Blockchain: As good as the rumours say?

A close look at blockchain technology and its applications in business, beyond cryptocurrency

150015673
11 October 2019

[2135 words]

CONTENTS

1 INTRODUCTION

Blockchain is a popular emerging technology. Many have claimed it will revolutionise technology, with some comparing it to the invention of TCP/IP. This report aims to take a closer look at how blockchain works and, through a couple of case studies, examine whether there is truth to the rumours and if it would be advisable for businesses to invest in or develop blockchain-based solutions for their systems.

2 AN EXPLANATION OF BLOCKCHAIN TECHNOLOGY

Blockchain was first described in 2008 and implemented in 2009 by Nakamoto as a decentralised, public ledger (a collection of financial accounts [4, 11]) for storing the transactions of the Bitcoin cryptocurrency [14]. However, the problem blockchain technology solves is broader than cryptocurrency use: it provides a way of establishing trust in a distributed network of nodes [17].

2.1 BLOCKCHAIN LAYOUT

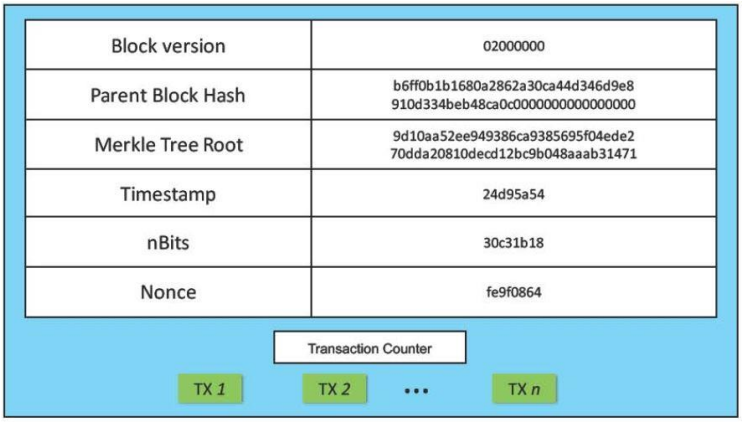

Figure 1: Layout of a block (from [23])

A block on the blockchain has a *block header* and a *block body*. The header contains what version of rules to follow, the hash of the previous block, the hash of all the transactions in the block, the timestamp of when the block was mined (in seconds), the maximum valid block hash, and a 4-byte field (the "*nonce*") which is a random number used to verify the hash of the current block [15, 22]. Since each block stores the hash of the previous, tamper detection is easy as any modification to, or removal of, the blocks would lead to different hash values [17]. Modifying the blockchain without being detected would require finding a modification whose data is a hash-collision, which is considered computationally infeasible [17]. The body of a block contains a transaction counter and several transactions. The number of transactions that can be contained in a block is limited by the maximum block size.

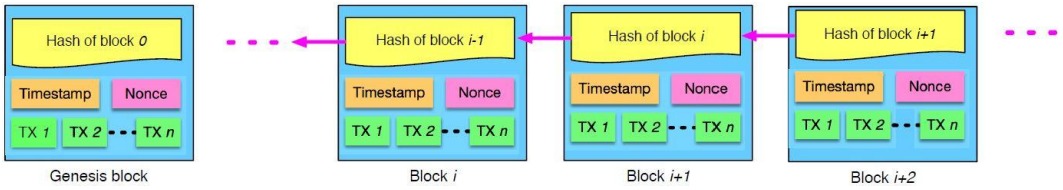

Figure 2: A visualisation of a blockchain (from [23])

The blockchain is then a chain of these blocks. The first block is called the *genesis block* and is unique in that it has no parent block. As each block contains a number of transactions, one can audit the complete transaction records by going through the blockchain.

2.2 How it works

The blockchain is distributed across the network of nodes contributing to it. Adding a block to the blockchain is done through solving a computationally difficult problem, a process known as mining. There is a reward for successfully mining a block, e.g. the miners in Bitcoin receive a small portion of bitcoin for successfully mining a block [23]. Different blockchain implementations use different puzzles, for example Bitcoin requires miners to try different nonce values until the current block hash is at most a number specified in the header [22]. Mining is done for each node in the entire network participating in the blockchain and so there needs to be a way of deciding what mined block is the next one to commit to the chain. There are various consensus algorithms for deciding which blocks to choose and the choice of algorithm can affect the transaction speed [13]. In fact, according to Vukolić [19] it is impossible to achieve a high transaction throughput and scalability across a large number of nodes simultaneously. Hybrid approaches which try to find a balance between scalability and transaction throughput are currently a question open for research [19].

2.3 Features

Through its design, blockchain has various features which can be appealing for different reasons:

- It is decentralised, meaning that transactions can be conducted peer-to-peer, i.e. without going through a trusted third party or a central authority.
- A further advantage to being decentralised is that there is no single point of failure which could be attacked to take down the blockchain.
- Since anyone can see the transactions stored, the blockchain is transparent and easy to audit.
- The distribution of the blockchain means that a user could generate identities to prevent their identity being disclosed.
- The immutability of the blockchain by using hash-values means that it is reasonably tamper-proof.

3 Public and Private Blockchains

Blockchains can be roughly split into three different categories [16]:

Public Blockchains, where anyone can join or leave the network and contribute to the blockchain. Public blockchains have the advantage of being heavily distributed and transparent, but also come with a number of challenges. Each update to a blockchain has to propagate through the

network as all nodes must be able to verify it. This takes time and imposes limitations on the block size, which in turn limits the number of transactions that can be stored in a block. For example, Bitcoin can only process a maximum of around 7 transactions per second [22, 23] which is insignificant compared to a centralised system like Visa which can process upwards of 60,000 transactions per second [18]. Another challenge of public blockchains is that trust is very low because of the lack of control over who joins. To then be able to trust the network, expensive consensus algorithms must be deployed [19], leading to a lot of wasted compute time and energy [5].

Private Blockchains, where there is strict control over who can read and write to the blockchain. This solves many of the problems public blockchains have: since there is control over who can access, all nodes are trusted meaning more efficient consensus algorithms can be used [19, 22], saving energy and enabling a higher transaction throughput [19]. The network also has a fixed size, and is likely within an organisation, meaning transfer speeds can be higher than an arbitrary, global distribution of nodes with varying internet suppliers. Furthermore, if a node goes offline it is possible to bring it online again reasonably quickly, as all nodes are known [16]. The downsides to private blockchains are that they are not decentralised [16, 22, 23], potentially restoring the single point of failure (e.g. the organisation's network), they are more susceptible to modifications due to the low number of participating nodes [22, 23], and they potentially lose their transparency, depending on whether the controlling body decides to make read-access public [16, 22, 23].

Consortium Blockchains, can be considered a hybrid approach between public and private blockchains. In consortium blockchains, the nodes used for validating and confirming additions to the blockchain are pre-selected [16, 22, 23]. Similar to a private blockchain, this solves the problem of trust, as the nodes which change the blockchain have been pre-selected as trustworthy. However, in contrast to a private blockchain, the nodes do not have to all come from the same organisation, making it partially decentralised (not fully, as not anyone can maintain a copy) [16]. Consortium blockchains can use similar techniques as private blockchains to increase performance. Although they are partially decentralised, consortium blockchains are still susceptible to tampering due to the low number of nodes, and may also not be transparent depending on whether all the involved regulating bodies agree to allow read-access to the public [16, 22, 23].

Table 1: Overview of the different types of blockchain and their properties (adapted from [13])

Property	*Public*	*Consortium*	*Private*
Consensus determination	All miners	Selected set of nodes	One organisation
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralised	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

4 Blockchain for Data Storage and Access

It is easy to see the potential advantages of using blockchain for data storage and access: through transactions, it would be possible to see precisely who accessed what data; as there is no

central party, permissions could be given and revoked without the need for the data to leave the original owner; if the data were encrypted and stored on the blockchain, then there would be numerous backups over the distributed network. Unfortunately, due to the limitations of block size, blockchain is not well suited for raw data storage [2, 24] and there may be complications with regard to data protection (see Section 5). Instead, Azaria et al. describe a system for managing access to medical data in [2]. In this system, a blockchain is used to manage access to the data through so-called "*smart contracts*". These are small pieces of code which execute given certain conditions, specified in the contract, are met [2], e.g. "if patient A authorises pharmacy B to access their data, then the access request will be executed". By storing the pointers to the data and managing access control on the blockchain instead of storing the data itself, the block size does not have to be large, and traditional methods like SQL-databases can be used for secure data-storage [2]. However, Azaria et al. admit that their approach does not improve the security of the data storage, nor change the legal complications which arise with medical data [2].

Azaria et al. base their work on a paper by Zyskind et al. [24], which describes a system that also uses blockchain for access management. The difference between [2] (Azaria et al.) and [24] (Zyskind et al.) is that [24] stores the key for a key-value system on the blockchain, with the key-value pair being stored in a third-party off-blockchain solution [24]. This allows users to directly control their data and see who accesses it without the involvement of a third-party. As the key and access permissions are stored and processed on the blockchain, there is a record of whose data was accessed when and by whom [24]. A working implementation was later developed, by Zyskind et al., as the open-source "*Enigma*" project [25]. It is an interesting system, however, similar to [2], the storage of data is done using a traditional data storage method. Zyskind et al. admit in their initial paper that this may be key for the system to scale [24], as traditional databases scale better than blockchain, similar to the scalability findings in [5, 23].

5 Legal Considerations of Blockchain

Blockchain being distributed and immutable is described as two of its strengths [15, 17, 22]. However, these pose certain legal problems. Immutability may be good from an auditing and transparency perspective, but it leaves little space for malicious or erroneous entries [6]. Additionally, the introduction of the European Union's General Data Protection Regulation (GDPR) [26] (introduced in 2016) could cause problems for blockchain. Article 17, commonly known as the "Right to be Forgotten", allows users to request data deletion when the data is no longer relevant for processing purposes or they no longer consent to its storage [26]. As blockchains are immutable, this could be a problem because technologies using it could be deemed non-GDPR compliant, heavily limiting a blockchain application's business scope in the EU. As the GDPR has consequences outside the EU, it could also mean that the application needs redesigning [7]. The use of blockchain for data-pointer storage examined in the previous section could be a solution [7]. It is also ambiguous whether blockchain is considered privacy-guarding enough [3], as Article 25 of the GDPR requires systems dealing with personal data to have "Data protection by design and by default" [26].

Due to blockchain being a fairly new technology which has only recently been gaining traction and laws being slow to change, the law and blockchain may shape each other [3, 20]. Currently, the law is ambiguous with regards to blockchain and its various attributes [3, 7, 20].

6 BUSINESS ADVICE AND CONCLUSION

The majority of industry projects using blockchain have been abandoned [1, 9, 12]. The technology is still rapidly developing and potential legal incompatibility is a serious concern for local and international businesses. Additionally, there are many extra considerations for business implementations, e.g. compatibility with existing systems, identity management, and liability, just to name a few [10]. As such, there is very little guarantee that investing time and effort into a blockchain system will be worth it. That being said, blockchain still has potential, and it may be good to start a small blockchain-based system and see where it goes [8]. If a project is started, a private blockchain, or at most a consortium blockchain, will probably be best as it reduces the risk of leaking sensitive information as well as the worry of having anyone be able to access the system. For most applications however, it may be best to use existing solutions or follow of Wust and Gervai's flowchart (see Appendix A) [21].

Through the examples and case studies in this report, it has become adamantly clear that blockchain may not be as good as initially proclaimed by enthusiasts. Indeed, it may be best to rely on existing, scalable, and tried and true systems. However, some of the problems it solves, it seems to solve very well. And it could be that research into new consensus algorithms and blockchain protocols lead to a breakthrough. For now, it seems best to wait and see.

BIBLIOGRAPHY

[1] As Some Companies Abandon Blockchain, Ethical Questions Arise: 2019. *https://www.financemagnates.com/cryptocurrency/news/as-some-companies-abandon-blockchain-ethical-questions-arise/*. Accessed: 2019-10-07.

[2] Azaria, A. et al. 2016. MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)* (Vienna, Austria, Aug. 2016), 25–30.

[3] Berberich, M. and Steiner, M. 2016. Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers Reports? *European Data Protection Law Review*. 2, (2016), 422.

[4] Bookkeeping | business: *https://www.britannica.com/topic/bookkeeping*. Accessed: 2019-10-07.

[5] Croman, K. et al. 2016. On Scaling Decentralized Blockchains: (A Position Paper). *Financial Cryptography and Data Security*. J. Clark et al., eds. Springer Berlin Heidelberg. 106–125.

[6] Gabison, G. 2016. Policy Considerations for the Blockchain Technology Public and Private Applications. *SMU Science and Technology Law Review*. 19, 3 (2016), 25.

[7] Herian, R. 2018. Regulating Disruption: Blockchain, GDPR, and Questions of Data Sovereignty. *Journal of Internet Law*. 22, 2 (2018), 12.

[8] Iansiti, M. and Lakhani, K.R. 2017. The Truth About Blockchain. *Harvard Business Review*. (2017), 11.

[9] Kharif, O. 2018. Blockchain, Once Seen as a Corporate Cure-All, Suffers Slowdown. *Bloomberg.com*.

[10] Lai, R. and LEE Kuo Chuen, D. 2018. Blockchain – From Public to Private. *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2*. Elsevier. 145–177.

[11] Ledger | Definition of Ledger by Lexico: *https://www.lexico.com/en/definition/ledger*. Accessed: 2019-10-09.

[12] McCrum, D. 2018. Sell all crypto and abandon all blockchain. *Financial Times*.

[13] Mingxiao, D. et al. 2017. A review on consensus algorithm of blockchain. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (Banff, AB, Oct. 2017), 2567–2572.

[14] Nakamoto, S. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. (2009), 9.

[15] Nofer, M. et al. 2017. Blockchain. *Business & Information Systems Engineering*. 59, 3 (Jun. 2017), 183–187. DOI:https://doi.org/10.1007/s12599-017-0467-3.

[16] On Public and Private Blockchains: 2015. *https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/*.

[17] Pierro, M.D. 2017. What Is the Blockchain? *Computing in Science Engineering*. 19, (2017), 92–95. DOI:https://doi.org/10.1109/MCSE.2017.3421554.

[18] Visa Fact Sheet: 2018. *https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf*.

[19] Vukolić, M. 2016. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. *Open Problems in Network Security*. J. Camenisch and D. Kesdoğan, eds. Springer International Publishing. 112–125.

[20] Werbacht, K. 2018. TRUST, BUT VERIFY: WHY THE BLOCKCHAIN NEEDS THE LAW. *Berkeley Technology Law Journal*. 33, 2 (2018), 65.

[21] Wust, K. and Gervais, A. 2018. Do you Need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (Zug, Jun. 2018), 45–54.

[22] Zheng, Z. et al. 2017. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)* (Honolulu, HI, USA, Jun. 2017), 557–564.

[23] Zheng, Z. et al. 2018. Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*. 14, 4 (2018), 352. DOI:https://doi.org/10.1504/IJWGS.2018.10016848.

[24] Zyskind, G. et al. 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE Security and Privacy Workshops* (San Jose, CA, May 2015), 180–184.

[25] Zyskind, G. et al. 2018. Enigma: Decentralized Computation Platform with Guaranteed Privacy. *New Solutions for Cybersecurity*. H. Shrobe et al., eds. The MIT Press.

[26] 2016. REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation). *Official Journal of the European Union*. 59, (Apr. 2016), 88.

Appendix A

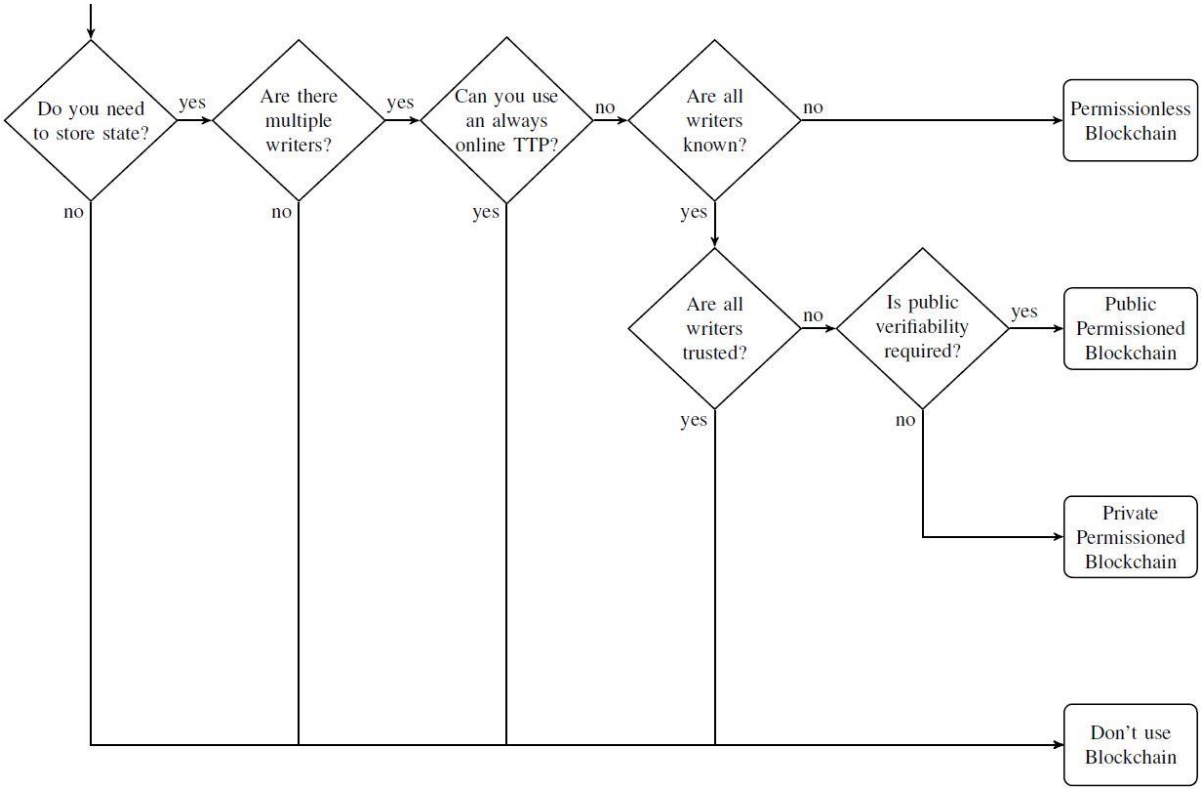

Figure 3: Flowchart for deciding whether to use a blockchain (from [21])