DR Diritto del Risparmio

BLOCKCHAIN-BASED SMART CONTRACTS FOR BEGINNERS

di Riet Pier Luigi*

The paper aims to provide a clear explanation of the concepts of blockchain and smart contracts to non-technical readers. Despite being one of the main topics debated worldwide, a law-oriented person may still struggle to comprehend these technologies. To understand these concepts, this study will trace the historical roots of blockchain and smart contracts. When analyzing the former, one will note that it is embodied within philosophy and cryptography. By using the same study-method with the latter, one will see why they have been developed. There will be also two described examples, one for both the technologies. The last paragraph aims to clarify some related concepts, in order to enlarge the understanding of the present topic.

ISSN 2704-6184

issue 2/2020

*Juris Doctor Trieste

Rivista di Diritto del Risparmio

Blockchain-Based Smart Contracts for beginners[*]

Riet Pier Luigi[**]

The paper aims to provide a clear explanation of the concepts of blockchain and smart contracts to non-technical readers. Despite being one of the main topics debated worldwide, a law-oriented person may still struggle to comprehend these technologies. To understand these concepts, this study will trace the historical roots of blockchain and smart contracts. When analyzing the former, one will note that it is embodied within philosophy and cryptography. By using the same study-method with the latter, one will see why they have been developed. There will be also two described examples, one for both the technologies. The last paragraph aims to clarify some related concepts, in order to enlarge the understanding of the present topic.

May

issue 2/2020

[*] This paper was approved by the referees.

[**] J.D. Trieste.

1. The first step by Haber and Stornetta

During the 1990s the digital world grew at an incredible speed rate. In 1991 CD Audio appeared on the market[1], about 20% of American families bought a personal computer[2], and within the aisles of Geneve's CERN headquarters, the very first website was developed[3]. In these circumstances, two cryptographers, Dr. Stuart Haber and Dr. W. Scott Stornetta, recognized that all of these new digital entities needed an urgent timestamp solution, as every single digital data, just as it stood, could be copied. According to these two scientists, this was mainly a copyright problem[4]. Consequently, they began working on a cryptographic method to guarantee everyone the authorship of their efforts.

The two scientists purposely imagined a naïve system to stress the critical issues that affected the timestamp solutions known at the time, calling it the "digital-safety deposit box". By using this system, all authors had to send their work to a centralized entity that kept a copy of that data and the date of the dispatch. However, this process revealed serious shortcomings: privacy was heavily undermined, costs would have been very high to send great data, and no one could ensure that the system would actually save the correct date[5]. To overcome these problems, Dr. Haber and Dr. Stornetta suggested the application of two different tools: hash functions, and digital signatures. With the first tool, it is possible to dwindle any data into a given-length "new" one[6], so every author may be able to "transform" their work into a sort of string that would then be sent to a centralized system. The safety box would later apply its digital signature and the date of the dispatch onto the string. The document created by the usage of these three previous documents would then be sent to the author. In this way, privacy would be preserved more efficiently, but no one could still guarantee that the system would certify the exact date.

Thereby the scientists advanced two alternative solutions to resolve this last issue[7]. One method was forcing the central system to certify the exact date of the document by attaching a hash string to some bits of the previous (document's) hash string. Consequently, the system could be unable to postpone the dates because to do so, it would need some hash strings that it had not received yet. It could not either backdate them because in doing so,

[1] https://www.philips.com/a-w/research/technologies/cd/beginning.html.

[2] https://www.census.gov/content/dam/Census/library/publications/2017/acs/acs-37.pdf.

[3] D. Raggett, J. Lam, I. Alexander, *Html 3.0: Electronic Publishing on the World Wide Web*, Addison-Wesley, Boston, 1996.

[4] S. Haber, W. S. Stornetta, *How to time-stamp a digital document*, in *Journal of Cryptology*, 1991.

[5] Ibidem.

[6] D. Carboni, *Le tecnologie alla base della blockchain*, in Raffaele Battaglini, Marco Tullio Giordano (curr.), *Blockchain e Smart Contract*, Giuffrè Francis Lefebvre, Milano, 2019.

[7] S. Haber, W. Scott Stornetta, How to time-stamp a digital document, cit.

the system would require some "hash pieces" already used. This system was interesting, though the method that sparks our enthusiasm is the second one: Dr. Haber and Dr. Stornetta proposed sending the hash code, with the author's identification, to every single member of the network. The users subsequently would put their signature on the just received hash code, attach the date onto it, and eventually deliver the resulting document to the original sender. This final solution is crucial. It is impossible to tamper with dates - for this purpose, collaboration would be requested between network members, but the "pseudorandom generator" forbids this[8] - and, mainly, it deletes the need of a central system. Most importantly, this pattern reveals to the reader some features that are considered as the main core of blockchain technology. As will be shown in the essence of this paper, blockchain is founded on cryptography, hash functions, and "distributed trust"[9].

Seventeen years after these studies, Satoshi Nakamoto released bitcoin and blockchain to the world. Three articles out of eight cited in the Bitcoin White Paper - the document that explains these technologies, formulated by Nakamoto himself - were, indeed, by Dr. Haber and Dr. Stornetta[10].

2. The route to the decentralized architecture

While Dr. Stornetta and Dr. Haber were developing a solution that would have been useful to achieve an efficient timestamp system, around San Francisco a group of internet-philosophers was born. One of the top members was the Berkeley mathematician Eric Hughes[11], who wrote in 1988 "A Cypherpunk's Manifesto" – but he released it in 1993[12].

In this movement's perspective – how it is explained in the Manifesto[13] - the internet should have been a totally free space, devoid of any government's interference. They were concerned mainly on privacy, claiming that it was a right to be obtained by the citizens on the net.

The movement's members recognized the digital money as the most powerful tool – among others, like cryptography and digital signatures[14] - to gain the privacy they yearned for[15]. Nick Szabo, Eric Hughes, David

[8] Ibidem.

[9] R. De Caria, *Definitions of Smart Contracts – Between Law and Code*, in Larry A. Di Matteo, Michel Cannarsa, Cristina Poncibò (eds.), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, Cambridge University Press, Cambridge, 2020.

[10] S. Nakamoto, *Bitcoin: a Peer-to-Peer Electronic Cash System,* http://www.**bitcoin**.org/**bitcoin**.pdf .

[11] R. Manne, *The Cypherpunk Revolutionary*, in *The Monthly.*

[12] P. De Filippi, A. Wright, *Blockchain and the law – the rule of code,* Harvard University Press, Cambridge, Massachusetts, 2019.

[13] https://www.activism.net/cypherpunk/manifesto.html.

[14] D. Chaum, *Security without Identification, Card Computers to make Big Brother Obsolete*, 28, 10, Communications of the ACM, 1985.

[15] P. De Filippi, A. Wright, *Blockchain and the law – the rule of code*, cit.

Chaum[16], and others addressed their experiments in this direction, but they were stuck on the need for a central system that could manage the digital-money transactions[17]. In the movement's perspective, anyway, a single point of control did not match their beliefs about privacy.

Thus, they realized that the next step to conquer their target was to leave the centralized system pattern, escaping from any form of control: Wei Dai, another member of the movement, invented the "b-money" following this direction. This awareness played a key role in blockchain and bitcoin's history: the very first article cited by Nakamoto in the Bitcoin White Paper is the b-money White Paper[18].

Nevertheless, the movement did not succeed to adopt decentralized, free-from-interferences money. All of those efforts shattered on another issue: double-spending. As explained before, every single digital data can be recopied, and this is a disrupting process with money. Spending the same amount of cash for two or more transactions makes the concept of money itself meaningless[19].

3. Smart contracts' history

During the Cold War, in 1948, URSS cut all the railroads directed to West Berlin. The "Berlin Blockade" crisis forced the United States of America to deliver two million tons of supplies by air, but the difficulty was enormous because every shipping manifest was written in different forms and languages.

Master Sergeant Edward Guilbert won the challenge of managing the cargo operations by creating a unique standard for the manifests: this method allowed him to transmit the information by telex, telephone or radio-teletype[20].

Having left the military career, Guilbert kept developing this standard during the 1960s while he was working for Du Pont Co.: the innovation spread widely during the next decade in the business field and in 1975 the first Electronic Data Interchange (EDI) specifications was officially adopted by the Transportation Data Coordinating Committee. EDI system is based on translating in electronic form the contractual terms that have been written in the traditional way by the parties before.

EDI solution, however, did not satisfy the cypherpunk movement's member Nick Szabo. He claimed that this standard was not able to bind the parties, precisely because it was just the translation of previous contracts[21].

Thus he advanced in the same paper the idea of writing pieces of software - based on cryptographic protocols - specifically designed to create

[16] D. CHAUM, *Blind Signatures for Untraceable Payments*, Advances in Cryptology: Proceedings of Crypto 82, 1983.

[17] P. DE FILIPPI, A. WRIGHT, *Blockchain and the law – the rule of code*, cit.

[18] S. NAKAMOTO, *Bitcoin: a Peer-to-Peer Electronic Cash System*, cit.

[19] A. PERNA, *Le origini della blockchain*,cit.

[20] P. DE FILIPPI, A. WRIGHT, *Blockchain and the law – the rule of code*, cit.

[21] N. SZABO, *Formalizing and Securing Relationships on Public Networks*, in FirstMonday.org.

real contractual terms (and not just a translation of pre-existing ones): by this way, Nick Szabo believed that the contractual obligations would have been "more binding" than the EDI forms.

The idea of "smart contracts" was born, but despite the huge interest it had aroused no one was able to develop this concept. The main issue relied on the absence of an architecture to support the features of the smart contract as imagined by his creator.

4. Bitcoin, blockchain, and Ethereum

While the ghosts of the financial crisis were haunting the world, on October the 31st 2008 someone called Satoshi Nakamoto wrote a message to the cypherpunk's mailing list. He asserted he had created a digital cash system without relying on a centralized scheme, using a peer-to-peer architecture instead[22]. He shared bitcoin's White Paper and since then this digital money has gained large popularity all over the world.

Bitcoin's birth is imbued by democratic and economical instances. Satoshi Nakamoto – following the cypherpunk experiments' results - chose a decentralized pattern for managing bitcoin to escape from a single-point-control-system- the then-notorious "blockchain". He reported The Times title "Chancellor on brink of second bailout for bank" on the first block he mined[23] - a choice believed to be a quarrel against the traditional economic sets -; and, mainly, he chose to realize an open-source project.

Thanks to the latter characteristic, many computer programmers could handle this software, being able to develop new features. By this way, they started to believe that the newborn blockchain structure could serve not just as an architecture for money transactions, but also for new and undiscovered purposes[24].

In 2013, the nineteen-year-old Vitalik Buterin had the revelation: the blockchain, built by Satoshi Nakamoto to create the needed environment for bitcoin's transactions, was the architecture they need to write Smart Contracts as ideated by their creator, Nick Szabo[25].

Supported by a successful crowdfunding campaign, Buterin thus developed Ethereum, the first blockchain purposely built for generating and deploying this kind of smart contracts[26]. It is useful underlying that these tools can be used without a blockchain architecture behind too[27], but as

[22] G. J. SICIGNANO, *Bitcoin e riciclaggio*, G. Giappichelli Editore, Torino, 2019.

[23] A. M. ANTONOPOULOS, *Mastering bitcoin: Programming the Open Blockchain*, Oreilly & Associates Inc., Sebastopol, California, 2017.

[24] A. PERNA, *Le origini della blockchain*, in Raffaele Battaglini, Marco Tullio Giordano (curr.), Blockchain e Smart Contract, Giuffrè Francis Lefebvre, Milano, 2019.

[25] Ibidem.

[26] Vitalik Buterin, Ethereum White Paper.

[27] M. DUROVIC, A. JANSSEN, FORMATION OF SMART CONTRACTS UNDER CONTRACT LAW, in Larry A. DiMatteo, Michel Cannarsa, Cristina Poncibò (eds.), The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, Cambridge University Press, Cambridge, 2020.

explained in the following pages the highest explication of smart contracts is provided by the blockchain pattern.

5. Blockchain and smart contracts in action: definitions and functioning

By retracing these technologies' history, we got acquainted with the features they have been developing with.

In the following steps, we are going to systematize these notions by providing clear definitions of these technologies and, mostly, we are going to check their working.

5.1 Blockchain

To understand what is a distributed ledger technology (in fact, blockchain is a "species" of this "genus"[28]) we have to – once again – look to the internet's history.

In his early days, the web relied on the "client-server" scheme: websites were hosted by servers, and every user had "to reach" the server by his client to get the information he was looking for. As the reader may clearly see, the data hardly ever goes from client to server and, even more rarely, from client to client[29]. At the dawn of the new millennium, this pattern already showed its shortcomings: it simply could not manage many synchronous requests. The system was affected by the "bottle-neck" effect, causing the service's suspension when the server was "crowded"[30].

To solve this problem, programmers postulate the peer-to-peer working scheme: by this method, every single web-user (the "peer") is, at the same time, both a user and a provider of data[31]. The peer-to-peer networks are designed as a pool of connected nodes (the ledgers): every single ledger contains all the data that has flooded over the network; in this way, every change made on a ledger is recopied on all the other ones[32].

That is one of the main differences between peer-to-peer scheme and client-server one: the former is much more resilient because if every node - except one - is destroyed or damaged, a copy of the ledger will continue to

[28] O. BORGOGNO, USEFULNESS AND DANGERS OF SMART CONTRACTS IN CONSUMER TRANSACTIONS, in Larry A. DiMatteo, Michel Cannarsa, Cristina Poncibò (eds.), The Cambridge Handbook of Smart Contracts, cit.

[29] M. D. HANSON, *The client/server architecture*, in Gilbert Held (cur.), Server Management, Auerbach Publications, Boca Raton, Florida, 2000.

[30] V. CARDELLINI, M. COLAJANNI, P. S. YU, *Dynamic load balancing on web server systems*, IEEE Internet Computing, 1999.

[31] R. SCHOLLMEIER, *A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications*, in Proceedings First International Conference on Peer-to-Peer Computing, IEEE, 2001.

[32] A. GASCHI, V. PORTALE, *La definizione di blockchain e* distributed ledger, in Raffaele Battaglini, Marco Tullio Giordano (curr.), Blockchain e Smart Contract, Giuffrè Francis Lefebvre, Milano, 2019.

exist[33]. This is not possible on a centralized, based-on-server working scheme.

As it is possible to note now, there is not a single point of control over a peer-to-peer network[34] (as opposed to the server's pattern): a single user can never delete or modify a data that has been written into the ledgers[35].

However, to define blockchain we need to see its functioning. At the end of the explanation, we may be able to finally understand why this technology is called in this manner. To achieve this result it may be useful to use bitcoin's blockchain as an example.

A user called Mary wants to transmit some money to another user, William. Their "wallet" identifies them, as every user onto this blockchain. The wallet is simply an alphanumeric code.

To succeed in her intent, Mary has to write a message that includes the exact amount of money to transfer, the starting wallet, and the arriving one. Mary puts onto the message her private key (a cryptographic tool that, if combined with a public key, can guarantee a high level of security) and subsequently sends the resulting message to the net (and, in this way, to every single node). At this point, the nodes proceed to check both the message's origin (by scanning Mary's signature on the message) and the operation's feasibility (by examining Mary's balance: this check is possible because every transaction is reported on all the nodes, so nodes can see if Mary has enough money).

If this twofold check's result is positive, the system regroups this transaction with other transactions that have occurred in the same time frame on the network (in bitcoin's blockchain, this time is ten minutes[36]; in ethereum is twelve seconds). All these transactions are thus saved in a new "block".

Now we can see the reason why this technology's name is "blockchain". The newborn block has to be attached to the other blocks, already existing in the network. In this circumstance, nodes start the famous "mining" process. They all start trying to find a casual number that, when added to the amount of the "old" blocks and to the sum of the "new" block's transactions, provides another given number.

When the winning node finds a suitable figure, it communicates the number to the other nodes. If the check's result is positive for the 51% of the nodes, then all the nodes attach the new block to the old ones. There we have the "block-chain". The winning node will receive its bounty – in

[33] P. DE FILIPPI, A. WRIGHT, *Blockchain and the law – the rule of code*, cit.

[34] L. PIATTI, *Dal Codice Civile al codice binario*: blockchain *e* smart contracts, in Ciberspazio e diritto, 2016.

[35] F. S. DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, Wolters Kluver, 2019.

[36] M. CHIERICI, *La blockchain: una lettura giuridica per uno sguardo verso il futuro*, in Ciberspazio e diritto, 2018.

cryptocurrencies – and William's wallet will be eventually enriched by Mary's money[37].

In this example, we can recognize some of the main features of the blockchain' system, as data saved in every node and the non-feasibility of tampering with a node[38] (in doing so it would be requested to falsify all the following nodes too).

It may be fruitful to linger a bit on the consensus mechanism: as explained in the example, 51% of the nodes have to agree on a data to save it on the network (and thus in all nodes). This method is called "Proof of Work"[39], but due to its shortcomings (one for all, the extremely high amount of electricity requested for processing the mining operations[40]) some other solutions have been deployed for the same purpose (as Proof of Stake[41], Proof of Authority[42] or others).

Now we can comprehend the blockchain's definition released by European Central Bank: "the ledger (book of records) of all transactions, grouped in blocks, made with a decentralised virtual currency scheme"[43].

5.2 Smart contracts

To provide an efficient explication of smart contracts' working we have to get acquainted with another element of the blockchain. As said before, blockchain is a virtual world which vehiculates digital goods. However, can users put into this virtual system related-to-real-world data? For instance, can they imagine a transaction on a blockchain that includes a suspensive condition based on a real-world event?

Yes, they can, by using a feature called "Oracle". This name encompasses different solutions, but all of these "entities" can put into blockchain real-world's data[44]. Oracle's topic is quite a thorny issue: in the following example, we are going to consider Oracle's working for the purpose we are pursuing, and we delay the discussion on this subject to the last chapter of this paper.

[37] V. Gatteschi, F. Lamberti, C. Demartini, *Technology of Smart Contracts*, in Larry A. DiMatteo, Michel Cannarsa, Cristina Poncibò (eds.), The Cambridge Handbook of Smart Contracts, cit.

[38] P. De Filippi, A. Wright, *Blockchain and the law – the rule of code*,cit.

[39] G. Rinaldi, *Criptovalute e* blockchain, in Vita Notarile, 2018.

[40] Jon Truby, Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies, Energy Research & Social Science, 2018.

[41] F. S. di S. Ippolito, M. Nicotra, *Diritto della blockchain, intelligenza artificiale e IoT*, cit.

[42] F. S. di S. Ippolito, M. Nicotra, *Diritto della blockchain, intelligenza artificiale e IoT*, cit.

[43] https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[44] E. Mik, *Smart contracts: terminology, technical limitations and real world complexity*, in *Law, innovation and technology*, 2017.

A smart contract is a software that activates itself when a condition occurs[45] (these conditions are known as "trigger points"[46].) They are automated[47], and when a smart contract starts, it is impossible to stop it (unless this provision is included in the software's code)[48]. Thus, they are designed to be able to control mathematics variables: when the latter change their "status", a condition becomes true or false and finally, the smart contract can start (or stay motionless, according to its provisions about the condition itself).

Mary wrote her last will on a smart contract. This software includes two testamentary forecasts: Mary's virtual goods will be transferred to William's wallet at Mary's death, and this transfer could not be completed before William's graduation.

Mary's will contains three variables: the first one is "owner alive", and its starting status is "true"; the second one is "payee's address" (William's wallet identification number); the third one is "payee's graduation", and its starting status is "false"[49].

Now we can clearly understand Oracle's role in the blockchain environment: these entities are the only ones who can change the variable's status, by checking the related changes in the real world. When they "warn" the blockchain that the variables have changed their condition, smart contracts can eventually be ready to start (more precisely, because of their automated soul, smart contracts will start immediately).

Like blockchains, smart contracts do not have a unique definition[50]. Nick Szabo himself released three definitions during the years: by reading them, we can finally realize their power in cypherpunk's vision (Szabo was a movement's member) and why, due to their automated soul, they have found their perfect habitat on distributed ledger technologies (thanks to Buterin's efforts).

In 1994, Szabo declared that a smart contract was "a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other

[45] K. WERBACH, N. CORNELL, *Contracts ex machina*, in Duke Law Journal, 2017.

[46] M. T. GIORDANO, *Il problema degli oracoli*, in Raffaele Battaglini, Marco Tullio Giordano (curr.), Blockchain e Smart Contract, Giuffrè Francis Lefebvre, Milano, 2019.

[47] S. CAPACCIOLI, *Smart contracts: traiettoria di un'utopia divenuta attuabile*, in *Ciberspazio e diritto*, 2016.

[48] P. DE FILIPPI, A. WRIGHT, *Blockchain and the law – the rule of code*, cit.

[49] V. GATTESCHI, F. LAMBERTI, C. DEMARTINI, Technology of Smart Contracts, in Larry A. DiMatteo, Michel Cannarsa, Cristina Poncibò (eds.), The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, Cambridge University Press, Cambridge, 2020.

[50] L. W. CONG, Z. HE, *Blockchain Disruption and Smart Contracts*, in *Review of financial studies*, 2019.

transaction costs"[51]. The following year Szabo claimed: "Smart contract: a set of promises, including protocols, within which the parties perform on the other promises. The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics, thus these contracts are 'smarter' than their paper-based ancestors. No use of artificial intelligence is implied"[52]. In 1996 he defined this technology as "A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises"[53].

6. Quick facts for a further understanding

The reader has now gained all the elements he needs to achieve a deeper knowledge of the topic. The following paragraphs are going to finally explain some topics often related to blockchain and smart contracts.

6.1 Distributed trust and disintermediation

Blockchain enthusiasts often claim that this technology is a tool that can free us from intermediation's issues, like corruption, privacy violations, and costs[54]. Basing their emphasis on the blockchain consensus mechanism, they declare that distributed ledgers do not need any trust to work. Nakamoto built a distributed and decentralized pattern that removes the logic of the central point: every data has to be confirmed by the members' majority to get verified and written on the ledgers.

Trust distribution (aka trust to the many) as opposed to trusting to a single person is an idea that firstly emerged in Haber and Stornetta's paper; but is this a real perspective?

Someone cleverly wrote that blockchain does not delete (or distribute) trust. Looking closer at the architecture's working one may realize that there is still trust, but in another place: software developers' skills[55].

6.2 Immutability

A connected topic is blockchain's immutability. How it is explained before, all the ledgers contain all the data and it is almost impossible to tamper with them (unless one may control 51% of the nodes, but it is a titanic operation). This feature guarantees data immutability. This is one of the most publicized blockchain's characteristics, but one of its main shortcomings too. As one may have guessed, how is it possible to change a

[51] N. SZABO, *Smart contracts, 1994*, in Claudia Linnhoff-Popien, Ralf Schneider, Michael Zaddach, *Digital Marketplaces Unleashed*, Springer, Berlin, 2018.

[52] N. SZABO, *Smart Contracts Glossary, 1995*, in Tatiana Antipova, Alvaro Rocha, Digital Science, Springer, Cham, 2019.

[53] N. SZABO, *Smart Contracts: Building Blocks for Digital Markets, 1996*, in Mateja Durovic, André Janssen, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, in *European Review of Private Law*, 2018.

[54] L. PIATTI, *Blockchain, decentralizzazione e privacy: un nuovo approccio del diritto*, cit.

[55] E. MIK, *Blockchains - A Technology for Decentralized Marketplaces*, in Larry A. DiMatteo, Michel Cannarsa, Cristina Poncibò (eds.), The Cambridge Handbook of Smart Contracts, cit.

wrong data? If transactions containing false data have been elaborated into the system, who is eligible for liability?

This is a smart contracts' characteristic too. These tools operate without human intervention[56], because when a "trigger point" - the condition that controls the smart contract's working - is activated the software autonomously starts its route.

These two combined characteristics show us a fundamental problem, known as "garbage in, garbage out"[57]. If a wrong data is introduced into the blockchain, and then this data is processed by a transaction, the transaction will invariably be wrong. How is it possible to remedy this situation?

This is quite a tough issue. Two different ideas have been proposed to settle this problem: the first relies on writing a second smart contract that contains "in-reverse" previsions than the first one[58]; the second one imagines a "kill function" within the smart contract itself, that can be activated only by both the parties to stop the software' working[59]. It is possible to realize that the first method – due to the immutability of blockchains – do not erase the first contract, but simply nullify its result[60].

6.3 Different blockchain versions

In the previous paragraphs, we have underlined blockchain's philosophy, inspired by freedom and democratic instances. These beliefs heavily influenced the architecture's design: the needed trust to verify the transactions is distributed; no one owns the total control; the data is readable by anyone.

These main features, claimed to be the preeminent qualities of this technology, are also its limitations: as it happened with the Ethereum project, many software developers built different distributed ledger technologies for different purposes[61]. The result is that there is not a unique definition of blockchain[62].

[56] O. BORGOGNO, *Smart Contracts as the (new) Power of the Powerless? The Stakes For Consumers*, in *European Review of Private Law*, 2019.

[57] P. DE FILIPPI, A. WRIGHT, *Blockchain and the law – the rule of code*, cit.

[58] J. SCHREY, T. THALHOFER, *Rechtliche Aspekte der Blockchain*, IN *Neue juristische Wochenschrift*, 2017.

[59] S. A. CERRATO, *Contratti tradizionali, diritto dei contratti e smart contract*, in Raffaele Battaglini, Marco Tullio Giordano (curr.), cit.

[60] B. PASA, L. A. DIMATTEO, *Observations on the Impact of Technology on Contract Law*, in Larry A. DiMatteo, Michel Cannarsa, Cristina Poncibò (eds.), The Cambridge Handbook of Smart Contracts, cit.

[61] E. TJONG TJIN TAI, *Challenges of Smart Contracts – implementing excuses*, in Larry A. DiMatteo, Michel Cannarsa, Cristina Poncibò (eds.), The Cambridge Handbook of Smart Contracts, cit.

[62] A. WALCH, *The Path of the Blockchain Lexicon (and the Law)*, in *Boston University Review of Banking & Financial Law*, 36, 2016.

The main dichotomy can be drafted between “public” and “private” blockchain[63]: in the former, the user does not need any permission to access the data[64], but in the latter, only predetermined users are able to examine them[65].

Another dichotomy is founded on users’ role on the system: if they all can (after having checked data) validate transactions, this would be a “permissionless” blockchain; if just a few of them can be part of this process, this would be a "permissioned" blockchain instead[66].

Following blockchain’s history the reader may have appreciated why scholars recognize in the public, permissionless blockchain the real innovation[67]; however, it is quite interesting that Vitalik Buterin, founder of the ethereum public blockchain, admitted that the private ones could provide many advantages to the users[68]. For instance, this version’s consensus mechanism would be faster than the public one; costs would be lower; and, mostly, in the private blockchain, some predetermined users can verify data, so they can delete wrong transactions.

This feature solves also one of the biggest issues that businesses face when they are approaching blockchain technology: liability. If, in the public version, there is not a mid person anymore because the trust is distributed, who is eligible for net's misuses or damages? They often opt for a private one to remedy this shortcoming, by pointing the nodes that will process the transactions and, thus, will be eligible for liability.

Businesses often prefer private blockchains for another advantage it brings: privacy. Business practices are often informed by confidentiality, that cannot be guaranteed in a public system (where every user can inspect data).

6.4 Pseudonymity or anonymity

This is another feature that leads to a distinction between blockchain’s versions. Bitcoin, for instance, is based on a pseudonym blockchain because every user is combined with a private key. Although some techniques are known to reveal users’ identity, this operation is often hard to complete - but not impossible[69]. Some other systems, like Monero or ZCash, rely on a totally anonymous parameter instead[70].

[63] A. GASCHI, V. PORTALE, *La definizione di blockchain e distributed ledger*, in Raffaele Battaglini, Marco Tullio Giordano (curr.), Blockchain e Smart Contract, cit.

[64] E. TJONG TJIN TAI, *Challenges of Smart Contracts – implementing excuses*, in Larry A. DiMatteo, Michel Cannarsa, Cristina Poncibò (eds.), The Cambridge Handbook of Smart Contracts, cit.

[65] E. MIK, *Electronic Platforms: Openness, Transparency & Privacy Issues*, cit.

[66] A. GASCHI, V. PORTALE, *La definizione di blockchain e distributed ledger*, in Raffaele Battaglini, Marco Tullio Giordano (curr.), Blockchain e Smart Contract, cit.

[67] P. DE FILIPPI, A. WRIGHT, *Blockchain and the law – the rule of code*, cit.

[68] E. MIK, *Electronic Platforms: Openness, Transparency & Privacy Issues*, cit.

[69] P. CUCCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in *Nuova giuridica editore*, Matelica, 2017.

[70] L. PIATTI, *Blockchain, decentralizzazione e privacy: un nuovo approccio del diritto*, cit.

6.5 Oracles

As we have described before, Oracles are the entities that can import real-world data on a blockchain (or export blockchain's data to the real world)[71]. There are three versions of these tools: the automated type, the trusted third party, and the expert type[72]. Vehicles that can send signals after a car accident exemplify the first one; the second type oracles are trusted humans, as the courier who certifies the dispatch; the last one is the version we use when the operation is (still) too difficult to be completed by a machine, as in the arbitrations' decisions[73].

If the reader has fully understood blockchain's logic, he realized that distributed ledger technologies do not have a "single point of failure"[74] (unlike in the client/server architecture); but if we introduce Oracles in a smart contract software, the blockchain loses this characteristic. Oracle's information cannot be verified as other data inside the blockchain[75], because these data are "upstream": we are forced to trust Oracle's result, disrupting the "distributed trust" philosophy.

7. Conclusion

Blockchain and bitcoin were born as parts of a monetary system, but during the years they have gained a major role in other fields too. The legal world is very interested in distributed ledger technologies and smart contracts, which are powerful tools to build automated transactions. Their field of action spans from real estates' purchase[76] to voting in shareholders' meetings[77], from supply chains[78] to public health[79]. Recently, the topic has reached the parliaments too: many States have adopted specific regulations – or they have covered this subject with pre-existing laws.

Thus, a sparkling atmosphere cloaks the topic. This paper strived to provide to the reader the essential elements he needs to fully comprehend the different perspectives and proposals that have been advanced since these technologies' dawn – being able to appreciate the reasons behind a belief.

[71] V. GATTESCHI, F. LAMBERTI, C. DEMARTINI, TECHNOLOGY OF SMART CONTRACTS, in Larry A. DiMatteo, Michel Cannarsa, Cristina Poncibò (eds.), The Cambridge Handbook of Smart Contracts, cit.

[72] E. TJONG TJIN TAI, *Force Majeure and Excuses in Smart Contracts*, cit.

[73] M. ABRAMOWICZ, *Cryptocurrency-based law*, in *Arizona Law Review*, 2016.

[74] M. T. GIORDANO, *Il problema degli oracoli*, in Raffaele Battaglini, Marco Tullio Giordano (curr.), Blockchain e Smart Contract, cit.

[75] E. MIK, *Electronic Platforms: Openness, Transparency & Privacy Issues*, cit.

[76] https://www2.deloitte.com/us/en/pages/financial-services/articles/blockchain-in-commercial-real-estate.html.

[77] D. YERMACK, *Corporate Governance and Blockchains*, in Review of Finance, 2017.

[78] Ž. TURK, R. KLINC, *Potentials of Blockchain Technology for Construction Management*, in *Procedia Engineering*, 2017.

[79] https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf.