Valiente, María-Cruz; Tschorsch, Florian

Article

Blockchain-based technologies

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Valiente, María-Cruz; Tschorsch, Florian (2021) : Blockchain-based technologies, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 2, pp. 1-6, https://doi.org/10.14763/2021.2.1552

This Version is available at:
https://hdl.handle.net/10419/235956

INTERNET POLICY REVIEW
Journal on internet regulation

Blockchain-based technologies
Volume 10 **Issue** 2

GLOSSARY ENTRY

OPEN ACCESS

PEER REVIEWED

Blockchain-based technologies

María-Cruz Valiente *Universidad Complutense de Madrid* mcvaliente@ucm.es
Florian Tschorsch *Technical University Berlin* florian.tschorsch@tu-berlin.de

DOI: https://doi.org/10.14763/2021.2.1552

Published: 20 April 2021
Received: 18 November 2020 **Accepted:** 30 November 2020

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Valiente, M.-C. & Tschorsch, F. (2021). Blockchain-based technologies. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1552

Keywords: Blockchain

Abstract: Blockchain-based technologies can be understood as a distributed network of computers, ideally organised in a decentralised way, mutually agreeing on a common state while tolerating failures (incl. malicious behaviour) to some extent.

This article belongs to the **Glossary of decentralised technosocial systems**, a special section of *Internet Policy Review*.

Definition

Blockchain-based technologies can be understood as a distributed network of computers, ideally organised in a decentralised way, mutually agreeing on a common state while tolerating failures (incl. malicious behaviour) to some extent.

Origin and evolution of the term

In recent years, blockchain(-based) technologies have attracted the interest of a wide variety of actors and stimulated a large amount of academic research. The topic is increasingly part of academic and public debates. Unfortunately, there is neither a formal definition nor a common understanding of what *blockchain-based technologies* means, that is, what properties and technical features the term implies. Therefore, a good understanding of the term *blockchain* is needed to design, develop, and manage such technologies effectively, especially also for researchers and society concerned with the intention to use and their actual usage. The main question that needs to be answered is: what fundamental requirements have to be met in order for a proposal or solution to be classified as blockchain technology?

According to the literature, there are several concepts and aspects to be taken into account when defining the inherent properties associated with blockchain technologies. The main attempts to define the notion of blockchain technologies can be summarised as follows: a network composed of decentralised databases or distributed computing nodes sharing a global data structure to record chronologically connected blocks of transactions, which use cryptographic techniques and distributed consensus that lead to secure, transparent and immutable distributed ledgers (García-Barriocanal et al., 2017, p. 39; Governatori et al., 2018, pp. 385 ff; Iansiti & Lakhani, 2017). The network executes smart contracts (i.e., a programme) as transactions (Staples et al., 2017), and should provide trust, anonymity, security, and data integrity without requiring any third party controlling the process (Janssen et al., 2020). .

The complex relationships between all the aspects concerned with governance, business information (namely business processes), and technical issues that must be taken into account in the adoption process of blockchain technologies are presented in the work of Janssen et al. (2020).

In summary, we observe that the meaning of the word *blockchain* is and remains controversial. It has no standard technical definition. Rather it is used as a loose umbrella term to refer to systems that bear resemblance to the Bitcoin protocol, or more generally the Nakamoto Consensus (Narayanan & Clark, 2017). At the same time, blockchain technologies are influenced by other research areas and existing technologies, e.g., peer-to-peer networks, fault tolerance, distributed timestamping, and cryptography (Tschorsch & Scheuermann, 2016; Narayanan & Clark, 2017). In order to facilitate an unambiguous understanding of blockchains, they have been classified as a subset of *Distributed Ledger Technologies* (DLTs). Hence, DLT becomes the technical accurate term, referring to consensus of replicated data in a peer-to-peer network.

Issues currently associated with the term

Blockchain technology originally emerged to support new forms of digital money. It was first proposed in the birth of *Bitcoin* by Satoshi Nakamoto in 2008 and presented at a time where the trust in banks and other financial institutions was at a low due to the world-wide financial crisis. In short, Bitcoin can be defined as the first and (at the time of writing) most popular cryptocurrency. It consists of a digital currency (i.e., bitcoin) and online payments (i.e., the Bitcoin network), which operates independently of a central bank (Swan, 2015). In this way, Karlstrøm (2014) defends that payments performed through Bitcoin avoid the services of a middleman, such as commercial banks, lawyers, and notaries, which destabilises adopted state monopolies on the production and verification of money and transactions. Since the blockchain records every single change made in the network (first and foremost to reject double spends), Bitcoin probably became the most transparent financial system. In the following, we look beyond Bitcoin to convey the technological diversity with respect to blockchains. By doing this, we intend to emphasise the difficulties to capture this technology in a single definition.

By the end of 2013, Vitalik Buterin created *Ethereum*, a general-purpose blockchain-based distributed computing technology (Buterin, 2014). Using Ethereum, developers can create web applications known as *decentralized applications* (dapps) without knowledge about the underlying mechanisms, such as peer-to-peer networks and blockchain in general.

However, eleven years have passed since the invention of Bitcoin and seven years since Ethereum was first presented and no widely accepted definition for blockchain technology exists yet. A prime example to highlight the ambiguity of the term *blockchain* is the tension between so-called *permissionless* and *permis-*

sioned blockchains. *Permissionless blockchains*, such as Bitcoin, do not require a permission to contribute to the consensus. The permission to generate a new block is organised in a completely decentralised manner. In contrast, permissioned blockchains, such as Hyperledger, define a closed group of nodes, who can contribute to the consensus. This group is often determined by a central entity. In the literature, both are referred to as blockchains. While permissionless blockchains are clearly in line with the Nakamoto consensus, permissioned blockchains exhibit more resemblance to the area of Byzantine fault tolerance (Lamport, Shostak, & Pease, 2019). Agreement protocols offering this particular type of fault tolerance typically require a well-defined distributed system. Such ambiguities between permissionless and permissioned blockchains and many more misconceptions motivated articles that explore suitable application domains of blockchains by trying to give an answer to the question "do you need a blockchain?" (Wüst & Gervais, 2018). This dissonance clearly emphasises the issues that we observe with the definition of the term blockchain.

Conclusion

Blockchains are supposed to offer diverse technological possibilities. With a range of use cases that go far beyond virtual currencies applications, they are proposed as a technological means to achieve trust, security, and privacy. After more than a decade of research and experimentation, however, the utility of blockchains seems to be circumscribed to few use cases, with cryptocurrencies still representing their most relevant application.

The value proposition of blockchain seems to be that of offering a global, open and censorship-resistant network for peer-to-peer transactions. Its key innovation is the deployment of consensus algorithms that offer reasonable security in open peer-to-peer networks. The main characteristics attributed to blockchain-based technologies include: (i) decentralised consensus, i.e., no central entity or third party is responsible for decision-making; (ii) immutable archive, i.e., an ordered list of transactions that cannot be removed or altered; (iii) transparency and verifiability, i.e., all recorded entries can be accessed and verified locally; (iv) resilience to failure, i.e., the system can handle Byzantine failure up to a certain threshold.

The term *blockchain* remains vague, even controversial. Sometimes, the term 'blockchain technology' instead of 'blockchain' is preferred in order to remark that blockchain is concerned about computers or technical aspects. Often, the term is used merely to point at the ideologies that have been attached to it, with imprecise references to technological specifications. This makes it difficult to classify a

given application as blockchain-based technology. While not clearly defined, blockchains typically exhibit a resemblance to Bitcoin, which is commonly considered its archetypal example, repeating its technical characteristics or following similar goals. From a purely technical point of view, blockchains are a type of DLT. Therefore, they can be understood as a distributed network of computers, ideally organised in a decentralised way, mutually agreeing on a common state while tolerating failures (incl. malicious behaviour) to some extent.

References

Buterin, V. (2014, January 23). Ethereum: A Next-Generation Cryptocurrency And Decentralized Application Platform. *Bitcoin Magazine*. https://bitcoinmagazine.com/business/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211

García-Barriocanal, E., Sánchez-Alonso, S., & Sicilia, M.-A. (2017). Deploying Metadata on Blockchain Technologies. In E. Garoufallou, S. Virkus, R. Siatri, & D. Koutsomiha (Eds.), *Metadata and Semantic Research* (pp. 38–49). Springer International Publishing. https://doi.org/10.1007/978-3-319-70863-8_4

Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*, *26*, 377–409. https://doi.org/10.1007/s10506-018-9223-3

Iansiti, M., & Lakhani, K. R. (2017, January). The Truth About Blockchain. *Harvard Business Review*, *95*, 118–127. https://hbr.org/2017/01/the-truth-about-blockchain

Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management*, *50*, 302–309. https://doi.org/10.1016/j.ijinfomgt.2019.08.012

Karlstrøm, H. (2014). Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Journal of Social Theory*, *15*(1), 23–36. https://doi.org/10.1080/1600910X.2013.870083

Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals problem. In *Concurrency: The Works of Leslie Lamport* (pp. 203–226). https://doi.org/10.1145/3335772.3335936

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf

Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM*, *60*(12), 36–45. https://doi.org/10.1145/3132259

Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A. B., Weber, I., Xu, X., & Zhu, J. (2017). *Risks and opportunities for systems using blockchain and smart contracts* [Technical report]. Data61 (CSIRO). https://doi.org/10.4225/08/596E5AB7917BC

Swan, M. (2015). *Blockchain: Blueprint for a new economy* (First edition.). O'Reilly.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18*(3). https://doi.org/10.1109/COMST.2016.2535718

Wüst, K., & Gervais, A. (2018). Do you need a blockchain? *Crypto Valley Conference on Blockchain Technology (CVCBT 2018)*. https://doi.org/10.1109/CVCBT.2018.00011

Published by

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with

centre
internet
et societe