ISSN 2281-5147

LOST IN THE WEB: THE DARK SIDES OF SMART CONTRACTS. EXCEPT THERE IS STILL HOPE

Sara Rigazio[*]

Abstract

This article addresses the issue related to the potential harms and the abuses arising from the application of the latest and disruptive decentralized ledger technologies (DLTs) to self-executing software, commonly known as smart contracts. To this end, the article identifies and describes the main features of the DLT– namely the blockchain – most frequently underlying smart contracts, showing their innovative yet challenging profiles. As a matter of fact, these same features may lead to mishandlings and distorted uses when applied to smart contracts, as it happened in the case study presented. Notwithstanding these undeniable 'dark sides' then, this paper suggests that it is still possible to balance the need for regulation and the development and encouragement of an (informed) implementation of the new information technologies, through a law by design approach.

Indice Contributo

Abstract.. 694

Keywords.. 695

1. Introduction... 695

2. The Blockchain revolution... 696

3. Smart contracts: a fancy name for a complex issue tructural remarks............ 700

3.1 TheDAO case: what could go wrong, (almost) went wrong 705

[*] Assistant professor of private law, University of Palermo. sara.rigazio@unipa.it

4. Is there still hope? The 'law by design' approach. Conclusive remarks. 709

Keywords

Blockchain - Smart Contracts - Decentralized Autonomous Organizations (Daos) - Self-Regulation - Law By Design Approach.

1. Introduction

This article addresses the dangers potentially deriving from self-executing processes or code-oriented contracts, widely known as smart contracts, in the contractual relationships. The analysis focuses in particular on the abuses that might occur and that can lead to reach illicit agreements.

The first part of the paper briefly introduces smart contracts highlighting the main features of the technology behind them, namely the blockchain. It focuses on decentralization, immutability and pseudonymity. It is important to note that smart contracts can also exist thanks to the traditional technologies, ie centralized data bases and, therefore, even without a blockchain[1]. However, I choose to look at blockchain-based smart contracts because of the recent uprising in the use of this technology in virtually every area and aspect of life, including daily life[2].

[1] In this regard, see Roberto Pardolesi and Antonio Davola, 'What is wrong in the debate about smart contracts', (2020), 9 (5) *Journal of European Consumer and Market Law* 201, who underline the fact that "the blockchain is not the condition sine qua non for the functioning of smart contracts, but just one of the possible tools for their implementation; if smart contracts are meant to spread in the legal practice, this might as well happen through technologies, other than the blockchain, that will reveal themselves as more suited to adapt to users' needs".

[2] For an example of a very positive account on blockchain's potential, see Jamie Smith, 'There Is More to Blockchain than Moving Money. It Has the Potential to Transform Our Lives—Here's How', WORLD ECON. F. (Nov. 9, 2016), <https://www.weforum.org/agenda/2016/11/there-is-more-to-blockchain-than-moving-money/ [https://perma.cc/7GLT-XPD3]>. More generally, on the applications of the blockchain technology in the daily life, consider, for example, the agri-food system. See, Gianpiero Ruggero, 'Tracciabilità e blockchain: le sfide nella filiera agroalimentare', (2019) Agenda digitale EU, <https://www.agendadigitale.eu/documenti/tracciabilita-e-blockchain-le-sfide-nella-filiera-agroalimentare/>. Last accessed on April 2022. Also, one of the latest applications of the blockchain technology is in the art law sector. In this regard, see Martin Zeilinger, 'Digital Art as 'Monetised Graphic': Enforcing Intellectual Property

ISSN 2281-5147

The second part of the paper shows how blockchain-based smart contracts can result in twisted applications and could be executed for illegitimate purposes[3]. In this regard, I will analyze the case of the U.S. digital platform *TheDAO*, where leaks of confidential information and theft of cryptographic keys occurred.

The topic of smart contracts recalls the debate on the relationship between law and technology, certainly not new to the scholars and extremely complex. While a study on such an issue is definitely beyond the scope of this analysis, this paper shows how smart contracts, despite their 'dark sides', can still contribute in a positive way to this debate thanks to their intrinsic (positive) potentials and a law by design approach by the interpreters.

2. The Blockchain revolution

Over the past two decades, computers and digital platforms have risen to such level of prominence in several different industries that devices have been able to perform automatically countless tasks. In the very recent years, some advanced and innovative information technologies have had such a fast and disruptive impact over business, social interactions and, of course, contractual relationships, to the point of getting rid of (almost) any human interventions.

Among these technologies, the ones characterized by a decentralized structure have gained a lot of attention: first by the programmers, then by the users and, finally, by the legal experts. They are called 'distributed ledger technologies (DLTs)' and blockchain is one of them.

DLTs are different from the traditional technologies (the centralized databases): they are indeed completely decentralized, meaning that there is no need for intermediaries

on the Blockchain', (2018) 31 Philos. Technol., 15-41. Last accessed on March 2022. R. M"!]:#, "Blockchain: Xe Invisible Technology Xat's Changing the World", PC Magazine 2017. Available at: https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor

[3] Ex multis, Ari Juels, Ahmed Kosba, Elaine Shi, 'The Ring of Gyges: Investigating the Future of Criminal Smart Contracts', (2016), *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communicationns Security*, NY 283.

ISSN 2281-5147

because the users (called 'nodes') themselves participate to the update and the maintenance of the network through a specific algorithm called 'consensus protocol'[4].

Therefore, the autonomy of the single node, in terms of the transactions to be carried out, represents the core idea at the basis of these networks as opposed to what happens in the traditional ones, where only the administrator of the system is in charge of the decisions to be made and the users can either accept those decisions or exit the system.

To make this concept clearer we refer to the famous large Internet companies or cloud computing operators (called gate keepers for their dominant position in the digital market) such as Amazon, Microsoft or Google that are in charge of all the data. Blockchains dramatically change this dynamic offering the management of these data to new single operators, not dependent on centralized control.

It is a different hierarchical structure that relies on shared databases operating globally and borderless. Because of this decentralized structure, anyone with an Internet connection can retrieve information stored on a blockchain, by downloading the available opensource software[5].

Being intrinsically transnational implies the critical potential to support global disintermediated services and to facilitate the parties to engage with one another in an easier way than usual for a series of different reasons. To get an idea of the potential vastity of online services available it is just sufficient to look at what happened with Bitcoin from its launch in late 2008.

[4] See, Christian Cachin and Marco Vukolic, 'Blockchain Consensus Protocols in the Wild', (2017), <https://arxiv.org/abs/1707.01873>, Cornell University, who specify that "A blockchain is a distributed ledger for recording transactions, maintained by many nodes without central authority through a distributed cryptographic protocol. All nodes validate the information to be appended to the blockchain, and a consensus protocol ensures that the nodes agree on a unique order in which entries are appended" accessed March 2022. See, also, Andrea D'Anna, 'La formazione del consenso nella blockchain in assenza di autorità centralizzate, il problema dei generali bizantini e prospettive future', (2018), CyberLaws <https://www.cyberlaws.it/2020/formazione-consenso-blockchain-prospettive-future/> accessed February 2022.

[5] Arvind Narayan and others, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press 2016.

ISSN 2281-5147

One thing to remember is that the more 'engagements' by the nodes the blockchain gains, the more complex it becomes in terms of managing the protocol. This has of course consequences for leaving the system exposed to security flaws.

Another characteristic that makes the blockchain so unique is its immutability. Once the information has been recorded to a block, it becomes very hard to change the record or to delete it. It would be indeed very expensive to convince the other nodes to implement a change to the protocol and it would be a difficult and time-consuming process. Moreover, it is the technical design of the blockchain that favors the status quo, making the networks very resistant to changes. In any case, if the majority of the nodes does not agree on a change, the blockchain remains the same.

The tamper-resistant nature of the data stored on the blockchain combines with the transparency of the overall system. In this case it is a slightly different concept of transparency than the one commonly known because the information maybe in fact encrypted[6]. However, the information about the sequence of the transactions and the accounts that are engaging in those transactions are available for anyone using the chain. In other words, there are different degrees of transparency depending on the domain of application: there are blockchains where data are publicly shared, such as in the case of Bitcoin (called permissionless) and blockchains where transactions data remain confidential and, as mentioned above, the information is encrypted (called permissioned)[7].

The blockchain system helps to create trust in the network because the parties can review (without changing of course) the blockchain and verify that the transaction has

[6] The issue of transparency in blockchain systems has been investigated at many levels. An interesting article published in February 2020 on Forbes concluded that the blockchain technology could represent the solution for corporates and companies in the USA: indeed, the article argues that through this system complete transparency is granted at reasonable costs. In addition, the 'good practice of transparency' is encouraged and it becomes of benefit for the whole market. The actual system prescribed by the US federal rules, instead, is not only prohibitively expensive, but achieves the exact opposite of the intended effect. Companies, as a matter of fact, try in every way possible to avoid the prescribed procedure and do not comply with the obligation of transparency with obvious negative consequences on the market. See <https://www.forbes.com/sites/forbestechcouncil/2020/02/14/how-the-transparency-of-blockchain-drives-value/?sh=d0ab19431a6d>.

[7] See, Giusella Finocchiaro and Chantal Bomprezzi, 'A legal Analysis of the use of blockchain technology for the formation of smart legal contract', (2020), MediaLaws <https://www.medialaws.eu/wp-content/uploads/2020/07/RDM_2_2020-Finocchiaro.pdf>.

ISSN 2281-5147

indeed occurred or that the information is authentic in relation to its source (without necessarily trust each other). This represents a useful tool also for governmental authorities in the organization of their records, making data paperless and available worldwide to anyone who is connected to the Internet[8].

Another element that makes blockchains so unique is the pseudonymity. Generally speaking, pseudonymity represents a weaker form than anonymity since the user appears with a different identity than the real one, but the at the same time he can be still identifiable[9].

As already mentioned, in the case of the blockchain, the system allows the nodes to store information or to engage in transactions: all these actions can be assessed by relying on digital signatures or public-private keys without revealing the true identity of the user. As a matter of fact, pseudonymity makes it possible to assign the transactions to the same user and, therefore, to identify the users behind. Needless to say, at the same time this system may facilitate parties to engage in suspicious activities[10].

[8] An example of the use of the blockchain technology can be found in some States of the US. In Georgia, Vermont and Wyoming, for example, the local government has employed this technology to speed up and to manage the land registry. See, https://www.ncsl.org/research/financial-services-and-commerce/thefundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx. See, also, Pierluigi Matera who analyses the evolution of the use of the blockchain technology in relation to the specific sector of corporate law, 'Delaware's Dominance, Wyoming's Dare. New Challenges, Same Outcome?', (2021), 1 Cersig Research Paper <https:// ssrn.com/abstract=3763106>.

[9] Alex Biryukov and Sergei Tikhomirov, 'Deanonymization and linkability of cryptocurrency transactions based on network analysis' (2019) *European Symposium on Security and Privacy* <https://doi.org/10.1109/eurosp.2019.00022>. Francesco Rampone, 'I dati personali in ambiente blockchain tra anonimato e pseudonimato', (2018), 19 *Ciberspazio e Diritto* 457.

[10] Omri Marian, 'Are Cryptocurrencies *Super* Tax Heavens?', 112 (2013), Michigan Law Review (First Impressions) 38.

ISSN 2281-5147

3. Smart contracts: a fancy name for a complex issue tructural remarks

As briefly mentioned above, one of the most frequent applications arising from the use of technologies based on distributed ledgers, and in particular those of blockchain type, is represented by smart contracts.

As a matter of fact, the story of digital contracts dates back to 1948, when in response to the Soviet Union block of the western Germany, the USA and its allies developed a 'manifest system that could be transmitted by telex, radio-teletype or telephone' to organize the cargos sent to West Berlin[11]. Later on, in 1965, also the private sector benefited from the Berlin system and developed a new method of electronic messages (called EDI- electronic data interchange).

The EDI system continued to be used in the decades that followed mainly for transforming paper agreements and orders into digital representations. Nonetheless, EDI came with some limits, namely the fact that it restated only what was already established on the paper.

In the late 90s a computer scientist, Nick Szabo, seeing those limits, conceived a new system of executing electronic contracts. In his famous paper "Formalizing and Securing Relationships on Public Networks" he described how it would have been possible to have new computer software that resemble 'contractual clauses', and in so doing, to bound the parties 'in a way that would narrow opportunities for either party to terminate its performance obligations'. His idea started from the simple functioning of a vending machine, that he takes as a model for a 'contract with bearer' and that 'minimizes the need for trusted intermediaries'[12].

The following years other scientists developed computer-based contractual languages: it happened, for example, when Microsoft teamed up with the researchers of the University of Glasgow to study the case of computerized financial contracts, or when

[11] Frank Hayes, 'The Story so Far' (2002) <https://www.computerworld.com/article/2588199/the-story-so-far.html> cited also by Primavera De Filippi and Aaron Wright, *Blockchain and the Law* (Harvard University Press 2018), 73.

[12] Nick Szabo, 'Formalizing and Securing Relationships on Public Networks', (1997) <http://ojphi.org/ojs/index.php/fm/article/view/548/469>.

a contract readable by both machines and humans was developed in 2004 at the University of Colorado[13].

With the rise of bitcoins and the consequent growing interest in the blockchain technology, the idea described by Szabo started to become concrete. Blockchain based protocols could provide the adequate technical structure to enter into automated commercial-binding relationships, ie smart contracts.

One of the main differences with traditional legal agreements is that in the case of smart contracts the promises are memorialized in a code (not in the natural language, ie legal prose) and once started, the terms will be executed and cannot be stopped unless there is a specific program that provides for this option. This implies a great effort both by the parties and by the programmers: in some cases, third-party sources, commonly referred to as *oracles*, can be employed to adjust performance obligations during the term of an agreement. Oracles can be real persons or programs and their principal function is to respond almost in real time to the changing conditions and necessities of the parties[14]. Moreover, oracles can also be seen as an opportunity for the automatic system to communicate with the real world[15].

Since the launch of Ethereum, the first and most famous platform for running smart contracts, we have witnessed the rise of a series of different types of such agreements regarding commercial arrangements, from the transfer of digital money to the exchange of fungible or non-fungible assets in several different industries.

Upon the enthusiasm smart contracts spawned in the international arena, they raised some concerns as well[16].

[13] Primavera De Filippi and Aaron Wright, 74. Harry Surden, 'Computable Contracts', 46 (2012) *University of California -Davis Law Review* 629.

[14] M. T. Giordano, (2019) 'Il problema degli oracoli,' in Raffaele Battaglini, Marco Tullio Giordano (ed.), Blockchain e Smart Contract (Giuffrè, 2019).

[15] M. Ethan Katsh, *Law in a Digital World* (Oxford University Press, 1995); Primavera de Filippi and Aaron Wright, Blockchain and the Law, 71.

[16] For example, George Smart, 'Smart Contracts: Tools for Transactional Lawyers', (2018) 81 *Texas B. J.* 403, affirms that "There is [...] no agreed upon definition for smart contract, this creates the greatest confusion and an incomparable level of disagreement for regulators". See, also, M. Dell'Erba, (2018) 'Do Smart Contracts require a new legal framework?Regulatory fragmentation, self-regulation, public regulation', *University of Pennsylvania Journal of Law & Public Affairs* 3. For a general overview, Larry A. Di Matteo, Michael Cannarsa and

In particular, part of the existing literature has focused the attention on the basic question about their nature: can smart contracts be really considered a contract according to the legal definition commonly accepted in the legal systems? While the compatibility with the traditional categories belonging to contract law is not the specific subject of analysis in this paper, it is worth to be noted that, in general, scholars are divided between those who do not recognize any legal nature to smart contracts; those who, instead, consider them simply the digital transposition of traditional contracts, and those, finally, who prefer to focus on the concrete applications of such agreements suggesting, therefore, a functionalist approach[17].

It is not certainly the first time that contract law and technology meet[18]. This has indeed already happened with the case of telematic contracts where electronic means were used to put distant parties in contact. At that time, scholars have tried to reconcile, with different solutions, the categories traditionally belonging to contract law to the new technological instruments. In that context, notwithstanding the different levels of automation involved in the different types of contracts, the 'human factor', tough reduced, was still an essential part of the main phases of the contract.

Cristina Poncibò, *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019); Andrea Stazi, *Automazione contrattuale e contratti intelligenti. Gli smart contracts nel diritto comparato* (Giappichelli, 2019).

[17] Among the many contributions, see Riccardo De Caria, 'The Legal meaning of smart contracts', (2019) 6 *European Review of Private Law* 731; Gideon Greenspan, 'Beware of the Impossible Smart Contract', (2016) *Multichain* <https://www.multichain.com/blog/2016/04/beware-impossible-smart-contract/ >, accessed April 2022; S.D. Levi and A.B. Lipton, 'Smart Contracts and Their Potential and Inherent Limitations', (2018) <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and inherent-limitation/>, accessed April 2022, where the authors define the transactions executed by smart contracts "fairly rudimentary", so that they are considered "ancillary smart contracts". According to the authors, "we are many years away from code being able to determine more subjective legal criteria". Also, see Francesco Di Ciommo, 'Smart contracts and (Non) Law. The case of the Financial Markets', 7 (2018) II, *Law and Economics Yearly Review* 291, who believe that "smart contracts are not contracts", e "any attempt made by jurists to understand and regulate the phenomenon risks becoming obsolete at the very moment is carried out". Among the authors who suggest a functionalist approach, see Roberto Pardolesi and Antonio Davola, 10, who believe that "Considering these (still unsolved) issues, a viable solution for legal scholars could be "giving up" on qualifying smart contracts as a general topic". For a general analysis, see Marisaria Maugeri, *Smart contracts e disciplina dei contratti*, (Il Mulino, 2021).

[18] In this regard, see the extremely interesting doctrinal debate between N. Irti and E. Severino, 'Le domande del giurista e le risposte del filosofo (un dialogo su diritto e tecnica)', (2006) *Contratto e impresa* 665 and 'La Filosofia di una generazione', (2011) *Contratto e impresa* 1309; L. Mengoni, 'Diritto e tecnica', (2001) 1 in *Riv. trim. dir. e proc. civ.* See, also, in general on this issue, Giovanni Perlingeri, 'Le nuove tecnologie e il contratto', (2004), Manuale di diritto dell'informatica 17.

In the case of smart contracts, instead, the specific structure and functioning are designed to *avoid* the human action (as much as possible), as the definition given by their creator recalls. This leads to a condition of extreme uncertainty - due to the novelty and to the unfamiliarity with this new dimension - that necessarily requires a completely different approach by the scholars[19].

The main doubts regard: the area of privacy, the difficulty of adapting some particular types of agreements to the code and the potential use of smart contracts also for illegitimate purposes. While both privacy issues (in terms of the necessary protections about sensitive data disclosed on the blockchain) and the formalization of legal obligations (in terms of reconciling these new realities to the traditional legal categories known and applied) have been widely investigated, the aspect connected to the potential use of smart contracts for illegitimate goals has not received the same attention so far[20]. It is true that these aspects are strictly connected, but at the same time, as we will see, the use case involving this specific trait casts a new light on the overall picture.

In 2015 a provocative paper titled "The Ring of Gyges: using smart contracts for crime" was published by a team of researchers from Cornell University and the University of Maryland[21]. Taking the example of the mythical magical artifact described by Plato, which granted the owner the power of becoming invisible at will, the authors show how smart contracts might become the source of illicit activities taking advantage of the pseudonymity and the decentralized structure of the

[19] Francesco Di Ciommo, 'Gli Smart Contract e lo smarrimento del giurista nel mondo che cambia. Il caso dell'High Frequency Trading (HFT) finanziario', (2019), Fintech, by F. Fimman- G. Falcone, Napoli, 157.

[20] The main area of interest in the literature has been about the compatibility of smart contracts and the blockchain technology and, for example, with the European regulation, the GDPR. See, Francesco Rampone, 'I dati personali in ambiente blockchain tra anonimato e pseudonimato', 61 (2018), 19 *Ciberspazio e diritto*, 457; Ramya Ratham Kumar, Impact of Blockchain Technology on Data Protection and Privacy" 2017, available at SSRN <https://ssrn.com/abstract=3040969> accessed April 2022; M. F:#$K, "Blockchain and Data Protection in European Union", Max Planck Institute for Innovation & Competition Research Paper No. 18-01, feb. 2018.

Available at SSRN: https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3080322; S. Ramsay, 'The General Data Protection Regulation vs. the Blockchain – A legal study on the compatibility between blockchain technology and the GDPR', (2016), http://www.diva-portal.se/smash/get/diva2:1221579/FULLTEXT01.pdf (last accessed April 2022).

[21] See, Jules et al., 'The Ring of Gyges: using smart contracts for crime', (2015) <

ISSN 2281-5147

blockchain technology behind. Specifically, they refer to these activities as to ‘criminal smart contracts (CSCs)’ and divide them in three different categories: leakage/sale of secret documents, theft of private keys and a very broad class of physical-world crimes (murders, terrorism acts) that are referred to as ‘calling-card’ crimes. To get a concrete idea we can think of someone who has access to confidential information and, behind payment, will reveal the information. The smart contract expresses precisely this situation through the well-known structure ‘if-then’ and works automatically (meaning it delivers the payment) once the condition is met (meaning the final goal of obtaining the confidential information).

The same mechanism works also for crimes in the real physical world. For example, the assassination of a person could be arranged through a smart contract: subject A posts a contract for the murder and establishes a reward for the commission of the crime to a potential perpetrator P. Receiving an input from any P, the contract establishes in advance all the necessary details for the murder (date, time, place). Before P can claim his reward, the contract itself looks for authenticated data feed or news confirming the murder and, if verified, P can get the money. The example also shows how difficult it would be for the law enforcement to trace the perpetrators, due to the fact that the contract can easily provide for no further contact between the parties other than the initial input by P[22].

What it is extremely interesting and critical in the analysis presented is that the nodes simply take advantage of the architecture of the program (specifically the immutability of the blockchain and its pseudonymity) to support the exchange between them about the crime to be committed, and the consequent commensurate payment for the perpetrator. In other words, they simply use the ‘if-then’ clause and build their promises.

A few years later, Kevin Werbach, a professor of law from the University of Pennsylvania, published a book titled “After the Digital Tornado: Networks, Algorithms, Humanity” where he supports and explains the idea that blockchain

[22] Ibid., assassination CSC.

technology could wreak unintentional havoc if its characteristics are not understood fully and completely[23].

According to Werbach, smart contracts have an implicit dark side due to the immutability of the blockchain, which he considers the real weakness of these instruments. To overcome or, at least, to contain this weakness he suggests an external intervention, for example by the institutions. As a matter of fact, in his opinion, the blockchain technology should be considered, nonetheless, a governance technology: therefore, torn between the desire to guarantee freedom to its nodes, and the necessity of imposing some constraints, to maintain the system working[24].

3.1 TheDAO case: what could go wrong, (almost) went wrong

A concrete example of smart contracts used for illicit purposes is given by *TheDAO* case, a decentralized autonomous organization (DAO) created in 2016 by a team behind a German company, Slock.it.

Decentralized autonomous organizations (DAOs) consist of a set of smart contracts that do not have any owner[25]. Essentially, these organizations act on the basis of a code deployed on a blockchain and sustain themselves relying on digital currency accounts to fund their operations[26]. In general, a DAO works as follows: the programmers write the smart contracts that will run the DAO; a funding window is open and this means that during this period people add funds to the DAO buying the

[23] Kevin Werbach, *After the Digital Tornado: Networks, Algorithms, Humanity* (Cambridge University Press, 2020).

[24] Ibid., 239.

[25] See, Vitalik Buterin, 'DAOs, DACs, Das and More: An Incomplete Terminology Guide', Ethereum Blog, 6 May 2014, https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/, accessed April 2022.

[26] See, for example, the document issued by the US Securities and Exchange Commission (SEC), in 2017, that defines decentralized autonomous organizations as "virtual organizations embodied in computer code and executed on a distributed ledger technology or blockchain", Release No. 81207 / July 25, 2017.

ISSN 2281-5147

tokens[27] (digital assets that represent the organization) related to the DAO itself; finally, at the closure of the window, the DAO starts to work. At this point people participate to managing the DAO making proposals and voting to eventually approve them. People who bought in, have the right to vote.

There are different types of DAOs depending on their level of automation: it could be a simple lottery or a more sophisticated system that requires layers of smart contracts.

Usually, the protocol of the blockchain determines the overall organization of the DAO (how to distribute rewards for example) without any third-party involved. This organization is then: self-sufficient, borderless and open to any user who wants to join.

Even though the simple idea of algorithm systems governing an organization seems closer to science fiction than to reality, it is worth to remember that in 2014 a company based in Hong Kong employed an algorithm to the board of directors to help the firm with the investments[28]. Other famous CEOs, as Jack Ma, the founder of the giant Alibaba, believe that such experiment will gain much more attention in the next future[29].

Among the benefits related to DAOs we find: more certainty for the overall organization than the traditional models due to the immutability of the blockchain; more efficiency in the decision-making process in terms of speed, and also more alignment with the shareholders' interests, considering that the smart contracts would

[27] In this regard, see the definition by Riccardo De Caria who defines the process of tokenization as "un processo, collegato ma diverso, di conversione della ricchezza in *token* digitali che vengono poi emessi su piattaforme basate su una *blockchain* tramite *smart contracts*", (2020) 1 Il Diritto dell'economia 855.

[28] Primavera De Filippi and Aaron Wright, *Blockchain and the Law,* 151, note 19. See, also, Simon Sharwood, 'Software appointed to board of venture capital firm', 2014, The Register, https://www.theregister.com/2014/05/18/software_appointed_to_board_of_venture_capital_firm/, accessed April 2022.

[29] See, Sherrisse Pham, 'Jack Ma: in 30 years, the best CEO could be a robot', Technology, CNN, 2017, <https://money.cnn.com/2017/04/24/technology/alibaba-jack-ma-30-years-pain-robot-ceo/index.html>. Accessed April 2022. Also, Primavera De Filippi and Aaron Wright, 146.

be designed to serve exclusively the latter, without being at the mercy of the CEOs' will[30].

Among the side-effects we certainly find the jurisdictional issue: since the DAOs are maintained by a series of nodes located around the world, it would be indeed very hard to identify the applicable law. And even assuming some kind of legal liability, some questions arise on which law has to be applied, for example, to seize the DAO's assets, considering their digital nature[31].

Perhaps the most critical concern regards the autonomy of the DAO in terms of the execution of the code: as long as it collects funds to operate on the blockchain, the organization will keep running without paying attention if the program has negative consequences or runs illicit activities. Moreover, being the code automatically enforced by the blockchain, it would be very hard to force an intervention such as, for example, an amendment.

TheDAO affair is a perfect example of what we have just described. This particular DAO was deployed on the Ethereum blockchain and launched on April 2016. For reasons that are not clear, it became very popular and raised a lot of money (ether coins), more than expected, by the end of the funding period. Even though soon after the funding window was closed some concerns arose on potential bugs, the organization kept running. Voters (token holders) were then waiting to express their vote on the proposals. While the programmers were still working to fix the initial problems, an attack started to drain funds from the organization and transfer them in a different DAO, called by the experts, 'a child DAO'. It is estimated that the attack led to a loss of over $50 million worth of ether just in a few hours. Since no one was

[30] See, Anthony J. Bellia, 'Contracting with Electronic Agents', 50 (2001), *Emory Law Journal* 1047; Norman H. Nie and Lutz Erbring, 'Internet and Society', 3 (2000) *Stanford Institute for the Quantitative Study of Society* 14.

[31] According to Aaron Wright, the co-author of *Blockchain and the law* with Primavera De Filippi, there could be a possibility that DAOs could 'go to court': the conditio sine qua non, tough, would be first to establish the jurisdiction and secondly, in case of a US one, to have a cause of action to bring it to court. In this case, DAOs could be indeed considered some sort of implied partnerships. Nevertheless, Wright thinks that it would be less likely to see any case in front of a judge, at least not in the next future. See his interview available at https://unchainedpodcast.com/can-a-dao-go-to-court-according-to-two-dao-legal-experts-probably/. Last accessed on April 2022.

in control, there was not any possibility to fix the code and, therefore, the smart contract (even defective) still continue to run.

After a complicated deliberation by the majority of the nodes, the organization eventually agreed on intervening directly on the blockchain (through what is called the practice of forking)[32]. This is an extreme solution since it implies, basically, to 'rewrite' the history of the transactions (forcing the immutability) to change the protocol and retrieve the funds. In this way, there was a 'new' version of the blockchain where the hack has never occurred[33]. Moreover, this intervention allowed to 'freeze' the assets, so that the attacker could not physically withdraw any ether from the funds.

Needless to say, the decision 'to fork' has raised more than one concern among the users. Some believed this action was completely contrary to the founding principles of the blockchain; others, instead, fully agreed with this decision considering it still an expression of the will of the nodes[34]. Also, it should be noted that some nodes simply pointed out that the alleged 'hacker' could not in fact be considered as such. As a matter of fact, as mentioned earlier, this person just took advantage of some bugs in the system for his own interests but did not commit any prohibited action according to the code[35]. Given the fact that this case has never been brought to court, it is extremely complicated to predict how a judge would have decided it.

[32] See, Cristina Poncibò, *Il diritto comparato e la blockchain* (Edizioni Scientifiche Italiane, 2020), 62.

[33] See, Quinn DuPoint, *Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance* (Routledge, 2017).

[34] See, Robbie Morrison, Natasha C. H. L. Mazey and Stephen C. Wingreen, 'The DAO Controversy: The Case for a New Species of Corporate Governance?', 3 (2020) *Frontiers in blockchain* 1. Regarding the different positions of the nodes concerning the decision 'to fork', see Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., ... & Laskowski, M., 'Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack' (2019) 21 Journal of Cases on Information Technology (JCIT) 1 19.

[35] On this consideration, see Ibid., 7, where the authors report that "At worst, the hack was a perfectly valid but unethical maneuver, at best it was not even unethical. Many would still argue that The DAO's solution to the problem was the only unethical behavior in evidence".

ISSN 2281-5147

4. Is there still hope? The 'law by design' approach. Conclusive remarks.

This overview showed that it is credible that smart contracts might be deployed for running illicit agreements as well as that their applications could lead to distorted consequences. In this respect, we can certainly affirm that these are aspects that fall within the ‘dark sides’ or, at least, the ‘grey area’. Against this background, tough, it is the system itself that suggests that a solution is possible[36]. Primarily, it should be noted that any thoughts on the matter is strictly connected to the technology smart contracts are most likely to run on, that is the blockchain.

As we have described above, this particular type of distributed ledger technology is characterized by distinctive yet challenging features that can be reasonably defined disruptive. Not only do they differ radically from the traditional known data systems regarding the technical aspects of the code-execution (decentralization, immutability, pseudonymity) but, more generally, they are designed to avoid any kind of human intervention such as in the specific case of the smart contracts. “Code is law” would seem to be indeed the perfect motto[37].

TheDAO affair has proven, however, that this is not always exactly the case: in the face of an event, even if exceptional, in fact, the system has been stopped, forced and modified and, more important, 'human' actors were the ones who decided to intervene. This happened and allegedly could happen again since, as it has been noted, “no blockchain is an island” and many factors contribute to this ecosystem[38]. Among

[36] In this respect, see the definition of DLT by Primavera De Filippi, who compares DLTs to plantoids, artificial protolife forms conceived and realized for the first time by a research team at IIT (a lab based in Italy, Ponetedera). See, LiftLab, Geneva, 11 February 2016.

[37] Lawrence Lessig, *Code and other laws of cyberspace* (New York, 1999). The work is considered a sort of 'manifesto' on the role of information technology in society and on the complex relationship between law and technology. See, also, Samer Hassan and Primavera De Filippi, ‘The Expansion of Algorithmic Governance: From Code is Law to Law is Code’, (2017) 17 *Field Actions Science Reports* 88.

[38] See Primavera De Filippi, https://www.coindesk.com/markets/2018/02/28/no-blockchain-is-an-island/, (2018), last accessed on April 2022.

them, we find law, social norms, market, as well as the technical infrastructure, that is the code[39].

Under this perspective, then, any attempt aimed at removing or, worse, denying these 'dark sides' would seem pointless, mostly given the widespread use of smart contracts, as mentioned at the beginning, in many areas of interest.

A more adequate approach, then, seems the one which acknowledges the possibility of these drawbacks as part of the structure of the technology and, at the same time, tries to limit and model this structure towards a more sustainable architecture. In so doing, the outcome (that is the direct application of the technology, ie the smart contract) should not be a CSC or, worse, a 'calling card' crime anymore. A valid help in this direction comes, therefore, from an innovative and quite recent approach that has received some attention in the literature in the very last years: the legal design.

This new way of approaching the legal issues is based on the idea that through a human-centered vision to the challenges of the legal system, the latter can be improved.

As a matter of fact, as declared in the manifesto published by the Legal Design Alliance in 2018, legal design is a growing movement to make the legal system work better for people[40]. Moreover, according to Margaret Hagan, the pioneer of the legal design and actual director of the Stanford legal design lab, a design-driven approach is what is needed to face legal innovation in a sustainable way. In other words, a way to bring together the world of law and the world of innovation (especially technological innovation) and prevent them from remaining two separate and conflicting fields[41]. Critical for succeeding is the interdisciplinarity intersection among the designers (lawyers, computer scientists, engineers, designers …).

In practice, the legal design approach works as a process: it identifies the challenge area and the status quo through an 'on-site' action, moves through synthesizing a

[39] Lawrence Lessig, *Code and other laws of cyberspace*. See, also, Cristina Poncibò, *Il diritto comparato e la blockchain,* 37, who recalls Lessig's theory and talks about 'formanti della blockchain' referring specifically to law, social norms, market and architecture.

[40] See, Legal Design Alliance, '"he Legal Design Manifesto' (2018), <https:// www.legaldesignalliance.org/> .

[41] See, Margaret Hagan, Law by design < https://lawbydesign.co>, accessed April 2022.

ISSN 2281-5147

specific user or group of users, ends up with prototypes which consist of pilots and scaled implementations. In this respect, for example, the Stanford design lab teamed up for a project work aimed at building new tools to help foreign students navigating the U.S. legal system[42]: first they studied the state of the art, and this activity implied knowing all the issues that these students were facing. They did that through interviews and data collection. Then, through multidisciplinary groups, they reunited their ideas and drafted a series of projects, and finally presented them though the testing phase to the final users, who gave them constant feedbacks. The successful projects were ultimately implemented and coded for use by the computer scientists (through prototypes).

The Stanford lab works in many other projects such as, for example, LIST (Legal Issues Taxonomy) which is a user-centered system on the legal problems that people might have in the U.S., or the eviction legal help platform, that covers renters' rights and protections during the Covid 19 pandemic, as well as many others[43]. These examples are valuable since they show how the legal-design approach is indeed a use-case based approach aimed at giving practical solutions, not limited to abstract speculation.

The key words related to this approach are indeed: process - that recalls a dynamic conception of law as an experience - interdisciplinary perspective and a user-centered perspective - that refer respectively to the necessity of receiving inputs from other areas of expertise, especially in this new digital reality, and the importance of focusing on the user's needs and not on the developer's ones.

Interestingly, if we look closely, these are key concepts that can also be referred to the context we have presented and analyzed above. New technologies, such as the blockchain, indeed relate to a natural dynamic, although complex, legal framework

[42] This was the Immigration workshop projects, ran by Margaret Hagan. She illustrated this project in 2014 in New York, during the conference 'Reinventing law'.

[43] See, https://www.legaltechdesign.com/our-projects/. The *eviction legal help* project consists of a national network of housing law experts to be able to present, in plain language, if renters could be evicted, how much time they had to pay rent, and what new protections they might have in court. It also has a national database of local legal aid groups, court self-help sites, emergency rental programs, and other services that we could connect renters to in each state. In particular, technological innovations are investigated and used to build new regulations and models to be used in the future. *Learned Hands* is another design project, a machine learning project to use interactive games to build tools that can automatically spot people's legal issues.

(specifically in terms of compatibility with the traditional categories and in terms of facing completely new issues). Similarly, the character of interdisciplinary distinguishes this particular technology where it requires an evident synergy at least between the legal expert on the one hand, and the computer scientist on the other. Finally, and this is the challenging profile, as *TheDAO* affair has widely shown, the 'human' intervention, within the meaning of the user's will, is fundamental even in a technology that is the means of subsequent self-executions, as in the case of smart contracts.

In this respect, it is worth pointing out that technology can very well be built and designed to respond adequately and efficiently to the needs of those who use it.

This means, therefore, that in the specific case of the blockchain, and consequently the deployment of smart contracts, the architecture (that is the code) should be written so to avoid illicit 'if-then' structures or questionable operations on the chain. It may be argued that this is only a matter for computer technicians', i.e. those who "write" the code. While the material act of writing the code certainly pertains to the competent professionals, it is worth to remember that the blockchain technology is the object of attention nowadays by the entire international community.

Not only, in fact, the individual states have moved towards regulating, at different levels, blockchain and DLTs in general, but the European Union, as well as some of the most important international actors, such as UNICEF, have embraced and implemented the idea of a blockchain *designed* to respond to specific purposes[44].

Among the benefits of adopting such an approach, there is also the fact that it would put the users in a more conscious role, than just simple passive consumers of

[44] The European Union has been particularly active concerning the study and the measures to supoport the investigations around the blockchain technology. See the initiatives promoted by the Commission in order to better undertand this new phenomenon. See, https://www.eublockchainforum.eu. More generally, the E.U. has been active regarding the study of cryptocurrency as well as the digital market with the recent proposed directive on the matter (Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive", (EU) 2019/1937, COM/2020/593 final (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0593&from=EN). See the projects run by UNICEF about a conscious use of the blockchain technoklogy and its applications (smart contracts). Some of them: the Digicus project, where UNICEF is studying how the blockchain can be used to increase efficiency and transparency in the payments between the agency and its partners (https://www.unicef.org/innovation/blockchain/digicus); Project Connect that aims at providing real-time data assessing the quality of each school's internet connectivity (https://projectconnect.unicef.org/map).

ISSN 2281-5147

technology, since they could participate actively to the testing and prototype phase[45]. This would also not betray the idea at the basis of the blockchain technology itself, which is to be a disintermediated and not centralized one, with no intermediaries and able to build direct relationships among the participants.

A final observation should be made regarding the area of application of the legal design. It could be argued, in fact, that this is an approach exclusively aimed at the regulatory process and, therefore, reserved for policy issues. Although it is undeniable that this approach involves the choices made by the legislators in terms of policies, it should be emphasized that the field of private relationships also represents – specifically in the field of contract law - a suitable framework for the application of the legal design approach. The intrinsic flexibility of this approach proves to be particularly adequate to enhance the autonomy of the parties[46].

While the law by design approach may not be the *panacea* for solving the undoubtful issues related to smart contracts, its focus on the interaction between the law and the users' actual needs can help to facilitate the process of bringing technological innovation and law closer, in a more conscious and legitimate way.

[45] See, Matthew J. Koehler and Punya Mishra, Teachers Learning Technology by Design, (2005) https://www.researchgate.net/publication/240273300_Teachers_Learning_Technology_by_Design/link/00b49530 38a5a3b2ef000000/download. Margaret Hagan 2016. 'The User Experience of the Internet as a Legal Help Service : Defining Standards for the next Generation of User-Friendly Online Legal Services' 20 *Va. JL & Tech.* (2)395.

[46] In this regard, see the project run by Margaret Hagan, still on going, that studies how to improve people's health insurance contracts through the legal design approach and the use of computable contracts. See, https://medium.com/legal-design-and-innovation/there-has-to-be-a-better-way-than-this-ee2ab7df80b8.

ISSN 2281-5147