Challenges and opportunities of blockchain and smart contracts for democracy in the distributed, algorithmic state

Goossens, Jurgen

Published in:
Blockchain and public law

Publication date:
2021

Document Version
Version created as part of publication process; publisher's layout; not normally made publicly available

5. Blockchain and democracy: Challenges and opportunities of blockchain and smart contracts for democracy in the distributed, algorithmic state

Jurgen Goossens[1]

I. INTRODUCTION: TRUST-BUILDING IN A HYPER-COMPLEX, HYPER-CONNECTED SOCIETY

Given the increasing complexity in society and the evolution of the night watchman state to the social welfare state, the amount of rule-making has increased and the so-called 'administrative state' has developed.[2] In order to deal with this complexity, traditional legislators have increasingly delegated regulatory and legislative powers to the executive branch, independent agencies and private rule-makers. Additionally, these legislators often leave room for policy choices and balancing of interests by using framework legislation and vague notions. Due to this 'deparliamentarisation of the law'[3] the executive branch takes an increasingly important role. Administrative authorities no longer only have to execute legislation, but increasingly also establish rules and make important policy choices. More recently, administrative authorities increasingly use digitization and technologies based on algorithms and big data in order to deal with the aggregation of these tasks. This, however, leads to another kind of complexity, namely technical complexity, also referred to as 'the black box'.[4]

As a response to growing distrust in intermediaries or 'trusted third parties', such as banks, in the aftermath of the financial crisis of 2008, the first blockchain application 'Bitcoin' was described in 2008 by a person (or group of persons) known under the pseudonym Satoshi

[1] Associate Professor of Constitutional and Administrative Law at Tilburg University and Project Leader of the research project 'Blockchain in the network society: in search of transparency, trust and legitimacy'. This research is financially supported by the Dutch Research Council (NWO) as part of the program 'Responsible Innovation. Designing for public values in a digital world.'

[2] Dwight Waldo, *The administrative state: A study of the political theory of American public administration* (Ronald Press Co, 1948).

[3] See Rob Van Gestel, 'The 'Deparliamentarisation' of Legislation: Framework Laws and the Primacy of the Legislature' (2013) 9(2) *Utrecht Law Review*, 106–22.

[4] See Frank Pasquale, *The black box society. The secret algorithms that control money and information* (Harvard University Press 2015).

Nakamoto.[5] It is difficult to make sure one cannot spend the same money more than once in the digital world, a task usually performed by banks. For the first time, however, Bitcoin managed to address the double spend-problem for electronic transactions of the digital currency (cryptocurrency) 'bitcoin' without the need for a trusted third party.[6] This has led blockchain-believers to picture a utopian world without the need for centralized trusted third parties, such as banks, notaries, social media companies, administrative authorities or even courts. Blockchain is a distributed ledger technology, namely a data structure (the ledger) to which data can be added that is collectively shared and kept secure. Blockchain facilitates the exchange of value and the execution of rules through smart contracts based on collective verification by the participants, i.e. 'nodes', who also collectively guarantee the inalterability of the blockchain, without the need for an intermediary actor to ensure relational trust. As a result, blockchain-based smart contracts enable the execution and enforcement of rules and transaction between parties who do not fully have to trust each other. In principle, no one can unilaterally influence the correct execution of the smart contract (unless you have more than 50 per cent of the computing power in the network). The need for trust does not disappear, but 'actor trust' is being replaced by 'distributed (technology) trust'.

In the wake of Bitcoin's popularity, not only the currently more than 2,000 virtual currencies representing approximately $175 billion saw the light,[7] but the underlying blockchain technology became a hype. Both private companies and governments have been developing a plethora of use cases, Proof of Concepts and pilots. Admittedly, many of these have not been implemented into real applications. Nonetheless, according to a forecast of Gartner the business value produced by blockchain would grow to slightly more than $176 billion and then increase to more than $3.1 trillion by 2030.[8] At the same time, vigilance is required as Gartner also predicted that by 2021 90 per cent of existing enterprise implementations blockchain platform must be replaced within 18 months to remain competitive, secure and avoid obsolescence. Clearly, the technology is still in its infancy, is rapidly evolving and has a large future potential. Marco Iansiti en Karim Lakhani aptly articulated in the *Harvard Business Review* (2017): 'Blockchain is a foundational technology: It has the potential to create new foundations for our economic and social systems. But while the impact will be enormous, it will take decades for blockchain to seep into our economic and social infrastructure.'[9]

---

[5] Nakamoto Satoshi, 'Bitcoin: A peer-to-peer electronic cash system' (Bitcoin 2008) https://bitcoin.org/bitcoin.pdf accessed 29 January 2020.

[6] Jurgen Goossens, Kristof Verslype and Eric Tjong Tjin Tai, *Blockchain en smart contracts: herijking van de rol van de vertrouwde tussenpersoon in de algoritmische samenleving* [*Blockchain and smart contracts: reassessment of the role of the trusted third party in the algorithmic society*] (Sdu 2020) 63.

[7] 'All Cryptocurrencies' (CoinMarketCap) https://coinmarketcap.com/all/views/all accessed 30 March 2020.

[8] 'Gartner Predicts 90% of Current Enterprise Blockchain Platform Implementations Will Require Replacement by 2021' (Gartner 3 June 2019) https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain accessed 21 January 2020.

[9] Marco Iansiti and Karim R. Lakhani, 'The Truth About Blockchain' (*Harvard Business Review*, January–February 2017) https://hbr.org/2017/01/the-truth-about-blockchain accessed 21 December 2019.

In addition to hierarchical, vertical relations, increasingly horizontal relations and networks have been established in the so-called 'network society'.[10] In the network society, public authority is no longer only unilaterally exercised by public actors, but increasingly private actors are also involved in the exercise of public authority. An ever more blurred distinction between public and private, an increase of horizontal relations and network governance have become important evolutions in the functioning of public administration. In the private sector as well, the role of networks is undeniable. Think for instance about the development of the sharing economy. More general, markets and ecosystems are increasingly based on digital platforms, provided by intermediaries such as Google, Facebook, AirBnB or Uber.[11] Blockchain, as a distributed ledger technology, however, enables the verification and execution of simple rule-based 'if x, then y' algorithms (in this case called 'smart contracts') without these intermediaries. One could thus call blockchain a trust-building technology.

The trust-building promise of blockchain is an interesting evolution in the network economy and more broadly in the network society which is characterized by ever-increasing relations and hyper-connectivity as well as more recently technological hyper-complexity in a world of Big Data, Internet of Things, algorithms and Artificial Intelligence. When administrative authorities use algorithms and more recently distributed technologies such as blockchain, the 'administrative state' meets the 'algorithmic, distributed state'. As a result, it is important to identify and design the conditions necessary for public actors using blockchain and smart contracts to ensure the public values of transparency, trust and legitimacy. Transparency is important to generate trust and accountability in case of hyper-connectivity and hyper-complexity and to use blockchain-applications in public administration in a legitimate way. (*II. The use of blockchain-based smart contracts in the algorithmic administrative state*). In general, the use of blockchain and smart contracts must always comply with the existing legal rules (*III. 'Code is not law': blockchain vs. the rule of law*). However, the use of blockchain and smart contracts pressurizes some essential principles of the rule of law, such as safeguarding fundamental rights, for instance the right to privacy, as well as the proper functioning of checks and balances, including effective judicial review.

After the traction blockchain-based cryptocurrencies gained as a response to distrust towards financial institutions due to the financial crisis, the use of blockchain technology has among others also been proposed as a response to growing distrust in democratic institutions and their ability to create the conditions for fair elections. Fair, secure political campaigns and voting procedures are a prerequisite of sustainable democracies. Therefore, it will be explored whether distributed ledger technologies, such as blockchain, might be able to contribute to the efficiency and reliability of voting procedures and their monitoring (*IV. Blockchain and the composition of democratic institutions*). Moreover, political campaign rules, including the regulation of income and spending by political parties and electoral candidates, also play an important role in the fairness of elections. International IDEA shows that unregulated cryptocurrencies are used to finance political parties,[12] which poses serious risks for the proper

---

[10] Manuel Castells, *The rise of the network society* (John Wiley & Sons, 2011, Vol. 12).

[11] Martin Kenney and John Zysman, 'The rise of the platform economy' (2016) 32(3) *Issues in Science and Technology*, 61.

[12] International IDEA, Catalina Uribe Burcher, 'Cryptocurrencies and Political Finance' (Discussion Paper, 2/2019) https://www.idea.int/sites/default/files/publications/cryptocurrrencies-and-political-finance.pdf accessed 7 December 2019, 9–18.

functioning of democracy. A suboptimal level of reliability might decrease the legitimacy of democratic institutions, leading to societal distrust and democratic decay. As a result, the chapter examines the need to prevent the abuse of blockchain-based cryptocurrencies to evade political campaign finance rules due to anonymity and a lack of sufficiently efficient national and supranational rules (*V. Political campaign financing and the threat of cryptocurrencies*). Democratic oversight agencies are yet to develop guidelines and regulations.

The chapter thus identifies the main challenges and opportunities of blockchain and smart contracts for the functioning of public administration and the composition of democratic institutions. Moreover, it sets an agenda for the near future which is relevant for involved stakeholders, such as legislative jurists, law and policy-makers, public authorities, electoral management bodies and political finance oversight agencies. It is important to identify the necessary conditions in order to ultimately design distributed technology applications with the aim of maximizing their potential to strengthen trust in the electoral processes, the composition of democratic institutions and the functioning of the administrative state (*VI. Conclusion: blockchain as democratic trust-generator?*).

II. THE USE OF BLOCKCHAIN-BASED SMART CONTRACTS IN THE ALGORITHMIC ADMINISTRATIVE STATE

As mentioned above, in order to deal with rising complexity in society an administrative state with broad regulatory powers for executive authorities has been developed in many countries. In this administrative state, more recently administrative authorities increasingly use algorithms to support or fully automate their decision-making processes. Due to new technological evolutions in the digital era and the ever-increasing computing power, algorithms can easily be automatically executed via software programs. An algorithm is basically a set of instructions to execute a certain task. Hill describes them as 'mathematical constructs with a finite, abstract, effective, compound control structure, imperatively given, accomplishing a given purpose under given provisions'.[13] Based on the input and processing of data different steps lead to a certain result, in this case (the support of) processes and decisions of public authorities.

Although there is a broad spectrum of algorithms, one could make a basic distinction between 'rule-based' and 'case-based algorithms for the purpose of simplicity and insight.[14] On the one hand, rule-based algorithms reach a certain conclusion or result based on a number of fixed rules. These code-driven algorithms take the form of a more or less simple decision tree and are constructed as 'if x, then y'. Case-based data-driven algorithms, on the other hand, learn to make predictions about unknown cases based on a number of known cases. The computer program trains itself to recognize patterns and correlations usually based on sets of big data and subsequently make predictions based thereon. This is the deployment of forms of Artificial Intelligence such as machine learning, deep learning and self-learning algorithms.

Smart contracts are such deterministic 'if x, than y', rule-based algorithms. Blockchain-based smart contract technology enables that these rules are automatically executed and collectively

---

[13] Robin K. Hill, 'What an algorithm is' (2015) 29(1) *Philosophy and Technology*, 35.

[14] See Jurgen de Poorter and Jurgen Goossens, 'Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht' [Effective legal protection against algorithmic decision-making in administrative law] (2019) 44 *Nederlands Juristenblad*, 3305.

verified by a distributed network without the need of an intervention of a trusted intermediary. The use of smart contracts enormously expands the possibilities of blockchain applications, though it is important to make a clear distinction between the distributed technology (blockchain) on the one hand and the used algorithms (smart contracts) on the other hand. Blockchain-based smart contract technology generally enables a secure, distributed execution of three types of actions which normally require a trusted third party: 1. register facts; 2. transfer value (or at least a representation thereof, i.e. a 'token'); and 3. enforce rules.[15] In practice, a blockchain application usually deploys a combination of these actions. With regard to the second type of action, all assets or value that that can be registered and transferred on the blockchain (i.e. tokenized) can be received, blocked and transferred by smart contract technology. These possibilities enormously increase the potential of blockchain technology. Think for instance about copyrights, domain names, diamonds or houses.

The notion 'smart contract' has already been around for a while and has been coined by Nick Szabo in the midst of the nineties of the past century. He defined it as follows:

> A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.[16]

Szabo thus described 'smart contracts' as technology that supports the execution of legal contracts based on algorithms.[17] As a matter of fact, a smart contract thus does not need to use underlying blockchain technology, nor does it even have to be executed in a distributed manner. Nevertheless, if one nowadays mentions smart contracts, in almost every case – the same goes for this chapter – one means blockchain-based smart contracts.

Notwithstanding Szabo's initial limitation of the use of smart contracts to the execution of the terms of a contract, smart contracts do not necessarily have to be characterized as the conclusion or execution of (clauses of) legal contracts. They can also constitute, inter alia, suspensive or dissolving conditions of a contract, unilateral legal acts (such as a gift or will), (unilateral) decisions of administrative authorities (e.g. granting subsidies), means of evidence (e.g. registered facts in a police file), automatic execution of (legal or other) processes or compliance with legal obligations (e.g. fiscal law).[18]

Consequently, smart contracts could support administrative authorities in the administrative state to deal with the aggregation of their tasks and responsibilities. All kinds of applications

---

[15] Goossens, et al (n 6), 111.

[16] Nick Szabo, 'Smart contracts' (1994) http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html accessed 3 March 2020.

[17] Nick Szabo, 'Formalizing and securing relationships on public networks' (First Monday no. 9 1997) https://doi.org/10.5210/fm.v2i9.548 accessed 3 March 2020.

[18] Dutch Blockchain Coalition Smart Contract Working Group, 'Smart contracts as a specific application of blockchain technology' (2017) 21–34 https://dutchblockchaincoalition.org/uploads/pdf/Smart-Contracts-ENG-report.pdf accessed 13 November 2019.

are conceivable in the administrative algorithmic state, such as information sharing[19] or a smart contract could, for example, enable to automatically and securely award government subsidies, allowances or licenses if certain conditions are fulfilled. Another interesting example is a so-called 'Digital Data Safe' which aims to give citizens the possibility to decide for themselves which organization can consult which part of their personal data and more specifically for example the 'Financial Emergency Brake' blockchain pilot of the Dutch Central Judicial Collection Agency (CJIB) to help people in debt pay their fines by signalling inability to pay in a timely fashion.[20] The application is based on blockchain, zero-knowledge-proofs and self-sovereign identity.

Competences of administrative authorities can be discretionary or circumscribed. Rather than in the case of competences where the administrative authority has a margin of appreciation that requires balancing of interests or interpretive discretion, rigid rule-based smart contracts realistically seem to be deployable in case of circumscribed competences without discretion. In the latter case, an administrative authority can actually only take one certain decision given the circumstances or conditions. Moreover, administrative authorities should always abide by the applicable laws and regulations when exercising its competences. Nonetheless, general principles of good administration, such as the principle of due diligence and reason-giving, the proportionality and equality principle, the right to be heard, the principle of legal certainty and protection of legitimate expectations, could pose a challenge when using deterministic blockchain-based smart contracts that could be perceived as a 'black box'.[21] Principles of good administration play an important role to guarantee accountability. It is generally accepted that administrative accountability requires transparency and participation, both *a priori* during administrative proceedings and *a posteriori* in judicial proceedings. These principles of good administration may also play an important role as a framework for effective judicial review of algorithmic decision-making.[22] Therefore, it is important to analyse how administrative accountability and the principles of good administration should be operationalized by administrative authorities and to which extent these principles are sufficiently resilient as substantive grounds for judicial review.

In order to address the technical complexity or 'black box' character of the use of distributed technology and algorithms,[23] we can observe a trend – both in traditional and judicial law-making – towards developing a right to (meaningful) information and explanation. Article 15 of the General Data Protection Regulation (GDPR), for instance, enshrines the data subject's right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, as well as, among others, whether automated decision-making took place. In the latter case *meaningful* information should be provided

---

[19] Svein Øines, Jolien Ubacht and Marijn Janssen, 'Blockchain in government: Benefits and implications of distributed ledger technology for information sharing' (2017) 34(3) *Government Information Quarterly*, 355–64.

[20] Central Judicial Collection Agency (Ministry of Justice and Security), 'The Financial Emergency Brake. CJIB app provides citizens with a GDPR-proof way to declare payment inability' https://northsearegion.eu/media/9067/cjib-the-financial-emergency-brake.pdf accessed 12 June 2020.

[21] See Dutch Blockchain Coalition Smart Contract Working Group (n 18), 37–9.

[22] de Poorter and Goossens (n 14).

[23] See Pasquale (n 4).

about the logic involved, the significance and the envisaged consequences of such processing for the data subject.

Such transparency is crucial, not only for legal subjects themselves to understand what happened and why, but it is also essential to make effective judicial review possible. Nonetheless, it remains to be seen whether a right to meaningful explanation about algorithmic decision-making is in practice always feasible and whether it does not lead to a new 'transparency fallacy',[24] namely the illusion that the right to be informed will actually contribute to substantively better decision-making. In this regard, not only the legislative and executive branch have to take this danger into account, but also the judiciary awaits an important task to ensure an effective remedy as regards the right to meaningful information.[25]

Additionally, one should be aware that smart contracts could be considered to be 'deaf and blind'.[26] Rather than 'smart' they are deterministic. Moreover, the smart contract has no knowledge other than its own status, nor access to its transaction history or to other data on the blockchain. It cannot easily know the status of other smart contracts, nor does it have access to data from the real world or elsewhere on the Internet. Nonetheless, such information can be delivered to the smart contract by a so-called 'oracle', which is usually provided by an entity that must (again) be trusted, for instance a judge, notary or administrative authority. The information is delivered through a transaction containing that information and is published on the underlying blockchain. Oracles can for instance be used for the use of smart locks or the award of automatic compensation in case of noise pollution or flight delays. Nonetheless, trust is still needed. One must, for instance, trust that the software does not contain programming errors (bugs) or that the input by the oracle is correct. Incorrect or false input leads to an unintended result (i.e. 'crap in, crap out').

III. 'CODE IS NOT LAW': BLOCKCHAIN VS. THE RULE OF LAW

In general, the use of blockchain-based smart contracts must always comply with the existing legal rules (i.e. 'code is not law'). However, the use of blockchain as a distributed ledger technology creates tension with some essential principles of the rule of law, such as checks and balances as well as safeguarding fundamental rights, for instance the right to privacy. Regarding the latter, the GDPR, for instance, is based on a number of key principles of processing of personal data that must be respected. Particularly relevant in the context of the use of blockchain are, among others, the principles of fair, lawful and transparent processing of data (cfr. the black box); purpose and storage limitation, data minimization; integrity and confidentiality (Art 5 of the GDPR). Moreover, Articles 16 and 17 respectively guarantee the right of rectification and the right to erasure ('the right be forgotten'). Many blockchain projects experience serious difficulties complying with the GDPR with respect to these principles and rights. The main benefit of blockchain, namely immutably registering all transactions in the

---

[24] Lilian Edwards and Michael Veale, 'Enslaving the algorithm: from a 'right to an explanation' to a 'right to better decisions'?' (2018) 16(3) *IEEE Security & Privacy*, 1 and 7.

[25] See de Poorter and Goossens (n 14), 3305.

[26] Goossens, et al (n 6), 47–8.

blockchain in order to make fraud impossible, is after all obviously in tension with these key principles and rights under the GDPR.

The GDPR was designed to regulate a world in which data are collected, processed and stored mainly in centralized databases, whereas when one uses the distributed technology blockchain these processes are decentralized. This unavoidably causes tension between the GDPR and blockchain. The GDPR represents a world of centralized databases and processing, while blockchain exercises a – potentially disruptive – distributed way of storing data and processing transactions. As a result, Michèle Finck argues that: '[t]here are many tensions and uncertainties between GDPR and blockchain and many blockchain projects are likely not compatible with GDPR'.[27] Nonetheless, Finck also rightfully argues that '[b]oth GDPR and blockchain at heart share the objective of data sovereignty, so blockchain could become a tool to achieve this objective. Blockchain is also still an immature technology, so maybe could be shaped to be GDPR compliant, allowing us to have data protection by design'.[28]

Sometimes, non-compliance with the GDPR can only be avoided by not including personal data in the blockchain, but storing them outside the blockchain or subjecting the data to prior anonymization before storing them on the blockchain. In contrast to a public non-permissioned blockchain, a private permissioned blockchain makes it is easier to process personal data in accordance with privacy regulation, as there is some kind of control or controlling party, called 'the controller' in the GDPR. Moreover, it is recommended that an intervention mechanism is provided by design, for instance the possibility to add a transaction to the blockchain that undoes a previous transaction.

With regard to the proper functioning of checks and balances, transparency and accountability are important rule of law mechanisms. In a parliamentary democracy, the (directly elected) Parliament must be able to exercise control over the functioning of the executive branch and its administrative authorities, for whose actions Parliament can usually hold members of the government accountable due to ministerial responsibility. This indirect democratic accountability is necessary for legitimate state action. In this regard, transparency plays a pivotal role to be able to hold someone accountable. Moreover, as described above, in order to guarantee the right to a fair trial and an effective remedy based on Articles 6 and 13 of the European Convention of Human Rights, the possibility of an appeal to a court that can offer an effective remedy must be provided, though might be difficult to achieve in practice due to the black box character of blockchain technology.

IV. BLOCKCHAIN AND THE COMPOSITION OF DEMOCRATIC INSTITUTIONS

Bitcoin was famously developed as a response to distrust towards financial institutions due to the financial crisis. In the wake of Bitcoin's popularity, the use of blockchain technology has also been proposed, among others to counter concerns of growing distrust in democratic institutions and political parties. More specifically, in some countries the state's ability and

---

[27] EU Blockchain Observatory and Forum, 'GDPR Workshop Report' (8 June 2018) www.eublockchainforum.eu/sites/default/files/reports/workshop_2_report_-_gdpr.pdf accessed 28 August 2020.

[28] Ibid.

commitment to create the necessary conditions for fair and reliable elections can be questioned, such as the preservation of voting secrecy, the reliability of the procedures to count votes, the independence of oversight agencies and of courts reviewing the electoral process. Nonetheless, fair and trustworthy voting procedures are a prerequisite of sustainable democracies. Therefore, one could explore the possibility of using distributed ledger technology, such as blockchain, in order to contribute to the efficiency and reliability of voting procedures and their monitoring.

Recently, the COVID-19 pandemic sparked an immense wave of digitization, for instance in education, in order to limit the spread of the virus. In this regard, it is likely that increasingly calls will be launched to organize elections and other ways of citizen participation in a digital manner. This might suddenly even become a necessity in case of a future new lockdown. An important design principle for the organization of online or digital elections and other ways of direct participation of citizens, such as a referendum or citizen budget, should be the assumption that no single party in the process can be regarded as 100 per cent trustworthy. As a result, there might be a need for additional mechanisms and socio-technical design and governance of computational infrastructure, such as blockchain, that establish (cyber) security, resilience and trust, even in the case that one or more parties – now or in the future – are not considered trustworthy. In other words, trustworthy, resilient computational infrastructure such as blockchain could actually make trust in the behaviour of other actors redundant.

Of course, blockchain technology ought to be secure and 'future-proof' to be trustworthy, but not only as regards the use of advanced cryptology and the future impact of for instance quantum computing. As said, in the design of technology we also have to take into account that actors generally considered trustworthy today (e.g. political parties, the government or financial institutions) might in the future become a threat to the proper functioning of the democratic, economic or societal system. In this regard, all partners of the ecosystem must be considered a potential future threat. In the democratic process of elections, one can think about the citizens or voters (who could for instance violate the constitutionally required voting secrecy or unlawfully pressure other voters), politicians both as political candidates in the election (who could evade campaign financing rules through the use of cryptocurrencies or the use of other illegal or unethical instruments such as the distribution of fake news via social media) and/or as guardians of the electoral process at the same time as members of Parliament, independent electoral oversight bodies (who might be 'packed' with candidates by the leading political elite who wants to ensure staying in power at all costs), social media platforms (allowing illegal or unethical sponsored political campaigns or distribution of fake news).

In a well-functioning democratic state, government regularly organizes fair elections that enable competition and rotation of power. Moreover, in an ideal situation, the chance of fraud during the casting and counting of the votes would be excluded. No single party or actor could falsify the election results, in which case theoretically witnesses, national and international observers or recounts would no longer be needed. Blockchain indeed has the potential to contribute to this ideal situation.[29] Blockchain could theoretically be used to actually cast votes. If that would, however, not be feasible or preferred, blockchain technology could also be used in order to simultaneously register and count the votes unchangeably in a blockchain. As a result,

[29] See Nir Kshetri and Jeffrey Voas, 'Blockchain-Enabled E-Voting' (2018) 35(4) *IEEE Software*, 95–9.

possible fraud when counting the votes could be detected and checked through the blockchain, as in principle everyone can check all the (pseudonymized) transactions unchangeably registered in the blockchain. Nonetheless, the organization of digital elections has regularly been considered controversial in many countries and the arguments against e-voting could *a fortiori* play a role when using a technology that has an inherent tension with privacy regulation more general and voting secrecy specifically.

Voting secrecy is usually constitutionally guaranteed, as it is considered an important constitutional guarantee, and might be invoked to denounce the use of blockchain. At least, advanced, 'future-proof' cryptologic encryption must be adopted. Moreover, in order to prevent external pressure on voters or identity fraud one could consider organizing the elections in designated places where voters must individually cast their vote secluded in a voting booth, also when blockchain technology is used to cast the vote or to simultaneously register the vote. In this way, one might counter an important critique regarding voting secrecy and the prevention of unlawful pressure on voters, while still benefiting from the advantages such as unchangeability of the technology.

In June 2018, the Swiss city of Zug, for instance, organized a small-scale consultative vote based on blockchain technology and using the city's e-ID system based on the Ethereum blockchain. This first local blockchain-based test vote in Switzerland was generally considered to be successful.[30] As opposed to regular e-voting systems, the voting process did not take place via a single central server but took place in a distributed manner through distinct computers using blockchain technology.

Another example took place on 21 March 2018 in the Dutch municipality of Groningen, namely a blockchain experiment to count the votes a second time with blockchain in the referendum relating to the Act on the intelligence and security services.[31] In five polling stations the votes were counted not only by hand, but were also unchangeably registered in the blockchain. In practice, the polling station scanned the QR code on the ballot one extra time. As a result, the turnout counted with blockchain technology could be followed in real time and a smart contract afterwards enabled comparing the turnout with the number of votes counted, so that mistakes in counting could be easily detected. It was the main aim to prevent human errors and make the voting process more transparent. As regards voting secrecy, the official vote was casted on paper and could allegedly not be traced back to the identity of a voter nor the exact time of voting.

It seems easier to comply with voting secrecy when blockchain technology is used only to count the votes and compare the results to detect human mistakes or potential fraud afterwards. Especially in fragile democracies, threatened by abuse of power and corruption, blockchain could prove particularly valuable because of its unchangeability which can prevent fraud. Nonetheless, blockchain technology is actually still in its infancy, so that one should be careful to deploy it in the context of voting. One should always be aware of the possibility of cybersecurity risks, such as hacking and malware. Access to the private keys could give access to

---

30 'Switzerland's first municipal blockchain vote hailed a success' (2 July 2018) www.swissinfo.ch/eng/crypto-valley-_-switzerland-s-first-municipal-blockchain-vote-hailed-a-success/44230928 accessed 15 March 2020.

31 'Proef stemmen tellen met blockchain afgerond' [Test vote count with blockchain completed] (Berenschot 22 March 2018) www.berenschot.nl/actueel/2018/maart/stemmen-met-blockchain/> and <https://stemmen-telt.nl/groningen/#pilot accessed 15 March 2020.

the transactions on the blockchain. Moreover, if deployed on a large scale, network saturation might occur. The use of blockchain for voting is thus a 'work-in-progress', although conceptually a blockchain-based e-voting system could potentially become a secure and reliable computational infrastructure that could avoid fraud, optimize voting transparency and voter access, and contribute to trust in the electoral process and democracy more general.[32]

V. POLITICAL CAMPAIGN FINANCING AND THE THREAT OF CRYPTOCURRENCIES

Besides a reliable, trustworthy voting procedure, rules on political campaigns and oversight also play a crucial role in the fairness of elections. Among others income and spending by political parties and electoral candidates must be properly registered, regulated and reviewed. Research of International IDEA has demonstrated that unregulated blockchain-based cryptocurrencies are used to finance political parties,[33] which in the current state might pose serious risks for the proper functioning of democracy. This is particularly the case as the use of cryptocurrencies is still not properly regulated in many parts of the world and often not traceable and controllable by oversight agencies or other actors due to the use of pseudonyms and thus anonymity when conducting transactions with blockchain.

A suboptimal level of oversight and fairness of political campaign funding, however, might decrease the legitimacy of elections and by extension of democratic institutions, which might ultimately result in societal distrust and democratic decay. The possibility of quasi-untraceable interference in (national or foreign) elections could decrease the legitimacy of the distribution of power in a country and by extension potentially even the power balance of the global legal order. Therefore, there is an urgent need to better regulate the use of cryptocurrencies and to prevent the abuse of cryptocurrencies in order to evade political campaign finance rules due to anonymity and a lack of sufficiently effective national and supranational rules. In addition, democratic oversight agencies must urgently start to develop clear guidelines and regulations.

The network of a virtual currency quickly consists of many participants located all over the world. Consequently, it is almost impossible for an individual state to restrict or regulate such a network that does not have a central party which is in control of the network. Nonetheless, the trading platforms where virtual currencies can be converted into fiat money as well as the providers of online wallets for virtual coins could be more easily regulated and identified as possible liable actors.[34] In this regard, the European Union adopted the Fifth Anti-Money Laundering (AML) Directive in April 2018.[35] It is the Directive's aim that Member States subject both virtual currency trading platforms and wallet providers under the Anti-Money Laundering / Combating the Financing of Terrorism (AML / CFT) regulation.[36] By 10 January

---

[32] See Ahmed Ben Ayes, 'A conceptual secure blockchain-based electronic voting system' (2017) 9(3) *International Journal of Network Security & Its Applications*, 1–9.

[33] International IDEA, Catalina Uribe Burcher (n 12), 9–18.

[34] Goossens, et al (n 6), 88.

[35] EU Directive no. 2018/843 of the European Parliament and of the Council of 30 May 2018 amending EU Directive no. 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives np. 2009/138/EC and 2013/36/EU

[36] See Tom Keatinge, David Carlisle and Florence Keen, 'Virtual currencies and terrorist financing: assessing the risks and evaluating responses' (European Parliament Think Tank 4 June 2018) www

2020, the EU Member States should have adopted legislation to register trading platforms and wallet providers.

This is a first stepping stone towards necessary transparency in the networks of virtual coins. However, the Directive is only applicable to the exchange of virtual currency into fiat money and vice versa. It is not applicable to trading platforms that only allow the exchange of virtual coins with other virtual currencies, which would be tackled in one of the following regulatory steps. It is the intention of the Directive that customers are identified and trading platforms are obliged to report suspicious activities.[37] Nonetheless, it is still possible to trade virtual coins outside a trading platform and it is theoretically also possible to mine its own virtual coins, although that is often rather cumbersome and energy-intensive.

This first regulatory step in the EU is an important one, also in light of establishing transparency regarding the use or abuse of virtual currencies in political campaigns. It is a necessary step to enable reliable control of campaign spending or financial support through cryptocurrencies. Globally, countries deploy diverse approaches regarding the use and regulation of virtual currencies.[38] It ranges from lenient and supportive policy, such as in Switzerland, to restrictive policy, such as in China. Nonetheless, Christine Lagarde, former IMF's managing director, rightly stated: 'To be truly effective, all these efforts require close international cooperation. Since crypto assets know no borders, the framework to regulate them must be global as well.'[39]

VI. CONCLUSION: BLOCKCHAIN AS DEMOCRATIC TRUST-GENERATOR?

The use of distributed ledger technology requires less relational trust and at the same time there is no longer one single, central point of failure. If the applied technology is trustworthy, blockchain has the potential to function as a (democratic) trust generator in our society. Nonetheless, one should notice that relational trust is being replaced by distributed trust through technology. Therefore, the technical design and socio-technical implementation and governance of blockchain-technology is crucial to strengthen trust in the functioning of our democratic society. In this regard, this chapter distinguishes three important phases: 1. the potential use of blockchain in the framework of elections; 2. the use of distributed technology in the algorithmic, administrative state by administrative authorities to carry out public tasks; and 3. effective legal protection.

Not only public actors but also private actors – both (tech) companies and citizens – have a distinct role in big data usage and distributed technologies: not only as final subject of algorithmic rules but also as (co-)creator of data and (co-)designer of these rules. As a result, there is an evolution towards co-creation and horizontalization in the network society, which might

---

.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604970 accessed 14 June 2020

[37] See 'Statement By First Vice-President Timmermans, Vice-President Dombrovskis and Commissioner Jourovà on the adoption by the European Parliament of the 5th Anti-Money Laundering Directive' (European Commission 19 April 2018) http://europa.eu/rapid/press-release_STATEMENT-18-3429_en.htm accessed 14 June 2020.

[38] Goossens, et al (n 6), 89.

[39] Christine Lagarde, 'Addressing the Dark Side of the Crypto World' (IMF Blog 13 March 2018) https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world accessed 14 June 2020.

ultimately improve resilience in our democratic society. Therefore, it is important to identify and analyse the role of all relevant actors in the (blockchain) ecosystem to establish transparency and trust in a distributed, algorithmic network: both state actors (e.g. parliamentary legislator, administrative authorities and courts) and private actors (citizens and (tech) companies).

Private actors and public actors are indeed increasingly entangled due to the co-creation of data and socio-technical infrastructure to address societal challenges, which gives rise to potential advantages, such as increased resilience, self-determination, (co-)ownership of technological infrastructure and data. At the same time, it raises threats, for instance with regard to trust, security, fundamental rights, including privacy and non-discrimination, checks and balances, and principles of good governance. The role and responsibilities of both public and private actors therefore need to be clearly defined and governed in order to maximize the use for democracy while minimizing the threats when deploying distributed technology. The use of distributed technologies requires a rethinking of the democratic playing field and the establishment of guarantees in order to create secure, trustworthy, resilient, future-proof socio-technical infrastructure.

In general, regarding these guarantees, one could for instance consider the introduction of a supervisory authority or regulator with warning, penalty and regulatory powers; an obligation to conduct an impact assessment; the introduction of specific legal guarantees; effective judicial review; a participatory and/or oversight role for experts, citizens and other private parties. Specifically, the undesirable abuse of cryptocurrencies to undermine campaign finance rules has been identified and requires the development of specific rules and effective oversight.

Finally, blockchain technology ought to be 'future-proof' to be trustworthy, not only as regards the use of advanced cryptology and the future impact of for instance quantum computing. In the design of technology we also have to take into account that actors generally considered trustworthy today (e.g. the government or financial institutions) might in the future become a threat to the proper functioning of the democratic, economic and societal system. In this regard all partners in the democratic system must be considered as a potential future threat. Taking this into account, a distributed technology such as blockchain could contribute to a decrease of the necessary trust one has to put in these actors as it could be replaced by distributed trust through technology.