions to remove or prevent the use of unfair terms existing in contractual texts in contracts that have been drawn up for general use. The current state of smart contracts does not allow abstract factors to be assessed as good faith, whereas unfair terms can be seen from the contract performance. However, removing and preventing the use of unfair terms may not be appropriate due to the tamper-proof nature of the system at the moment.

In the United States, the Uniform Commercial Code ("UCC") regulates the commercial relationships, as well as commercial contracts, relating to corporate affairs. The UCC has

been adopted by most of the states in the United States. In addition, another specific regulation, the UETA, governs commercial affairs if the parties have agreed to conduct transactions by electronic means. However, UETA principles are not accepted by some states, such as New York City, Washington DC, and Illinois. Instead of UETA, these states have created alternative regulations to govern commercial contracts on online platforms and electronic signatures[177].

2.7.3. What would be the advantages of smart contracts in International Sales Contracts?

Global sale of goods transactions are generally based on exhaustive invoicing and a detailed documentation system (called bills of lading). These documents include the details of the transaction and the goods that are couriered and they are not secret to the contracting parties, even common cargo company employees can see them because these documents need to be inspected at least at the loading and unloading phases of shipping. This may not be particularly reliable for large international transactions. Smart contracts can provide a more confidential and protected environment for the parties, where every contracting party can see and check every phase of the transaction[178]. For instance, the relevant information (the agreed terms and condition for the transaction) can be embedded into the system, together with the Global Positioning System (GPS) implementation[179]. This could give information regarding the status of the cargo goods. Parties can easily track the transaction without the need for an outside inspection.

[177] Chamber of Digital Commerce, United States of America. (2018). Smart Contracts Legal Primer Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable. Report. Available at: https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf. [22 March 2019].

[178] (Morrison 2019). p145-151. and *also see* Allen, T., Widdison, R. (1996). Can Computers make Contracts? *Harvard Journal of Law and Technology*, Volume9(1), p26-47. Available at: http://jolt.law.harvard.edu/articles/pdf/v09/09HarvJLTech025.pdf. [March2019].

[179] (Morrison 2019).

2.8. Contract Liability in a General Sense

Basically, to be able to talk about liability, the parties make sure that there is a contract. The first and the most critical question is: Has a contract been established between the parties? In the existing contract-making rules, the simple receipt rule (once the acceptance is communicated to the oferror, the contract is formatted) is challenged in digital contracts. With transactions that are run using digital platforms, there is always a risk of communication interruption that might create issues surrounding the definition of responsibility, especially as there is no contract. It is very important to determine and allocate liability at first hand if there is a contract. Moreover, it is also critical to know the time and place of the contract conclusion to be able to designate the taxation liabilities as applicable by law.

In digital contracting scenarios, the most important question to be asked is when and where the customer receives messages because the answer to this will give a clue as to whether there is a contract or if the contract has been concluded. In the EC Directive[180], the time and place when and wherever the message reaches the mail server has been accepted. This might not be the same time and place as the customer actually receives the message. In Turkey, while explaining this dichotomy, the general approach is to look at the control (dominance) area of the customer[181]; the server cannot always be in the control area of the addressee. The receiving time and place is accepted when the message arrives in the inbox of the customer. The time and place determination plays a critical role in designating the applicable law and jurisdiction. In order to achieve this, understanding the technical and business needs of the transaction and creating a clear contracting structure is the key.

For instance, Amazon made it clear to everyone that when people ordered a product, it meant an offer, and that there was no contract until Amazon sent the acknowledgement

[180] (Reed 1996).

[181] Turan, G. (2008). Elektronik Sözleşmeler ve Elektronik Sözleşmelere Uygulanacak hukukun Tespiti. TBB Dergisi, Volume77. P87-119.

email saying that they had dispatched the goods. This model is fair for both parties in online shopping since people cannot examine the product and it gives the service provider time to check the product availability with the supplier, correct the price if necessary, and delay tax payments as long as possible. I must say that this system might not be ideal for every business; for instance, it does not work for online grocery shopping. In online grocery shopping, the contract is concluded when the order is delivered to the customer's door and accepted. ,

2.9. Contracting Principles Appearance on Smart Contracts

In this part of the thesis, the history of the smart contract will be covered, with examples. First, as can be seen in most smart contract-related research, vending machines are accepted as the earliest examples of smart contracts. In vending machine systems, once the machine takes the coins, it runs the mechanism and gives the product[182]. In the vending machine structure, when the user sends the coin into the vending machine and chooses the product (gums, candies, crackers, beverages, nuts, etc.) the code in the system of the vending machine executes and confirms that the payment has been made and operates the transaction,[183] without any third party intervention. In this mechanism, the potential loss is obviously less than the cost of breaking the mechanism.

"The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow the profitable deployment of vending machines in a wide variety of areas."[184] The very first appearance of a vending machine was seen in the work of Hero of Alexandria[185]. In 62 A.D., Hero of Alexandria

[182] (Schulpen 2018).

[183] Levi, S.D. and Lipton, A.B. Skadden, Arps, Slate, Meagher & Flom LLP. (2018). An Introduction to Smart Contracts and Their Potential and Inherent Limitations. Harvard Law School Forum on Corporate Governance and financial Regulation. Available at: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ [10 March 2019].

[184] (Szabo 1997).

[185] A first-century AD Greek engineer, and mathematician.

created a machine to work with a coin to dispense holy water[186]. In this application of a primitive smart contract, people were able to take the product without any third party action needed. This mechanism works based on the intention of an individual to get a product after inserting the necessary coin. The individual decides to have the product based on the information stated on the vending machine. The machine promises to give the product once the coin is received. The machine is liable to provide the product in good shape without any damage. If the machine supplies a damaged product, the buyer can go to the product producer company, according to the principles set forth under the TCO.

This section analyses how smart contracts can be considered a legally binding agreement. Therefore, instead of technical hurdles, the main contract conclusion scheme on smart contracts will be examined in this section. The author considers that the basic elements in traditional contracting must be looked for, as in section 2.1 of this thesis. Basically, a physical contract needs the consensus of the parties to come together with the intention of entering into a contract, and the admissibility is generally based on the text.

It is very important to understand the components that make a physical contract valid.

- First, the mutual and consentaneous (*karşılıklı*) intent of the parties: in smart contracts, there is no doubt concerning the intent of the parties since they enter into the system with a private key, and all their activities will be traceable. The author considers that intent is demonstrated once the parties enter into the system. Even though the system runs automatically, it needs the intent of the parties to launch the operation. The terms and conditions of the transaction have to be agreed on by the parties. At this point, the parties can prove the intention to conclude a contract.

- Material Obligations: as in most contractual relationship, in smart contracts the author considers that the transfer of certain obligations (Material Obligations,

[186] Segrave, K. (2002). *Vending Machines: An American Social History*. North Carolina: McFarland & Co. p3.

Essential Obligations[187] (*Asli Edimler)*) can also act as prominent proof of a contractual relationship. These obligations can be: "price, subject matter of the agreement, the time and term of payment, closing dates"[188]. For example, the transfer of digital assets from one party to another is a typical subject matter of a smart contract, and this basically constitutes a legal effect as well[189].

As explained in detail in the comparison of physical contracts and smart contracts above, the rules and the principles that are applied for the physical contracts under the TCO can be applied to the contractual relationships established in smart contracts as well. The critical point is proving how, where and when the contract is concluded. The author considers that the existing rules and principles for digital contracting can make a path for smart contracts.

2.9.1. Criticism of the Terminology

Especially from the technical aspect, the term smart contract is often criticized. Tom Allen and Robin Widdison have stated this clearly by saying that 'in spite of their name, smart contracts are not legally binding contracts in a technical meaning'[190]. However, this terminology is not problematic for the author; the word smart represents the main feature of smart contract technology: *automation*[191]. This means the system is able to work on its own based on the conditions set forth by the parties. Szabo says: 'I call these new contracts smart because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform

[187] (Cardozo Blockchain Project 2018). P13.

[188] (Cardozo Blockchain Project 2018). P13.

[189] (Savelyev 2016).

[190] (Allen & Widdison 1996). p25. and (Morrison 2019).

[191] Farrell, S., Machin, H., Hinchliffe, R. (2018). Lost and found in smart contract translation - considerations in transitioning to automation in legal architecture. *Journal of International Banking Law and Regulation* Volume 33(1), p24-31.

on these promises.'[192] It must be understood that smart contracts are not AI smart; a smart contract cannot execute on a self-learning basis similar to the human brain, it can only automatically run the system in accordance with the terms and conditions set forth in advance.

In being a software program, a smart contract does not merely constitute a contract as in the traditional sense. *Contract* means a legal act based on the manifestation of the mutual wills of the parties to make a contract[193]. Therefore, the terminology does not exactly reflect the nature of smart contracts since they are technically not contracts per se. However, they might gain contract features when the parties enter into the system and the system actually works.

2.9.2. Computer Programs as a Contract

He smart contract has distinguished itself from a physical contract with two key qualities; (i) there is no physical text as in physical contracts. Smart contracts perform without the need of the parties' intervention; (ii) they have a tamper-proof[194] nature. The author considers that the written text problem can be overcome as analysed in section 2.2; a contract can be concluded even verbally unless the law needs a special format. The feature of immutability or being tamper-proof can be a problem in terms of contract termination[195]. In blockchain, intervening in the system once the chains are created is difficult because the system works on blockchain technology, which is under the control of multiple parties. This makes it difficult to halt the autonomously performing system.

[192] (Szabo 1997).

[193] Article 1 of TCO.

[194] Clifford Chance. (2017). Are smart contracts contracts? Talking Tech looks at the concepts and realities of smart contracts. Available at: https://www.cliffordchance.com/briefings/2017/08/are_smart_contractscontracts.html.[22March2019]

[195] *see section* 2.9.3 and 3.6.1.

From the technical point of view, smart contracts are based on the idea of embedding contract clauses in the software program. Smart contracts may not amount to a contract since technically they are basically computer programs[196]. However, smart contracts gain contractual sense with the implementation of real life transactions. This technology-based contracting method also makes breaching the contractual obligations expensive; therefore, it automatically creates a deterrent for the potential violating party. In the software, the contract terms are written in computer language consisting of strictly defined semantics and syntax[197].

In physical contracts, conflicts are mostly based on the misinterpretation of terms and this leads parties to consult with a third party, such as the courts or mediators, to solve the issues. In smart contracts, the system does not allow misinterpretation by its nature. Since interpretation is based on the machine, not performed by the human brain, it does not create subjectivity (it runs according to the terms agreed on by the parties and embedded in the code) in its execution, and cancels any potential conflicts raised by misinterpretation, thus negating the need for a third party mediator.

2.9.3. Tamper-Proof Quality

As the natural result of being a software program created over a distributed ledger, the blockchain platform cannot be changed easily once it has been created. Each block is connected to the other blocks created both before and after it (consecutively in the chain). Once the chain has been created, it is not easy to amend it since every block has to be then re-generated. This also means that in blockchain driven operations, once the parties have entered into the system, they cannot easily intervene in the execution[198].

[196] (Finck 2018). p25.

[197] (Savelyev 2016).

[198] (Schulpen 2018). p18.

This feature of blockchain is also called being *immutable*; however, this term has been criticized since the system is technologically amendable, per se[199]. I also believe this word can be misleading but, on the other hand, it is not completely misused since tampering with the system is difficult, costly and impractical. This is not likely to be an option that people will go to in practice. I will use the term tamper-proof since it is more relevant to its nature, unless it is necessary to use immutable in order to emphasize the needs of the section, as in section 3.6.1.

Contrary to the legal difficulties it may cause, the tamper-proof feature creates transparency and gives the business owners the ability to operate their businesses with numerous different stakeholders in a more transparent and secure environment. This is because if there is an attempt to change a block or some data in a block, the whole transaction will have to be re-written and approved by more than 50% of the network, otherwise it will be rejected. Each party has to be honest at the beginning since they all have copies of the system database synchronized with the other participants in the network. This consensus mechanism[200] in the system makes it difficult to tamper with the system and creates a transparent, trust-based environment, accordingly. [201] On the other hand, in a blockchain-based transaction, the actions are irreversible and this means, in terms of a cyber-attack, the parties may not claim recovery of their losses[202] although, depending on the nature of the transaction, there might be different precautions to avoid potential losses. For instance, in bank transactions, people can call and ask for the cancellation of a card, an account or for the cessation of transaction. Loss does not have to be the result of an illegal act; there might be a code-typing error that causes certain losses.

[199] (Finck 2018). p90.

[200] (Cardozo Blockchain Project 2018). p2.

[201] (Savelyev 2016).

[202] Hari, O. and Pasquier,U. (2018). International Business Law Journal. *Blockchain and distributed ledger technology (DLT): academic overview of the technical and legal framework and challenges for lawyers*. 5. p423-447.

I must emphasize here that once the system is implemented, it cannot be amended easily in technical means. In other words, it is not impossible to amend the system although it is a challenging and costly procedure, which may not be practical in real life: "Because blocks are linked through hashes, changing information on a blockchain is difficult and expensive"[203].

2.9.4. How Do Smart Contracts Fit Into Existing Laws?

As mentioned earlier in this research, basic principles of contract formation are accepted in the contracts concluded on digital platforms, with some clarifications for the service providers[204]. A contract requires an offer and acceptance to be concluded, consideration to support the promises made in the agreement, and an intention to create legal relations[205].

Smart contract technology offers people a means of establishing a contractual relationship through blockchain technology based on a computer program. It is necessary for the parties to express their mutual and consentaneous (*karşılıklı*) intents in order to be able to talk about a legal contract. The main components for a contract to be deemed legally valid are mutual and consentaneous (*karşılıklı*) intents, as well as the contract provisions complying with the mandatory legal rules, personal rights and morality, and having a subject that is not impossible. Article 27 of the TOC states: "*Contacts that are contrary to the compulsory provisions of law, to morality, to personal rights and of which subject matter is impossible, are null and void. The null and void nature of a part of the terms that a contract includes does not affect the validity of the other terms. Nonetheless, if it is inferred clearly that without those terms the contract would not have been concluded, the entire contract becomes null and void.*"

---

[203] (Finck 2018). 30.

[204] *see* section 2.3.

[205] (Reed 1996). p250.

The self-executive and automated nature of smart contracts does not mean that these components will not be needed for the validity of the contract. For the application of contract law principles to smart contracts, the author considers that people have to look for the existence of intent in the parties as a first step. In smart contracts, the intent usually can be seen at the time of entering into the contract[206]; intent and the other above mentioned components will be looked for in smart contracts and the most important point might be proving the mutual and consentaneous (*karşılıklı*) intents of the parties.

It is useful to take an example to analyse this subject. In a smart contract-driven crowd-funding project, the crowd-funding provisions are generally designed by the beneficiary and the donors accept these predefined contract provisions and provide a value to the fund (transferring an asset). By transferring an asset, people are accepting the beneficiary's offer, and this demonstrates mutual and consentaneous (*karşılıklı*) intent. In most smart contract scenarios, there is an asset transfer and this (as a material obligation) helps to prove the existence of the mutual and consentaneous (*karşılıklı*) intent.

The program is able to perform contractual obligations without needing human intervention at any level of a transaction. However, this nature of smart contracts does not mean that with smart contract technology people will not need any legal procedures. "A smart contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable, either by legal enforcement of rights and obligations or tamper-proof execution of computer code."[207] This means new intermediaries might be needed in terms of tackling some issues[208].

Under Turkish law, for the formation of a contract, parties must express their mutual and consentaneous (*karşılıklı*) intent to enter into a contract. In practice, contracts are mostly

[206] (Schönfeld 2018). p13.

[207] Clack, C., Bakshi V.A. and Braine, L. (2017). Smart Contract Templates: foundations, design landscape and research directions. *Cornell University, Computer Science, Computers and Society*. Available at: https://arxiv.org/abs/1608.00771. [19 April 2018].

[208] *see* section 1.7.

established around this premise and the freedom of contract principle; there are no strict formation rules for contracts to have to be valid.

In contracting, the most important point is to be able to determine if the contract has been concluded: when and where it has been concluded and how, no matter if it is a physical contract, a digital contract or a smart contract. The crucial point will be in determining what constitutes an offer and acceptance, regardless of what platform they are in. As seen in digital contracts, for instance, these may be click wrap agreements. Technology has already affected traditional practices of contracting; now people can show their approval by clicking an accept button on a web-site and this is accepted the same as an ink signature in a physical contract[209].

The author considers that transactions carried out using smart contract technology can also be subject to the rules of physical contracts, and that meeting the minimum criteria for a physical contract to be valid will be considered necessary in making smart contracts valid as well. However, in smart contract transactions, as with the first step in every contracting scheme, to be able to say there is a contract or not, people must know who and where the parties are, otherwise a governing law can be an issue[210]. Before applying traditional contract rules, one must know these main components of a transaction. Unfortunately, these may not always be clear in every transaction; therefore, it is not possible to come up with one solution that suits all transactions. Each transaction has to be assessed at that point separately. With this approach, the author considers that rather than a whole new legal regulation having to be passed, practical guidelines on implementation and application procedures would be more helpful. The rules of verification between the parties, for instance, order requests to banks, or the phases where human intervention may be needed can be regulated specifically to ease the use of smart contract technology for people.

[209] (Deveci 2007).

[210] Rogers, J., Jones-Fenleigh, H. and Sanitt, A. (2017). Arbitrating Smart Contract Disputes: Negotiation and Drafting Considerations. *International Arbitration Report,* Volume9, p21-24.

The system that has been adopted in e-commerce transactions demonstrates a great example of regulating the smart contract approach. In most jurisdictions, electronic commerce is not strictly regulated; for instance, in Europe, the EC Directive says that every business has to explain, when the contracts are made, the technical and business needs of the transaction/operation[211]. In line with this, Amazon has come up with a detailed terms and use list which explains the contracting process to customers in advance. Essentially, it says that when a customer orders a product, he makes an offer but that there is no contract until Amazon sends the customer an email saying that they have dispatched the goods.

In smart contract transactions, parties can do the same. They can lay down a structure regarding where and when the contract has been made, considering the needs of the transactions, in order to demonstrate they have achieved a meeting of the minds[212]. As in the e-commerce sector, in smart contract-driven transactions, the author considers that every transaction will be individual; thus, it is hard to give one answer that fits them all. It should also be borne in mind that the rapidly changing nature of technology makes it hard for the legal realm to keep up with technological developments.

In the US, the Statute of Frauds applies to the contracting processes. Smart contracts must comply with these rules in the contracting sense. Briefly in contract conclusion, the parties of the contract have to manifest their intent to enter into a contract and to be liable for it. They need to demonstrate the main components to concluding a contract, those being: a definition of the parties, clarification of the substantial elements of the transaction, and it must be signed using an admissible signature scheme[213].

[211] Directive 2000/31/EC, Article 10(1)(a).

[212] (Schönfeld 2018). p13.

[213] (Cardozo Blockchain Project 2018). P17.

In the US, the State and Federal Common Law and related statutory laws govern commercial contracts.[214] 'Smart contracts may exist in commerce. No contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract contains a smart contract term.'[215] Therefore, creating novel regulations for the application of smart contracts has also been seen as needless by the Chamber of Digital Commerce. The idea is clearly put forward that if a contract established using smart contract technology has the legal conditions necessary for the validation of a physical contract, this smart contract is considered to be subject to the relevant existing law applicable to its contracts. Otherwise, it might create a huge burden on the stakeholders in the market and will be far away from efficient. Similarly, in the UK, the legal side is seeking to find ways to apply existing legal principals to smart contracts as well[216].

In a nutshell, entering into a smart contract will not affect its assessment as a contract[217], provided that the parties have the legal capacity to do so enter said contract ("Entering into a binding contract requires the legal capacity and the capacity to act, otherwise the contract is void *ab initio*"[218]). Parties will be able to manage the performance of obligation in electronic contracts unless an obligation is strictly regulated to be performed in a certain way under the law (e.g., a deed or a real estate sale agreement). For instance, in subcontracting contracts, the liability must be shared between the parties. In other words, the contractor and the employer are held mutually responsible for the employees; the clauses contradicting this rule are deemed invalid, according to sub-employment regulation.

[214] (Chamber of Digital Commerce, United States of America 2018).

[215] (Chamber of Digital Commerce, United States of America 2018).

[216] (Maclean 2017).

[217] (Schönfeld 2018). p13.

[218] (Schönfeld 2018). P13.

2.9.5. Smart Contract Governance Issues

Smart contracts may not amount to a full contract since technically they are computer programs[219]. However, smart contracts will gain contractual sense once they are implemented in real life transactions. In physical contracts, the first thing to put in place is the intention of the parties to enter into a contract or to be bound in a legal relationship for the contract to be considered valid.

In smart contracts, it may not be clear if the parties intend to form a contract; smart contracts are a form of contract between strangers, created in a code that is not readable by humans. Identification of the parties is important regarding contractual obligations; not being able to identify the parties is a problem in terms of applying contracting principles. If the contracting parties are hard to identify, legal enforcement is a problem[220]. In the blockchain system, a user's identity is often hidden in the public keys[221]. In permissionless blockchain systems, there might be a large number of users involved and they are not easily identifiable. Also, if the parties do not know where the other contracting parties are, the governing law will also be an issue. To be able to talk about the application of contract rules to smart contracts, these issues must be addressed as well. While accepting the benefits and contributions of smart contracts in the operation of corporate transactions, it is critical to know that they are not 'stand-alone'[222].

As discussed in detail within this dissertation, technically a smart contract is a program created via computer codes operating transactions pursuant to the terms set forth primarily; therefore, smart contracts do not automatically constitute a contract[223]. Its

[219] (Finck 2018). p25.

[220] (Finck 2018). p27.

[221] (Finck 2018). p90.

[222] (Mehta 2017).

[223] Davine, A. and Boring, P. (2018). Coindesk. State-by-State Smart Contract Laws? If It Ain't Broke, Don't Fix It. Available at: https://www.coindesk.com/state-state-smart-contract-laws-aint-broke-dont-fix. [20 March 2019].

nature is a digital instruction set to operate subject to the agreed consecutive events. The act of the parties, starting from the execution of the transaction (such as the expression of intents of the parties), gives the smart contract a chance to be considered equivalent to a physical contract.

In terms of ownership of crypto-currencies, property law principles may also be applicable with interpretation[224]. For example, in crypto currency transfers, only the account owner can control the money. Other than the crypto currencies, there are different assets that can be exchanged on a blockchain driven systems. These assets can be physical devices, such as embedded microchips that are controlled electronically[225]. Before spending their crypto currency, people have to prove to the network they have the right to spend it by being in possession of a private key allowing them to operate transactions in the system. Otherwise, the system does not allow them to spend the money.

The contracts used for digital rights management, for instance, copying music or video and other content created online, are considered an example of how to understand the way smart contracts work since they also provide a self-executing sanctioning system for contract breach, for instance, in terms of breaching the copyrights of an author by copying his/her work or sharing it without permission. Another automatically executing example can be Microsoft Word, the computer program used in almost every office daily. Once the license of the program has expired, the system automatically ceases the service by locking the program. The system stops working and then notifies the user to update the license.

There is no specific legal regulation in terms of governance of smart contracts in Turkey or around the world. However, the interpretation of existing contracting principles and of e-commerce laws seem promising to the extent that a smart contract concludes with the same minimum requirements necessary for a physical contract to be considered valid,;

[224] Legalar eBook. (2018). Blockchain for Lawyers. p24.

[225] (Walsh 2015).

i.e., the rules applicable for physical contracts could be applicable for smart contracts, as well. In order for the system to work efficiently and for people to be able to use the smart contract systems in practice, specifications regarding smart contracts could be regulated in accordance with the existing contracting principles. For example, the physical steps in terms of a breach of a smart contract can be clarified for people to understand. This could lead to more trust in smart contract-driven transactions.

As mentioned earlier, the Chamber of Digital Commerce has made it clear in the US by saying: "Existing legal frameworks for defining and giving legal effect to contracts cover smart contract technology, and nothing regarding smart contracts ought to change existing definitions or the application of current contract law. Additional laws are largely unnecessary and will only serve to confuse the application of current law"[226]. In the US, provided that the contracting parties have agreed on a written consensus to operate the business on an electronic platform and agreed on essential contract terms[227], they will be subject to the provisions of the Uniform Electronic Transactions Act (UETA) and the Electronic Signatures in Global and National Commerce Act (ESIGN).

Specifically, the UETA and ESIGN ensure the following; (i) If a law requires a signature, an electronic signature satisfies the law; (ii) If a law requires a record to be in writing, an electronic record satisfies the law; (iii) a contract, signature, or related record may not be denied legal effect or enforceability solely because it is in electronic form; (iv) A contract may not be denied legal effect solely because an electronic record was used in forming the contract.'[228] Also, in Arizona, the Arizona Electronics Transactions Act (AETA) was amended in 2017[229] to accelerate the enforceability of blockchain-based transactions and

[226] The Chamber of Digital Commerce is an American advocacy group that promotes the emerging industry behind blockchain technology, bitcoin, digital currency and digital assets.

[227] (Cardozo Blockchain Project 2018). P17.

[228] (Chamber of Digital Commerce, United States of America 2018).

[229] Ramberg, C.H. (2001). The Ecommerce Directive and formation of contract in a comparative perspective. *Global Jurist Advances*, Volume1(2). Available at: https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/globjur1&id=782&men_tab=srchresults. [19 March 2019].

signatures relating to the sale of goods, leases and documents in 2017.[230] The functional equivalency principle in the UETA might be illuminating for the legal realm for the better interpretation of smart contracts. UETA sec 7: "(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form. (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation." UETA was introduced in August 1999 and has been a success.

In the meantime, the Law Commission of England and Wales has just started working on regulations for smart contract enforceability. They are working on being able to say if 'the law is sufficiently certain and flexible to apply in a global, digital context and to highlight any topics which lack clarity or certainty'[231]. This report is proposed to be published by the end of 2019. In the meantime, in the United States, initial steps have already been taken in terms of regulation; it has been approved and permitted by the US Securities and Exchange Commission that a retailer company (operating over the internet) can issue company stocks using a blockchain technology platform and the distributed ledger has been recognized by the State of Vermont[232].

In Australia, smart contracts have been stated in the law; the Australian Electronic Transactions Act 1999 presents a legal application structure for smart contracts to be considered the same as traditional contracts and to be bound in existing contracting principles[233]. In the end, it will be useful to define the liability of the parties in the smart

[230] Legal Blockchain. (2018). State Laws Recognize Impact of Blockchain on legal Sector. Medium. Available at: https://medium.com/blockchain-for-law/state-laws-recognize-impact-of-blockchain-on-legal-sector-6749d71fc982[19Jan2019].

[231] UK Law Commission. (2019). Smart Contracts Current Project Status. https://www.lawcom.gov.uk/project/smart-contracts/.

[232] Gapgemini Consulting. (2016). Smart Contracts in Financial Services: Getting from Hype to Reality. Available at: https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf.

[233] Law Business Research Ltd. (2018). Cryptocurrencies and Icos. *Financial Technology Law Review*, p9. Available at: https://thelawreviews.co.uk//digital_assets/67c3bd30-3e6e-4663-b760-753f64fadb43/The-Financial-Technology-Law-Review----Edition-1.pdf.

contract system, as well as the people who created the system[234]. It will ease the conflict of knowing in advance who is liable for what.

Governance of smart contracts can be achieved only if it is regulated on an international basis as the technology that lies behind this phenomenon is emerging simultaneously around the world. People need global remedies rather than local regulating rules[235]. Another important point in regulating smart contracts and blockchain technology is to look into the uses and working principles of the systems and regulate its uses, not the technology itself. People will need guides and explanatory reports to encourage them to implement this system in their business transactions. Also, being a system that interacts and works in cyberspace, smart contracts can be in multiple places at the same time when connected to the Internet[236]. Therefore, looking at this matter globally is vital.

In terms of a legal approach, blockchain technology might be analysed in the light of other legal principles[237]: property law, financial market regulations and company law, as well. In this study, only contract law principles will be visited in terms of their applications to smart contracts.

2.9.6. Contractual Liability in Smart Contracts*

In smart contracts, the liability scheme for traditional contracts may be applicable in accordance with the scope of the transaction. Also, the scope of liability may include liability related to computer program defects (generally, in the code). User safety is important in this scheme; attention paid to this could also contribute to the trustworthiness of the system. The author considers that liability for damages can be regulated as in commercial agreements; parties can determine the limitation of liability considering the nature of the transactions (considering carefully the consumer regulations

[234] (Schönfeld 2018). p29.

[235] (Schönfeld 2018). p29.

[236] (Finck 2018). p20.

[237] (Hari & Pasquier 2018).

and local jurisdiction). In addition to this, general contract liability rules for defects can be applicable.

Determining a liability scheme in advance would be useful for the parties, given the system's tamper-proof nature; once an unlawful event occurs, it is not easy to deactivate and halt an ongoing transaction. In such a case, parties cannot blame the system as a contractual party[238]. At this point, Lessig's article written in the late '90s sounds more relevant than ever: "while benefiting the technology uses in transactions, computer programs encourage the evolution or convergence of the legal realm to it "[239].

The author considers that the situation of liability schemes on computer programs may also be relevant when looking at liability in smart contract-driven technologies. That being tedious about the defect-free nature of the programs could affect the development of the industry is a major criticism. This will not be analysed here but, in a nutshell, the technology realm generally believes that innovation must be preferred over safety in order to foster development: 'information itself depends on the innovation but not on the safety and in the long run the innovation also leads to the development of the information's quality and safety.'[240]

2.9.7. Governing Law

In physical contracts, the parties generally designate the governing law. Particularly in international contracts having foreign elements, the parties freely agree on the governing law for the resolution of any conflicts arising from the contract. The general rule is to

[238] (Finck 2018). P28.

[239] Ieva, Giedrimaite. (2019). IPKat Blok. Smart Contracts: Pros and Cons of the New Shiny Thing. Available at: http://ipkitten.blogspot.com/2019/03/smart-contracts-pros-and-cons-of-new.html. [22March2019].

[240] Olgierd Pankiewicz. (2012). Freedom of contract in computer programming and the information society: why statutes deserve more than coup de grace? PhD. Newcastle University, England. Available at: https://theses.ncl.ac.uk/dspace/bitstream/10443/1912/1/Al-Eliwi%2C%20A.M.K%2C%2013.pdf.[10Feb2019].

apply the Turkish law in the Turkish Courts. However, for transactions having foreign elements, it is possible to apply foreign law. This is explicitly stated under Turkish Law in Article 9 of the Law on Private International Law and Procedural Law, law no 5718 ("PIL"). Foreign elements might be in different components of the contract: execution of the contractual obligations might take place in a foreign country, the parties might be foreign or they might be residing abroad, the habitual residence or work place of a party can be in a foreign country. These are accepted as objective foreign elements. Also, without having these objective elements in the contract, the parties can agree upon a foreign law as the governing law. The parties' mutual choice on the governing law is accepted as a foreign element, as well.

Once the parties have agreed on a governing law explicitly in the contract, this designated law is applied. According to Article 24 of the PIL, even if the governing law is not explicitly designated, if it can be concluded without hesitation from the provisions of the contract, it is accepted as valid. It is critical to designate a governing law in the contract; it helps the parties when seeking ways to remedy a conflict when there is no provision for it in the contract. The parties do not have to designate a governing law in the contract; the lack of this provision does not make the contract invalid. In the case where this arises, the most connected law to the contract is applied to the conflict. The governing law is generally accepted to be based on the debtor's habitual place of jurisdiction at the time the contract was established or, if this is not a relevant jurisdiction of residence, the law of the work place If the contract is a commercial contract and the debtor is not based in one work place, the most relevant work place jurisdiction is applicable. Despite these options, if there is a more strictly relevant place of jurisdiction for the contract, that will be applicable.

It does not make any difference in terms of online contracts; the governing law is designated in accordance with the rules stated above, depending on the content of the contract scope. In a conflict arising from smart contract-driven transactions, the parties might have damages or claims arising from the transaction. In this case, the issue might be taken to court. For those conflicts, the author considers that the governing law should

be designated in the following order; i) if the parties have a written consensus on the governing law, this law will be applied subject to the discretion of the court (maybe following emails of negotiation before implementing the system); ii) if there is no written arrangement in this regard (the author considers that it is like to be the case for smart contract transactions) the most connected law to the contract is applied, which can be the law of the habitual residence of the debtor of the characteristic performance, the law of the workplace or (in the absence of a workplace) the law of the residence of the abovementioned debtor in cases where the contract is concluded as a result of commercial and professional activities. I would like to rephrase here that this scheme is possible only where there is a contract. It is of paramount importance to determine first that the transaction has the components that are looked for in traditional contract conclusions.

In permissionless blockchain systems, as in Bitcoin an Ethereum, where there are large numbers of users (miners) involved, it may not be easy to identify the users and their locations. This could cause severe legal problems when enforcing contracting principles, including when determining the governing law. These issues are mentioned in the following section III in detail.

SECTION III

3. Obstacles and Challenges

In this study, I aim to explain the concept of the smart contract and its benefits to the actors of the leading sectors and governmental bodies. In order to achieve this, I understand that I have to analyse the potential challenges in practice and assess what smart contract technology promises to overhaul those practical challenges. However, there are challenges that come with this system. The first is not being able to amend a transaction once it has been launched. In the legal realm, this might create problems with data protection compliance procedures or contract termination can be challenging. Ari Juels, professor at Cornell University, stated once: "Contract law makes provisions for the modification, amendment or annulment of contracts. Technical mechanisms in smart contracts can achieve analogous goals. One possible approach is what people often refer to as an escape hatch, a pre-programmed way of changing the terms of smart contracts. Ensuring that the right permissions are incorporated into the escape hatch itself is as tricky, though, as is ensuring its correct implementation"[241].

Currently, people are not able to fully negotiate the contract terms that they are entering into once the system is already set forth in most of the cases. This may not be the same in all types of transaction, although it can be an issue in standardized contracts, where it is not practically possible for people to negotiate the contract terms. For instance, in electricity subscription contracts, people are still investigating a good example of this. However, their ability to suggest legally binding online contractual arrangements has lost its common practice lately.

A further potential problem is not knowing the contracting parties. This could be a problem in terms of applying traditional contracting rules: to be able to enforce the contract terms or claims, the contracting parties must be determined. If the contracting

[241] (Gapgemini Consulting 2016).

parties are hard to enforce legally, that is a problem. If a party does know where the other parties are, they will also face an issue in determining the governing law.

Even though having a huge potential in mitigating the long lasting, complicated procedures involved in transactions, smart contracts come with a number of questions and hurdles. For instance, in the application of Ethereum, to make it available for people to use in order to spread across and work on transactions, customized platforms supporting the smart contract technology are necessary[242].

Although blockchain technology is paving the way for the development of smart contracts in practice, the author considers that people still need some time to get used to implementing the system. This time can be shortened by cooperation between the technological and legal realms in mitigating the ambiguous points in the system, both legal and technical. A more transparent system will make its way more quickly into practise. Generally, people (especially corporations) would not like to take a risk, and they want to see examples of uses that have worked in practice before they go ahead and implement a brand new system to work within their operations. This is very understandable behaviour in the corporate world. Besides, the smart contract implementation process is still not quite smooth and easy. It requires a lot of work and expenses. First, the technical substructure must be created, and this can be challenging considering how difficult it is to match their existing systems with the new smart contract system.

Real life interaction is still quite confusing. Since smart contracts are basically run using a computer program, it is difficult to ascertain how the parties in such an automated system will act in real life. The system cannot determine by itself whether a party is being untrue or not or make sure the delivery is being carried out properly or not. Depending on the features of the transaction, it can confirm certain things, such as when the payment was made, but not all the obligations are easily tracked. Obviously, it is not easy for a computer program to guarantee actions in the physical world. For example, the system

[242] (Hertig 2014).

cannot easily control whether a product has really been delivered to the recipient as agreed in the contract, or a developer, in accordance with the terms of the contract, has completed the work according to the technical requirements agreed. As Ripple's Codius put forward: "A smart contract execution is only as good as the inputs it takes in, and it may be difficult to find inputs which are sufficient to the job which both parties trust."[243]. Smart contracts can manage simple transactions, such as vending machines. However, there are actually myriad complexities when determining the conditions with details. For example, in lease contracts, a landlord typically complies with reasonable wear and tear, but requires compensation for substantial damage. In smart contracts, it is hard for the code to discern that difference, as well as other intangible ideas such as good faith, reasonable care and skill, or acting as a reasonable entrepreneur[244].

It must be critical to know that even if it were an automated system, in smart contract-driven projects, organisations would still need human interaction. In addition to the implementation of the technical substructure, they would need to hire experts[245] to run the system and to track the transactions[246]. In a smart contract-based operation, it is clearly very important for the developers and lawyers to work closely together, coordinating with other parties in multilateral transactions, for instance, with suppliers and their lawyers.

3.6. Practical Challenges

The benefits of smart contract technology have been discussed in this study in detail. The most appealing benefits can be listed as: the potential of decreasing the level of fraud and an increase in efficiency, speed and transparency in operations and incomes, while helping to decrease the costs. However, while this smart contract technology promises very efficient solutions that could be applicable to the majority of operations in practice, the inevitable question arises: Why does the world hesitate to use this technology despite

[243] (Walsh 2015).

[244] (Mehta 2017).

[245] See section 1.7.

[246] (Farrell, Machin, Hinchliffe 2018).

all the benefits? The reasons can be noted down as follows: lack of clarity, legal governance, question marks in terms of efficiency.

Using such technology is still not common practice, especially in Turkey; there are a few instances of blockchain driven projects. These examples are often internal; the companies who create and use these blockchain-driven smart contracts usually run such projects with transactions completed within the framework of a legal entity (not including a party outside of the legal entity) and that is the biggest reason why these operations remain only as pilot smart contract applications. In fact, this technology can shows its best potential and benefits in transactions where there are many different stakeholders.

3.6.1. Being Immutable as A Challenge

Since the smart contracts are created on blockchain platforms on distributed ledgers as software programs, this makes them difficult to change after the parties have entered the system. Briefly, the first blocks are created consecutively, and in each block, the creation of the previous and the next blocks are verified, so the blocks are connected to each other and amount to a chain. In other words, each block is chained to each other and recorded and then hashed with a time stamp in the ledger[247]. In this sequence, it is quite difficult to intervene once the blocks have been generated. This feature is named immutability or being tamper-proof[248]. As mentioned earlier in section 2.9.3, this term is fairly criticized. Although I find the criticisms appropriate at this point, I would like to use these terms in this section to analyse challenges.

The immutable feature of smart contract technology has fundamental implications for the users of the systems that are set out on the blockchain platforms. Transferring data through the Internet can carry risks of it being tampered with or copied[249]. In blockchain-

[247] Finck p90.

[248] see section 2.9.3.

[249] (Hari & Pasquier 2018).

based systems, parties can transfer data knowing that it cannot be duplicated. This gives the business owners the ability to operate their business with numerous different stakeholders in a more transparent and secure environment, even though the parties will not be able to say much relating to an operation that they are engaged or about to be engaged in[250]. Despite being a huge advantage, this feature of immutability has a great potential to create challenges in practice.

Considering the nature of immutability, there are troubling questions: is it possible to have a mistakenly written chain? How can people correct the mistake in the chain? The answers to these questions, the author considers, lie in the creation of the chain. During the creation phase of the chain, users have to check and approve the accuracy of the code. Since there are (especially in the permissionless blockchain systems) a lot of users in the system, the risk of having a wrong chain is quite low. These users in the system check the codes and approve them. This may reduce the risk of having a broken chain and thus a broken block.

Immutability can create other challenges for people to deal with in smart contract-driven transactions. Smart contracts do not need human intervention for the system to work once it is created. However, as mentioned above in section V in detail, in some examples human intervention in some specific phases might be inevitable. For example, in a supply chain transaction, the truck that carries a product for delivery could be delayed for a number of reasons and the system would not know the reason for this delay and not be able to prevent the unwanted consequences. This kind of lack of information, or system fallibility, can interrupt the transaction.

From the legal side of this immutable concept, the parties which are in the economically deficient position might find a legal protection mechanism. First of all, everyone is obliged to comply with the acting in good faith principle regulated in Article 2 of the TCC and to act in accordance with the good faith rules when performing rights and obligations. It has been clearly stated in the text of Article 2 that legal regulations do not

[250] (Gapgemini Consulting 2016).

protect the explicit abuse of a right. On the other hand, if there are conditions in the situation, the provision of prohibiting abuse of dominant position (*Hâkim Durumun Kötüye Kullanılması*) can be applicable[251].

3.7.Technical Challenges

The author considers that the most important technical challenge is also the most beneficial aspect of the smart contract system, which is immutability. In smart contracts, the parties generally express their consent to the contract terms designated in advance and the automatic execution of the contract at the moment of entering into the system[252]. As a result of immutability, the parties are not able to say much during the execution process. Once the system has been launched, from that point on, the parties have only one option: to trust the system. They cannot change the main characteristic of the transactions that make the system work as only the data entered into the system may be updated. In physical contracts, the parties can enter into additional protocols if they want to amend the initial terms that they have agreed upon. This can even apply to the main characteristic of the transaction. Unlike with physical contracts, in smart contracts, the parties rely on the system which is a computer program, instead of on the other party to perform the contractual obligations[253].

It must be acknowledged that smart contracts do not eliminate the problems arising from contractual relationships totally, thus creating a total hurdle-free contracting process. It may only help on resolving basic conflicts between the parties without going through legal procedures if agreed on and implemented in advance. As a result of being a computer program, there are risks that may arise from the computer code bugs and errors, and it is impossible to ensure prevention of hacking completely. For example, risk-

[251] Competition Protection Act, no 4045, date 13/12/1994. – Art 6: "The abuse, by one or more undertakings, of their dominant position in a market for goods or services within the whole or a part of the country on their own or through agreements with others or through concerted practices, is illegal and prohibited."

[252] (De Filippi & Wright 2018). p74.

[253] (Savelyev 2016).

causing matters have been evaluated, and ether equal to more than 30 million US dollars may be at risk in half of the smart contracts written on Ethereum[254].

I think it is important that, while analysing the contractual acceptance of smart contracts, the technical aspect of this phenomenon should work relentlessly on drawing up technical guidelines. In order to have a correctly implemented smart contract system, people must adopt an escape hatch based on the nature of the transaction in order to avoid challenges, and this is only possible if they are given proper and clear guidance in advance.

3.7.1. Hacking

There are always flaws (i.e., errors, bugs) in computer programs and there always will be. Hackers will keep finding ways to attack the systems via those errors. This correlation grows in alignment. For instance, in June 2016, an attack took place at the Decentralized Autonomous Organization (DAO), an organization established on the Ethereum system as a smart contract, and attackers escaped with around 50 million US Dollars-worth of ether, squeezing it into the system via security flaws in the code[255]. This means the smart contract-friendly corporations and institutions have to consider intense security precautions. Moreover, the liability implications of such events must be pre-considered. Other risks at the technical end might arise from the following situations.

Private encryption keys potentially can be hacked as well. This has always been an obstacle for companies relying on software programs for their transactions, as big corporations like J.P. Morgan, Home Depot and Target have experienced. Briefly, these three institutions have a very critical point in common: they are all centralized. They have "one central repository of information"[256], so when the system is hacked once this

[254] (Bhargavan, Delignat-Lavaud, Fournet, Gollamudi, Gonthier, Hal 2016).

[255] Maria P. Gomez Gelvez. (2016). Explaining the DAO exploit for beginners in Solidity. Medium. Available at: https://medium.com/@MyPaoG/explaining-the-dao-exploit-for-beginners-in-solidity-80ee84f0d470. [5March2019].

[256] Banking on Bitcoin. (2016). Documentary. Christopher Canucciari. USA. https://www.imdb.com/title/tt5033790/. [3April2019].

centralized set-up enables the attackers to reach all the other accounts and gives them access to money and data. In blockchain mentality, it is not one hundred per cent possible to eliminate or prevent hacking, but the risks are not very disruptive. The decentralized nature of blockchain-driven smart contracts may lower these risks since the distributed ledger works without a centralized intermediary, being based on the consensus of thousands of users. This ledger is kept on their computers, and it is very difficult to hack a large number of computers.

3.7.2. Losing the Private Key

In the blockchain-driven systems, all the users have a private key allowing them to access the system. This key is personal to the users, and losing the key might create log-in problems. As discussed in section 1.2 of this thesis, in blockchain-driven systems, the working principle is based on a mutual consensus of the users in the systems; therefore, a missing actor failing to log into the system might affect a whole transaction. Even if the system is quite secure, there is always the risk of losing a private key. Although memorizing the private key is the best option, this is not so feasible in real life, as in the case of a Canadian bitcoin company[257]; the CEO who alone knew the private key passed away and the company could not pay their customers in bitcoin equivalent to £41m.

Therefore, different types of storage options have been created to keep the private key safe. One is called a cold wallet, meaning it is not connected to the Internet.[258] In another option, the hot wallet, the private key is kept in an online wallet application programming interface (API). These are not seen as ideal methods of protection; there still risks of them being stolen or hacked. There is quite an interesting way of keeping the private key safe suggested by the Coca-Cola recipe myth stories; users can write the private key on different pieces of paper and keep them in safes in different banks.

[257] Anthony Cuthbertson, (2019). Bitcoin: Millions of Dollars of Cryptocurrency Lost after Man Dies with only Password. *Independent*. Available at:https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-exchange-quadrigacx-password-cryptocurrency-scam-a8763676.html. [10Feb2019].

[258] (Hari & Pasquier 2018).

3.7.3. Connectivity Problem

The smart contract system is based on a computer program and naturally has codes that work with Internet connections. Therefore, interruption of these connections can halt the transaction entirely. In blockchain, every chain represents a transaction; data regarding transactions is embedded in blocks. When someone creates a block, the data relevant to the proposed transaction begins to spread as gossip within the network; everyone tells each other about the data that has been entered and, in blockchain terminology, users verify it. While this is happening, the technical situation of users can affect the system. If a user has faster Internet, he or she will receive the data first, while some other users may not be able to reach the data at all. This situation can also halt the flow and execution of the system.

Connection interruption may also affect the speed of reaching out for consensus within the system. This can occur in the case where users do not have powerful computers or enough electrical power. For instance, blockchain transactions cannot be run and verified over smart phones at the moment; to create blocks and run the system, extremely powerful computers are needed. This technological issue definitely affects the growth of blockchain use negatively.

Implementing a smart contract system requires uploading external data necessary for the transaction, for instance, payment methods, service conditions, sanctions and other details. These are subject to the type of transaction that has been set forth by the parties. In terms of connection interruptions, smart contracts may fail to link this necessary external data to the system[259]. This connectivity problem may also affect the consensus method in the blockchain system. If even only one of the miners in the system fails to connect while a relevant block is undergoing verification, this can affect the entire chain and the system.

[259] Connect Smart Contracts to your Application, Data Feeds, APIs, and Bank Payments. (2018). Available at: http://about.smartcontract.com/. [23 March2019].

4. Enablers

Blockchain technology is promising huge potential in different aspects of contracted transactions, from speeding up the transactions to making people feel more secure through providing more transparency and efficiency,[260] especially in multilateral and global transactions. Having said that, smart contracts may not be an efficient tool for bilateral contractual relationships. Their main power is in providing an unfailing verification system in terms of transactions with multilateral parties in need of third party verification. Their potential to contribute to supply chain transactions and the financial sector is likely to be the most appealing.

In multilateral transactions, using smart contracts could help people save a lot of time[261]. For instance, in overseas supply chain transactions, smart contract technology helps parties to initiate and develop their business through enabling them to complete transactions in countries where there is no functional banking substructure. Together with vendors and suppliers, smart contracts can be a great tool for organising the internal operations of companies: for instance, in terms of employment contracts. I must make a caveat here that it is not just use cases that are relevant to smart contracts in this section; the main technology underlying smart contracts, blockchain, will be considered as well.

The use cases for smart contracts will be quite similar; they are both based on a distributed ledger that enables transactions to be recorded and stored as a whole and that gives a clear picture of the transaction[262]. This is important for multilateral-partied transactions and big companies dealing with large amounts of data in order to keep up with the procedures easily as this technology allows them to reach the verified history of a transaction with its time stamps and every other detail[263]. This would be helpful for due diligence schemes to be developed in the future.

---

[260] (Farrell, Machin, Hinchliffe 2018).

[261] (Morrison 2019).

[262] Nigel Gopie. (2018). What are the smart contracts on blockchain? IBM blockchain blog. Available at: https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/ [20March 2019].

[263] (Savelyev 2016).

The practical benefit of smart contracts in terms of internal organization demonstrates itself in legal enforcement cases, as well. Following up the procedures for the legal enforcement of contractual obligations is difficult for individuals; they require external parties (a trusted legal authority; the courts, lawyers, judges and investigators), which are invariably costly. Smart contract technology can also contribute to mitigating long-running legal procedures. This includes using smart contract technology in legal enforcement and also for mitigating legal processes; as an autonomous system, it has the potential to ease conflicts without going into the court phases.

Szabo made a very useful comparison when explaining the smart contract concept to people to help them understand it: "As much as smart phones are more functional than traditional phones, which in turn are in many ways more functional than messages written on paper, smart contracts can be more functional than their inanimate paper-based ancestors. Smart contracts can automate many different kinds of processes and operations, most obviously payment and actions conditional on payment. For example, making control of collateral dependent on whether a debtor has chosen to pay a loan on time – the fundamental logic here is automating 'if-this-then-that' on a self-executing basis with finality."[264] This means that the main working principle in smart contracts is based on conditions[265]. As Szabo emphasized at the Symposium in New York in December 2016 organised by the Chamber of Digital Commerce, as in the case of smart phones and standard phones, smart contracts can mitigate the hurdles of transactions and ease the problem-solving process with the if-this-then-that approach in the cyberspace management of physical transactions[266].

The objective and neutral features of smart contracts, as well as the promise of mitigating the long-lasting procedures, have caught people's attention. The author considers that its

[264] (Szabo 1997).

[265] (Schönfeld 2018). p23.

[266] (Schönfeld 2018). p23.

potential for allowing people to run complicated operations smoothly makes it appealing to different stakeholders from different fields of business. In practice, there are examples of a range of transfers, from easy fund transfers to complex transitions such as mortgage rate arrangements, disposing of a will, as well as controlling the household and cars via linking them to the Internet of things[267].

Another feature of the smart contract which is just as attractive as (maybe more) the fact it is objective is that it is tamper-proof, which means that smart contracts cannot easily be altered once they are built. Hence, it is believed that they can guarantee more secure online interactions and experiences. For example, security is a major concern in terms of bank transactions; smart contracts can be a solution by offering more secure relationships between the customers and the banks or other payment institutions.

In banking services, such as the issue and offering of loans, automatic payments can be made directly between the parties by smart contracts. In terms of online shopping, customers and sellers will be able to connect without using a third party, such as Amazon, if they create their own payment services systems. In insurance transactions, companies can use smart contracts to easily verify and process claims, and in postal services, smart contracts enable verification before payment on deliveries.

In practice, concerns related to the identification of parties for physical contracting are often solved by using notaries or the apostil system (especially for the international circulation of documents). Blockchain technology promises to maintain trustworthiness without the involvement of an intermediary (a registrar, financial institution, notary, etc.)[268]. Thus blockchain has the potential to provide equal access to transparent and trustworthy information to stakeholders from different sectors.

[267] Jay Cassano. (2014). What Are Smart Contracts? Cryptocurrency's Killer App. AppEconomy. Available at:https://www.fastcompany.com/3035723/smart-contracts-could-be-cryptocurrencys-killer-app. [30April2019].

[268] (Savelyev 2016).

Smart contracts can help speed up the procedural steps in notarization or in the registration process before land registry[269] since there is a very reliable verification phase in the system. For example, in terms of notarization, even though notarization does not always constitute a validity element for contracts, parties prefer to do notarization to avoid claims regarding illegal signatures. Notarization confirms the signatures on a range of types of document (e.g., share transfer agreements for limited liability companies, sales of immovable property). Notarization is not a mandatory procedure and does not affect the validity of a contract. In an international commercial conflict involving a link agreement, one of my clients faced recently, even though the original copy of the contract was submitted to the court, the judge requested a notarized copy before taking the link agreement into consideration as reliable evidence. Notarization provides reliability to the parties in commercial relationships; this is the equivalent of verification in smart contracts. Smart contracts naturally provide a reliable verification system, which eliminates the need of notarization, and thus costs. The tamper-proof nature of the distributed ledger is a great asset for proving the accuracy and admissibility of data regarding transactions in court actions[270].

There are stamp duty obligations for parties in terms of contracts involving a financial value. This might be the trigger for opting for smart contract-based transactions. An update can be made to the related legislation to help the smart contract system connect directly to the tax authorization system and facilitate the calculation of the tax amount to be paid, and then make the payment automatically. According to Article 18/3 of the Turkish Commercial Code[271] ("TCC"): "merchants make the notices and warnings to put the other party in default, to cancel the contract, renege on a contract via a notary, registered letter, telegraph or registered electronic mail system with an e-signature."

[269] (Meyer 2017).

[270] (Pentland, Nathan & Zyskind 2015). p5.

[271] Turkish Commercial Code, no 6102, date 14/02/2011.

The registered electronic mail system presents a great example to help us to understand the operational structure of smart contracts and help us to adapt this technology to the existing systems. For instance, in the smart contracts system, parties do not need to check and see if the other party has fulfilled their obligations and taken action; the system is able to confirm the status of the fulfilment of contractual obligations and automatically creates notices or warnings to put the other party in default.

In a study published by the Smart Contracts Alliance, a working group of the Chamber of Digital Commerce collaborating with Deloitte outlined the twelve industries in which smart contracts could be implemented. These include: digital ıdentity, records, securities, trade finance, derivatives, financial data recording, mortgages, land, title recording, supply chains, auto ınsurance, clinical trials, and cancer research[272]. Below I will try to give details about the industries that smart contracts can add value to, taking into consideration those listed by the Chamber of Digital Commerce. I would like to start with financial transactions since this industry has the most potential and motivation to use smart contract technology.

4.6. Financial Transactions

In the fast-paced developing environment of the finance sector, the actors are seeking to find the best tools to make transactions more automatic and more practical. Nowadays, most monetary transactions are operated via banks or payment institutions. Banks and payment institutions are the middlemen making the transfers. For example, people use these centralized institutions in order to transfer money, even though this structure does not always operate in a smooth and problem-free manner.

In 2009, the sale, transfer and delivery procedure of Williams & Glyn, a division of Royal Bank of Scotland, was taking a lot longer than desired. Williams & Glyn had more

[272] Chamber of Digital Commerce, Smart Contracts Alliance. (2016). Smart Contracts: 12 Use Cases for Business & Beyond, Smart Contracts Alliance. Available at: http://digitalchamber.org/assets/smart-contracts-12-use-cases-for-business-and-beyond.pdf. [April2018].

than 200 years of experience in financial services. It is still receiving more than 50,000 orders every month on a fax machine. It still needs to keep a huge amount of records in physical form, though some of the records are now kept in digital platforms. Such a complex structure makes it almost impossible to achieve a smooth transition process[273]. This one example explains why financial institutions need to adopt blockchain technology and smart contracts.

One simple version of a smart contract other than the vending machine is Point of Sale (POS) terminals and cards. EDI systems are used for ordering and other transactions between large corporations, and the SWIFT, ACK/NACKs and FedWire networks are used for transferring and clearing payments between banks. These examples discharge commercial security models, usually upon a fee paid for the contractual needs and obligations of the parties[274].

Smart contracts can help to ease this centralized and heavy bureaucratic procedure. For instance, with the use of smart contracts, intercontinental deliveries of products can be made using quick letters of credit (normally these require a costly and lengthy procedure) or trade payments can be initiated, making financial asset liquidity possible. Thus, smart contracts may help to advance financial transactions for the involved parties (i.e. buyers, suppliers and institutions). Also, in terms of Financial Data Recording, because of the interoperability nature of the distributed ledger network system (the ability to exchange and make use of information) smart contracts can be a great help in making markets more consistent and uniform, thus enabling actors in the market to carry out more transparent projects concerning financial data recording. By making consistent and singular financial data available for the related actors, this can also help to create cost-sharing programs between the actors, reduce the accounting and audit expenses, and enhance the potential ways of reporting and gathering financial data[275].

[273] (Gapgemini Consulting 2016).

[274] (Szabo 1997).

[275] (Chamber of Digital Commerce, Smart Contracts Alliance 2016).

In financial transactions, the middle men and intermediary parties, such as banks and payment institutions, are seen as the reason why procedures take such a time,. This can lead to complicated legal procedures in terms of a conflict between the parties. However, if the transactions are discharged from the middlemen, this may save the parties from complex legal procedures. Discharge does not mean eliminating those third parties from the whole project; parties still need banks to make transfers. Smart contract technology can help stakeholders to make verifications through a distributed ledger and this saves a lot of time since, in practice, this verification process is currently a very lengthy process. For instance, "Consumers can use automated consumer-grade purchasing agents, tied to Bitcoin wallets and pre-programmed with consumer preferences, to reclaim their ability to negotiate in online transactions"[276]

In the cryptocurrency world, customers are able to operate transactions without being forced to share their personal information. In this kind of transaction, the suppliers, for example, do not need to know the identity of the customer as long as the digital money is transferred[277]. It can be seen that as long as the purposes of the transaction, which is a money transfer for the supplier, and the delivery of a product for the customer, are satisfied, there is no need for the customers to expose their personal data.

There are systems which can monitor auction bids automatically, determine the highest bid and pay back to the rest of the bidders automatically. Also, in the auction example, once an auction item is up in the system, the parties who are interested in the item can trust their smart contract to verify the item or prices, and thus they will not be tricked by anyone[278]. The BurstCoin system uses a simple form of smart contracts to take these

[276] (Fairfield 2014).

[277] (Fairfield 2014).

[278] (Cardozo Blockchain Project 2018). P8.

actions. It works via a cryptocurrency protocol to run a financial transaction[279]; the same process is used in selling pegged assets of Bitshares.

Ensuring transparency at every stage of a process can also be time-consuming[280]. In the online version of this example, the concerns are the same, plus it is critical to be sure that the parties who sign the agreement are the actual people involved. Also, the information flow must be clear; the user must know the financial conditions of the transactions[281].

In the UK, an electronic signature has been accepted in financial services since 2004. Also, following a High Court decision,[282] an electronic signature has been found sufficient as proof that a credit agreement is legally entered into in accordance with the law. In the EU, with eIDAS, the trust is fostered on the signee's identification, and electronic signature use is encouraged[283]. While these developments have bestowed a good deal of trust on electronic signature use in financial services, the author considers that this can lead the way to better understanding smart contracts as well.

4.7. Loan Agreements

The loan process is usually lengthy, expensive and exhausting for both parties. It requires a detailed investigation into the individual, along with a credit score. Sometimes it can take up to 30 days to conclude the process and determine the credit amount. For example, for a mortgage application, the process includes complex stages that require confirmation at almost every stage and these (along with much detail that cannot be included here) all

[279] BurstCoin. (2018). What's up with smart contracts? the Burstcoinist. Available at: https://www.burstcoin.ist/2018/04/04/whats-up-with-smart-contracts-an-interview-with-ant/.[10April2019].

[280] Aneeza Haleem. (2018). Smart Contracts for Smarter Lending. Mortgage Bankers Association. Available at: https://www.mba.org/publications/insights/archive/mba-insights-archive/2018/smart-contracts-for-smarter-lending[30April2019].

[281] Mike Boyle. (2017). The Need for Identity in Financial Electronic Transactions. GlobalSign blog. Available at: https://www.globalsign.com/en/blog/identity-in-electronic-transactions/. [Dec2018].

[282] Bassano v Toft & Ors [2014] EWHC 377 (QB).

[283] (Boyle 2017).

add up to create a costly procedure. Smart contracts can provide a system of loan enforcement and extension for properties.

Most forms of loan agreements have a similar structure; if the debtor fails to make a payment, the property can be retained. This structure can be run by a smart contracts system automatically. There are no illegal applications here since, in real time mortgage and loan contracts, the basic terms and conditions are set forth around the premise of paying the due money. If the debtor fails to make or delays payment, there are consequences for being in default, according to the contract and the law. For instance, in a smart contract-driven loan procedure, in the case where a customer buys a car with credit and does not make the payments on time (through a cryptocurrency payment over the blockchain channel) the system promises to lock the car down and take it back to the seller. This system may work for other devices as well; it can control the device from a distance and check if the obligations of the contract are constantly being met[284].

In loan transactions, a myriad number of signatures need to be verified; this is necessary for the avoidance of loss and fraud. However, this procedure does not prevent unlawful acts in bank transactions. Recently, one of our clients had money transferred by a Singapore-based bank to Turkey based on a counterfeit order sent to the bank via fax.

Smart contracts have the great potential to ease lengthy, tiring and expensive loan processes. They help to decrease the number of delays which may occur due to documentation and physical arrangements required amongst the multiple parties since they work on a distributed ledger where all the phases can be achieved, be seen and be affirmed by all the parties in the projects[285]. The author considers that the most critical part of the smart contract system is to carefully explain the verification scheme.

[284] (Walsh 2015).

[285] Empirica. (2016). Three use cases of Smart Contracts in Financial services. Financial Markets software blog. Available at: http://empirica-software.com/three-use-case-smart-contracts-financial-services/. [23March2019].

4.8. Government Services

The distributed ledger technology in the blockchain basically works as a database which is able to store financial, physical, and electronic records to be shared. This process also contributes to the digitalization of government records. This system can be used to store huge amounts of data safely; the aspect of immutability serves very well in this scenario. Transparency and accuracy can be achieved and this helps to refresh the relationship between government and the citizen in terms of transparency[286]. Tunisia has announced it will issue digital currency on a blockchain, and it is expected that the government will collect taxes by using blockchain technology by 2023[287].

There are countries that have already started to work on how to implement blockchain-driven systems; for instance, in Estonia, the government has adopted blockchain technology. This is not recent; the Estonian people have been using an identity proof scheme based on PKI since 1991, and later on, in 2012, they started using technology similar to blockchain which works on data integrity in different sectors; health, legal and other public services[288]

The Swiss government has announced that they want crypto currency organizations to be part of authorized monetary institutions and be subject to the related monetary legislation. In India, the authorities are working on their own crypto currency to be used in transactions. Australia is also working on new regulations on this subject. In the EU, 22 countries are preparing to enter into a blockchain cooperation agreement.

[286] UK Government Office for Science. (2016). Distributed ledger technology: Blackett review. Report by the UK Government Chief Scientific Adviser. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. [15March 2019].

[287] Rick Huckstep. (2016). What does the future hold for blockchain and insurance? Daily Fintech blog. Available at: https://dailyfintech.com/2016/01/14/what-does-the-future-hold-for-blockchain-and-insurance/. [3March 2019].

[288] (Bacon, Michels, Millard & Singh 2018). p31.

Other than providing fundamental services, blockchain technology can also be used in the voting process. For instance, in Russia, the government has created a distributed ledger-based electronic voting system; the database is secured with an encrypted system and the system stores the data and related information. The government authorities can access it by connecting to the database[289].

Also in Switzerland, an electronic voting platform has been created on Hyperledger Fabric - integrated with Zug's Ethereum-based digital ID registration application. This system is enabling people to vote on a blockchain-based platform. The votes are anonymized and encrypted. In this system, of course, the main concerns are security and transparency, but simplicity is also important as people want to know how the system works. This is key if this technology is to be adopted in other countries[290]. Anonymity is not mandatory; in fact, this has been overlooked in some countries[291]; In the US, Delaware, a registry of company shareholders is being kept using blockchain-based technology. This system allows people to access commercial extracts and proves their admissibility.

4.9. Employment Contracts

In practice, companies use almost the same model employment contracts for new employees. In these types of contracts, only certain pieces of information, such as personal details, dates, and positions, vary. Also, there are cases where companies create different types of employment contracts for managerial level employees, but they are still based on the same model. At the end of every employment process, these contracts are signed by the company and the employees. Until this signature phase, there is usually a period of exhausting document gathering for each employee. This creates a heavy burden

[289] (Savelyev 2016).

[290] Yahya Mohamed Mao. (2018). Creating the first customizable blockchain-based e-voting system in Switzerland. Medium Article. Available at: https://medium.com/nworld-publications/creating-the-first-customizable-blockchain-based-e-voting-system-in-switzerland-global-it-service-9a994a6f221c. [10Dec2018]

[291] (Hari & Pasquier 2018).

for both the employees and the human resources departments. The HR departments usually cannot proceed to the signature and insurance registration in some cases without having received a long list of documents.

A smart contracts-based system can ease this exhausting phase for the employer and employee. After the parties shake hands, the employee can upload the requested documents to the system and the system will check and confirm them. If there is nothing preventing the establishment of an employment contract, the system automatically executes the contract. During the employment period, the system can send notices to the employer when necessary. This might need human intervention in companies with thousands of branches but still, smart contracts can ease up the whole process, from confirmation of employment to termination (if necessary). Not every notice of termination is sent for notarisation in the employment process since it is not a legal requirement. In term of mass layoffs, the smart contracts system can be used to send notices to employees. In practice, notices can be sent via the national postal services, in the future, perhaps the system can be linked to the postal system, sending automatic notices subject to the approval of the employer.

4.10. Insurance

In practice, insurance policies work on the insurance holder's claim and, in most cases, insurance cards have to be submitted to take advantage of the insurance deals agreed upon between the claimant and the insurance company. With smart contracts, declaration or approval by the insurance holder may not be necessary as long as the insurance holder is registered with the hospital; the system enables the insurance and automatically verifies the insurance company. Not only in health insurance situations but also in terms of any insurable event, smart contracts can automatically verify the situation and pay the insurance if necessary, without needing any notification[292].

[292] (Rick 2016).

In terms of life insurance policies, if the insurance holder dies, smart contracts can automatically check and confirm from online death records at the registries and make the payment to the designated beneficiaries. The best example offered regarding smart contract insurance transactions is the situation of travel insurance in terms of a delay in designated flights. A team at the London FinTech Week hackathon in 2015 developed a smart contract-driven system by interchanging a large volume of online data, including flight information, to smart contracts in the Ethereum, system, enabling passengers to receive compensation for their insurance claims automatically[293].

In online flight reservations, the airlines mostly provide an insurance option. When people purchase insurance with the flight ticket, in the case of any delay or cancellation on the ticket, passengers naturally require a refund for the ticket and payment of the insurance amount too. Insurance refund procedures are normally cumbersome since there are three parties involved: the airline company, a bank and the insurance company running the scheme.

When passengers purchase the insurance together with the ticket, the insurance is purchased via a bank from another insurance company. In the case of a cancellation, the airline company notifies the bank and the bank notifies the insurance company in order to confirm the insurance and refund the money. In practice, the airline company, bank and the insurance company keep the data in their own records in different databases, and with every cancellation, the verification process takes a lot of time and creates high costs since they all have to confirm the details in their own databases. In lieu of this complicated procedure, the airline companies, banks and insurance companies can use a single shared database on a blockchain system for the verification of cancellations. It has been suggested that this cuts the costs and mitigates the process.

[293] Stephen Linennenbank, Sia Partners. (2015). The impact of Blockchain's Smart Contracts on Insurance. Banking & Insurance Newsletter. Available at: http://en.finance.sia-partners.com/impact-blockchains-smart-contracts-insurance. [2March2019].

Apart from the advantages of this example, the parties must be careful regarding details; in the case of a cancellation, the system automatically refunds the insurance fee. These kinds of situations tend to have more nuances than could be explained here. Yet as an example, a cancellation might actually be a delay; the airline might have changed the basis of reporting a delay or cancellation. Should the money be paid? The system cannot solely determine what to do. This concerns connectivity between the machine and real life. To further complicate matters, in a case where a passenger causes the delay in a flight, he/she might get compensated automatically; it is hard for the system to determine that this person actually caused the delay[294].

4.11. Supply Chain/Retail

Currently, in retail businesses, operations are spread amongst multiple parties: operators, suppliers, customers, and banks. All the parties operate on a different database, and these are mostly executed across countries. Also, many operations are based on paper-based, physically bulky systems, which makes the procedures long and complicated. A single-shared ledger approach on blockchain has huge potential to mitigate these procedures for all the parties, covering many different aspects.

In terms of security, a single-shared ledger provides access to the parties to check and see digital versions of the documentation necessary for the transaction. In today's world, every year the equivalent of 18 trillion US dollars is transferred using paper-based systems[295]. Imagine the cost of transferring this amount of money and the transaction steps required. Smart contracts can make a huge difference by checking approvals automatically and collecting or verifying signatures.

[294] (Hari & Pasquier 2018).

[295] John Ream, Yang Chu, David Schatsky. (2016). Upgrading blockchains Smart contract use cases in industry. Deloitte University Press. *Signals for Strategists*. Available at: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/innovatie/deloitte-nl-innovatie-upgrading-blockchains-smart-contract-use-cases-in-industry.pdf. [March2019].

Smart contracts can mitigate complex retail transaction; however, the ability to streamline the procedural steps has been widely misunderstood as a desire to eliminate intermediary parties completely. This is not the case unless the system only works on a crypto currency-based system. With smart contracts, people still need banks or other payment institutions to transfer the money. The smart contract only enables the verification process in terms of transferring the money in a single-shared ledger in a short amount of time. A retailer cannot operate a business without intermediaries, such as MasterCard, or by using blockchain systems alone.

Retailers can benefit from smart contracts in managing relationships with suppliers. As is the nature of the retail sector, there are an endless number of suppliers and a similar number of supply agreements amongst retail companies and suppliers. This makes it almost impossible to keep track of whether all the obligations have been met using paper-based contracts since it requires many man-hours to do so. Smart contracts can ease the difficulty of tracking of contractual obligations in supply contracts for the parties. For example, in most supply services contracts, there are performance rates called key performance indicators designated for the delivery achievement by the supplier. Tracking and checking these rates in practise is almost lost in the fast-paced workflow. With a smart contract system set up for suppliers, the system checks and controls if the criteria have been met or not automatically and applies sanctions accordingly. It would be useful to mention here once again that the system does not totally eliminate human involvement as the smart contracts' terms are written by the parties or by representatives of the parties with the help of developers and lawyer (these can be oracles[296]).

4.12. Consumer Transactions

Entrepreneurs and analysts have largely agreed that the blockchain system of online relationships between the consumer and business owners can be restructured in favour of consumers. As discussed in detail in section 4.11 above: "Retail, big technology

[296] See section 1.7.

companies can build up their own payments systems and remove the intermediary parties between themselves and the customers for their marketing and sales operations. For instance, if a company uses its own payment systems for the sales of goods over electronic commerce website the need for banks can be removed for specifically to this regard[297]. This might suggest that the role of the intermediary may be declining after almost twenty years of dominance in the online economy.

4.13. Energy Sector

In countries where the market economy has been adopted, certain institutions and authorities are in a dominant position in terms of providing essential goods and services needed by society. This creates an environment where the members of society are exposed to heavy burdens when purchasing their essential needs, such as gas or electricity. In order to protect the rights of the people who are in the economically deficient position against the big institutions and companies, a rule has been adopted called *entering into a contract*[298].

In Turkey, regarding essential services such as electricity, the process of entering into a contract will fade and the principle of freedom of contract has the potential to be more widely adopted[299]. However, currently, there are specific regulations for the energy sector that are regulating the application of the obligation to enter into a contract principle. Article 9/2 of the Turkish Electricity Market Law[300] states: "*The distribution company shall be responsible for operating the distribution system specified in the license thereof in accordance with the competitive environment in electrical energy generation and sales, renewing such facilities, making substitution and capacity expansion investments,*

[297] (Fairfield 2014).

[298] Alparslan Altan. (2004). Enerji Sağlama Sözleşmeleri Bakımından Sözleşme Özgürlüğü ve Sözleşme Yapma Zorunluluğu İlkesinin Uygulanması. *Ankara Barosu Journal*, Volume2004(4). p61. Available at: http://www.ankarabarosu.org.tr/siteler/ankarabarosu/tekmakale/2004-4/3.pdf. [Marc2019].

[299] (Okumus 2018). p29.

[300] Turkish Electricity Market Law, no 6446, date 14/3/2013.

and for providing services to users connected, or to connect to the distribution system in accordance with the provisions of the relevant legislation, without discrimination among equal parties." This is applicable to non-eligible consumers who are not entitled to select their suppliers as their consumption of electrical power is not greater than that designated by the Energy Market Regulatory Board (EMRB), or because they are not directly connected to the transmission system, or because they are not in an organized industrial zone legal entity[301]. Therefore, the distribution of services in the energy sector is generally being provided through contacts, whether they are mandatory or not. It should be pointed out that when there are mandatory requirements to enter into a contract to provide services and in the case of a breach of this obligation, the EMRB is authorized to apply administrative penalties.

A form of smart contracts have been used with energy smart grids and this has helped to lower the costs of distribution transactions in the energy sector. In choosing a distribution system, people could have the option of using smart contracts or retain the old service with the existing (default) agreements[302].

Using the smart contracts alternative can be useful in different ways and it may yield several advantages With the help of smart contracts technology, the distribution system can be created and shaped in accordance with the needs of customer requirements; this also reduces the facility establishment costs for the operators. This system allows people to understand price logic and to have clear pricing and tariff models if it applies to the existing smart grid applications. It has been also suggested that it is not necessary to create a whole new pricing system to adopt smart contracts with the existing smart grids, it only requires a remodelling and regulatory involvement. Therefore, it does not cause an unbearable obligation[303]. I would like to emphasize here that people must be given this

[301] Article 3 of Turkish Electricity Market Law, no 6446, date 14/3/2013.

[302] Christine Brandstätt, Gert Brunekreeft and Nele Friedrichsen. (2001). Improving investment coordination in electricity networks through smart contracts. Jacobs University. Available at: https://www.researchgate.net/publication/254392399_Improving_Investment_Coordination_in_Electricity_Networks_Through_Smart_Contracts. [2March2019].

[303] (Brandstätt, Brunekreeft & Friedrichsen 2001).

smart contract-modelled system as an option; it will be up to their discretion to choose it. Otherwise, it must be ensured that the customers are protected against the potential bad faith and burdensome applications of the market monopolists.

A US-based start-up, Transactive Grid, has enabled its members to trade energy using smart contracts over blockchain[304]. The transaction was successfully launched in early 2016, connecting five homes on one side of a street in Brooklyn that produce energy through solar power with five consumers on the other side of the street who are interested in buying excess energy from their neighbours. A similar initiative has been launched by a start-up called Power Ledger in Perth, Australia[305]. A more specific use of smart contracts in the energy sector can found in be gas distributions. The distribution infrastructures set up using a blockchain-driven system provide an easier means of payment, with the service providing distribution details, times and amounts[306].

In gas distribution, building a facility and infrastructure is expensive; therefore, while the initiating business requires a lot of work and money in terms of the management of the distribution of the gas, smart contracts can be extremely helpful in easing the process for both parties. For instance, a distributing platform can be created using a blockchain technology such as Ethereum and this enables people to run codes by paying for their gas charges.

[304] Randy Wilson. Deloitte UK. (2016). Blockchain applications in energy trading. Available at: https://www2.deloitte.com/uk/en/pages/energy-and-resources/articles/blockchain-applications-in-energy-trading.html. [5March2019].

[305] (Singh 2017).

[306] Kimberly Henderson, Emily Knoll, and Matt Rogers. (2018). What every utility CEO should know about blockchain. Mckinsey & Company Report. Available at: https://www.mckinsey.com/industries/electric-power-and-natural-gas/our-insights/what-every-utility-ceo-should-know-about-blockchain. [17March2019].

4.14. Automobile Industry

Smart contracts can be used in the automobile industry. Sensors in smart vehicles are able to measure, for example, the distance between the driver's vehicle and those vehicles behind and in front. This makes manoeuvring and contending with blind spots safer. Although cars with these features still get into accidents, this is where a smart contract can play an important role in terms of designating damages, fault and liability by stipulating which car had been at fault.

4.15. Leasing

The system in a smart contract works subject to certain conditions. For example, in a lease agreement, the purpose of the contract is to provide premises to a tenant and a deposit to the landlord. In this sense, smart contracts are ideal for leasing transactions; there is no need for a real estate or agency. The system will enable the tenant to access the keys as soon as the rent or deposit has been paid to the landlord. In this example, the tenant does not need to wait for the landlord to confirm the payment has been made, which usually slows down the process.

5. Advantages and Disadvantages

In the current system in practise, most monetary transactions are operated through banks and/or payment institutions. These centralized intermediary institutions are generally the main tools that people use for money transfers. This structure does not always operate in a smooth and trouble-free way, as mentioned in section 4.6 and 4.7. Blockchain works using a distributed ledger, which enables data to be recorded on a single database where it is available for other stakeholder/users to see. This feature of blockchain technology makes it easy for the authorized users of the system to locate specific (trusted) data. Since the data has been automatically verified over the system, the parties do not need to go to a third party authority to verify it. At the same time, the tamper-proof nature of the system makes the transactions trustworthy and prevents fraud. The timestamp also creates

reliable proof regarding the chronological order of transactions, while also being a potential solution to any double-spending problems[307].

In the blockchain system, decentralized money transfer is possible, which removes a huge burden regarding the transactions. Blockchain technology overcomes the old belief that no transaction is possible without having banks and payment institutions involved. Szabo states: "blockchain technology appears very much to be the jet fuel necessary for smart contracts to become commonplace in business transactions and beyond. It is a delight to be part of a community committed to fostering the tenants of open source cooperation, privacy and security, education in technology, and working for a common social good."[308] As Szabo, the creator of smart contracts puts forward, smart contract technology promises to mitigate the needs of people in a more practical way than it does nowadays.

5.6. Advantages

Merely by their nature, smart contracts provide a resilient environment[309]. While the blockchain is being created, it works on a copying base since the miners/users are copying blocks in the system onto their computers[310]. In the case of a system interruption, users might need help to correct the problem.

Smart contracts have huge potential to mitigate the performance of sanctions subject to the breach of a contractual obligation as agreed upon in the contract by the parties. Even if the sanctions, such as a monetary penalty or the cessation of a service, are performed successfully in a smart contract-driven transaction, the parties still have the right to seek

[307] (Nakamoto 2008).

[308] (Chamber of Digital Commerce, Smart Contracts Alliance 2016).

[309] (Cardozo Blockchain Project 2018). p4.

[310] (De Filippi & Wright 2018). p2.

different legal remedies in courts[311]. Using smart contract technologies does not eliminate the right of seeking legal help in the courts.

In the case of a breach (in terms of performance of the obligations set forth in the contract), typically people go to the external regulators such as courts, mediators and arbitrators to solve the conflict, depending on the parties' determination under the governing law and dispute resolution sections of the contract. The court or arbitration processes generally take a long time to resolve cases and can be costly, involving application fees, advance payments, notification costs, expert opinion costs as well as site visit costs, if necessary. Having this kind of technology creates an environment where the current laws are studied in more detail in order to be able to make the system work without any obstacles and harm the fundamental rights of people.

In international sales of goods transactions, smart contracts can be used, through connecting to GPS, to track the goods and the prevailing conditions, for instance, the weather at the arrival port. The parties can consider the possible effects of the weather conditions on the goods. If there is a risk of a storm, they can create precautions,[312] or if the damage cannot be prevented, the system may measure the potential loss and create remedies in advance by implementing compensation schemes or price re-arrangements automatically.

5.6.1. Security

The blockchain system depends on the people who are helping the system to run by creating blocks. Therefore, the system expects the people to be honest and not cheat, otherwise the blocks will stop and this causes forks in the chain. And since the longest chain is considered most valid, each user (miner) is motivated to create true blocks and not to cheat and control the other users' work in the system. For example, in gas

[311] (Cardozo Blockchain Project 2018). p7.

[312] (Morrison 2019).

distribution services, smart contracts can be used to distribute gas using a platform driven by blockchain where the users can run codes by paying for the gas charges in the system through creating blocks. The success of the system in this example depends on the honesty of the majority of the miners. It is possible that some of the users (miners) in the system may cheat by blocking the system or running the block in a mistaken way; this does not prevent the system from working since the other users are able to reject wrongly created blocks and fork the untrusted chain[313].

Blockchain is maintained in a distributed manner in the distributed ledger; this means that there are copies of the system in separate places. This feature makes the system resilient and secure because it is not easy to alter the data unilaterally since there is no centralized control mechanism. This lowers hacking attacks since there is not only one copy so there is more than one target[314].

Despite all the criticism of its tamper-proof, immutable nature, it continues to provide a secure environment for the parties because, while initiating the blockchain-driven project, the first details of the transaction (the subject of the digital assets to be transferred and the authenticated information of the users) are recorded in the distributed ledger, and there is no way to amend them. It is very important to mention here that the solidarity of the blockchain provides a guarantee for the code to run correctly. However, it cannot control the actions of the parties regarding whether they are acting properly, in line with the contractual obligations as set forth in the smart contract.

People are now able to purchase almost everything online: from cosmetic products to automobiles. In Alibaba, more than 375,000 orders are being processed every day. In this growing environment, the greatest problem individuals face in terms of online shopping is trust. Engaging in a commercial relationship with unknown parties online, for example, hiring people online, creates a vague state in terms of security. Therefore, the author

[313] (Bhargavan, Delignat-Lavaud, Fournet, Gollamudi, Gonthier, Hal 2016).

[314] (Bacon, Michels, Millard & Singh 2018). p22.

considers that the system's optimization and security is of paramount importance. When shopping for a product online, people have to trust the other party to send the product after payment has been received and, vice versa, the supplier must trust the consumer not to reverse the payment made via credit card while receiving the product at the same time. Even though the major operators in the retail industry have overcome these kinds of trust issues, the security problem is still an issue in online-operated businesses. For example, on eBay, people conducting business (buying and selling goods) with ease A large portion of the P2P systems trade is happening through eBay, which has become a monopoly intermediary website for the western world. However, having security on eBay is not free; they charge a considerable amount of money for the services they provide. eBay is also able to impose very one-sided control mechanisms over the website terms of use that can easily limit business freedom[315]. More concerning eBay: both parties' concerns are understandable; the platform provider has business costs such as developer payments and server expenses; regarding the protection of data, it is not easy for eBay to solve the trust issue. However, from the consumer's perspective, paying intermediaries fees is not ideal, and this is where consumers have started to ask questions: Do we really need an intermediary? Can we eliminate the middleman? As examined in section1.7, the answer is yes, it is possible to conduct business freely without an intermediary institution by using smart contracts. However, this approach cannot be efficient in fields other than electronic commerce operations.

As mentioned earlier in section 3.7.1, the hacking attack on the Ethereum system (as committed by DAO)[316] showed people that there is no 100% secure environment in these systems. Having said that, these kinds of crises help experts to understand the problems and to create more effective security mechanisms.

[315] (Walsh 2015).

[316] (Bhargavan, Delignat-Lavaud, Fournet, Gollamudi, Gonthier, Hal 2016).

5.6.2. Transparency

Smart contracts provide a great deal of practicality for business, especially in multilateral transactions (which can be even more challenging in global projects). It might not be easy to track every phase of a transaction when the numbers of parties involved is high, so it is really important to have reliable parties for transactions to reach their successful conclusion. Problems often arise from not having enough transparency in real life; for example, in a shipment project, a person at the dock can cause a delay unintentionally and, until the parties discover this, they might end up with severe damages. Once the system is created, smart contracts are not easily amendable unless they are programmed to be so. In a well-structured system, this tamper-proof feature can be life-saving, especially in international multilateral projects. Moreover, the decentralized system gives the parties control and ability to query the transaction at every step.

"As transparency is amplified, trust becomes more likely."[317] This maxim would be beneficial in the resolution of legal disputes; the legal consequences of failure to perform a contract duty can be embedded in the code and executed automatically[318]. In other words, parties can authorize the smart contracts system to act as a judge. Even if the parties are not satisfied with the system's decision, the tamper-proof distributed ledger can constitute reliable evidence in court actions[319] since the data in the system has likely remained untouched and has not been amended.

5.7.Disadvantages

While considering the practise of software systems information technology-driven projects, the author considers that there are important questions that must be asked: Who are the creators of this software program? Are the program tools free from third party

[317] Building trust in government Exploring the potential of blockchains. IBM Institute for Business Value survey conducted by The Economist Intelligence Unit. 2018. Executive Report. Available at: https://www.ibm.com/downloads/cas/WJNPLNGZ.

[318] (Pentland, Nathan & Zyskind 2015). p5.

[319] (Pentland, Nathan & Zyskind 2015). p5

claims? In terms of a claim, who will liable? How shall I designate the responsible parties? In the real world, it is not always easy to find the right answers to these questions, and sometime it is almost impossible to determine the right person to be held responsible for the damages in terms of open source-created software. Even though these are quite challenging issues, in smart contracts (as a result of being created through blockchain technology) the creation mechanism (the validation scheme at the beginning) could ease some of those concerns.

In the blockchain system, the system's execution is based on the consecutive blocks that validate the accuracy of the prior and the next chain thus authenticating the users; the risk of cheating or creating a false chain is very low. In terms of the creation of an incorrect block, other users can easily determine this incorrect chain and can eliminate it from the system. This unique mechanism eliminates the concept of designating unlawful action against the developers of the system. However, concerns are considerable in the application phase of smart contracts since it is not possible for the system to control the contractual parties' performances and confirm whether they are being executed according to the contract terms or not.

Moreover, as a natural result of being immutable, the rights of the parties might be jeopardized since it is not easy (sometimes impossible) to make amendments to the implemented smart contract[320]. Even though the system might allow some additional data to be added (thereby meaning it can be changed), this does not mean the transaction can be changed entirely[321]. Another important thing to be considered is data protection compliance; the tamper-proof nature of blockchain technology is likely to create problems in terms of data protection compliance and principles[322]. Basically, parties (data controllers) might need to anonymize, pseudonymize, delete or remove personal data

[320] (Schulpen 2018). p22.

[321] (Morrison 2019).

[322] (Finck 2018). p31.

from the system and this could be problematic since it will affect the other chains in the block.

Particularly in permissionless blockchain systems, it is quite hard to allocate and determine the liability of the parties since there might be numerous miners involved in the creation of the system; they cannot be identified generally. This creates problems in contractual liabilities as well as in data protection compliance schemes[323]. It is suggested this may be overcome by using a more limited blockchain system where a limited group of identified miners are involved in the generation of the blockchain system.

In the smart contract system, there is a possibility (for certain projects) that one party may be the designator of the conditions of the transaction, and that the other parties might not have much involvement and might not be able to revise or change the smart contract at a later date. Although this is technically possible, this might challenge the first initiative to implement this system: the creation of an immutable system[324]. This feature can be an issue in multilateral transactions (in consumer-related projects, for instance), where the parties typically have to accept and comply with the provisions of contracts that have already been set forth by the service provider.

Also, as the result of executing a system like computer data through a software platform, the digital money or crypto currency could be at risk of being duplicated leading to double-spending[325]. This can be an issue in financial sector applications. In physical money and electronic money systems, transfers are authorized by a centralized trusted administrative authority such as a Central Bank, and are regulated by banking regulations and supervising institutions; therefore, the risk of duplication is almost impossible in the centralized systems. However, these systems are criticized for making the parties rely on

[323] See section 6.8.5.

[324] See section 3.6.1.

[325] Patricia Everaere, Isabelle Simplot-Ryl, and Issa Traor. (2010). Double Spending Protection for E-Cash based on Risk Management, Conference Paper, p394-408. ISC'10 Proceedings of the 13th international conference on Information security. Available at: https://dl.acm.org/citation.cfm?id=1949361.

an administrative body for almost every transaction in their daily business. The P2P nature of blockchain technology promises to overhaul this process by creating a database where people can access and verify transactions themselves; the miners in the network can go through the transaction and verify it over a publicly accessible database.

SECTION IV

6. Review Mechanism

Smart contracts are driven by computer codes; therefore, they are naturally subject to computational flaws and bugs. This is inevitable in computer programs. In the famous attack on the Ethereum smart contract system, where millions of ether was stolen, the attackers issued a statement regarding the theft, claiming that they had not committed any illegal actions[326]; they had just taken advantage of the flaws in the system. Therefore, as a computer program, smart contract technology is not fully free from human error. Additionally, there is a huge number of blockchain protocols that have been mined so far[327]. It is suggested that this is equivalent to 300 billion US dollars, which is an appealing amount for potential hackers.

It is important to emphasize here that, in terms of regulating technology, remaining at the territorial level is generally a hindrance standing in the way of progress in this realm. Technology changes rapidly and it is not easy for the legal realm to keep up with the technological developments at the same speed. The author considers that this most certainly will be the case for blockchain technology: 'a cyber libertarian utopia, arguing that regulation anchored in state sovereignty cannot function in cyberspace, making the Internet far from effectively regulated[328].

In terms of a review mechanism, both the legal and technical ends would be involved. On the legal side, rather than creating new regulations for the legal acceptance of smart contracts, it is more critical to inform people about the contracts' uses as well as risks. A model review mechanism cannot work for every single use. Guidelines and reports may direct people to create a secure environment for their organizations.

---

[326] (Savelyev 2016).

[327] (Nikolic, Kolluri, Sergey, Saxena, Hobor 2018).

[328] (Finck 2018). p37. and also *see;* David Post and David Johnson. (1996). Law and Borders: The Rise of Law in Cyberspace (1996) *Stanford Law Review,* volume48, p1367. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535.

Legal acceptance of smart contracts is obviously possible with the interpretation of contract formation conditions, but the review mechanism for smart contract-driven transactions should be clarified. This can be managed through good collaboration between the legal and technical ends because this will not only involve policies and legal documents; people will be implementing technology so technical specifications are of paramount importance. For instance, it can be clearly explained to people how they can develop security measures to minimise the computational risks. I do not believe a separate regulation is needed to describe every step of a smart contract transaction; this is not realistic nor practical. The existing contracting rules, together with the regulations on electronic commerce transactions, are great sources to help the legal and technology realms understand and explain the governance of smart contracts.

6.6. Lawyers Role

In practice, the majority of conflicts relating to contractual relationships arise from the misstatement and misinterpretation of the provisions agreed between the parties in the contract negotiation phases. In those kinds of scenarios, court cases tend to last some time and might be exhausting for the parties. However, in smart contract-driven transactions, this risk can be eliminated since the whole transaction is run by a computer program, and the terms of the contract are written in computer language (using semantics and syntax) and kept in the code[329]. Smart contracts can be set to solve a conflict automatically, as agreed by the parties; simply, parties can have the right to leave conflict resolution to the system instead of going into court. This can be time, energy and money saving.

In contrast to physical contracts, in smart contract technology, the parties do not write contract terms unless they are the developers who are creating the system from scratch. This feature of smart contracts makes them free from discretion on interpretation. "Smart contracts are meant to be stand-alone agreements: not subject to interpretation by outside entities or jurisdictions. The code itself is meant to be the ultimate arbiter of the deal it

[329] (Schulpen 2018). p20.

represents"[330]. This lowers the risk of having a subjective interpretation. A computer program has the huge potential of eliminating ambiguous interpretation of contractual terms[331]. Although ambiguity may exist in a computer program's technical structure for lawyers and nontechnical parties, the author considers that developers can illuminate these. This common legal problem of having unclear contract terms can be mitigated in smart contracts since the terms are written in codes in the blockchain system and "the P2P nature puts control back in the client's hands"[332].

Smart contract technology automatically assures that contractual obligation is performed as agreed by the parties[333]. I also believe that this system basically aims to mitigate issues in commercial practice, and helps to fasten the performance of the contractual obligations without waiting for one of the parties to take action before the authorities do, such as by sending notices via notaries, launching an enforcement proceeding or even filing a court case. I must make a caveat here that in smart contracts, at least into the near future, it will not be possible to insert abstract provisions (such as good faith, or representations and warranties, or confidentiality[334]). The system is not able to assess and guarantee if representations and warranties are in compliance with the law. The author considers that this will still be taken care of by lawyers in traditional ways, using the relevant legal regulations.

Moreover, this self-executing nature of the smart contract system does not constitute a waiver of the certain rights of the parties. No matter what the application of the system is or the smart contract agreed terms are, every party will still have the right to pursue their

[330] (Savelyev 2016).

[331] (Schönfeld 2018). p11.

[332] (Hertig 2014).

[333] (Farrell, Machin, Hinchliffe 2018).

[334] (De Filippi & Wright 2018). p77.

claims if not satisfied with the smart contract system, to go before the courts, or to dispute a resolution using other legal authorities[335].

Smart contracts can create an environment where there is a less (or in some cases no) need for human intervention; the distributed ledger technology enables the smart contract and automatically executes the obligations of the contract. However, this does not mean that this aspect of smart contracts totally eliminates the need for lawyers. With the development and increase in the use of smart contracts, the need for clear application of the legal principles will need to be met; at this point, lawyers will need to work together with the smart contract developers and business owners to make sure the implementation and transaction process is managed accurately[336]. Also at the writing phase regarding terminology and the clear statement of the contract provisions, lawyers' input will be of paramount necessity. As the Governance, Risk & Compliance Technology Centre stated: "smart contracts should be authored by both the lawyer and the developer"[337].

In the US, entrepreneurs have started to work on developing a system that helps people to automatically transform their legal documents and make them compatible for upload into a smart contract system[338]. In this transmission, it very important for the developers and lawyers to collaborate since it is critical to upload the legal provisions into the software accurately and operate this transmission process effectively. In terms of interference of lawyers into smart contracts, it has been mostly misinterpreted that smart contracts eliminate the need for intermediaries like lawyers[339]. It is very important to understand

[335] (Schönfeld 2018). p11.

[336] Matthew O'Toole, Christopher Kelly and David Hahn. Potter Anderson Corroon LLP, Delaware. (2018). Smart Contracts Need Smart Corporate Lawyers. Law360. Available at: http://www.potteranderson.com/newsroom-publications-OToole-Kelly-Hahn-Discuss-Why-Smart-Contracts-Need-Smart-Corporate-Lawyers.html. [23 March 2019].

[337] (O'Toole, Kelly & David Hahn. Potter Anderson Corroon LLP, Delaware 2018).

[338] (Gapgemini Consulting 2016).

[339] Iansiti, M., Lakhani, K. (2017). The Truth About Blockchain. *Harvard Business Review*, Volume-Jan-Feb 2017. Available at: https://hbr.org/2017/01/the-truth-about-blockchain.[10March2019].

here that the use of smart contracts will not give rise to a whole new legal system or set of regulations.

Rather than eliminating the lawyer's role entirely from the legal system, smart contracts can be used as a great tool for lawyers to understand the transactions and the conflicts together. This offers a path to reaching a fair examination and legally satisfying conclusion for the parties without the need of any legal action, as is required in the current mediation system. For instance, the working principle of Copy Robo[340], an application that helps to track copyright status, can help us to realise the potential profit of the smart contract in legal procedures. As in the copyright violation tracking applications, smart contracts can help lawyers to save time and energy on solving a case.

Generally, technology and innovation lead the way and the legal regulations follow in order to regulate the new technology. In the case of blockchain, there seems to be different relationship in terms of legal regulation; the legal regulation is struggling to cope with the rapid pace of technological development more than ever. So, this is the realm that needs strong collaboration between the technical side and the legal side; they need to intermingle, as the technological side needs legal answers for what they are doing on a daily basis. They are concerned about compliance with data protection principles, for instance.

6.7. Dispute Resolution

As is widely known, dispute resolution has evolved as a legal way to solve problems as an alternative to lengthy court procedures; it is a cheaper and more practical way of solving legal conflicts. Smart contracts have the potential to offer a new way of seeking legal remedy: "a cryptographic boost"[341]. The point here is to understand that a smart contract does not eliminate existing legal methods in the legal systems; instead, it

[340] Turkey's first blockchain initiative.

[341] (Hertig 2014).

provides an environment that has potential to reduce the number of court cases since it has the capacity to resolve disputes automatically. This can be seen as an alternative form of dispute resolution[342].

Courthouse procedures have been widely criticized for being slow and taking too long. This is the main reason for people choosing to go to arbitration. Besides avoiding the expenses of court procedures, practicality and speed are what are making dispute resolution more appealing. In smart contracts, the potential of parties having the ability to create bespoke dispute resolution schemes offers a good solution to easing the legal headaches.

In conflicts arising from the non-performance of obligations in physical contracts, the main tool of the court is the agreed contract texts between the parties; however, in most cases these terms are poorly written and ambiguous. In such cases, the trial outcome depends on the opinions of the judges (within the framework of the related legislation). In smart contracts, it can be said that this potential ambiguity is eliminated due to the algorithmic aspect of these contracts. As Hertig states: "the rules of the game are determined before the contract executes, rather than at the foot of a judge's podium."[343].

In dispute resolution schemes, smart contracts can benefit the system. The parties in the transaction can decide on a customized scheme for dispute resolution; instead of going into courts immediately, they can set up the system to go to the central blockchain administrator for resolving disputes; the administrator can come to a decision for the parties[344]. Parties can agree on a monetary limitation, the system can be set up to operate up to a certain threshold, and at the end, the decision will be kept in the records. This approach may also eliminate the use of unnecessary actions such as sending notices via a notary and generally ease the process for the parties where possible. Smart contracts can

[342] (Schulpen 2018). p19.

[343] (Hertig 2014).

[344] (Rogers, Jones-Fenleigh & Sanitt 2017).

"create a primitive dispute resolution mechanism allowing anonymous parties to settle a conflict without referring to courts or external arbitrators"[345].

Identification will play an important role here. In order to make a legal claim against someone, the parties and the system have to be able to identify the actors that are the contractual parties. If the system is based on pseudonymation of the parties, then this system may not serve[346]. This means application of this scheme in permissionless systems may be challenging.

6.8. Information Security

With the rapid evolution of the Internet, use cases have varied and this raises cyber security issues. While the use cases are getting bigger in terms of variety and the seriousness of the threads has increased because of the technology, hacking skills are evolving and developing, as well. In addition, with globalization, today there are a lot of third parties in different locations involved in business operations. All of these factors together make it really difficult to envisage the precise nature of cyber vulnerabilities. There are more vulnerabilities than approaches to cyber security (e.g., criminal) However, for this paper, the focus will be on liability for information security, the consequences of data breaches and, finally, actions to be taken to avoid risks. The author considers that those subjects are most relevant to the smart contracts system.

[345] Ortolani, Pietro. (2016). Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin. *Oxford Journal of Legal Studies,* Volume36(3) p595. And also see; (Morrison 2019).

[346] (Rogers, Jones-Fenleigh & Sanitt 2017).

6.8.1. Liability for Information Security

For a long time, cyber security has been seen as a technical issue which is should be solved at the IT department level[347], whereas it actually amounts to being an acutely pedantic concern and requires senior management attention. When talking about responsibility for information security breaches, the most common suspects are hackers, software developers, service providers, and users. Security in data processing engagements is critical since, as a result of a data breach, organizations might face huge f fines or the imprisonment of its directors or C-level employees. In Turkey and most jurisdictions, company law does not itself say companies have to secure the information, but regulations and interpretations around governance have been applied to the cyber security field. Basically, if companies do not follow their fiduciary obligations, they may face sanctions. It is not necessarily due diligence only, it comes under the scope of fiduciary obligations or compliance with fiduciary duties. The responsibility involves not only keeping the data safe; it amounts to a higher-level duty. Companies need to ensure that they appropriately identify their risks and manage those risks, and they must show that they have done their best for the benefit of the shareholders.

Organizations need to put in place a structured data security analysis and risk plan in advance. This is more than just creating perfect policies and procedures; the plan must clarify the company's needs, the employees' responsibilities, and any consequences related to fulfilling those responsibilities. Most importantly, security must be the main concern when they are designing their operations. Information security affects the value of their services and products, and thus their reputation[348]. It is a challenging job to define and allocate the liabilities for data security in a corporation. Nobody can know where they can be attacked or hacked, or how, although determining ill-protected and risky parts of a transaction would help to be prepared.

[347] Lipton, M. (2014). Risk Management and the Board of Directors. Harvard Law School Forum on Corporate Governance. Available at: https://corpgov.law.harvard.edu/2014/04/22/risk-management-and-the-board-of-directors-an-update-for- 2014/. [15april2019].

[348] (Lipton 2014).

This section aims to discuss corporate liability, especially regarding board of directors or C-level management liability for data breach situations. First, what might constitute a data breach and why it is important to define its scope and type of it will be analysed. Then, the consequences of a data breach and how it might directly affect the board of directors or C-level management will be discussed. Finally, the legal basis of board directors' liability and a close examination of where data security stands will be presented. Important cases will be mentioned, and a brief of what management should do to reduce security risks will be suggested.

6.8.2. What is a Data Breach?

A data breach may occur in various ways. It can happen as a result of data theft or loss, or the theft of equipment where the data is kept; unauthorized access and use; equipment or human error; natural disasters, such as floods, earthquakes, storms or fire; and finally, more technology supported threats, such as social engineering (blagging[349]).

A data breach may come as a violation of certain legal regulations. For example, in the US, if organizations dealing with health data fail to comply with the requirements in the Health Insurance Portability and Accountability Act (HIPAA), they automatically are credited as having a data breach. Under GDPR[350]: "destruction, loss, alteration, unauthorized disclosure or access on personal data (transmitted, stored or otherwise processed) occurred by accident or illegally amount to a security breach". At the same time, voluntarily implementing some standards (such as the International Organization for Standardization (ISO)), although it could indicate that an organization has an efficient data security plan, this does not necessarily constitute a *de jure* application. Moreover, according to the US Payment Card Industry Data Security Standards ("PCI-DSS"),

[349] These are some sort of offences targeted to the organizations. The aim is acquiring the information deceivingly by basically manipulating the information who has the information. Most common examples of this can be sending emails as a friend of the user or saying that 'you are a winner' of kind of made up prize.

[350] Art 4(12)).

standards constitute potential statutory liability for government agencies. In the Target case[351], the failure to comply with PCI-DSS standards has been seen as the basis for liability under the Data Protection Act. Briefly, the PCI-DSS is a system of contractual liabilities; failure to comply with the standard solely based on the contractual liability potential creates legal liability.

Determining the scope and type of data breach, scope (what type of data is involved) will help design the crisis aftermath and the risk management plan for the future. Another important point is balancing the rights in order not to overwhelm the authorities; minor breaches may, in some cases, not threaten individuals' rights and not require notification, whereas in others, they may[352]. For instance, merely releasing a name and address may not significantly hurt an individual, whereas in adoption cases, disclosure of this information (to the biological mother) is likely to cause a more serious situation. This should also be considered when notifying the individual[353]; there is no need to alarm people for insignificant reasons. There are different practices in the US; first of all, although all 50 states have data breach notification laws, some of them have requirements of public notification while some do not require notification by the authorities. In some states (Arizona, Iowa), the individual need only be notified where they need the individual's input and cooperation, for instance in identity theft cases. In California, there is a quantitative limitation; if more than 500 people are affected by the breach then the authorities are notified[354].

The author believes that the content of the breach must be considered before taking action, not its quantity. For instance, identity theft is acutely important and likely to cause

[351] 446 U.S. 643 (1980) (US Supreme Court).

[352] ART.29 Working Party. 2018. Guidelines on Personal data breach notification under Regulation 2016/679. 2018. Availabale at:https://iapp.org/media/pdf/resource_center/WP29-Breach-notification_02-2018.pdf.

[353] Tañà, L.V. (2013). EU Data Breach Notification Rule: The Key Elements. Available at: https://iapp.org/news/a/eu-data-breach-notification-rule-the-key-elements/.[5April2019].

[354] This number is 1,000 in Alaska and Hawaii.

severe consequences for the individual[355]. If companies wish to prevent identity theft, it would probably be very useful to take action and warn the individual concerned as soon as possible without waiting for a greater number of people to get affected.

6.8.3. Consequences of Data breach

If information security is not managed properly (at the corporate governance level), data breaches may occur. This may lead to monetary fines or criminal action. Besides the legal sanctions, there are business-related consequences; market value, reputation and customer trust may all be jeopardized.[356] Moreover, following cyber-attacks, companies may face severe organizational downturns in terms of losing devices and corruption of systems.

GDPR regulates fines of up to 20,000,000 EUR or 4% of the total global turnover. It does not mean that with every kind of data breach, organizations have to face sanctions. For example, under the Gramm–Leach–Bliley Act (GLBA), non-compliance with the requirements leads to a 100,000 USD fine for each violation by a financial institution and a 10,000 USD fine and/or imprisonment for up to five years for individuals[357]. Fines are generally imposed if organizations cannot prove they were compliant, they have demonstrated poor management in a crisis or they have not executed appropriate security measures[358]. In a case[359] in the US, the courts did not find a defendant liable since there was adequate risk assessment in place; therefore, the harm could not be predicted. The author considers that this case can amount to a positive indirect incentive, as having

[355] (Tañà 2013).

[356] (McGraw 2005).

[357] Brown, L. (2014). What You Need to Know About the Gramm-Leach-Bliley Act. Available at: https://www.shredit.com/en-us/blog/securing-your-information/august-2014/what-you-need-to-know-about-the-gramm-leach-bliley.

[358] (Tañà 2013).

[359] Guin v. Brazos Higher Education, Civ. No 05-668, 2006. (US District Court Minnesota).

information security plans may provide indirect benefits through avoiding legal sanctions to the company[360].

In the Tesco case, the FCA determined a £16,400,000 penalty, based on the Financial Services and Markets Act 2000 (Act), Section 206, for failure to comply with the obligations regulated under Principle 2 of the Act, which require organizations to demonstrate due skill, care and diligence while managing their businesses.

6.8.4. How can 'Appropriate' Information Security Plans be Implemented?

GDPR says controllers must 'implement appropriate technical and organisational measures to ensure an appropriate level of security to the risk'[361]. The terms 'reasonable, adequate, appropriate' may become ambiguous while performing duties. Firstly, information security is not only about creating perfect policies and procedures; it requires a structured analysis of data flow in the company. Companies must clarify their needs and the responsibilities of their employees, build awareness and, most importantly, security must be their main concern while designing their operations[362]. The measures may vary subject to the scope of the business, so the directors, consultants and lawyers must be creative. For instance, in the UK and the US, companies have started to include information about security risks in their annual reports (e.g., BT)[363]. The Wyndham and Tesco cases are good examples in terms of road-mapping information security and implementing effective methods.

---

[360] Smedinhoff, T. (2015). An Overview of Data Security Legal Requirements for All Business Sectors. Available at: https://media.lockelord.com/files/uploads/Insurance/Article%20-%20Data%20Security%20Requirments%20for%20All%20Business%20Sectors.pdf.[15April2019]

[361] Article (32).

[362] McGraw, G. (2005). Risk Management Framework. Available at: https://www.us-cert.gov/bsi/articles/best-practices/risk-management/risk-management-framework-%28rmf%29. [15April2019]

[363] Rahmani, V. (2017). Cyber Security: Corporate Insights for companies and their directors. Slaughter and May. p3. Available at: https://www.slaughterandmay.com/media/2536333/cyber-security-corporate-insights-for-companies-and-their-directors.pdf. p7. [15April2019]

Information security must be managed horizontally, vertically, and cross-functionally throughout the organization. Boards must make sure that responsibilities are allocated properly between employees while implementing information security policies[364]. It can be hard to motivate organizations to create information security systems since the reward for having even a perfect information security is actually "nothing"; in other words, companies are asked to make investments on information security for the best outcome of "nothing".

Information Security requires a case-by-case evaluation and implementation. There is no information security kit available. In a more practical sense, companies might have firewalls, regular virus checks, log-in and access controls, but these must be implemented subject to the specific needs of the organization after careful assessment. Sector-specific regulations can be helpful in designing security (e.g., GLBA, PCI-DSS).

1. **Knowing the Organisation.** First of all, it is critical to identify vulnerabilities and threats, clarify weak points in systems, and be able to identify who would attack the company, and why[365]. Companies must put in place more targeted and, most importantly, bespoke solutions in accordance with the needs of their organization[366]. This way they can determine which protective technology is needed to secure information.

2. **Periodic Risk and Harm Examination[367].** Information security is a living and continuous process, requiring regular review: "security is a process, not a product"[368]. It must be resilient[369] and up-to-date. Organizations must be checked

[364] (McGraw 2005).

[365] FCA. (2018). CA fines Tesco Bank £16.4m for failures in 2016 cyber-attack. https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack. [15April2019]

[366] (Lipton 2014).

[367] (Smedinhoff 2015). p12.

[368] Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons. p12.

[369] (Rahmani 2017). p4.

and plans must be monitored and reviewed on a regular basis. For instance, companies must be rigorous about what employees can access, what they can take home, where they keep the data, etc. Risk can be assessed properly when companies know the nature of their information and what might be their worst-case scenario.

3. **Crisis Plan.** Be prepared for a potential crisis; ad-hoc actions cannot serve as effective solutions in information security. It is very important not to act haphazardly. If there is an action plan ready, it is always easier to overhaul a crisis. For instance, having notification templates in advance can save a lot of effort.

4. **Prioritize.** It is not possible to address every little risk and prevent attacks 100%; therefore, evaluation and valuation are important[370]. Knowing the critical risks and dealing with them is vital, otherwise the process can get stuck. Companies must know what level of risk is acceptable for their operations. It is not possible to fully envisage where and how they can be attacked, but determining which are the less-protected and high-risk areas of a company is a good start.

6.8.5. Personal Data Protection in Blockchain

Data protection in blockchain systems and smart contracts will come with great ambiguity since the existing rules were created for centralized systems[371]. Therefore, the application of those rules to a decentralized system requires careful analysis. Although GPPR does not prevent the application of its provisions in decentralized public systems, it is not easy to cooperate with them.

Blockchain use cases are commonly commercial activities which may also involve personal data. “When assets are registered or transactions are recorded on blockchains,

[370] (Lipton 2014).

[371] (Finck 2018). p88.

the quest for transparency and right to privacy needn't be at odds. On blockchains, data can be shared widely, seamlessly and, when needed, anonymously."[372] So, once the data has been added in the system, it is visible to all the users in the system since they will be verifying this data when creating blocks; blockchain technology does not have a solution for privacy within the system yet[373]. This can be the barrier standing in the way of spreading the use cases of smart contracts technology more widely.

In a blockchain system, the data is generally in the blocks that create the chains[374], and once these chains have been created, it is very hard to intervene in those chains. This makes it almost impossible to amend the data sitting in the blocks. Although this feature provides benefits in transactions, not being able to intervene in the data in the system may not be an ideal case in the data protection realm.

In blockchain systems, data is stored commonly in digital form, but it can be stored in other forms, such as documents or merely as text[375]. Storing data does not seem to be a practical pursuit in blockchain systems since implementing the system itself is already expensive, and storing data can create more cost since the system's storage capacity is restricted[376]. If personal data is to be stored in the blockchain, the parties must comply with the relevant data protection regulations and be aware of data retention periods[377], which are not regulated under any law specifically. This can be analysed subject to the type of data and transaction necessities by the parties.

[372] Building trust in government Exploring the potential of blockchains. IBM Institute for Business Value survey conducted by The Economist Intelligence Unit. 2018. p2.

[373] (De Filippi & Wright 2018) p83.

[374] (Finck 2018) p90.

[375] (Finck 2018). p90.

[376] (Finck 2018). p90.

[377] (Finck 2018). p31.

Even if the stored data is encrypted, it can be linked to other data or data sets and this can amount to being personal data, and thus subject to data protection principles. So, encryption may not be the ultimate solution in blockchain systems unless the data *irreversibly prevents identification*[378]. Although Nakamoto suggested that privacy concerns are taken care of by keeping the data in different locations with anonymous public keys[379], it is not clear if this amounts to anonymisation in the sense of General Data Protection Regulation (GDPR)[380]. This does not provide fully satisfaction that the identification is irreversibly prevented. Data encrypted in public keys can rather be assumed to be 'pseudonimised'[381]

From another standpoint, storing encrypted data can be problematic because the encryption used today will not be secure enough in two years-time. Encryption functions do not provide high-level continuous security because as computing power progresses, it becomes easier to corrupt/crack encryption. Today, it is possible to download the entire chain and look at the data encrypted data. And in this system, how to handle a delete request is a problem as well.

Determining the data controller in blockchain ecosystems is complicated since the system is run by a computer program[382]. A data controller is: "A natural or legal person who is responsible for setting up and managing the data recording system, determining the means, and means of processing, the personal data (*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi)*"[383] under Turkish Data Protection Law, and: "the natural or

[378] Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques WP216.

[379] (Nakamoto 2008).

[380] GDPR Article 4(5).

[381] Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques WP216. and Article 4(2) GDPR.

[382] (Finck 2018). p99.

[383] Article 3(1) KVKK-Turkish Data Protection Law with no 6698, Official Gazette Publish date 7/4/2016.

legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law"[384] under GDPR. So, in a blockchain system, it is not absolutely clear who determines the purposes for personal data processing. In bilateral use cases, the data controller can be identified, whereas this is not easy in multilateral transactions[385]; this is important considering the most common use of blockchain will be for multilateral transactions. Particularly in public uses, where there are governmental bodies (hosting the system) and people (e.g., members, subscribers)[386] involved in the blockchain system, the author considers that the system becomes more vulnerable in terms of data security. The system might need more effective information security precautions since threats like fraud and identity theft are more likely to occur[387]. Also, in public blockchain systems, every user who has participated in the creation of blocks can be held liable as each user will have a copy of the system in their computers; this constitutes personal data processing. In these systems, it is difficult to assign the party who determines the purpose of processing as there is no unified control over the system[388]. It is not easy to draw the framework of liability in terms of current data protection laws. This may create a failure to comply with the transparency requirements in jointly-controlled projects under GDPR[389].

[384] Article 4(7) GDPR.

[385] (Finck 2018). p99.

[386] (Morrison 2019).

[387] (Morrison 2019).

[388] Matthias Berberich and Malgorzata Steiner. 2016. Blockchain Technology and the GDPR-How to Reconcile Privacy and Distributed Ledgers. European Data Protection Law Review, Volume422(2). Queen Mary University of London.

[389] Article 26(1) GDPR.

There is also ambiguity in blockchain ecosystems regarding how data subjects claim their rights against relevant data controllers where these controllers are not clear. [390]The question is: Who will be liable? All the miners in the system - can they be data controllers? Using a general interpretation, it can be said that a data subject can claim their rights from each user who has created the system in the legal sense, although technical implementation of this is not known to be feasible at the moment[391]. Because, especially in permissionless platforms, the miners may be too large in number to be identified, the data subjects may not be able to even reach any of them to make a claim.

Privacy by design can help while ensuring data protection compliance in blockchain systems. Privacy by design is regulated under article 25 of the GDPR and it basically means: "data protection through technology design"[392]. Privacy by design aims to bring privacy awareness in the technical infrastructure sense; privacy compliance should not be only seen as a legal requirement[393]. This can be considered in the blockchain creation phase as well; the system can be created with the proper technical and organisational privacy precautions, employing the best measurements (minimisation, pseudonimisation)[394] that suit each transaction. Achieving data minimisation might be challenging given the tamper-proof nature of the system; data that has been in the blocks and chains may not be easily amendable[395]. This seems to be a problem in the future as well.

Another critical subject that challenges blockchain systems would be the rectification right[396] of the data subject. This is also regulated under KVKK article 11(d). The right to

[390] (Kuner, Cate, Lynskey, Millard, Loideain & Svantesson 2018).

[391] (Finck 2018). p103.

[392] GDPR Key Issues. Intersoft Consulting. Available at: https://gdpr-info.eu/issues/privacy-by-design/ [20April2019].

[393] (Berberich & Steiner 2016).

[394] (Berberich & Steiner 2016).

[395] (Finck 2018). p104.

[396] Article 16 GDPR.

rectification enables data subjects to request corrections if their personal data is incomplete or processed incorrectly. With the tamper-proof feature of blockchain, how to implement this amendment right is not clear because the data is copied in every user's computer, it is encrypted and it is difficult to amend[397] (not impossible, technically, but far from practical). In public systems, the users involved may not even be identified.

The right to be forgotten[398] and the access rights[399] of data subjects require clarification. Not being able to (easily or practically) amend the data in blockchain systems will challenge the implementation of these rights, as well[400]. Data protection rules in Europe and Turkey are generally focused on the after-effect. In order to be able to achieve reconciliation with legal requirements and blockchain systems, a more "process-oriented"[401] approach will be needed because, at the moment, the only thing that can be done to fulfil the data delete request seems to be to use the Kill switch. Since it may not be possible to reach out all the miners who have stored the data, the system may need to be remotely taken down. In this case, no one will be able to reach the data.

Is it entirely impossible to use blockchain system for projects which include personal data? This question can be best answered in a lawyer's way: 'It depends'[402]. It depends on the system's ability to be designed to comply with data protection principles. This question requires legal and technical end collaboration to be solved. It may be hard in permissionless systems where there are large numbers of miners involved who may not even be recognized, although if a limited group of miners create the blockchain system and they are all identified, the system can be designed to be compatible to data protection rules.

[397] (Finck 2018). p105.

[398] Article 17 GDPR.

[399] Article 15 GDPR.

[400] (Berberich & Steiner 2016).

[401] (Finck 2018). p111.

[402] (Kuner, Cate, Lynskey, Millard, Loideain & Svantesson 2018).

SECTION V

CONCLUSION

Blockchain has great potential to regenerate existing business models. This thesis has attempted to analyse those areas that blockchain can make a drastic difference. Together with the potential use cases in practice, contractual relationships in smart contract-driven projects have been analysed by visiting existing contracting principals, as well as rules and practices for digital contracting. Although smart contracts have great potential to mitigate long-lasting procedures, they have their own risks and challenges.

Before moving on to legal interpretations regarding smart contracts, important aspects that are related to blockchain technology have been examined. Distributed ledger technology and the decentralized feature are often misunderstood or intermingled with each other. These two concepts are not completely different from each other. Distributed systems have been used for years by big companies. This does not mean that every distributed system is decentralized. Distributed networks are not decentralized; in practice, big tech companies (Dropbox, Google Drive, Onedrive) have relied on the distributed network concept for a long time. Most of the cloud services are run in a distributed manner. This system allows data to be stored in multiple computers in different locations. The decentralized concept, on the other hand, means that the system is not controlled by one party; all the nodes in the blockchain network participate in controlling it. The system is based on the consensus of the nodes. However, in the current state of blockchain, even in the open blockchain systems, the system is not quite decentralized given almost all of the miners for Bitcoin are in China. Although, in open blockchain systems, the idea is encouraging everyone to join the network to be miner, in practice this is very difficult. Mining requires a powerful computer and a reliable power source; not everybody has access to these. The power needed to run an open blockchain system is estimated at around four times that required for Google. This is a real obstacle standing in the way of the technology; it means only large companies with power will be able to run the system. Such a scenario suggests blockchain systems are not truly decentralized.

The core focus of this thesis has been to analyse smart contracts in the light of traditional contract principles. Smart contracts can make a great difference as a more practical option, especially in multilateral transactions, and can be applied in a range of business sectors, from finance to energy, automotive to supply chain. However, the governance of this technology is of paramount importance and much work is required in regulating the uses of it rather than only regulating the blockchain or smart contract as pieces of technology. Instead of creating brand new legal rules that will confuse people, examining and making the existing contract law principles clearer for everyone may serve a better purpose. Therefore, legal compliance in smart contracts in the light of contracting principals have been analysed, together with some of the major questions in the contracting approach:

1. What is required to make smart contracts?
2. Where do smart contracts stand in relation to existing contracting rules? Can existing digital contracts help to understand smart contracts?

Smart contracts are not regulated as a different legal matter as of yet. This new phenomenon has mostly been measured by the interpretation of general contracting principles. As analysed in section 2.9.4 of this thesis, it has been seen to be unnecessary to create a separate set of new legal rules for smart contracts, in the US, and the UK regulators tend to share this approach. In the contracting sense, the regulation of smart contracts needs clearance of the contract conclusion schemes. To be able to talk about a contract at all, the legal requirements for contract conclusion must be defined in advance. There is no major obstacle in applying physical contracting rules to smart contracts, yet people need a clear pathway. An example of this is discussed in section 2.3, whereby the EC Directive regulates digital contracting in the e-commerce sector and requires companies to explain the contract conclusion process on their web site. Amazon has applied this approach effectively, and smart contract projects may benefit from this approach.

Given the rapidly changing nature of technology and the variety of the potential operations, cooperation between the legal and technical realm is required to produce practical and effective guidelines. Therefore, brand new regulations for smart contracts are not necessary and could potentially create more problems than benefits.

Smart contract technology can be implemented in various scenarios and sectors that are subject to different legal rules on an international level; this also makes the job of regulation complicated. It is very important to think globally when regulating smart contracts. This system is still not so familiar and is gradually emerging; consequently, it is not so fully adapted in practice. New complicated regulations (as the author considers is always the case in regulating technology-focused operations where many points need to be analysed regarding the technology) make people more reluctant and sceptical about the implementation of new phenomena. Well-structured and clear regulations could encourage business owners, as well as regulatory bodies, to make smart contracts a favourable option for the market in general.

In almost every case of technological development, there is a phase where the stakeholders are not fully convinced and are sceptical about adapting the new technology for their transactions. People naturally first want to be satisfied about the legal rules, as do the governments supporting these new technology developments. The author considers that it is important, as a first step, to create guidelines and technical reports for smart contract use cases and review mechanism schemes. Moreover, governments should be encouraged to employ smart contracts as they can benefit as well. Once persuaded of their efficacy, they can then go on to offer inducements for wider application. The author considers that government authorities might incentivize blockchain technology, organize informative events to urge people to consider using it. If governments really incentivize and train people in the application of this technology, show them the right tools to use and how to integrate the systems properly, people will be keener to adapt them. The most critical point is to convince and satisfy the public that the system will work properly and securely. This can be achieved by more and more application of this technology in practice.

The author considers that the authorities' first approach to this new technology should be to question how blockchain technology can be implemented and aligned with existing transactions from a sector-specific perspective and publish the conditions, with special consideration for the technical and administrative aspects and any precautions about being part of a blockchain-driven system. These directives and decisions have to be created in accordance with the different sector needs.

Blockchain technology has still areas that need to be developed and clarified in the area of the identity of the users; this directly affects the application of contract law principles and data protection compliance. As being technically nothing more than software, smart contracts cannot constitute a contract; they gain the sense of being a contract once the parties become involved; in other words when a smart contract-driven transaction is executed. If the parties are not identified, there may not be a chance to establish a real contracting set-up, and thus no contractual claims can be asserted.

Moreover, the tamper-proof nature of the system is likely to create problems in the legal sense. In practice, termination of a contract is not easy since amending the information in the blocks is almost impossible once the chains have been created. Especially in GDPR compliance, a great deal of purification would be needed. It is far from clear how the system would deal with the right of deletion claim. The author considers that privacy is critical, which should incentivize adaptation of this technology, although these issues may be mitigated in non-open blockchain systems created by a limited group of miners who are identifiable. The situation in the permissionless blockchain systems is far from being solved at the moment.

In the end, although mainly the contracting situation and the application of existing contracting principles in smart contracts have been analysed here, there are other legal concerns regarding the application of smart contracts that need to be analysed in further detail. Smart contracts may be examined in the light of property law principles, financial market regulations, and rules of company law.

In its current state, blockchain technology has to clear data protection compliance schemes both in open and limited networks. In an open, public transaction, it must be clear how service providers can deal with deletion requests. The legal realm and technology side must cooperate in solving privacy issues in blockchain systems. The privacy by design concept could help, yet it is still not clear how this approach might be implemented into the system. Finally, it is of paramount importance that parties are able to identify each other in the network in order to have a contractual relationship, and thus be able to make contractual claims.

BIBLIOGRAPHY

ALTAN, Alparslan	Enerji Sağlama Sözleşmeleri Bakımından Sözleşme Özgürlüğü ve Sözleşme Yapma Zorunluluğu İlkesinin Uygulanması. Ankara Barosu Journal, Volume2004(4). p61. http://www.ankarabarosu.org.tr/siteler/ankarabarosu/tekmakale/2004-4/3.pdf(Online)
BACON, Jean, MICHELS, JohanDavid, MILLARD, Christopher & SINGH, Jatinder	Blockchain Demystified. Queen Mary School of Law Legal Studies Research Paper No. 268/2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218 (Online)
BAINBRIDGE, David	Introduction to Computer Law. 5th ed. Longman. 2004.
BERBERICH, Matthias & STEINER, Malgorzata	Blockchain Technology and the GDPR-How to Reconcile Privacy and Distributed Ledgers. European Data Protection Law Review, Volume422(2). 2016. Queen Mary University of London.
BOYLE, Mike	The Need for Identity in Financial Electronic Transactions. GlobalSign blog. 2017. https://www.globalsign.com/en/blog/identity-in-electronic-transactions/ (Online).
BRAZELL, Lorna	Electronic Signatures and Identities: Law and Regulation. Sweet & Maxwell, 2nd ed. 2018.
BRANDSTATT, Christine, BRUNEKREEFT, Gert & FRIEDRICHSEN, Nele	Improving investment coordination in electricity networks through smart contracts. Jacobs University. 2011. https://ideas.repec.org/p/bei/00bewp/0010.html (Online)
BUCHER, Eugen	Introduction to Swiss Law; 3rd Ed. Chapter 8 Law of Contracts. Available at: http://www.eugenbucher.ch/pdf_files/86.pdf (Online).
CARDOZO Law School	Smart Contracts & Legal Enforceability. 2018. Research Report#2.https://cardozo.yu.edu/sites/default/files/Smart%20Contracts%20Report%20%232_0.pdf (Online)

CASSANO, Jay	What Are Smart Contracts? Cryptocurrency's Killer App. AppEconomy.2014.https://www.fastcompany.com/3035723/smart-contracts-could-be-cryptocurrencys-killer-app(online)
CHAMBER of DIGITAL COMMERCE, United States of America	"Smart Contracts" Legal Primer Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable. 2018. https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf. (Online)
CLACK, ChristopherD., BAKSHI VikramA. & BRAINE, Lee	Smart Contract Templates: foundations, design landscape and research directions. 2017. Cornell University, Computer Science, Computers and Society. https://arxiv.org/abs/1608.00771 (Online).
DE FILIPI, Primavera & WRIGHT, Aaron	Blockchain and the Law The Rule of Code. Cambridge, Massachusetts: Harvard University Press. 2018.
DEVECİ, Hasan	Consent in online contracts: old wine in new bottles. 2007. Computer and Telecommunications Law Review, Volume13(8), p223-231.
EUROPEAN COMMISSION	Trust Services and Electronic identification (eID). https://ec.europa.eu/digital-single-market/en/trust-services-and-eid (Online)
EMPIRICA	Three use cases of Smart Contracts in Financial services. Financial Markets software blog. 2016. http://empirica-software.com/three-use-case-smart-contracts-financial-services/. (Online).
ENGHEIM, Erik	What is a Smart Contract and why do we need them? 2018. https://medium.com/@Jernfrost/what-is-a-smart-contract-and-why-do-we-need-them-7d92f2131f03 (Online)
FAIRFIELD, Jat	Smart Contracts, Bitcoin Bots, and Consumer Protection. Washington&Lee Law Review Online. Volume 71(2) p.36. 2014. http://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3 (Online)

FINANCIAL CONDUCT AUTHORITY, UK	FCA fines Tesco Bank £16.4m for failures in 2016 cyber attack. https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack (Online).
HENDERSON, Kimberly, KNOLL, Emily & ROGERS, Matt	What every utility CEO should know about blockchain. Mckinsey&Company Report. 2018. https://www.mckinsey.com/industries/electric-power-and-natural-gas/our-insights/what-every-utility-ceo-should-know-about-blockchain. (Online).
HERTIG, Alyssa	How Bitcoin Could Decentralize the Courtroom. 2014. Motherboard.https://motherboard.vice.com/en_us/article/vvb79d/code-as-law-how-bitcoin-could-decentralize-the-courtroom(Online)
HUCKSTEP, Rick	What does the future hold for blockchain and insurance? Daily Fintech blog. 2016. https://dailyfintech.com/2016/01/14/what-does-the-future-hold-for-blockchain-and-insurance/(Online).
HODLER, Axel	Proving ownership of a cryptocurrency. 2017. Medium. https://medium.com/yopiter/proving-ownership-of-a-cryptocurrency-86a96f2c52b. (Online)
IANSITI Marko & LAKHANI, Karim	The Truth About Blockchain. Harvard Business Review, Volume-Jan-Feb 2017. https://hbr.org/2017/01/the-truth-about-blockchain (Online)
GOMEZ GELVEZ, MariaP.	Explaining the DAO exploit for beginners in Solidity. 2016. Medium. https://medium.com/@MyPaoG/explaining-the-dao-exploit-for-beginners-in-solidity-80ee84f0d470. (Online).
IEVA, Giedrimaite	IPKat Blok. Smart Contracts: Pros and Cons of the New Shiny Thing.2019.http://ipkitten.blogspot.com/2019/03/smart-contracts-pros-and-cons-of-new.html(Online)
KUNER, Christopher, CATE, Fred, LYNSKEY, Orla, MILLARD, Christopher, NI	International Data Privacy Law. 2018. Volume8(2). https://academic.oup.com/idpl/article/8/2/103/5047578 (Online).

LOIDEAIN, Nora & SVANTESSON, Dan

LEVI, Stuart D., LIPTON, Alex B. & Skadden, Arps, Slate, Meagher & Flom LLP. An Introduction to Smart Contracts and Their Potential and Inherent Limitations. Harvard Law School Forum on Corporate Governance and financial Regulation. 2018. https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/(Online).

LIPTON, Martin Risk Management and the Board of Directors. Harvard Law School Forum on Corporate Governance. https://corpgov.law.harvard.edu/2014/04/22/risk-management-and-the-board-of-directors-an-update-for- 2014/.

MACLEAN, Fiona Governing the Blockchain: How to Determine Applicable Law. 2017. Butterworths Journal of International Banking & Financial Law, Volume. 32(6), 359-361

FINCK, Michele Blockchain Regulation and Governance in Europe. Cambridge: Cambridge University Press. 2018.

MURRAY, Andrew Information Technology Law: The Law and Society. 3rd ed. Oxford: OUP Oxford. 2016.

MORRISON, Scott Smart contracts for enforcement of Islamic finance deals. 2019. Journal of International Banking Law and Regulation. Volume34(4). p145-151

NAKAMOTO, Satoshi Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. https://bitcoin.org/bitcoin.pdf(Online).

GOPIE, Nigel What are the smart contracts on blockchain? IBM blockchain blog. 2018. https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/ (Online).

ORAL, Tuğçe Viyana Satım Antlaşması'nda Sözleşmenin Kurulması, Yetkin Yayınevi, Ankara. 2014.

RAHMANI, Val Cyber Security: Corporate Insights for companies and their

directors. Slaughter and May. https://www.slaughterandmay.com/media/2536333/cyber-security-corporate-insights-for-companies-and-their-directors.pdf(Online)

RAMBERG, Christina — The Ecommerce Directive and formation of contract in a comparative perspective. 2001.European Law Review, Volume26(5), p429-450

REED, Chris, Umamahesh Sathyanarayan, Shuhui Ruan, Justine Collins. — Beyond Bitcoin – Legal Impurities and Off-Chain Assets. Queen Mary School of Law Legal Studies Research Paper. 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3058945(Online)

REED, Chris — Digital information law: electronic documents and requirements of form. London: University of London, CCLS. 1996.

REED, Chris — Internet Law: Text and Materials, 2nd ed. Cambridge: Cambridge University Press. 2004.

REED, Chris — What is a signature?. 2000. Journal of Information, Law and Technology, Volume2000/3. https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/ (Online)

RIEFA, Christine — The Reform of Electronic Consumer Contracts in Europe: Towards An Effective Legal Framework?. 2009. Lex Electronica, Volume14(2).

ROWLAND Diane, KOHL, Uta & CHARLESWORTH, Andrew — Information Technology Law. 4th ed. London: Routledge. 2011.

RUHİ, Ahmet Cemal — Sözleşmeler Hukuku, 2nd ed. Istanbul: Seckin. 2013.

SAVELYEV, Alexander — Contract Law 2.0: Smart Contracts As the Beginning of the End of Classic Contract Law. Higher School of Economics Research Paper.WPBRP71/LAW/2016.SSRN: https://ssrn.com/abstract=2885241 (Online)

SCHULPEN, Ruben — Smart contracts in the Netherlands A legal research regarding

the use of smart contracts within Dutch contract law and legal framework. Master. Tilburg University. 2018. http://arno.uvt.nl/show.cgi?fid=146860(Online)

SEGRAVE, Kerry — Vending Machines: An American Social History. North Carolina: McFarland & Co. p3. 2002.

SMEDINHOFF, Thomas — An Overview of Data Security Legal Requirements for All Business Sectors. 2015. https://media.lockelord.com/files/uploads/Insurance/Article%20-%20Data%20Security%20Requirments%20for%20All%20Business%20Sectors.pdf (Online)

SZABO, Nick — Formalizing and Securing Relationships on Public Networks. Peer Review Journal On the Internet. 1997. https://ojphi.org/ojs/index.php/fm/article/view/548/469 (Online).

TURAN, Gamze — Elektronik Sözleşmeler ve Elektronik Sözleşmelere Uygulanacak hukukun Tespiti. 2018. TBB Dergisi, Volume77. P87-119.

OKUMUŞ, Şüheda Dalka — Elektrik-Doğal Gaz Piyasaları Abonelik Sözleşmeleri ve Bu Sözleşmelerde Yer Alan Genel İşlem Koşulları. Ankara: Yetkin. 2018.

OMOHUNDRO, Steve — Cryptocurrencies, Smart Contracts, and Artificial Intelligence. Newsletter AI Matters, Volume1(2), P19-21. 2014. https://dl.acm.org/citation.cfm?id=2685334

ORTOLANI, Pietro — Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin. Oxford Journal of Legal Studies, Volume36(3) p595. 2016.

UK LAW COMMISSION — Electronic Commerce: Formal Requirements in Commercial Transactions (Advice From the Law Commission 2001). https://www.lawcom.gov.uk/project/electronic-commerce-formal-requirements-in-commercial-transactions/ (Online).

UK GOVERNMETN OFFICE FOR SCIENCE — Distributed ledger technology: Blackett review. Report by the UK Government Chief Scientific Adviser. 2016.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (Online).

YILDIRIM, Oğuz — Basel Criteria in the Turkish Banking System. Finance, Politics and Economic Comments, Volume 52/6092015, p9-19. https://docplayer.biz.tr/38975405-Basel-criteria-in-the-turkish-banking-system-abstract-oguz-yildirim-1.html (Online)

ZACHARIADIS Markos & ÖZCAN Pinar — The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199 (Online)

WINN, Jane — The Secession of the Successful: the Rise of Amazon as Private Global Consumer Protection Regulator. 2016. Arizona Law Review, Volume58(193), p194-211.

- http://www.masak.gov.tr/media/portals/masak2/files/mevzuat/sucgelirlerinin_aklanmasi/uluslararas%C4%B1_mevzuat/BaselKomite/2.htm
- https://www.nortonrosefulbright.com/en/knowledge/publications/ea958758/arbitrating-smart-contract-disputes
- https://www.coindesk.com/state-state-smart-contract-laws-aint-broke-dont-fix
- https://iapp.org/news/a/eu-data-breach-notification-rule-the-key-elements/
- https://www.us-cert.gov/bsi/articles/best-practices/risk-management/risk-management-framework-%28rmf%29
- https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-exchange-quadrigacx-password-cryptocurrency-scam-a8763676.html
- https://gdpr-info.eu/issues/privacy-by-design/