**Blockchain as a Preventive Measure against Corruption: Navigating Conflicting Legal Interests and Technical Challenges On and Off the Chain**

 Gilberto Martins de Almeida,[[1]](#footnote-2) Pedro R. Borges de Carvalho,[[2]](#footnote-3) Fernando Felipe Bourguy de Medeiros.[[3]](#footnote-4)

1. Introduction

Popularized as the underlying technology of Bitcoin, Blockchain technology has benefited from the hype involving cryptocurrencies in recent years. However, despite the fame that promotes the inevitable association with the Cryptomarket, the applicability of Blockchain technologies is much more comprehensive, remarkably transcending the uses in virtual currencies. It is a means for “creating and preserving truths.” [[4]](#footnote-5)

Blockchains are distinguished by their characteristic nodality, which gives blockchain-based technologies are classified as distributed ledgers (DLT – Distributed Ledger Technologies). A DLT is a “multi-party consensus system that enables multiple distrusting entities to reach agreement over the ordering of transactions in an adversarial environment without relying on a central trusted party”.[[5]](#footnote-6) By eliminating the need for an intermediary in operations, blockchain constitutes a reliable and encrypted digital platform for direct, Peer-to-Peer transactions. As to how blockchain verification protocols work, Mike Orcutt offers plain terms:

“A blockchain protocol is a set of rules that dictate how the computers in the network, called nodes, should verify new transactions and add them to the database. The protocol employs cryptography, game theory, and economics to create incentives for the nodes to work toward securing the network instead of attacking it for personal gain. If set up correctly, this system can make it extremely difficult and expensive to add false transactions but relatively easy to verify valid ones.”[[6]](#footnote-7)

In addition to constituting generally immutable records, most blockchains are open ledgers: the history of all the transactions conducted through the blockchain are publicly recorded in it. When all these qualities are combined, the possibilities are varied, and the practical applications today are, indeed, countless. Possible applications are as numerous as the problems normally faced by the Public Administration anywhere in the world: management of public records and land registries, payment of public servants and public service concessionaires, digital rights management, conduction of elections [[7]](#footnote-8)– any field where transparency, security and efficiency are desirable and susceptible to improvements.

Notably, blockchain can be employed to safeguard public registries against tampering,[[8]](#footnote-9) facilitate financial reporting and accountability,[[9]](#footnote-10) and thus, prevent corruption. As explained by Aliyev & Safarov:

“Particularly, transparency and non-reversibility feature of public blockchain allow achieving transactional transparency and accountability in financial operations. By removing intermediaries, blockchain reduces the possibilities to third-party interventions to the accountability systems.”[[10]](#footnote-11)

Such features have led financial institutions to seek blockchain-based IT solutions to instil more transparency and reliability in their financial operations. A great example is “TruBudget”, originally developed by the German Development Bank (KfW). It is now being tested as a pilot project by the Brazilian Development Bank (BNDES), as a platform for registering transfers from the Amazon Fund [[11]](#footnote-12) to partner NGOs, Brazilian Organs of State and Universities. According to BNDES, the implementation of TruBudget aims to “enhance the guarantee that the funds are being adequately applied by means of direct and reliable sharing of critical information between the institutions involved”, citing the records’ intrinsic immutability as a major reason for employing blockchain in its processes.[[12]](#footnote-13)

Likewise, the Inter-American Development Bank’s blockchain procurement system, developed in partnership with the World Economic Forum and the Colombian Inspector General’s Office as a tool to curb public procurement corruption, is an exceptional testament to the suitability of blockchain technologies as public-sector corruption filters.[[13]](#footnote-14) The project, called Unlocking Government Transparency with Blockchain Technology (the “Transparency Project”), designed a blockchain-based software proof-of-concept (PoC) for the procurement of the Colombian public-school meal program, a historic venue for corruption in the country.[[14]](#footnote-15)

In effect, blockchain solutions could well be framed as preventive measures against corruption within the wording of international anti-corruption law. The United Nations Convention against Corruption, the only binding universal anti-corruption international instrument,[[15]](#footnote-16) sets forth preventive measures as one of its core areas, under Chapter II. States Parties shall, inter alia: “endeavour to establish and promote effective practices aimed at the prevention of corruption” (article 5.2); “take the necessary steps to establish appropriate systems of procurement, based on transparency, competition and objective criteria in decision-making, that are effective, inter alia, in preventing corruption” (article 9); promote “transparency among private entities” (article 12.2.c); prevent “the misuse of procedures regulating private entities, including procedures regarding subsidies and licenses granted by public authorities” (article 12.2.d); and, regarding money-laundering prevention, “consider implementing appropriate and feasible measures to require financial institutions, including money remitters: (a) To include on forms for the electronic transfer of funds and related messages accurate and meaningful information on the originator; (b) To maintain such information throughout the payment chain; and (c) To apply enhanced scrutiny to transfers of funds that do not contain complete information on the originator” (article 14). Blockchain’s potential to curb corruption spans the full range of preventive obligations under the Convention.

Notwithstanding its promise, it is accepted that “blockchain is not a one-size-fits-all solution”.[[16]](#footnote-17) There are several blockchain types and each of them is more or less suitable to the particular political and technological context of any given jurisdiction that may seek to implement it in its public policies.[[17]](#footnote-18)

In this piece, the technical aspects of the different blockchain variations will be explored with a view to shedding light on potential legal implications of the employment of blockchain platforms as preventive measures against corruption. Subsequently, political and technological issues will be considered.

1. On-chain and off-chain transactions

As summarized by Aarvik, “there are four major types of blockchains”, each fulfilling different purposes: the public, permissionless blockchain; the public, permissioned blockchain; the closed, permissioned blockchain; and the private blockchain.[[18]](#footnote-19)

Naturally, permissioned blockchains may be safer as the admittance of participants is controlled, and public blockchains may better inspire trust as they ensure more eyes to supervise and validate transactions.

Such kinds of options are fundamental axes for structuring the policies of a blockchain. Equally important is the choice on the governance model, which includes technical and political connotations.

Technically, an on-chain transaction happens inside the blockchain (for instance, the use of cryptomoney allocated on the blockchain for buying assets traded therein) and is validated by its participants, what may be uncertain and time-consuming, although the process of submission to validation by many players possibly implies greater level of trust. On the other hand, the off-chain model is based on the selection of events that shall take place outside the blockchain (e.g., an optical sensor connected to the Internet of Things which reads the arrival of some purchased item in a warehouse and automatically communicates that as an event that shall enable certain payment on the blockchain), which may provide desired agility assuming the selected event triggers an instantaneous response.

Alternatively, hybrid models may be developed by means of nominating independent third parties as escrow agents to confirm events (“oracles”) or release payments, or by requiring accession to rules previously established in protocols. In fact, in its Transparency Project Report, the World Economic Forum concluded that hybrid solutions, employing both permissioned and permissionless base-layer protocols for different activities, were currently “the most attractive”, striking an “ideal balance” of transparency, security, scalability and procedural integrity.[[19]](#footnote-20)

Similarly, smart contracts, which may serve as vehicles for carrying out transactions on the blockchain, may be “coded-only" (purely automated) or “hybrid” (a mix of rules coded on algorithms and on ancillary documents or instruments), the latter option being that which may better serve the purposes of ensuring automatic, objective response, in addition to room for thoughtful, subjective interpretation (for example, on the characterization of events as *force majeure*).

Turning again to the example of BNDES´s TruBudget blockchain for applying resources of the Amazon Fund, the cogitated model has been that of a private permissioned blockchain for off-chain transaction registries.[[20]](#footnote-21) Identified donors, fund managers and providers, such as NGO’s, are granted different permissions for specific functions on the TruBudget platform. Wherever fund managers determine how the donated funds should be spent in the “real world”, they shall declare the disbursement of the sum by indicating the due receiver and attaching the documental proof of the obligation (i.e. the agreement or work order). On the other end, the provider receives a different permission, by which it shall confirm the fulfillment of the obligation by attaching the proof of the transaction (i.e. a receipt or invoice). Whenever each of their declarations are made – manager’s and provider’s –, the acts are registered on the blockchain to be unalterable. Transactions themselves happen in the “real world”, outside the blockchain. Controlling from above by their own permission to the platform, the donors are able to oversee each transaction, their documental proof and the people responsible for it, trusting that, once registered on the blockchain, this data could not be tampered with. Furthermore, anti-corruption bodies may receive access to the platform, in order to enable their investigations.

Notwithstanding the transparency benefits of a registry allegedly not subject to tampering, BNDES’s TruBudget blockchain benefits may be limited to information security instead of a corruption-proof system. Appointing people responsible for off-chain transactions and registering the transaction’s documental proof not subject to alteration may allow donors and anti-corruption bodies to pinpoint accountable people and identify diversion of funds. However, it seems that the system is not able to totally prevent corruption, e.g. overbilling by providers. In order to mitigate the human factor, possibly, a further development of the Trubudget platform for the Amazon Fund should consider to automate the registries by tokenizing the donated funds and managing their flow by smart contracts, not only with respect to payment to the providers, but also on how and if providers themselves spent the funding accordance to their intended purpose. Such a cashflow footprint might enable anti-corruption bodies to identify misappropriation of funds or even money laundering.

1. Know your customer? Know your token

In a world of rapidly growing “tokenization”, to know inner and surrounding aspects of a transaction may translate into knowing the token[[21]](#footnote-22) which represents and materializes it.[[22]](#footnote-23)

For instance, a blockchain may tie payment flows to some sort of currency, and such elected currency may pose greater or lesser risks, depending on the trackability of its flow and on the anonymity of its possession.

In the proposal conjectured above, the use of financial resources apportioned to the Amazon Fund in the context of BNDES´ blockchain could be exercised by means of a new, specific currency, materialized by a token, which could represent transactions performed with the use of funds originated from BNDES´ financing. This way, any spending transaction supported by those funds could be evidenced and mapped out, preventing diversion or disguise. The level of trust ensured by such mechanism may be decisive for purposes of providing investors with the necessary confidence.

 Another important characteristic associated with tokens is the method of their generation and control, which basically opposes Proof-of-Work to Proof-of-Stake. Proof-of-Work means generating tokens by means of intensive efforts like *mining* (that is, to solve cryptographically hard puzzles by using computational resources), which normally does not attract wrongdoings given the poor cost-benefit of the required efforts, but actually allows the participation of anyone in such process, whether a reliable and well-intended actor, or not. Proof-of-Stake, instead, is based on decision-making by stakeholders, the ones who will own *stakes,* and one hand they may have wider chances of controlling the successive steps (“building blocks”) in a blockchain, but on the other hand, if stakeholders are not trustworthy players, the legitimacy and security of that blockchain may be at risk.

Of course, there are several factors which may strike a balance between the pros and cons of each method. A protocol (like *Casper*) may inhibit abusive decision-making by stakeholders. Additionally, requiring publicly visible enrollment data may put money laundering-interested investors under spotlights. Finally, New York State´s successful experience by requiring prior license for doing business with cryptocurrencies tells for itself.[[23]](#footnote-24)

1. Legal Issues On and Off the Chain

Blockchain can be employed in anti-corruption IT solutions by governments, but it can also be a deceptive focal point in the battle against financial crime. In many jurisdictions, local authorities are concerned with the potential for frauds and scams that blockchains may present, an understandable angst since the technology has been at the spotlight for money-laundering schemes.[[24]](#footnote-25)

Such concerns are illustrated by actions taken by securities exchange authorities, as well as by consumer protection entities.

The U. S. Securities Exchange Commission has taken a conservative, cautious approach, qualifying as collective investment a number of blockchains where crypto assets are traded. The rationale behind such strategy seems to be that, so far, in most cases the participants in the blockchain sponsor its development (in this sense, they collectively invest in the creation of the blockchain, aiming at getting return over such investment), and the inherent motivation seems to be the concern with initiatives that may lead to a massive number of investors being deceived (as in Ponzi schemes).

With regards to the bankruptcy of blockchain enterprises, Courts have been challenged in many jurisdictions with the question on whether victims of financial schemes perpetrated through blockchains used for investments shall be entitled to enjoin protection offered to victims of insolvency of financial institutions, as if that kind of blockchains should be viewed as *de facto* equivalent to participants in the financial market, given the possible analogy, in certain cases, between cryptomoney and credit, or even with fiat money). [[25]](#footnote-26)

Central Banks in several countries have followed the careful attitude shown by authorities in charge of supervising the securities market. Initially, many alerts have been published by Central Banks indicating that cryptocurrencies, generally traded over blockchain platforms, may not be a safe alternative for payments or investments. However, the volume of transactions which have migrated to non-traditional actors such as fintechs and to cryptomoney, and which pose challenges to controlling transborder exchange operations and to prevent schemes which may cause systemic impact to the financial market, have gradually induced Central Banks to consider the idea of creating a national cryptocurrency, which, again, brings blockchain into the scene.[[26]](#footnote-27)

Tax authorities, on their turn, have acknowledged the reality of capital gains which may arise out of transactions of purchase and sale of cryptocurrencies, and have required, for example, that such transactions be declared in annual income tax statements, if total gains in a certain fiscal year have reached certain level.[[27]](#footnote-28) That official treatment may give this sort of transactions indirect, ultimate recognition of the blockchains where they take effect, as the declarations made by taxpayers are subject to later verification, on a possible sampling basis, so they may be accepted *a priori*, based on the assumption of legitimate declarations, or *a posteriori,* in the event the verification of supporting evidence (inclusively, of the blockchain) is checked.

Certainly not the least, data protection authorities, as well as consumer defense entities, also have a say with regards to blockchains. Enrollment in a blockchain may contain identifiable personal data, notwithstanding the encryption, which may preserve anonymity from undesirable access. The enrollment data, which identifies a natural person, may be found either in the main or ancillary structure of the blockchain, or in its ecosystem, as in exchanges which convert cryptocurrencies into nominal, traditional money and vice-versa. The concern with data protection may be alleged in different circumstances, as it was the case of the joint public statement from the data protection authorities and privacy regulators from the UK, Australia, Canada, EU and the US concerning Facebook’s Libra project.[[28]](#footnote-29) Due to prior cases of personal data mishandling by Facebook, such authorities stressed the need for strict compliance with data protection laws by the Libra Association (of which Facebook is a founding member), in its project to launch a cryptocurrency anchored to the Libra Blockchain.[[29]](#footnote-30) Needless to say that protection of personal data might demand, in anti-corruption investigations, a balance between the goal of tacking wrongdoings and the principle of sacrificing privacy the least as possible, which translates into preserving the secrecy of enrollment data at the blockchain and of the *hash* of performed transactions to the maximum possible, considering overall circumstances.

Political disputes might also exploit blockchain and harm the legitimacy of the democratic process. Some countries have shown interest in blockchain based e-voting, e.g. the new U.S. Post Services patent for a voting system[[30]](#footnote-31) and discussions in the Brazilian Congress regarding new instruments for strengthening popular petitioning.[[31]](#footnote-32)

These initiatives raise grave concerns for representative democracies. Failing to secure citizens’ e-identities might result in election frauds difficult to discover and investigate. Moreover, countries are expected to expand these projects to other areas relating to elections, eyeing better transparency and democratic representability. Some countries have political election laws that require a formal registry of candidates, parties and financial information, besides subjecting electoral publicity to judicial control. [[32]](#footnote-33) In this regard, the quality of data inserted in the blockchain is an important issue. Once data is recorded in the blockchain, it becomes immutable and that utility may be exploited by political rivals. Fake users might be created to declare false donations or to store offensive or false content that could be accessed by the public (if it is a public permissionless blockchain, for instance). This possibility seems to require new instruments to prosecute slander or defamation crimes and to guarantee the exercise of an effective right to reply able to prevail over “immutable” blockchain misinformation.

Consumer protection authorities may be concerned with many aspects surrounding blockchain, which coincide with relevant anticorruption agendas. The possibility of supervening change in the rules of a blockchain, which may be detrimental to some participants to the benefit of others, shall certainly attract attention, to the extent it may be viewed as a breach of contract and as misleading advertising. A great deal of cases have involved *nodes* or *super-nodes* which used their prerogatives to divert funds, causing great losses to other participants in the blockchain, and many criminal investigations have taken place in connection therewith.[[33]](#footnote-34)

As seen above, a number of legal developments can be expected from the increasing popularity of blockchains and crypto assets. Those implications have driven discussions on strategies and preferences to be adopted by governments.

All these new concerns result in the necessity of designing a blockchain with legal expectations in mind (“law by design”). As explained by C. Reed, U. Sathyanarayan, S. Ruan and J. Collins, the use of a pure blockchain – meaning a DTL with the least features possible to perform its basic functions – could put rights at risk, rather than protect them.[[34]](#footnote-35) Therefore, extra functionalities should be embedded in the blockchain dynamics in order to prevent harm. These “legal impurities” – as named by the authors – include, inter alia, the registry of identification data (e.g. names, id numbers), imposing legal obligations regarding mandatory entries of an off-chain transaction, to keep the blockchain up-to-date (e.g. ownership of land) or bestowing power for an impartial third party to manage and control the transactions. On the other hand, introducing legal impurities into a blockchain, such as the need for a controlling third-party, could undermine the main benefits of blockchain, and identity disclosure could eliminate the necessary anonymity for voters in an election; the issue of a third-party controller could revive trust discussions over “*quis custodiet ipsos custodes*?”;[[35]](#footnote-36) and inserting indiscriminate footprints on financial transactions involving a national digital currency could harm privacy. In sum, the balance between reaping the benefits of blockchain in the fight against corruption and mitigating abuse in connection with it is fragile.

Therefore, governments shall seek to review traditional formal requirements for the exercise of rights, balancing them with this new technological instrument and its characteristics, in order to profit from its benefits effectively.

1. Blockchain Implementation by Governments: Technological and Political Issues

An impressive number of States and provinces have enacted legislation specifically referring to blockchains. Among others, China, Italy, the United Kingdom, and several U.S. States such as Illinois,[[36]](#footnote-37) have regulated the conditions which render blockchain records legally valid evidence, like transactions performed in traditional fashion. Usually, those conditions comprise the requirement of the use of advanced certified digital signatures and of time-stamping, and such efforts are often rewarded with the right to reversing the burden of proof.

By legislating on the matter, those jurisdictions try to attract businesses which aim to engage into blockchain transactions with appropriate level of comfort. Such kind of normative policy tends to widely spread over all latitudes, irrespective of local government´s political style, assuming the main motivation behind such movement to attract businesses seems to be of strategic socioeconomic development.

As a matter of fact, such goal is closely related to anti-corruption and to anti-money-laundering targets, as it is of the essence of blockchain as a technology to offer trackable, reliable records.

However, public authorities are faced with complexities which may come together with blockchains.

 Besides legal challenges, scholars have identified several technological and political difficulties faced in the implementation of blockchain solutions by the Public Administration.

With regards to technological issues, it is essential to note that blockchain is not actually unhackable and completely immune to tampering as usually raised by hype-inducers. An actor that manages to overtake 51% of the blockchain network’s mining power (i.e., the majority of its nodes or computing power) gains the power to deliberately alter the blockchain and write new fraudulent (albeit verified) transaction records. Smaller networks are especially vulnerable to such attacks,[[37]](#footnote-38) but even open permissionless blockchains, which utilise highly demanding Proof-of-Work (or “mining”) verification protocols, are susceptible to being defrauded through the so-called “51% Rule”.[[38]](#footnote-39)

It is true that attempting this sort of heist against very popular blockchains is likely to be extremely expensive,[[39]](#footnote-40) but skilled crackers have powerful tactics that could circumvent the need for renting mining power. For instance, in the recent past hackers have employed cryptomining malware to launch notorious computer-hijacking cyberattacks against critical IT infrastructure (such as hospital devices),[[40]](#footnote-41) directing their processing power to cryptocurrency mining. Such “cryptojacking” campaigns have most recently targeted European supercomputers and academic data centres.[[41]](#footnote-42) Cryptojackers could also target computers sustaining government “anti-corruption” blockchains in order to divert their processing power to cryptocurrency mining. This would be no frivolous conjecture given that cryptojacking has seen enormous spikes in popularity amongst cyber criminals, increasingly overtaking ransomware, according to reports released by the IBM X-Force[[42]](#footnote-43) and Kaspersky Lab[[43]](#footnote-44) in the past couple of years.

Moreover, using certain Trojan malware, hackers can infect other computers and launch cyberattacks from a network of "zombie botnets",[[44]](#footnote-45) such as large spam campaigns with spambots, or distributed denial-of-service (DDoS) attacks. DDoS attacks are usually launched to prevent legitimate users from accessing a particular system, but more complex DDoSs can co-opt huge zombie botnet networks (millions of computers, potentially) to attack servers from multiple locations and in various ways.[[45]](#footnote-46)

Authorities have contended that the encroached reliance on the Internet and computing that the use of blockchain instils in the public administration could make governments more vulnerable to domestic and foreign cybersecurity threats.[[46]](#footnote-47) States can muster cyber operatives (either from their formal organs of State or in varying degrees of cooperation with non-State actors) to conduct cyber operations against other States’ cyber infrastructure, and thus interfere in other countries’ “anti-corruption” public blockchains.

Blockchain-based software can also be afflicted by bugs. Smart contracts errors have produced high-profile losses due to security bugs which had been inserted in their code (either inadvertently or arbitrarily),[[47]](#footnote-48) and smart contract vulnerabilities are further aggravated when exposed to dynamic environments such as the Internet of Things.[[48]](#footnote-49)

Perhaps Decentralized Autonomous Organizations (DAOs) – or Decentralized Autonomous Corporations – will pose the most stringent emerging challenges to blockchain governance. The major pitfall they may entail does not necessarily reside in their decentralized aspect, but rather in the difficulty to navigate the technology in the long run, as it may require ease of adaptation, not contemplated in its architecture. Indeed, DAOs are structures planned for short to medium-term operations, in which period it is reasonably expected that the predefined tight rules which govern them will be enough, in the absence of centralized, case-by-case decision-making. However, in the event a blockchain is taken for illegitimate purposes, such rigidity of DAOs may preclude any chance for appropriate corrective measures.

A final technological challenge raised by blockchain specialists that should be noted here is the so-called “blockchain trilemma”. The trilemma poses that “blockchain systems can only at most have two of the following three properties”: decentralization (the system’s capacity to run in a scenario where participants only have access to restricted resources, such as a regular laptop), scalability (the system’s capacity to effectively process transactions), and security (the system’s capacity to resist attackers).[[49]](#footnote-50)

Decentralization in blockchain systems is directly proportional to security, but inversely proportional to scalability. That’s why highly decentralized blockchains operating Proof-of-Work consensus are so secure, yet so slow in their transaction validation, given their enormous demand for computing power.[[50]](#footnote-51) For that reason, private and permissioned blockchains are often favoured, being hailed as more energy efficient, faster and more secure, albeit unable to support trustless transactions due to their inherent centralization.[[51]](#footnote-52)

Furthermore, the implementation of anti-corruption blockchain governance must also deal with a series of political impediments.

First, it is paramount to realize that the “trust in code” blockchain inspires cannot completely replace the “trust in gatekeepers”, trust in the people in charge, insofar as there are elements off-chain (e.g. physical assets).[[52]](#footnote-53)

Moreover, some scholars argue that, inasmuch as “trust in government institutions and elected representatives is replaced by trust in the administrators of the blockchain”, “political power on the blockchain is not truly distributed, but rather re-centralized in a ‘tech elite’ — creating a new avenue for corruption through the abuse of their powers.”[[53]](#footnote-54)

By a similar token, governmental blockchains may be structured with off-chain governance (for establishing censorship, or for approving particular deals or events), which may jeopardize anti-corruption efforts. Allegations for adopting the off-chain model may attach to a centralized political style, and to the defence of national sovereignty against foreign monitoring. If such scenario were to materialize, blockchain could be used not for anti-corruption purposes, but rather as a technological tool to legitimate corruption (by resorting to the appealing aesthetics of a technically reliable platform and omitting details on the selected governance model).

Overall, blockchains seem to be powerful tools for combating corruption and money-laundering. However, the various choices available for structuring their governance shall be determinant for the success of such endeavour, and so shall be the underlying political peculiarities of the jurisdictions pursuing their implementation.

1. Conclusions

In the recent past, to combat corruption meant to uphold security. Security against cyberattacks or data leakages which favoured insider trading, and against the by-passing of controls designed to prevent the diversion of funds. In other words, anti-corruption meant secrecy.

Nowadays, to fight against corruption means to grant access, e.g. to blockchains which favour oversight and monitoring aimed at giving visibility to compliance with smart contracts and with proper investment of funds. In other words, anti-corruption means transparency.

Such radical change requires a radical new conscience with regards to IT governance, and more specifically, to blockchain governance. As a matter of fact, blockchains have as their main purpose, precisely, the possibility of building anti-corruption by means of transparency.

Therefore, in designing their governance, amongst multiple options, the models, architectures and features which are most compatible with anti-corruption and anti-money laundering shall be selected.

Such selection can only be properly made in view of contextual circumstances. On-chain governance may be the right choice for obtaining a maximum number of participants who shall validate the transactions in a blockchain, however, if most participants are not well-intended, anti-corruption would probably be best served with off-chain governance, controlled by a smaller group of participants, picked from a reliable group.

Civil society and governments are on the verge of increasing popularization of blockchains, and dissemination of awareness towards digital literacy seems to be imperative at this time.

References

The Economist, “The great chain of being sure about things” (31 October 2015) <https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things> accessed 9 October 2020.

 Per Aarvik, ‘Blockchain as an anticorruption tool: Case examples and introduction to the technology’ (2020) 7 U4 <https://www.cmi.no/publications/7208-blockchain-as-an-anti-corruption-tool-case-examples-and-introduction-to-the-technology> accessed 9 October 2020.

 Mike Orcutt, ‘Once hailed as unhackable, blockchains are now getting hacked’ (2019) MIT Technology Review <https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/> accessed 9 October 2020.

Malcolm Campbell-Verduyn, “Bitcoin, crypto-coins, and global anti-money laundering governance” [2018] 69 Crime Law Soc Change 283-305 <https://doi.org/10.1007/s10611-017-9756-5> accessed 14 October 2020.

The Economist, ‘Governments may be big backers of the blockchain’ (1 June 2017) <https://www.economist.com/business/2017/06/01/governments-may-be-big-backers-of-the-blockchain> accessed 9 October 2020.

Ziya Aliyev and Igbal Safarov, ‘Logos, Mythos and Ethos Of Blockchain: An Integrated Framework For Anti-Corruption’ (2019) OECD Global Anti-Corruption & Integrity Forum 10 <https://www.oecd.org/corruption/integrity-forum/academic-papers/Z-Aliyev-I-Safarov-Blockchain-anti-corruption.pdf> accessed 9 October 2020.

Rachel Davidson Raycraft and Ashley Lannquist, ‘How governments can leverage policy and blockchain technology to stunt public corruption’ (2020) World Economic Forum <https://www.weforum.org/agenda/2020/06/governments-leverage-blockchain-public-procurement-corruption/> accessed 12 October 2020.

World Economic Forum, ‘Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption’ (2020) <http://www3.weforum.org/docs/WEF\_Blockchain\_Government\_Transparency\_Report.pdf> accessed 12 October 2020.

Nikita Aggarwal and Luciano Floridi, 1The Opportunities and Challenges of Blockchain in the Fight against Government Corruption’ (2018) 19th General Activity Report of the Council of Europe Group of States against Corruption (GRECO) <https://www.oii.ox.ac.uk/wp-content/uploads/2019/06/Blockchain-and-Corruption-GRECO-article\_AggarwalFloridi.pdf> accessed 9 October 2020.

Mike Orcutt, ‘Criminals laundered $2.8 billion in 2019 using crypto exchanges, finds a new analysis’ MIT Technology Review <https://www.technologyreview.com/2020/01/16/130843/cryptocurrency-money-laundering-exchanges/> accessed 14 October 2020.

Malcolm Campbell-Verduyn, “Bitcoin, crypto-coins, and global anti-money laundering governance” [2018] 69 Crime Law Soc Change 283, 299 <https://doi.org/10.1007/s10611-017-9756-5> accessed 14 October 2020.

Urszula McCormack et al, ‘“Know Your Token": A guide to participating in token sales’ (2017) KWM <https://www.kwm.com/en/hk/knowledge/insights/know-your-token-guide-on-token-sales-20170731> accessed 10 October 2020.

John Mendiola, ‘Cryptocurrencies in Bankruptcy: A Complex Affair’ (2018) Silk Legal <https://silklegal.com/cryptocurrencies-in-bankruptcy/> accessed 14 October 2020.

Sri Ramamoorti et al, ‘Fraudsters are exploiting blockchains and digital currencies’ (2020) Fraud Magazine <https://www.fraud-magazine.com/article.aspx?id=4295010599> accessed 14 October 2020.

Chris Reed et al, ‘Beyond BitCoin – Legal Impurities and Off-Chain Assets’ (2017) Queen Mary University of London School of Law Legal Studies Research Paper No. 260/2017 <https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3058945> accessed 9 October 2020.

Yaroslav Radziwill, Cyber-Attacks and the Exploitable Imperfections of International Law (1st edn, Koninklijke Brill 2015).

Reza M. Parizi et al, ‘Empirical Vulnerability Analysis of Automated Smart Contracts

Security Testing on Blockchains’ (2018) CASCON’ 18 <https://arxiv.org/pdf/1809.02702.pdf> accessed 13/10/2020.

1. Founder, IDTEC – Instituto de Direito e Tecnologia, gilberto@mda.com.br. [↑](#footnote-ref-2)
2. Associate Researcher, IDTEC – Instituto de Direito e Tecnologia, pedroborgesdecarvalho@hotmail.com. [↑](#footnote-ref-3)
3. Partner, Martins de Almeida - Advogados, fernando@mda.com.br. [↑](#footnote-ref-4)
4. The Economist, “The great chain of being sure about things”(31 October 2015) <https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things> accessed 9 October 2020. [↑](#footnote-ref-5)
5. Per Aarvik, ‘Blockchain as an anticorruption tool: Case examples and introduction to the technology’ (2020) 7 U4 <https://www.cmi.no/publications/7208-blockchain-as-an-anti-corruption-tool-case-examples-and-introduction-to-the-technology> accessed 9 October 2020. [↑](#footnote-ref-6)
6. Mike Orcutt, ‘Once hailed as unhackable, blockchains are now getting hacked’ (2019) MIT Technology Review <https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/> accessed 9 October 2020. [↑](#footnote-ref-7)
7. The Economist, ‘Governments may be big backers of the blockchain’ (1 June 2017) <https://www.economist.com/business/2017/06/01/governments-may-be-big-backers-of-the-blockchain> accessed 9 October 2020. [↑](#footnote-ref-8)
8. Per Aarvik, ‘Blockchain as an anticorruption tool: Case examples and introduction to the technology’ (2020) 7 U4 <https://www.cmi.no/publications/7208-blockchain-as-an-anti-corruption-tool-case-examples-and-introduction-to-the-technology> accessed 9 October 2020. [↑](#footnote-ref-9)
9. Ziya Aliyev and Igbal Safarov, ‘Logos, Mythos and Ethos Of Blockchain: An Integrated Framework For Anti-Corruption’ (2019) OECD Global Anti-Corruption & Integrity Forum 10 <https://www.oecd.org/corruption/integrity-forum/academic-papers/Z-Aliyev-I-Safarov-Blockchain-anti-corruption.pdf> accessed 9 October 2020. [↑](#footnote-ref-10)
10. Ibid. [↑](#footnote-ref-11)
11. “The Amazon Fund is a REDD+ mechanism created to raise donations for non-reimbursable investments in efforts to prevent, monitor and combat deforestation, as well as to promote the preservation and sustainable use in the Brazilian Amazon.”<http://www.amazonfund.gov.br/en/home/> accessed 9 October 2020. [↑](#footnote-ref-12)
12. BNDES, ‘TruBudget’ <https://www.bndes.gov.br/wps/portal/site/home/onde-atuamos/inovacao/trubudget/!ut/p/z1/04\_iUlDg4tKPAFJABpSA0fpReYllmemJJZn5eYk5-hH6kVFm8eaB7s4ejiaGPv4-vo4GgZ6GviHB\_qbGoUaG-l76UfgVFGQHKgIAUQT47A!!/#modalCurtir> accessed 9 October 2020. [↑](#footnote-ref-13)
13. Rachel Davidson Raycraft and Ashley Lannquist, ‘How governments can leverage policy and blockchain technology to stunt public corruption’ (2020) World Economic Forum <https://www.weforum.org/agenda/2020/06/governments-leverage-blockchain-public-procurement-corruption/> accessed 12 October 2020. [↑](#footnote-ref-14)
14. World Economic Forum, ‘Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption’ (2020) <http://www3.weforum.org/docs/WEF\_Blockchain\_Government\_Transparency\_Report.pdf> accessed 12 October 2020. [↑](#footnote-ref-15)
15. UNODC, “United Nations Convention against Corruption” <https://www.unodc.org/unodc/en/treaties/CAC/> accessed 9 October 2020. [↑](#footnote-ref-16)
16. Nikita Aggarwal and Luciano Floridi, 1The Opportunities and Challenges of Blockchain in the Fight against Government Corruption’ (2018) 19th General Activity Report of the Council of Europe Group of States against Corruption (GRECO) < https://www.oii.ox.ac.uk/wp-content/uploads/2019/06/Blockchain-and-Corruption-GRECO-article\_AggarwalFloridi.pdf> accessed 9 October 2020. [↑](#footnote-ref-17)
17. Ibid. [↑](#footnote-ref-18)
18. Per Aarvik, ‘Blockchain as an anticorruption tool: Case examples and introduction to the technology’ [2020] 7 U4 <https://www.cmi.no/publications/7208-blockchain-as-an-anti-corruption-tool-case-examples-and-introduction-to-the-technology> accessed 9 October 2020. [↑](#footnote-ref-19)
19. World Economic Forum, ‘Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption’ (2020) <http://www3.weforum.org/docs/WEF\_Blockchain\_Government\_Transparency\_Report.pdf> accessed 12 October 2020. [↑](#footnote-ref-20)
20. BNDES, ‘TruBudget’ <https://www.bndes.gov.br/wps/portal/site/home/onde-atuamos/inovacao/trubudget> accessed 13 October 2020; KfW, ‘TruBudget’ <https://openkfw.github.io/trubudget-website/> accessed 13 October 2020. [↑](#footnote-ref-21)
21. Generally, a token is an intangible asset utilising blockchain technology. It typically entitles the token holder to a bundle of rights (and possibly liabilities) set out in smart contracts and other relevant documentation, such as an offering document or a whitepaper (or both). Urszula McCormack et al, ‘“Know Your Token": A guide to participating in token sales’(2017) KWM <https://www.kwm.com/en/hk/knowledge/insights/know-your-token-guide-on-token-sales-20170731> accessed 10 October 2020. [↑](#footnote-ref-22)
22. Many individuals, hedge funds and businesses are potentially purchasing tokens for projects that may not be technically possible, economically feasible – or, frankly, that may not ever happen. Additionally, an increasing number of token sales are attracting adverse regulatory attention, including under securities laws (United States) and anti-Ponzi scheme laws (United States and United Kingdom). Hacking and disputes are also increasingly prevalent. Urszula McCormack et al, ‘“Know Your Token": A guide to participating in token sales’(2017) KWM <https://www.kwm.com/en/hk/knowledge/insights/know-your-token-guide-on-token-sales-20170731> accessed 10 October 2020. [↑](#footnote-ref-23)
23. See, for instance: Shipkevich, ‘New York Money Transmitter License and Bitcoin License’ <https://moneytransmitterlaw.com/state-laws/new-york-bitcoin-law-bitlicense/> 13 October 2020; Corinne Chen, ‘The Ins and Outs of Operating a Crypto Business in New York’ (2019) Romano Law <https://www.romanolaw.com/2019/03/08/operating-a-crypto-business-in-new-york/> accessed 13 October 2020. [↑](#footnote-ref-24)
24. Mike Orcutt, ‘Criminals laundered $2.8 billion in 2019 using crypto exchanges, finds a new analysis’ MIT Technology Review <https://www.technologyreview.com/2020/01/16/130843/cryptocurrency-money-laundering-exchanges/> accessed 14 October 2020. However, it has been argued that “the threats CCs pose to global AML efforts are presently more theoretical than actual. Despite at times sensationalistic media coverage, little evidence directly implicates CCs in widespread money laundering.” Malcolm Campbell-Verduyn, “Bitcoin, crypto-coins, and global anti-money laundering governance” [2018] 69 Crime Law Soc Change 283, 299 <https://doi.org/10.1007/s10611-017-9756-5> accessed 14 October 2020. [↑](#footnote-ref-25)
25. John Mendiola, ‘Cryptocurrencies in Bankruptcy: A Complex Affair’ (2018) Silk Legal <https://silklegal.com/cryptocurrencies-in-bankruptcy/> accessed 14 October 2020. [↑](#footnote-ref-26)
26. See: Ryan Browne, ‘Central banks are considering their own digital currencies – this is what they could look like’ (9 October 2020) CNBC <https://www.cnbc.com/2020/10/09/central-banks-lay-out-a-framework-for-digital-currencies.html> accessed 14 October 2020. [↑](#footnote-ref-27)
27. See: Chandan Lodha and Shehan Chandrasekera, ‘Cryptocurrency & Bitcoin Tax Guide (2020 Edition)’ (2019) Coin Tracker <https://www.cointracker.io/blog/crypto-tax-guide> accessed 14 October 2020. [↑](#footnote-ref-28)
28. OAIC, “OAIC joins with global privacy regulators to call for more information from the Libra Network” (6 August 2019) <https://www.oaic.gov.au/updates/news-and-media/global-privacy-expectations-of-the-libra-network/> accessed 14 October 2020. [↑](#footnote-ref-29)
29. European Data Protection Supervisor, “Joint statement on global privacy expectations of the Libra network” (5 August 2019) <https://edps.europa.eu/data-protection/our-work/publications/other-documents/joint-statement-global-privacy-expectations\_en> accessed 14 October 2020. [↑](#footnote-ref-30)
30. Vipin Bharathan, ‘US Postal Service Files A Patent For Voting System Combining Mail And A Blockchain’ (20 September 2020) <https://www.forbes.com/sites/vipinbharathan/2020/09/20/us-postal-service-files-a-patent-for--voting-system-combining-mail-and-a-blockchain/#b204b763336f> accessed 14 October 2020. [↑](#footnote-ref-31)
31. Joon Ian Wong, ‘Brazil may write new laws with data stored on the ethereum blockchain’ (5 January 2018) Quartz <https://qz.com/1163660/brazil-may-write-new-laws-based-on-data-stored-on-the-ethereum-blockchain/> accessed 14 October 2020; Consultoria Legislativa da Câmara dos Deputados, ‘Reforma Política: Aspectos técnicos das proposições’ <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/reforma-politica/documentos/outros-documentos/reforma-politica-aspectos-tecnicos-das-proposicoes> 14 October 2020. [↑](#footnote-ref-32)
32. For instance, the Brazilian electoral legislation: Planalto, ‘Código Eleitoral’ (1965) <http://www.planalto.gov.br/ccivil\_03/Leis/L4737compilado.htm> accessed 14 October 2020. [↑](#footnote-ref-33)
33. Sri Ramamoorti et al, ‘Fraudsters are exploiting blockchains and digital currencies’ (2020) Fraud Magazine <https://www.fraud-magazine.com/article.aspx?id=4295010599> accessed 14 October 2020. [↑](#footnote-ref-34)
34. *Primus*, data registered on the ledger with no existence on the real world would disappear, if the system ceased to operate, in detriment of their legal owner. *Secundus*, the distributed nature of the ledger would prevent authorities from intervening to change records. Chris Reed et al, ‘Beyond BitCoin – Legal Impurities and Off-Chain Assets’ (2017) Queen Mary University of London School of Law Legal Studies Research Paper No. 260/2017 <https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3058945> accessed 9 October 2020. [↑](#footnote-ref-35)
35. “Who will guard the guard themselves?” [↑](#footnote-ref-36)
36. David Zaslowsky, ‘Illinois Becomes Latest US State to Recognize Blockchain’ (2020) Lexology <https://www.lexology.com/library/detail.aspx?g=2cfcdcd9-2d90-4898-914a-44e0ff3a5a99> accessed 14 October 2020. [↑](#footnote-ref-37)
37. Cipher, ‘How Blockchain Can Be Hacked: The 51% Rule and More’ <https://cipher.com/blog/how-blockchain-can-be-hacked-the-51-rule-and-more/#:~:text=The%2051%25%20Rule%20refers%20to,yet%20personally%20validated%20transactions%20records.&text=If%20trust%20is%20lost%20in,then%20the%20currency%20might%20crash.> accessed 13/10/2020. [↑](#footnote-ref-38)
38. Mike Orcutt, ‘Once hailed as unhackable, blockchains are now getting hacked’ (2019) MIT Technology Review <https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/> accessed 13/10/2020. [↑](#footnote-ref-39)
39. Ibid. [↑](#footnote-ref-40)
40. Rod Piechowski, ‘Cryptojacking Rises in Popularity and Threatens Healthcare Productivity’ (2018) HealthTech <https://healthtechmagazine.net/article/2018/09/cryptojacking-rises-popularity-and-threatens-healthcare-productivity> accessed 13/10/2020. [↑](#footnote-ref-41)
41. BBC, ‘Europe's supercomputers hijacked by attackers for crypto mining’ (18 May 2020) <https://www.bbc.com/news/technology-52709660> accessed 13 October 2020. [↑](#footnote-ref-42)
42. IBM, ‘IBM X-Force Report: Ransomware Doesn't Pay in 2018 as Cybercriminals Turn to Cryptojacking for Profit’ (2019) <https://newsroom.ibm.com/2019-02-26-IBM-X-Force-Report-Ransomware-Doesnt-Pay-in-2018-as-Cybercriminals-Turn-to-Cryptojacking-for-Profit> accessed 13 October 2020. [↑](#footnote-ref-43)
43. Kaspersky, ‘Cryptominers gain ground’ (2018) <https://www.kaspersky.com/blog/cryptominers-almost-double/22898/> accessed 13 October 2020. [↑](#footnote-ref-44)
44. KASPERSY. ‘What is a Botnet? – Definition’. <https://www.kaspersky.com/resource-center/threats/botnet-attacks> accessed 9/10/2020. [↑](#footnote-ref-45)
45. Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperfections of International Law* (1st edn, Koninklijke Brill 2015) 328. [↑](#footnote-ref-46)
46. Nikita Aggarwal and Luciano Floridi, ‘The Opportunities and Challenges of Blockchain in the Fight against Government Corruption’ (2018) 19th General Activity Report of the Council of Europe Group of States against Corruption (GRECO) <https://www.oii.ox.ac.uk/wp-content/uploads/2019/06/Blockchain-and-Corruption-GRECO-article\_AggarwalFloridi.pdf> accessed 9 October 2020. [↑](#footnote-ref-47)
47. Reza M. Parizi et al, ‘Empirical Vulnerability Analysis of Automated Smart Contracts

Security Testing on Blockchains’ (2018) CASCON’ 18 <https://arxiv.org/pdf/1809.02702.pdf> accessed 13/10/2020. [↑](#footnote-ref-48)
48. Ibid. [↑](#footnote-ref-49)
49. Ethereum Wiki, ‘On sharding blockchains FAQs’ <https://eth.wiki/sharding/Sharding-FAQs> accessed 14 October 2020. See also: Joseph Abadi and Markus Brunnermeier, ‘Blockchain Economics’ (2018) NBER Working Paper Series < https://www.nber.org/papers/w25407.pdf> accessed 14/10/2020. [↑](#footnote-ref-50)
50. Nikita Aggarwal and Luciano Floridi, ‘The Opportunities and Challenges of Blockchain in the Fight against Government Corruption’ (2018) 19th General Activity Report of the Council of Europe Group of States against Corruption (GRECO) <https://www.oii.ox.ac.uk/wp-content/uploads/2019/06/Blockchain-and-Corruption-GRECO-article\_AggarwalFloridi.pdf> accessed 9 October 2020. [↑](#footnote-ref-51)
51. Ibid. [↑](#footnote-ref-52)
52. Per Aarvik, ‘Blockchain as an anticorruption tool: Case examples and introduction to the technology’ [2020] 7 U4 <https://www.cmi.no/publications/7208-blockchain-as-an-anti-corruption-tool-case-examples-and-introduction-to-the-technology> accessed 9 October 2020. [↑](#footnote-ref-53)
53. Nikita Aggarwal and Luciano Floridi, ‘The Opportunities and Challenges of Blockchain in the Fight against Government Corruption’ (2018) 19th General Activity Report of the Council of Europe Group of States against Corruption (GRECO) <https://www.oii.ox.ac.uk/wp-content/uploads/2019/06/Blockchain-and-Corruption-GRECO-article\_AggarwalFloridi.pdf> accessed 9 October 2020. [↑](#footnote-ref-54)