THE POLITICS OF BLOCKCHAIN

EMANUELE MARTINELLI

INTRODUCTION

At the end of 2008, an unknown by the pseudonym of Satoshi Nakamoto proposed a technological innovation that could lead us to a revolution in the way we relate to each other in society. His main goal was to employ the last advancements of computer science in a new kind of money, in order to trade goods and services freely; thanks to many other great authors – Vitalik Buterin, Eric Hughes, Cody Wilson, among others – we began to see the opportunity to stretch the applications of this system toward limits we are still hardly able to draw today.

The common essence of these innovations is one and only, and precisely pointed out by the author: rebuilding the fundamental interactions between people so that trust will be unnecessary and power banished. On the most basic level, blockchain is a web of individuals connected to each other to plan their actions and agreements without the need of any intermediary or arbiter.

Through praises and controversies, successes and bans, one thing is certain: critiques about the *modus operandi* of the traditional mechanisms within society are getting closer and closer. Such big news will surely open fundamental questions on our principles of justice and political systems, as well as on the options that blockchain's applications will open for the public sector.

This paper will start with a brief[1] explanation of how blockchain works in general. This will gather all the elements that are necessary to rethink the practices and dynamics of social life. We will attempt to give some sense to the words Nakamoto used to describe his creation: «a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions»[2].

After that, the paper will examine the implications of this powerful innovation from a more abstract point of view. We will also focus on the roots of this technology in the words and works of the *cypherpunk* movement, that arguably gave birth to the core ideas of the project.

Finally, a special attention will be payed to blockchain's political uses – which probably give rise to the most complex issues. Different opinions on the role of authority in the peer-to-peer environment of a *digital community* will be dealt with, after a brief introduction to their typical features and dynamics.

[1] - For a more complete understanding of how blockchain works: cfr. Satoshi NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin Foundation, 2008.

[2] - NAKAMOTO, *ibidem*, p.1.

HOW BLOCKCHAIN WORKS

1.1 *OPEN SOURCE PEER-TO-PEER SOFTWARE*

Blockchain is supported by online and open source platform where participants can send and trade any kind of data, in such a way that counterfeiting, fraud and theft are *mathematically* impossible. In order to do so, particular cryptographic techniques are deployed to recreate self-securing *peer-to-peer* environments, in which no central server or entity is necessary to keep track of transactions. The nodes are thus required to solve some specific algorithms to unlock their exchanges of information. This implies that transfers have to be acknowledged and accepted by all terminals connected to the web.

Nakamoto's aim was to extend to any kind of social relation the freedom of interaction that is characteristic to peer-to-peer architectures. Just as no server has to fuel/operate transactions, blockchain technology tries to enable people to, say, exchange digital money with no banks involved, claim property rights with no notary involved, enforce laws, rules or contracts with no authority involved.

Any transfer is assigned a *digital signature*, consisting of its time, date, receiver's address and sender's address, and a unique *transaction identifier* (*txid*); the system only executes those transactions whose digital signature has been reconstructed through certain decryption algorithms. The txid, in particular, is a string of alphanumerical code that has been encrypted several times through a function named *hash*. This procedure, enabling the software to unveil the cryptographic keys of the digital signature thanks to a numerous series of operations, is called *proof-of-work*, and it is what in fact allows a new transaction to be authorized and take place.

Nakamoto's desired goal should appear clear by now: empowering peer-to-peer technology and its decentralization through cryptographical techniques, able to make controls and supervision by central entities unnecessary. Nowadays, organizations that are too individualistic, where people are totally independent from external influences for their business, are penalized by the fact that any private agreement might be violated or manipulated. It has always been indispensable to reintroduce some sort of institution, an authority with the privilege and task to establish the official registry of all transactions happening in the net. This has been the only way to objectively settle the criteria to distinguish between licit and illicit operations.

Let's take an example: we are free to perform payments with our credit card in total autonomy. However, transactions have to be signed by our bank, in order to avoid theft or fraud. Because of this, the whole system relies on the trust we have on the institution, its benevolence and its solidity. Speaking of IT, server/client architectures always show an analogous weakness, a so-called *single point of failure*: if the provider is corrupted, bugged or malfunctioning, the nodes of the web cannot use the service anymore.

The human and therefore fallible component of social relations is replaced by mathematical processes. There is a general registry of transactions, but it is not managed by any server: the software itself has the custody of a *public ledger* that is locally downloaded on every terminal and updated in real time. Only those exchanges whose digital signatures have been correctly decrypted through their proofs-of-work, and can therefore be enlisted.

This allows blockchain to have an absolute transparency, more than ever in traditional social organizations with centralized ledgers. Any data package can be tracked, transfer by transfer, back to its origin, for anyone to see. Secondly, there is no way that the public ledger can get rigged, falsified, hidden, or that unlisted transactions can be executed – because, literally, no one is writing exchanges. Modifications in the system have to follow specific algorithms, all happen in the same time, and even software developers cannot do anything about the operations of the protocol.

1.2 The Double Spending Problem and Nakamoto's Answer

The particular cryptographical techniques of the proof-of-work are such that, for any terminal connected to the web, possessing the correct and most updated version of the public ledger becomes a necessary condition for performing new transactions. All the features that make these characteristics possible were already there when Nakamoto published his white paper. His truly new innovation was the solution he proposed with his technology to the so-called *double spending problem*.

In fact, nothing excludes that two different addresses, up to now, may claim the same data package at the same time. How can we objectively determine which one shall be executed? This uncertainty is a big flaw in peer-to-peer systems, leading to the need of central servers and controls: a malicious user might at all times falsify a transfer in the net and catch some data that was not entitled to him just by requesting it more or less simultaneously as the rightful owner. With no other criteria at work, that amount could be given to any of the two.

The solution is to deploy a kind of proof-of-work such that only *one* specific transaction is the one that necessarily builds the new entry in the public ledger. The protocol proposed by Nakamoto is called *hashcash* and was patented by Adam Back in 1997[3]. Briefly put, the core idea of this system is that txid are not calculated in a totally random way, but are elaborated in such a way that each one contains fragments of the digital signatures of preceding transactions. By doing so, a hypothetical thief or hacker has to have not only the computing power that is necessary to duplicate the digital signature of the transfer he wants to deviate, but enough power to falsify the hash of every single transaction in the public ledger, from start to finish – in the same time during which all other participants on the platform conjunctively work on one single new entry.

[3] - Cfr. http://www.hashcash.org/papers/announce.txt.

PREMISES AND IMPLICATIONS

2.1 BLOCKCHAIN'S ROOTS: FROM CYPHERPUNK TO CRYPTOANARCHISM

Nakamoto's white paper was first posted on the *cypherpunk*'s mailing list, and this fact is very useful in order to grasp the aims and purposes blockchain was formulated for. Cypherpunk (a pun from the word *cipher* and the *cyberpunk* literary genre) is an informal association, born in 1992, trying to elaborate digital tools to enhance private relations with privacy and total autonomy[4]. The movement's origins reach back to the occasional meetings between Eric Hughes (mathematician and author of the *Cypherpunk's Manifesto*), Timothy May, John Gilmore and other twenty friends; those eventually evolved into a periodical mailing list, where many of those preparatory devices listed in chapter 1 appeared for the first time. These include Adam Back's hashcash, Wei Dai's B-Money[5], along with a first cryptocurrency prototype, Nick Szabo's Bitgold, and the famous case of Julian Assange's WikiLeaks.

The huge opportunities opened by internet and IT in general, notoriously came together with enhanced possibilities for powerful people to enforce controls, censorship and manipulations on online relations. This movement has the ambition to use cryptography to get rid of these weaknesses of the digital world, without having to give up on the great gains in terms of personal liberty and mobility. Such essence is well represented from the first lines of Hughes's 1993 manifesto[6]: «privacy is necessary for an open society in the electronic age. […] Privacy is the power to selectively reveal oneself to the world. […] When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must *always* reveal myself. Therefore, privacy in an open society requires anonymous transaction systems.» It is now clear that blockchain is nothing but the last step of this process.

The movement's social claims, from many of its members, did in fact assume an obvious political perspective. In his iconic *A Declaration of the Independence of Cyberspace*, John Perry Barlow utters the ambition to recreate a proper social environment outside of the physical world, were traditional state authorities limit our freedom of interaction: online cryptographical techniques must constitute a brand-new way to live in society, just in another

[4] - Cfr. PETRIB, *The Untold History of Bitcoin: Enter the Cypherpunks*, 2018, https://medium.com/swlh/the-untold-history-of-bitcoin-enter-the-cypherpunks-f764dee962a1.

[5] - Both mentioned in NAKAMOTO, *ibidem*.

[6] - Eric HUGHES, *A Cypherpunk's Manifesto*, 1993, https://www.activism.net/cypherpunk/manifesto.html.

dimension. «The dreams of Jefferson, Washington, Mill, Madison, Tocqueville e Brandeis […] must now be born anew in us.»[7]

So, although the mere application of the blockchain technology into politics does not seem to have political implications per se, who in fact contributed to its invention and is currently working to make it better is pacing fast in the direction of specific political theories. A single sentence in Hughes's manifesto suggests something of this kind: «cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act»[8]. One may say, to sum up, that this technology was born as a tool to fulfill initially anarchical dreams: the final goal is «freedom from external coercion»[9] in general.

This being said, Timothy May[10] or Cody Wilson explicitly refer to libertarianism and anarcho-capitalism. They believe external restrictions on private transactions are inacceptable as a matter of principle, and that political coercion is a violation of individual rights. This can be held only assuming anybody has a natural sovereignty over himself (in this particular case, over his digital identity), over his actions and his estates (including confidential information about himself). This interpretation of justice and social life is deeply rooted in John Locke and all those thinkers referring to themselves as classical liberals.

As a matter of fact, the forms of digital communities open to possibilities that have always been precluded to anarcho-capitalists until now. This could end all of the malfunctioning within societies due to toxic supervision by external agents: corruption, power-driven decisions, inefficiency due to the application of general schemes to particular situations, human error, lack of economic incentives for legislators. And, as a result, such projects seem to be *less directly* adaptable to those political theories according to which some authority is necessary in order to keep economic stability and/or justice in a community[11]. The standard view followed by our governments is that a completely free market would be subject to cyclical overproduction crisis, which can be only healed through regulation, for examples. These restrictions – being monetary, on trades or paternalistic – are greatly discouraged by the blockchain architecture.

---

[7] - John Perry BARLOW, *A Declaration of the Independence of Cyberspace*, in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, Peter LUDLOW (ed.), MIT Press, 2001, p.2.

[8] - HUGHES, *ibidem*.

[9] - Timothy C. MAY, *Crypto Anarchy and Virtual Communities*, in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, Peter LUDLOW (ed.), MIT Press, 2001, p.69.
Where *external* means involuntarily forced on us.

[10] - Cfr. Timothy C. MAY, *The Crypto Anarchist Manifesto*, in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, Peter LUDLOW (ed.), MIT Press, 2001.

[11] - Cfr. WRIGHT, Aaron, DE FILIPPI, Primavera, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN Electronic Journal, 2015.

The idea under which people can fulfill their goals completely only within the free dynamics of interactions between self-oriented individuals probably presupposes a subjective theory of value: the economic value does not stay in the traded objects as it were a property of them, but it is a psychological projection of personal and thus unpredictable desires of the subject on reality. The best market organization is that where any control on individual pursue of value has been eradicated from private relations, so where there is no political regulation at all. This theory of value has the virtue of explaining how a voluntary agreement between men is even possible, that is if and only if one considers the other's good more valuable than his and vice versa, thanks to their different perspectives on life and the world in general. Plus, this view can directly settle the curious case of trading strings of code on their mere digital scarcity.

All this makes the prices of encrypted data only susceptible to supply and demand on the market. So to speak, the preciousness of information derives from the interest of the potential buyer in it. Nothing guarantees its purchasing power right from the start, nor they can have any value in use. This brings us to a third consideration from the Austrian School of Economics and related political theories: the analysis of a market context is always based on a series of concrete, limited and well-defined agents, which are all influenced by the real conditions they are working under. Therefore, any general and mathematical standard model applied to the prices on a blockchain network can only supply qualitative predictions. Moreover, it is necessarily static and thus excludes innovation and surprise, having to forget a great component of entrepreneurial action: creativity.

Finally, the definition of a property right, as implied by smart property applications of blockchain, must embrace a theory of property as a *bundle of rights*[12]. Being the owner of something means to be entitled to execute actions whose object is that thing. There are two major consequences of this view: 1) each individual naturally has a right to own his private property, with no authority of intermediary needed to certify so, 2) the management of property can be described as a series of contracts that define one's titles. Smart properties are in fact compositions of smart contracts, that are furthermore fractionable into smaller individual agreements for potentially different title holders[13].

---

12 - Cfr. Wesley HOHFELD, *Some Fundamental Legal Conceptions as Applied in Legal Reasoning*, Yale Law Journal, 1913.
Cfr. WRIGHT, *ibidem*.

13 - These considerations open deeper philosophical questions, such as the grounding of private property in general. The classical Lockean justification, *original appropriation*, according to which an individual owns an object because, ultimately, he applied some of his faculties to some natural entity through his work, is difficult to adapt to *mining* processes and blockchain in general. An analysis of this yet interesting problem is beyond the scope of this paper; however, a solution that may be of great help can be found in Douglas RASMUSSEN, Douglas DEN

2.2 OVERCOMING TRUST

Blockchain technology can be described as what will enable us to pass from *trust-based* interaction patterns to *trust-free* ones[14]. Any relation between individuals, founded on some sort of contract, has always implied that both parties relied on trust for their goal to be achieved – trust toward the other party himself or some intermediary. It has always in fact been necessary to believe that all the people involved is interested in the correct fulfillment of the operation.

This is true in many different everyday cases. The way that most orders and organizations, both spontaneous and constructed, are thought of today implies no transaction can be realized based on the parties' consent only. Let's take a notable example. The customer going to the bank office to withdraw some money can be certain to get what he is asking for as far as he *trusts* the credit institution. He has to believe that it will be able to afford the transaction and that it will in fact want to do it (to preserve the relationship with the client himself, to avoid sanctions, to keep a good reputation…). In reverse, the bank will go into business with someone only if he manages to show the solidity of his assets, in order to prove the credit institution could profit from him. Any contractual relation today entails trust, just in the same way, in order for the contractors to respect the agreed conditions. It is always possible that one party break the pact, although there are great deterrents for this: juridical as well as social sanctions[15].

In all these situations, trust can be betrayed. Traditional systems are only *reasonably* safe, since any transaction ultimately depends on some imponderable conditions, such as a perfectly transparent representation of other people's interests, that their behavior will be perfectly rational, that any third party will want to act to my advantage and be able to do so. The solidity of social relations relies on the reasons we have to believe our goals will be achieved – just *approximating* the necessity that characterizes natural laws.

Blockchain will enable us to rethink this fundamental component of social relations, which has understandably been taken as the norm until now. The completion of blockchain transactions does not literally rely on anyone: this technology «can be compared with an unstaffed,

---

UYL, *Norms of Liberty: A Perfectionist Basis for Non-Perfectionist Politics*, Penn State University Press, 2015, pp.93-108.

[14] - Cfr. Roman BECK, Jacob STENUM CZEPLUCH, Nikolaj LOLLIKE, Simon MALONE, *Blockchain, The Gateway to Trust-Free Cryptographic Transactions*, Twenty-Fourth European Conference on Information Systems (ECIS), 2016.

[15] - Speaking of social sanctions, reputation mechanisms play a huge role in what is called *re-iterated games* in game theory. Cfr. Robert AXELROD, *Giochi di reciprocità: l'insorgenza della cooperazione*, R. PETRILLO (Trad.), Feltrinelli, 1985.

automatically navigating vessel or a driverless steering car, bringing safely passengers from A to B, completely controlled by a cryptographic protocol that is minimizing any malicious and accidental exceptions because no humans are involved»[16]. Anytime the sender and the receiver have agreed on some exchange and submitted their request to the system, they automatically get the mathematical certainty that it will be perfectly fulfilled. It is like the involved data were handed over to the code itself, so that the completion of the transfer stops being matter of human will and turns to be matter of immediately enforced algorithms. Whenever a transaction is bound to be inserted in the public ledger, no one will ever be able to modify or abort it: only one plausible output could follow the pre-set input chosen by the users, and this process is unknowingly operated by random miners on the web.

The formation of trust-free environments is the biggest difference from *sharing economy* platforms, although they partly share the same goals and principles with blockchain technology. Services as TripAdvidor, Uber, AirBnB, etc., are thought to create protected environments where individuals can sign free transactions in an independent and decentralized way, with no need for third intermediaries. On the other hand, they are *founded* upon trust between users[17]. AirBnB, for instance, supports direct interactions between people searching for accommodation and people offering it. Prices and conditions are freely set: there can be no external influence, let alone the general terms of use of the mother company (which are freely pre-set, anyway). Similarly, blockchain allows people to engage into relations on the sole basis of their mutual consent, without the need of any agencies executing them; the main difference here is that the sharing economy works *on the basis* of trust, from the user to those who wrote reviews on purchased services, as well as between users themselves.
This is the difference that, according to some[18], makes blockchain relations socially toxic: eliminating the need for intermediaries should be possible only whenever this does not endanger the trust bond between interacting individuals. Otherwise, we would fall into all those perils of an anti-social environment, where the other person is no more regarded as essential to one's goals. In such systems with too much of a high individual autonomy, one might argue,

16 - BECK, *ibidem*, p.2.
17 - Still not between users and intermediaries, for obvious reasons. The distinctions between different kinds of trust in social relations would be very interesting to deepen but would bring us too far from our point. Cfr. Sirkaa JARVENPAA, Robin TEIGLAND, *Trust in Digital Environments: From the Sharing Economy to Decentralized Autonomous Organizations*, 50th Hawaii International Confenence on System Sciences, 2017.
18 - Cfr. Charles STROSS, *Why I Want Bitcoin to Die in a Fire*, 2013, www.antipope.org/charlie/blog-static/2013/12/why-i-want-bitcoin-to-die-in-a.html.

the real connection only happens with the technological device, whereas the presence of another fellow human being becomes contingent. Starting from this point, all possible arguments are similar to Zygmunt Bauman's[19]: paradoxically, annihilating the importance of the other tends to annihilate the fundamentality of the self, at the same time.

Perhaps, though, getting rid of trust within social organization does not mean to reconfigure human relationships per se but simply is opportunity to solve a difficulty that has always (falsely) appeared to be intrinsic to them: the incompleteness of information suffered from the parties. Blockchain does not only recreate decentralized environments where there cannot be any influence from third entities, but it also requires all participants to supply their true intentions and assets. The presence of the other does not become obsolete: its characteristics are transformed, and its weaknesses are healed.

Moreover, making exchanges easier through new and totally reliable instruments will probably have the effect to enhance and encourage social relations. The number of interactions will grow, between people from every part of the world, just with a click from home and with no risks linked to geographical contingencies. It will be the culmination of that process of mutual integration started with globalization and, before that, the internationalization of markets. If men are social animals, maybe allowing people to seek their own goals and helping others pursuing theirs is the way to put aside toxic differences between individuals[20].

---

[19] - Cfr. Zygmunt BAUMAN, *Modernità liquida*, Sergio MINUCCI (trad.), Laterza, 1999.

[20] - The essence of these words is the same of the famous excerpt by Voltaire on the London Stock Exchange: «go into the London Stock Exchange – a more respectable place than many a court – and you will see representatives from all nations gathered together for the utility of men. Here Jew, Mohammedan and Christian deal with each other as though they were all of the same faith, and only apply the word infidel to people who go bankrupt. Here the Presbyterian trusts the Anabaptist and the Anglican accepts a promise from the Quaker. On leaving these peaceful and free assemblies some go to the Synagogue and others for a drink, this one goes to be baptized in a great bath in the name of Father, Son and Holy Ghost, that one has his son's foreskin cut and has some Hebrew words he doesn't understand mumbled over the child, others go to heir church and await the inspiration of God with their hats on, and everybody is happy.» (VOLTAIRE, *Letters on England*. Leonard TANCOCK (trad.), Penguin Books, 1980, pp.40-41.)

THE POLITICS OF BLOCKCHAIN: QUESTIONS AND IDEAS

3.1 VARIOUS FORMS OF DIGITAL COMMUNITIES

Some of blockchain's most important and elaborated applications certainly are so-called *Decentralized Autonomous Organizations* (*DAO*s): societies where members can freely join or quit anytime, uploading resources and claiming rights toward the institution of common rules and goals. Many questions arise from this concept, if we keep in mind the original purpose of Nakamoto: creating telematic relations with no third intermediary. From a political perspective, this could mean the concrete appearance of communities without any form of government – or, at least, any human form of government.

This idea was first introduced in the Ethereum white paper[21], in terms of smart contracts[22]. A DAO is nothing more than a series of smart contracts to which all participants choose to refer, locking some of their resources and letting the code enforce the rules they have collectively formulated. These organizations can be programmed to spend common funds, modify their own algorithms (i.e. intervention patterns), claim rights, activate machines and devices, enhance/restrict the abilities of some members' accounts[23], let in/kick out some members; the input would be the fulfillment of some pre-set conditions, probably with the aid of IoT applications.

Digital communities work exactly in the same way, but allow their members to execute the typical mansions of a government, even though with no possibility of abuse and/or human error. There are still big differences with traditional political communities: 1) any node in the network can constantly choose whether to take part in the organization or not, 2) the enforcement of rules does not entail any form of violence, neither among individuals nor by some central authority, and 3) are *immediately* applied. As a consequence, even these kinds of decisions are made trust-free for the first time in history: there is no more need to legitimate some political power to act in order to guarantee transactions within society, because no

---

21 - Cfr. Vitalik BUTERIN, *Ethereum White Paper, A Next Generation Smart Contract & Decentralized Application*, Ethereum Foundation, 2014.

22 - Smart contracts are further applications of the blockchain technology, where, briefly put, users can configure an interface through which specific operations are automatically performed as soon as pre-set conditions are met. Just like self-enforcing contractual rules.
Cfr. SZABO, Nick, *Smart Contracts*, 1994, www.for.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.
Cfr. BUTERIN, *ibidem*.

23 - That is, to change what is called *user's privileges* in IT, his possibility to manipulate files (in this particular case, the source code of smart contracts) or to view them in *read only* mode.

coercion in necessary to do so anymore. Finally, the system provides a complete transparence and thus public decisions perfectly match public interventions, since any established process can be expressed only through the inscription on the public ledger, which corresponds to its immediate realization.

DAOs' effort is to make everyday management and affairs totally free and personalized. The goal is to give back to people the sovereignty on what belongs to them, thanks to the last advancements in the fields of modern media. In the era of men, vehicles and information freely circulating in no time around the world, a centralized administration of goods and services is getting not only questionable, but obsolete too. This trend has been shown in the past years within our modern democratic systems, since «Facebook, Twitter and other social media platforms have become by proxy the main interfaces citizens use to influence everyday politics»[24].

The mere existence of DAOs lets us look forward to the possibility of a political order with no governmental entities, a *crypto-nation* where everyone could manage all the social aspects of his life choosing from a variety of blockchain software with the same purpose. This is even nowadays what seems to be at some extent an undisclosed desire of people on the internet around the world: «*likes* and *retweets* are a form of "voting" but are not optimal. There is no scarcity of *likes* and therefore no real value beyond signalling,»[25]. Nakamoto's technology could finally give us the practical tools to encourage this modern tendency to place many international agents on the scene alongside national states: multinational corporations, influent billionaires, supranational entities, major NGOs, mass movements, online organizations[26]…

Blockchain may be the political answer to the crisis of the modern state, begun along with globalization. Its features seem to predict the completion of the slow shift from centralized governance of society into *distributed*, i.e. *absolutely* decentralized, forms of administration. Many tasks that have always be considered only possible to fulfill in the hands of central authorities according to many theories of justice, are currently being showed as manageable from a totally individualistic perspective[27].

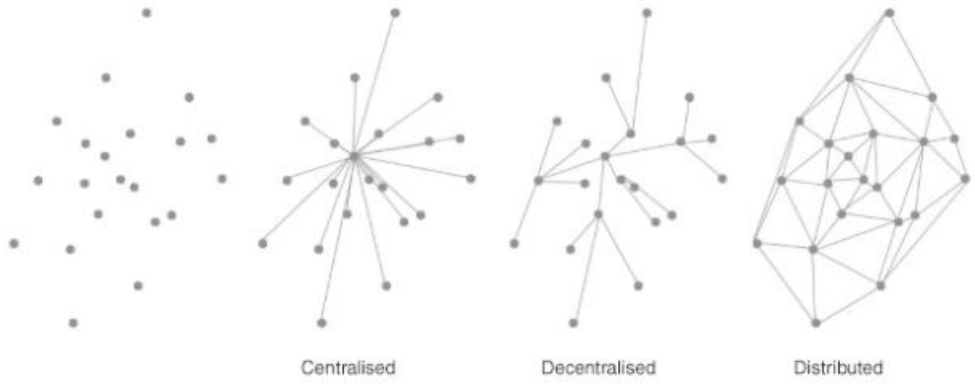
---

[24] - DEMOCRACY EARTH FOUNDATION, *The Social Smart Contract*, 2014, https://github.com/DemocracyEarth/paper.

[25] - Agnieszka ZIMOLAG, *Designing the UX of Distributed Governance*, 2011, https://words.democracy.earth/designing-the-ux-of-distributed-governance-71ce24fcafe5.

[26] - Cfr. Marcella ATZORI, *Blockchain Technologu and Decentralized Governance: Is the State Still Necessary?*, SSRN Electronic Journal, 2015.

[27] - Image taken by Susanne TARKOWSKI TEMPELHOF, *Bitnation Whitepaper*, 2015, https://tse.bitnation.co/documents/.



In a DAOs, law is replaced with digital contractual relations. People's faculty to interact with established rules and to try to modify them in accordance with others is made obsolete by the new possibility to directly change society through the manipulation of a smart contract's source code. Sanctions and coercion in general, as mentioned above, is generally substituted by the automatic and mathematical execution of transactions between users. Apparently, this is how any action that is reducible to algorithmic relations (*if x happens, then y happens*) regarding registered data can be organized with no third parties, as a matter of principle.

In reality, the idea to organize society without violence nor authority is not new. To get the power back to individuals is broadly speaking the goal of any anarchist view, from libertarian anarcho-capitalists to left anarchists. The core of both ideologies, with largely disserting interpretations of social reality and political procedures, is nonetheless the belief that the aim of a community should be to give each individual the right and the conditions to lead his life in total independence. The former will like the concept of bypassing central political authorities, while the latter that of eluding the monopolistic tyrannies of big banks and economic and financial corporations[28]. The difference, to be more precise, is the causal relation between the two sources of power and coercion. Blockchain's goal is to get rid of both.

The crisis of the national state and the era of globalization are showing under a bright light the relativity and arbitrariness of its authority. With today's means of transportation and communication, men as well as companies are migrating or delocalizing, in the effort of pursuing their own interests by selecting the best institutions on the world stage. Blockchain gives us the opportunity to privately organize our resources and rights fleeing this planet's sources of power, literally bringing them in another dimension, the *cyberspace*. This is the aim

[28] - Cfr. Brett SCOTT, *Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain*, ETH Zürich Presse, 2014.

of the first digital community projects, including Bitnation, self-defined as a «decentralized voluntary borderless nation»[29].

The fundamentality of states *in primis*, and of any regulating central intermediary in general, has been heavily questioned by the introduction of global telecommunication systems, connecting citizens across national borders. Wherever governments, banks, courts have promoted themselves as the cornerstone of political, financial and juridical relations between individuals, peer-to-peer technology in various forms allowed society to build more and more complex horizontal organizations of powers, rather than vertical ones. This path of needs and achievements brought to the invention of blockchain, the peak point of the elimination of any kind of external interference.

Developing protocols, from then on, have been the cumulative result of new questions and answers, new experiments, new perspectives, successes and failures. This process has been called the formulation of *digital common law*[30] or *lex cryptographia*[31], in the effort to emancipate society from its traditional forms of administrations. The elaboration of this spontaneous set of orders recalls the pattern that eventually built a whole law system, the *lex mercatoria*, from the individual agreements between merchants going from country to country[32]. This unregulated genesis makes us think that there is no intrinsic, pre-organized, political implication in the adoption of blockchain platforms[33]. All their features depend in fact from feedback, which is the supply and demand game of those who freely choose to join or leave software, rewarding or penalizing new solutions.

3.2 WHERE HAS AUTHORITY GONE?

Blockchain technology is often represented as the key to eliminate all authorities. However, in literature many are questioning this: is perhaps the software's protocol itself the real authority taking over the others? Do people become sovereign or is the system getting rid of all sovereigns to reign alone on people? Secondly, is it true that blockchain could administer every

29 - Cfr. Susanne TARKOWSKI TEMPELHOF, *Bitnation Whitepaper*, 2015, https://tse.bitnation.co/documents/.
30 - Cfr. John Henry CLIPPINGER, David BOLLIER, *The Rise of Digital Common Law, An Argument for Trust Frameworks, Digital Common Law and Digital Forms of Governance,* ID3, 2012.
31 - WRIGHT, *ibidem*.
32 - Cfr. WRIGHT, *ibidem*.
33 - Cfr. CLIPPINGER, *ibidem*.

aspect of social life well without any external supervision, for example on the good functioning of single platforms?

For what concerns the first question, there are two main views to be considered[34] (somewhat recalling the division between miniarchist and anarcho-capitalist libertarians):

- *Cryptoanarchism*: blockchain can eradicate any need for external control by social relations – a position held by the cypherpunk movement in general, Cody Wilson, Bitnation,
- *Technostatalism* or *technolibertarianism*: blockchain cannot eliminate the need for authorities in society, but can be a more efficient type of authority, because it is decentralized as a functioning political order can be – a position held by Marcella Atzori, Anton Antonopoulos, Melanie Swan, Democracy.earth and Flux.

The main idea of the latter is that cryptography could at best be a technological improvement of government[35]. The modern *Rechtsstaat* is an institution were single politicians are not directly responsible for the enforcement of rule and the application of power, but simply work in order to modify the set of rules to apply, the legislative code. Blockchain can be turned into a legislative code whose enforcement is under no one's control, but is automatically applied as far as it is programmed by every participant in the network. The law is not obsolete, *code is law*[36].

According to this theory, it would not be possible at all to establish norms in society without any forceful *super partes* entity with the ability to manipulate the rights of citizens at some extent – being that a government, a court, or a smart contract cryptographically locking away the contractors' data. For what concerns DAOs, decentralization cannot be absolute, because rules must be enforced by something or someone, even by the software itself[37]. The advantages of this technology are simply all the advantages of keeping people away from the steering committee. In other words, it is not possible to remain in the state of nature.

Furthermore, perhaps it is not even true that the blockchain protocol is totally independent from human influence. For example, the best programmers within society could manage to modify the source of the smart contracts composing their DAO, and thus could propose rules

34 - Cfr. ATZORI, *ibidem*.
35 - Cfr. ATZORI, *ibidem*.
36 - Cfr. Lawrence LESSIG, *Code and Other Laws of Cyberspace, Version 2.0*, Vol. 3, 2006.
37 - Cfr. Curtis YAVIS, *The DAO as a Lesson in Decentralized Governance*, 2016, https://urbit.org/blog/dao.

and new platform in a more versatile way. They could constitute a new form of *élite*[38]. The so flaunted equality among the nodes of the network could be greatly endangered. «In a world increasingly reliant on technology and ruled by networks, whoever owns and controls these platforms will always have a significant power over civil society on a global scale.»[39]
Finally, a threat to blockchain's lack of authorities is its vulnerability to external aggressions. The correct realization of transactions between individuals would completely rely on the correct operations of electricity and internet providers, which are companies and are thus potentially regulable or attackable by forms of traditional political power (such as states)[40].

Who, on the other hand, believes blockchain will really be able to free society from authorities, also claims this cannot happen without a profound reformulation of the concept of law itself[41]: no one should be forced to be subdued to any norm, so the automatic execution of operations regarding one's resources by smart contracts is not an obstacle to a just treatment of individuals. It is rather its condition of possibility. In other words, the system itself is not the ruler, because it does not choose the rules, it is the rules themselves. An intermediary is not an intermediary if it does not have his own will, i.e. if it is not human.
Cryptoanarchists must assume some preliminary claims:

- Any juridical relation can be described as a relation of imputation between facts, that is an algorithm – *if x, then y*,
- Any human organization can be reduced as a set of properties, and a set of rules in order to manage those properties over time[42],
- The human model of digital societies is the *Homo Oeconomicus*: «an agent renowned for being autonomous, instrumentally rational, psychologically self-sufficient, "under socialized" and motivated into action by the utilitarian principle of maximizing

[38] - Another big issue on this same trend is the possibility of the formation of a sort of dictatorship by a group of miners absorbing more than the 50% of the total computing power available on the market. We are not mentioning this, however, because this would require a full understanding of the dynamics of mining processes and of new developments proposed for blockchain technology in response to some of their difficulties. Cfr. ATZORI, *ibidem*.
[39] - ATZORI, *ibidem*, p.30.
[40] - Cfr. David S. BENNAHUM, *United Nodes of Internet: Are We Forming a Digital Nation?*, in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, Peter LUDLOW (ed.), MIT Press, 2001.
Cfr. Brett SCOTT, *Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain*, ETH Zürich Presse, 2014.
[41] - Cfr. CLIPPINGER, *ibidem*.
[42] - Cfr. Vitalik BUTERIN, *On Public and Private Blockchains*, 2015, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/, mentioned in ATZORI, *ibidem*.

pleasure»[43]. The cryptoanarchist condition is somewhat analogous to Locke's state of nature: rational men freely form associations and agreements with their instruments for administering their properties and face problems in life time after time,

If technology is developed enough, there is no room for central intermediaries of any kind in the perfect political order. Centralization in general is merely a practical means to administer what cannot still be controlled by individual contracts. Therefore, government in particular is both harmful and unnecessary.

3.3 ARE DAOS ANARCHICAL UTOPIAS?

The second question found in literature about authority and blockchain is if this technology could ever supply to all social aspects of life really with no external supervision at all. There are three reasons one might think DAOs could actually need to be integrated with some sort of coercion on them:

- To guarantee contractual conditions even under software malfunctioning (both violent or not),
- To prevent the creation of power unbalances and unfairness, compromising the same operations for the same platforms for all,
- To carry out some political tasks which could never be reduced to algorithmic/contractual terms.

There are again two general opinions regarding these points: the friends of technostatalism would hold them as a sufficient condition to advocate for external supervision of software, while the friends of cryptoanarchism would reject them and advocate for a complete market-driven management of such issues.

Although blockchain is a very secure technology, danger for external attacks remains high for newborn or weak software. Secondly, it is indeed possible for automatic algorithms to experience bugs or malfunctioning in general, also due to their hardware support. These

[43] - Reynald BOURQUE, Denis HARRISSON, György SZÉLL, *Social Innovation, The Social Economy, and World Economic Development*, Lang, 2009, p.85, mentioned in ATZORI, *ibidem*.

situations can lead to wrong transactions and *unjust* states of affairs, if the actual objective-state is not the one that should have been implied by the starting conditions.
There is no need to heal the tort retrospectively, if there is no active central entity that controls transactions[44]. An example is the controversy arose after Ethereum suffered from a 60 million dollars theft[45]. A bug of the system was exploited, and this allowed the hacker to regularly write on the public ledger the false transfer, just following the rules of the protocol: how could we decide whether considering the loot a right for the thief or rebooting the whole software in order to abort the operation[46]?
So, one alternative is to introduce some sort of steering committee with the extreme ability to reverse fraudulent transactions manually. Another alternative is to request to all the citizens of a DAO to sign for an "insurance" smart contract, whose role would be to execute some pre-set response to such controversies. Similarly, Buterin proposed the institution of some automatic private software, *oracles*, able to monitor the relations on the network and to heal torts on the basis of preceding deliberations[47]. The analogy is with anarcho-capitalist arguments for privatized courts on the market.
One may think, along these lines, that such problems could only be solved by the first option, by some form of *superior* control on the blockchain, because the occurrence of DAOs' failures and desertions would bring people to lose all their properties and rights forever. This could be caused by bugs or attacks, as seen before, but could also be caused by competition between software companies, or even by chance[48].

To sum up, «A reasonable conclusion is that the blockchain-based governance should be seen as an *organizational theory* […] while it is not meant to be a stand-alone *political theory*. Likewise, blockchain technology and decentralized platforms are not *hyper-political*, but rather *pre-political* tools.»[49] The way to get to emulate state coercion to the point of just the right amount of decentralization in society is to exploit a technical device included in the original

44 - Cfr. Vasilis KOSTAKIS, Chris GIOTITSAS, *The (A)Political Economy of Bitcoin*, TripleC, 2014.
Cfr. WRIGHT, *ibidem.*
45 - Cfr. Wessel REIJERS, Fiachra O'BROLCHÁIN, Paul HAYNES, *Governance in Blockchain Technology & Social Contract Theories*, Ledger Journal, 2016.
46 - As we will be showing in a while, this is a possibility for the particular protocol of Ethereum.
47 - Cfr. BUTERIN, *ibidem*.
48 - Cfr. ATZORI, *ibidem*.
49 - ATZORI, *ibidem*, p.33.

smart contract project[50]: blockchain can be either *permissioned* or *permissionless* (or *unpermissioned*)[51].

DAOs founded on permissioned contracts are ultimately run by a steering committee (initially formed by the software developers), which actively 1) lets in or kicks out members and 2) gives the system each authorization to process and unlock any new pending transaction. This reintroduction of human touch and control can be regarded as a solution to guard the public ledger on a certain platform, if participants think this is a better option than absolute anarchy. Starting from here, there are many ways to organize such environments: it is possible to implement smart contracts in order to assign privileges under some criteria (democratic vote, popular dethronement, time-limited mandate…), or it is possible that all participants are required to control everyone else's transfer.

Bitcoin is an example of permissionless blockchain (and all cryptocurrencies are in general); an example of permissioned blockchain (for the moment) is Ethereum, which keeps the right to freeze any modification to the source code if needed – just like the possibility to enter martial law in case of emergency[52].

50 - Cfr. ATZORI, *ibidem*.

51 - Cfr. SMART CONTRACT ALLIANCE, *Smart Contracts: 12 Use Cases for Business & Beyond*, Chamber of Digital Commerce, 2016.
Cfr. ATZORI, *ibidem*.

52 - Cfr. YAVIS, *ibidem*.

CONCLUSION

This summary of the features, difficulties, perspectives, and applications of blockchain enables us to evaluate at least partially the great potentiality of this technology. Questions have been opened, that lead us to rethink what it means to relate to others in society. For what concerns its political applications, the problems placed are exponentially and increasingly puzzling and substantial, making us also reconsider under a new light the most basic features of even today's political devices and institutions.

We are on the edge of a revolution that would at least be as important as the diffusion of internet was: the founding act of cyberspace, competing with the real world to gain our attention. We can be sure that, in the long term, blockchain technology will play a huge role in our social everyday lives, down our most common relations with fellow people and even things. What is not sure is the impact such a meaningful transformation will bring in the way we understand reality altogether.

Our opinion is that this will be an unspeakable occasion for renovation, toward the solutions to the flaws that have been making attempts to our realization of just and effective political orders for centuries. This is true at least for those who think individuality and its protection are the highest values in politics.

BIBLIOGRAPHY

ATZORI, Marcella, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, SSRN Electronic Journal, 2015

BECK, Roman, STENUM CZEPLUCH, Jacob, LOLLIKE, Nikolaj, MALONE, Simon, *Blockchain, The Gateway to Trust-Free Cryptographic Transactions*, Twenty-Fourth European Conference on Information Systems (ECIS), 2016

BUTERIN, Vitalik, *Ethereum White Paper, A Next Generation Smart Contract & Decentralized Application*, Ethereum Foundation, 2014

CARBONI, Davide, *Come funzionerebbe un'assicurazione auto con la Blockchain. Magie della "scarsità digitale"*, AGI Italia, 2017

CLIPPINGER, John Henry, BOLLIER, David, *The Rise of Digital Common Law, An Argument for Trust Frameworks, Digital Common Law and Digital Forms of Governance,* ID^3, 2012

FOTI, Lorenzo, *Capire blockchain*, Lorenzo Foti, 2017

GÜRING, Philipp, GRIGG, Ian, *Bitcoin & Gresham's Law, The Economic Inevitability of Collapse*, Financial Cryptography, 2011

JARVENPAA, Sirkaa, TEIGLAND, Robin, *Trust in Digital Environments: From the Sharing Economy to Decentralized Autonomous Organizations*, 50th Hawaii International Conference on System Sciences, 2017

KOSTAKIS, Vasilis, GIOTITSAS, Chris, *The (A)Political Economy of Bitcoin*, TripleC, 2014

LEE KUO CHUEN, David (ed.), *Handbook of Digital Currency, Bitcoin, Innovation, Financial Instruments, and Big Data*, Elsevier, 2015

LUDLOW, Peter (ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias*, MIT Press, 2001

NAKAMOTO, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin Foundation, 2008,

REIJERS, Wessel, O'BROLCHÁIN, Fiachra, HAYNES, Paul, *Governance in Blockchain Technology & Social Contract Theories*, Ledger Journal, 2016

SCOTT, Brett, *Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain*, ETH Zürich Presse, 2014

SMART CONTRACT ALLIANCE, *Smart Contracts: 12 Use Cases for Business & Beyond*, Chamber of Digital Commerce, 2016

WINNER, Langdon, *Do Artifacts Have Politics?*, in *Daedalus, Modern Technology: Problem of Opportunity?*, Vol. 109, n° 1, MIT Press, 1980

WRIGHT, Aaron, DE FILIPPI, Primavera, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN Electronic Journal, 2015

WEBLIOGRAPHY

BOVETTI, Maria, *Crittografia e numeri primi*, matematica.unibocconi.it/articoli/crittografia-e-numeri-primi

BUTERIN, Vitalik, *SchellingCoin: A Minimal-Trust Universal Data Feed*, 2014, https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/

DEMOCRACY EARTH FOUNDATION, *The Social Smart Contract*, 2014, https://github.com/DemocracyEarth/paper

HUGHES, Eric, *A Cypherpunk's Manifesto*, 1993, https://www.activism.net/cypherpunk/manifesto.html

PETRIB, *The Untold History of Bitcoin: Enter the Cypherpunks*, 2018, https://medium.com/swlh/the-untold-history-of-bitcoin-enter-the-cypherpunks-f764dee962a1

STROSS, Charles, *Why I Want Bitcoin to Die in a Fire*, 2013, www.antipope.org/charlie/blog-static/2013/12/why-i-want-bitcoin-to-die-in-a.html

SZABO, Nick, *Smart Contracts*, 1994, www.for.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

TARKOWSKI TEMPELHOF, Susanne, *Bitnation Whitepaper*, 2015, https://tse.bitnation.co/documents/

YAVIS, Curtis, *The DAO as a Lesson in Decentralized Governance*, 2016, https://urbit.org/blog/dao