Feature Article in the 19th General Activity Report (2018) of the Council of Europe Group of States against Corruption (GRECO), adopted by GRECO 82 (18-22 March 2019)

The Opportunities and Challenges of Blockchain in the Fight against Government Corruption

Nikita Aggarwal and Luciano Floridi

Digital Ethics Lab, Oxford Internet Institute

Broadly defined, government corruption is the abuse of public power for private gain. It can assume various forms, including bribery, embezzlement, cronyism, and electoral fraud. At root, however, government corruption is a problem of *trust*. Corrupt politicians abuse the powers entrusted to them by the electorate (the principal-agent problem). Politicians often resort to corruption out of a lack of trust that other politicians will abstain from it (the collective action problem). Corruption breeds greater mistrust in elected officials amongst the public. The problem of trust is compounded where a lack of transparency and asymmetric information impede effective control over the exercise of public powers.

The Blockchain Opportunity

The question arises whether distributed ledger technology (DLT), such as blockchain, could aid the fight against government corruption. In brief, a distributed ledger is a distributed database, held across a peer-to-peer network of computer devices, or 'nodes'. Each node in the network holds an identical copy of the database, and independently validates and records transactions on the network, using a combination of economic incentives, cryptographic proofs, and an algorithmic consensus mechanism. Blockchain is a type of DLT that organizes transaction records in a chronological, timestamped chain of 'blocks'. It is open source and publicly accessible (where 'permissionless'): transactions are transparent (although pseudonymized), and anyone can participate in the blockchain.[1]

There are many potential advantages of blockchain. These include greater transparency and security of data, due to the use of encryption, cryptography, and its distributed nature, which makes the network less vulnerable to the failure of a single node. Blockchain is also effectively tamper-proof: since each record is linked to all previous records on the ledger, it cannot be altered without repeating the costly and computationally impractical process of validating all other blocks in the chain. However, the core opportunity of blockchain is that it facilitates 'trustless' transactions. Unrelated parties can reach agreement and coordinate their activities without needing to know or trust one another, and without requiring a central coordinating authority.

Where government corruption is rooted in an abuse of trust by elected representatives, it stands to reason that corruption would be eradicated in a blockchain-based government, as power is not entrusted to any centralized institutions. Indeed, the original objective of the

[1] In contrast, 'permissioned' and 'private' blockchains restrict participation (write-controlled) and/or visibility (read-controlled). Whilst initially conceived to facilitate peer-to-peer financial transactions using Bitcoin, blockchain has since been adapted to support a much wider range of P2P transactions. For example, Ethereum is a public, permissioned blockchain-based platform that facilitates non-financial transactions, notably Smart Contracts and Distributed Applications (see <https://www.ethereum.org>).

Bitcoin blockchain was to disintermediate the financial institutions and 'trusted elites' that many blamed for causing the 2008 financial crisis.[2] For now, the cyberlibertarian vision of a fully distributed, 'techno-democracy' remains an unlikely prospect. In the meantime, however, blockchain offers to reduce government corruption by *augmenting*, rather than *substituting*, the existing institutions and processes of government.

For example, blockchain-based voting platforms could reduce the scope for corruption in elections by providing a tamper-proof record of votes and voters that does not rely on verification by a third party (e.g. vote counters, local and federal election authorities). The greater transparency and efficiency afforded by such platforms also promises to boost voter turnout, and to increase trust in the democratic process, particularly in countries where election results are often contested. Blockchain-based voting platforms have recently been piloted in Japan, Switzerland and the US (West Virginia), amongst others.[3]

Similarly, countries such as Brazil, Honduras, Ukraine and Georgia are experimenting with blockchain-based land registries, which provide greater legal certainty to land titles, and reduce the scope for corruption due to double-allocation of land and forged land deeds.[4] Likewise, blockchain-based health care, identity management, public procurement and contracting, refugee aid delivery, and social welfare payment systems, all stand to reduce the scope for government corruption.

Five Challenges of Blockchain

Yet blockchain is not a panacea. There are at least five salient challenges. The first of these concerns the incentives of incumbent governments to adopt blockchain technology. Governments may be reluctant to create an immutable and transparent record of their activities if this constrains their scope for private gain through corruption. As such, the promise of blockchain depends on the strength and integrity of a country's existing institutions to deploy the technology in the first instance. Moreover, the effectiveness of a blockchain-based platform depends on the wider regulatory and political context, as well as the strength of a country's (digital) infrastructure — the Internet, distributed and cloud computing, electricity supply, and digitized data, all of which power the blockchain, as well as the technological literacy of its population.

Indeed, early evidence from blockchain-based land registries points to greater success in countries with strong institutions and infrastructure — such as Georgia, where most land is already documented and the property registration process relatively streamlined and digitally-enabled. Blockchain itself does not provide a mechanism for recognizing land rights, nor for digitizing or ensuring the accuracy of data relating to land rights. Very few assets are entirely digitally-native, living exclusively on the blockchain, but rather depend on both real and virtual world institutions and mechanisms. Clearly, blockchain works best by becoming part

[2] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) <https://bitcoin.org/bitcoin.pdf>.

[3] See <https://blockchan.ge/curatedexamples.html?sector=elections-voting>.

[4] See for example <https://exonum.com/napr>.

of a virtuous cycle through which a not-very corrupt government introduces blockchain to reduce corruption, which in turn incentivizes greater uptake of blockchain, and further reduces corruption.

The second challenge relates to the governance and politics of blockchain technology itself. In a blockchain-based system, trust in government institutions and elected representatives is replaced by trust in the administrators of the blockchain: the network of nodes, source code, cryptographic tools, consensus mechanisms and private actors through which the blockchain operates. The operation of a blockchain-based platform is thus subject to the decisions of its developers, for example to upgrade the code or alter the consensus mechanism (a so-called 'hard' or 'soft fork'), as well as the motivations of node operators in validating and recording transactions.[5] It is noteworthy that network power on the Bitcoin blockchain is highly concentrated: by some accounts, as few as 6 groups of nodes ('mining pools') record or 'mine' 80% of the transactions (as well as being geographically concentrated, in China).[6] Likewise, the number of validation nodes is steadily falling, and becoming increasingly concentrated in the US and Europe.[7]

As such, 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. Re-centralization furthermore reintroduces the security risks that are mitigated through decentralization and distribution of power. And, although cryptographic tools and algorithmic consensus mechanisms offer security advantages, blockchain is not failsafe to an attack from malicious actors. This could occur either within the blockchain (for example, if attacker nodes take control of a majority of the computational power and cooperate to attack the network), or via software clients, third-party applications (such as cryptocurrency wallets) and smart contracts —as evidenced by the 2016 hack of the DAO, an investment fund operating on the Ethereum blockchain. More generally, the greater dependence on the Internet and computing entailed by the use of blockchain elevates cybersecurity risks in public administration.

The third challenge concerns an evident trade-off between decentralization or distribution, security, and scalability: the so-called blockchain 'trilemma'.[8] The more decentralized the blockchain is, the less scalable it is. For example, the highly decentralized Bitcoin blockchain is a slow system for validating transactions (through the Proof-of-Work consensus mechanism), and requires a considerable amount of computing power, making it less scalable.[9] These trade-offs have given rise to different forms of blockchain — notably, private

[5] See <https://en.wikipedia.org/wiki/Fork_(blockchain)>.

[6] See Kaiser, Jurado and Ledger, 'The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin' (2018), <https://arxiv.org/abs/1810.02466>, at 2.

[7] See <https://bitnodes.earn.com>.

[8] Vitalik Buterin (Ethereum co-founder) <https://github.com/ethereum/wiki/wiki/Sharding-FAQ>.

[9] Compare transaction processing on the Bitcoin and Ethereum blockchains (up to 15 transactions processed per second) with a system such as Visa (24,000 transactions per second).

and permissioned blockchains, which are typically faster, more energy efficient and secure than public blockchains. However, these blockchains are more centralized and as such do not support truly 'trustless' transactions. Changes to the blockchain designed to increase scalability (for example, through a hard fork) also raise governance questions relating to trust in miners and control of the network.

Fourthly, the use of cryptocurrencies, which run on DLT, give rise to a parallel set of public governance risks. Notably, the relative anonymity afforded by certain cryptocurrencies — such as Bitcoin and Ether— makes them more susceptible to use for money laundering and financing illicit activities, such as drug trafficking and terrorism, and frustrates regulatory efforts to prosecute them. Likewise, blockchain-based cryptocurrencies could themselves facilitate government corruption — for example, allowing elected officials to obfuscate more easily the identity of political donors and the sources of campaign funds. These concerns could, however, be partially addressed through the use of non-anonymous cryptocurrencies (such as the stablecoin Saga), and private or permissioned blockchains.[10]

Finally, there remains considerable legal and regulatory uncertainty over blockchain-based transactions. Inter alia, the difficulty of altering the blockchain makes it unclear how the 'right to erasure' under EU data privacy law will be enforced (Article 17, GDPR). Additionally, the distributed nature of the blockchain gives rise to conflict of laws questions, as the nodes are located across several different jurisdictions. Likewise, it remains unclear who will be held liable when the network malfunctions.

Conclusion

The distributed, encrypted and immutable nature of DLT, such as blockchain, makes it more difficult for centralized government institutions to regulate and control. Paradoxically, this presents both opportunities and challenges in the fight against government corruption, as this article has highlighted. Moreover, blockchain is not a one-size-fits-all solution. Different types of blockchain (public versus private/federated, permissioned versus permissionless) will be more or less suitable for different use cases. In some contexts, more fundamental infrastructural needs — for example, Internet access and digital identity — will need to be resolved first, before the deployment of blockchain and DLT-based platforms can be considered. At this nascent stage in the technology's growth, governments are advised to adopt an attitude of cautious optimism: embracing pilot studies and investing more in understanding blockchain technology, whilst remaining alert to its risks and challenges.

***

The Digital Ethics Lab is an interdisciplinary research lab based at the Oxford Internet Institute, University of Oxford. Its aim is to identify the benefits and enhance the positive opportunities of digital innovation as a force for good, and avoid or mitigate its risks and shortcomings.

[10] See <https://www.saga.org>.