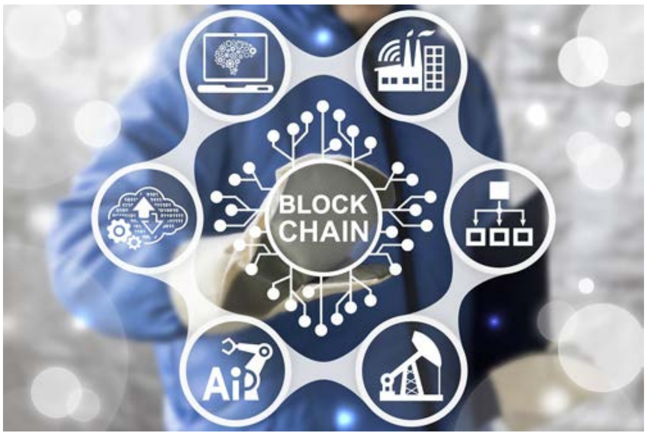
AT A GLANCE

Scientific Foresight: What if?

European Parliament

What if blockchain offered a way to reconcile privacy with transparency?

One of the most appealing aspects of blockchain technology is the degree of transparency that it can provide. Blockchain has the potential to improve supply chains and clinical trials, enforce the law, enable responsible consumption, and enhance democratic governance, through traceability of information as a means of ensuring that nothing is unduly modified. The level of transparency that blockchain affords adds a degree of accountability that has not existed to date. At the same time, one of the most appealing aspects of blockchain technology is the degree of privacy that it can provide. How could blockchain safeguard the rights to privacy and control over our data, whilst promoting data transparency?



© wladimir1804 / Fotolia.

Enabling transparency of information is one of the biggest promises of blockchain technology, which provides a fully auditable and valid ledger of transactions. Blockchain is supposed to be a transparency machine in which anyone can join the network and, as a result, view all information on that network. Through the necessary encryption and control mechanisms, blockchain safeguards transparency by storing information in such a way that it cannot be altered without recording the changes made. Thanks to the ability of the technology to prove – in a cryptographic way – to third parties that data is immutable, it has the potential to make payments more transparent and systems more accountable. The terms of every transaction remain irrevocable, being open for inspection to everyone or to authorised auditors in ways never witnessed before. In the case of crypto currencies, the transparency of blockchain offers users an opportunity to look through the history of all transactions. The transparency and accountability that blockchain technologies afford could play a role in limiting undue online surveillance, censorship and human rights abuses. For instance, in the case of an entirely public blockchain, all information becomes public: anyone can see all data stored as they are supposed to be both accessible for everyone and transparent, so as to prevent data manipulation. Blockchain could enable consumers to track anything across the supply chain, and to know exactly what their food contains, whether it is organic and fair trade, and whether the goods they buy are genuine or produced with respect for workers' rights. Via an audit log that is accessible through the government's portal and secures their privacy, people can also track all government-related transactions that use their personal information. As transparency is fundamentally concerned with the quality of being clear, obvious and understandable without doubt or ambiguity, improving accountability through blockchain will help us build an inclusive, transparent, and accountable digital economy.

Challenges to transparency

Transparency in the context of blockchain is neither absolute nor unconditional. In fact, blockchain offers various degrees of transparency depending on the domain of application. For example, in the case of bitcoin transactions, data is shared publicly in a permissionless ledger (a format allowing any user to join the network and start mining), which offers transparency. However, in the case of permissioned blockchain, a participant needs permission to transact with another network participant, and transactions take place in a closed ecosystem, where transaction data remain confidential and participants are known and authenticated. In that respect, the transparency potential of blockchain may be limited as a result of the need to ensure the privacy

EPRS | European Parliamentary Research Service
Author: Mihalis Kritikos, Scientific Foresight Unit (STOA)
PE 624.254 – September 2018

of the parties through powerful cryptography, meaning that linking public addresses to individual users is particularly difficult to achieve. The encryption and immutability features of blockchain indicate that certain types of blockchain prioritise privacy and confidentiality at the expense of transparency. The operation of blockchain as a carrier of privacy and transparency innovations for financial transactions raises the following questions: Can end-users be treated as controllers? Can a party be both a controller for certain data and a processor for other data? How does Article 22 of the General Data Protection Regulation (GDPR), which grants data subjects protection against the automated processing of their information, affect smart contracts?

The enforcement of the GDPR on public and permissionless blockchains may prove challenging from a legal standpoint, given that the mere idea of a right to erasure goes against everything blockchain stands for. After a public key and the associated transactions are identified, there is no way to 'erase' the information, which is now part of the blockchain and hence public knowledge. In addition, decentralised blockchains do not rely on central authorities to process data and, therefore, the idea of data controllers that can erase personal data from the blockchain is not straightforward. Questions have also been raised about how it will be possible for blockchains to adhere to the principle of data minimisation, given that data are continuously added to the chain without the possibility of deletion or editing, and blockchains are ever growing. Additionally, the efficiency and sustainability of this new technology-driven accountability paradigm depends on its capacity to handle the following challenge of incompatibility: to apply the GDPR, which is primarily designed for centralised data collection, storage and processing, in a ground-breaking technological domain that is inherently decentralised and features only a limited number of central intermediaries.

How will European policy-makers handle transparency-related challenges?

European policy-makers are currently focused on the identification of technical and legal solutions for safeguarding an effective co-existence of privacy and transparency. More concretely, privacy concerns arising from the transparency features of blockchain can be mitigated by end-to-end encryption of the communication, requiring private and public keys, and by finding alternatives to erasure. Rather than using a single key for encryption and decryption, separate keys (a public and a private key) are used, allowing users to send their public key to anyone, without worrying that someone else will gain access to their private key. Technology-based and legal solutions are needed for the development of privacy-protecting blockchains by design, which could enable an extra layer of security for off-chain transactions. These might include combining public blockchain with trusted computing enclaves to enhance privacy and security; limiting who can join the blockchain network to 'trusted' nodes; encrypting the data on the blockchain; and safeguarding the robustness of anonymisation techniques. These solutions will not only facilitate the protection of the privacy of sensitive health data, but could also pave the way for the design of a 'permissioned' blockchain network, shared between Member States, that would store personal data in a secure and flexible manner.

Any political or legal initiative in the privacy domain needs to define the terms of use and access of permissioned and/or hybrid blockchains, but also resolve the aforementioned tensions between the GDPR and blockchain. Given that blockchain introduces an IT-based paradigm of high social value that could lay the foundation for a true democratisation of data through its transparency features, all EU legal initiatives in this field also need to deal with the opaque character of algorithms that are required for the operation of blockchain protocols in an effective way. There are growing social expectations of algorithmic transparency and oversight, and of making automated decision systems accountable, more transparent and governable, possibly by outfitting them with new technological toolkits that could verify that automated decisions comply with key standards of legal fairness. Ensuring accountability through algorithm impact assessments (AIA), auditing and certification should also be part of all relevant political and legal initiatives in this field.

Last but not least, legislators, when drafting rules on providing data subjects with control over their data and requesting transparency of blockchain operations, need to keep in mind that this novel technology is still very incomprehensible. Given that blockchain is still in its development phase, any legal solution would not only potentially shape the technological trajectory itself but would also reconcile privacy with transparency, in a creative and efficient manner.

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

STOA@ep.europa.eu (contact) http://www.europarl.europa.eu/stoa http://www.europarl.europa.eu/thinktank (internet) http://epthinktank.eu (blog)