proceedings

MDPI

Proceedings

On The Case of Blockchain Adoption in the Internet of Things [†]

Davide Pedrini [1,‡], Mauro Migliardi [1,‡,*], Carlo Ferrari [1,‡] and Alessio Merlo [2,‡]

[1] DEI, University of Padua, 35131 Padova, Italy; ped.davide@gmail.com (D.P.); carlo.ferrari@unipd.it (C.F.)
[2] DIBRIS, University of Genoa, 16145 Genova, Italy; alessio.merlo@unige.it
[*] Correspondence: mauro.migliardi@unipd.it; Tel.: +39-3281003221

[†] Presented at the 12th International Conference on Ubiquitous Computing and Ambient Intelligence (UCAmI 2018), Punta Cana, Dominican Republic, 4–7 December 2018.

[‡] These authors contributed equally to this work.

Published: 23 October 2018

Abstract: Recently blockchain technology has been advocated as a solution fitting many different problems in several applicative fields; among these fields there is the Internet of Things (IoT) too. In this paper we show the most significant properties of a blockchain, how they suite the use case of a cryptocurrency and how they map onto the needs of IoT systems. We claim that a blockchain does not provide a significant advantage with respect to other database technologies in a field such as Internet of Things where computational power comes at a premium, energy is often scarce and storage scalability is a major challenge.

Keywords: blockchain; IoT; scalability; database

1. Introduction

A recent study from Cisco outlined the steadfast growth of the number of "always connected and always on" devices and it projected that they will outnumber human presence on the internet by a three to one ratio in the year 2021 [1]. The IoT eco-system includes a lot of significantly heterogeneous devices and most of them are characterized by limited computational resources, with regards to the energy supply and to the storage capability.

Recently, blockchain–based solutions have gained a large degree of popularity for solving problems that are typical of the IoT field [1–3]. A blockchain is a distributed database to record groups of transactions in the form of a linked chain of blocks. Each block includes a cryptographic hash of its predecessor, guaranteeing that old blocks cannot be tampered with avoiding re-writing also all the blocks that follow. All the participants in a blockchain system form a peer–to–peer network and anytime new blocks are generated they are spread to all the participants according to a gossip protocol. The database is also known as the ledger as it registers all the information in a create and read-only fashion, making the blockchain a distributed ledger technology.

Blockchain technology came into the spotlight thanks to its application in cryptocurrencies: Bitcoin [4] has proposed the first practical use of a blockchain and it has spurred the development of dedicated, high-energy footprint devices targeted at solving the crypto puzzle that allows adding a block at the chain. Cryptocurrencies in general and Bitcoin in particular are based on a blockchain

[1] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf.

because it appears to be a solid structure that allows performing and securing transactions without the control of a trusted central authority such as a bank.

The growing number of devices and, consequently, the faster growing number of potential interactions among them, suggest that scalability issues can pose a severe threath to the blockchain technology in its present form. This paper aims to investigate the impact scalability has on blockchain–based application in the IoT framework, resulting in some preliminar evaluation about the feasibility and the usability of blockchain technology inside IoT systems. The main characteristics of blockchain technology will be mapped onto the needs of a typical IoT system in order to come to a final answer about the suitability of blockchain in the field of IoT;

This paper is structured as follows: in Section 2 we will describe the main features of permissionless and permissioned blockchains because the choice between these two alternatives implies several very significant differences in the blockchain's properties (e.g., the mechanism of distributed consensus) that have a major impact on the usability in the IoT eco-system; in Section 3 we will show some possible applications of a blockchain in IoT, and we will compare these solutions with other based on different distributed database technology; in Section 4 we will analyze how the scalability problem impacts on the usability of blockchain technology in the IoT eco-system; Section 5 will provide some concluding remarks.

2. Blockchain Features

Blockchain–based networks are decentralized systems where anyone can join the network at any time and a distributed consensus in the absence of a trusted third party is reached thanks to the proof-of work (PoW). The PoW consists in solving a hash puzzle, finding a nonce that satisfies the inequality:

$$H(nonce||prev\_hash||tx||tx||...||tx) < target$$

Nonce is a random number, prev_hash is the hash of the previous block, tx is the list of transactions inside the block. The target is a value set by the network and it is automatically adjusted to maintain the block creation time constant. The need for a constant creation time arises from the fact that new blocks need to be spread to all the nodes in the peer-to-peer network, validated and attached to the blockchain before new blocks are created. This both reduces the number of accidental bifurcation of the chain and dampens the feasibility of a 51% attack [5]. The ledger records every transaction that is accepted by the network. In permissionless blockchain, the ledger is transparent and visible to everyone while in permissioned blockchain users needs proper permissions for both the read and write operations on the ledger.

Bitcoin is based on a permissionless blockchain: participants don't have to ask anyone for permission to read the ledger or to perform transactions. Everyone can become a "miner" and start to compete with the other nodes. Even if there are no regulations preventing anyone from becoming a "miner", the computational capability requirements and related energy costs, create an entry barrier that has already become very significant due to the need to increase the difficulty for solving the hash puzzle. As trust cannot be achieved in a network where anyone can anonymously perform transactions and there is no central authority that ensures a transaction validity, there should be a mechanism among participants that decides who will properly create the next block containing new transactions. Based on PoW, this mechanism impacts on the speed for validating transactions. The PoW can significantly slow down the transaction processing by varying the hash puzzle target. The Bitcoin network requires ten minutes to validate a block, and it is actually necessary to wait for more blocks to be attached to the chain. This dependency from additional blocks in the blockchain is very important; anytime there is a fork in the blockchain (e.g., two miners innocently find the PoW solution nearly at the same time), only one branch have to become a part of the blockchain avoiding both a double validation and a void validation. In a permissionless blockchain the only component of trust is placed in cryptographic mechanisms and in the distributed consensus protocol, and the price of an open, secure, decentralized and anonymous system is the steep performance cost both in terms of time required to reach consensus and in terms of needed resources.

Permissioned blockchains request permissions for read operations on the ledger and limit the group of participants who can execute the transactions. Furthermore, the writing of new blocks is allowed only to a set of nodes chosen by the parties involved in the administration of the system. Hence, there is an authority represented by a single trusted entity or a well-known set of trusted peers. Introducing centralization influences the consensus mode within the network. as the network becomes a trusted one. In permissioned blockchain, the concept of PoW loses its meaning since consensus can be reached more quickly and efficiently. A permissioned blockchain has a number of advantages over permissionless blockchains. In the case of a fork, the system is fully controlled by the company or company group, which is able to choose the validators and then to state the rules to be followed. The risk of attack by the nodes of the network is reduced, because the validators are known and they can be punished in case of harmful actions. The validation process is faster because few trusted nodes are involved to validate them. Since reading permission is subject to restrictions, privacy is enforced while anonymity is weakened. A weakness in permissioned blockchain is related to the potential modification of the consensus protocol rules at any time.

In conclusion, the permissioned blockchain is better suited to a network of nodes that trust each other and accept the presence of a central authority. The permissionless blockchain is more appropriate in the opposite case where there is no trust and you do not want an intermediary for the success of the transactions.

3. Blockchain and Database

Permissioned blockchains are good candidates for critical applications in resource constrained environments because they can achieve consensus quite efficiently without using PoW that requires huge computational resource instead. The focus of this section is about the differences between permissioned blockchain and traditional database technologies, in order to highlight some design guidelines. As shown in [6], a centralized database provide the best solution anytime either a single user or a trusted third party (TTP) are in charge of all the writing operations. Such a solution, shows a very good performance both in terms of latency and throughput while a blockchain–based solution would not provide any advantage. In systems where all the network nodes are known and trusted, the TTP can be selected by election and again the use of a blockchain provides no additional advantages. Anytime all the participants are not known in advance or it is not possibile to assure a complete mutual trust, only permissionless blockchain may provide a suitable solution, at higher computational costs. From the point of view of data, it is worth to note that a blockchain allows to add data to itself and to consult them without the possibility of modifications or deletion in any way. Moreover, the chain structure excludes any attempt to change that does not invalidate the system and the same applies to the deletion of a transaction on the blockchain. So the blockchain can be considered an immutable system and is useful for the transactions registration that can not be revoked. However, when the participants are known, or even more, when the network depends entirely on a central authority, it is feasible to reach a consensual decision to change the protocol underlying the blockchain evolution thus completely foiling the immutability properties [7,8].

After studying the cases that may lead to the choice of different blockchains compared to a traditional centralized database, it is also important to compare the features of a blockchain–based solution with the feature of a solution based on a distributed NoSQL database.

Considering distributed database, it is worth to note that they do not exhibit a single point of failure, meaning that a single malfunction of any part of the system does not lead to the service stop. The data are replicated on multiple nodes and data consistency is assured using a conflict management system. Cassandra [9] is a non-relational distributed database that offers excellent data availability at the expense of consistency. In fact, it has been shown that in distributed systems only two over the three properties of consistency, availability and partition tolerance can be reached. As in real distributed systems the possibility of a network partition is unavoidable, it is necessary to decide whether to require system consistency or system availability. Cassandra chooses to provide the maximum availability relaxing the consistency requirement to “eventual consistency” [9]. This property means that the data obtained by a client might not be consistent with another client obtains querying a different node. When a node in the network changes a piece of data, the change must be propagated to all the database replicas. Since the propagation is not instantaneous, it may happen that some nodes are updated while others are not, in the same time interval. The data inconsistency is temporary since at the end of the propagation all the nodes will be aligned. “Eventually”, the difference will be conciliated, but there is no guarantee for an un-fractured state at any given time. The required performance for the data reading speed determines the degree of consistency that a system wants to achieve. In Cassandra, to reach a high availability of data, it is possible to adjust the level of consistency according to the risk that can be incurred. This feature is called tunable consistency and is one of the biggest differences between noSQL database and SQL database. Permissionless blockchains provide an eventual consistency property that is similar to noSQL databases. In fact a blockchain fork leads to a temporary inconsistency of the data because some nodes consider the blocks to be correct in one branch, while other nodes evaluate as correct the other branch. In the end, all the nodes will agree on the correctness of the longest blockchain. A fork continues to exist as long as pairs of blocks are created in close succession, extending different branches, otherwise the nodes on the shorter branch would move on the longest chain. The probability that two branches are extended almost simultaneously decreases exponentially with the length of the fork. Finally, there will be a time when only one branch will be extended, becoming the main chain. Of course, noSQL databases and blockchains continue to differs from the point of view of the operations possible on data.

In the case of a permissioned blockchain, however, the consensus mechanism does not necessarily require incentives for the nodes to create blocks. Furthermore, the presence of a limited set of trusted parties cannot guarantee from collusion. Hence, the chain organization of blocks does not provide additional guarantees of tamper-proofing and using a noSQL database with a set of trusted DB-keepers would provide a similar level of transparency with a much better level of reading and writing performance and an excellent level of scalability.

The most part of the many application fields, which involve IoT devices, do not take advantage of the blockchain technology. Data storage management systems, such as the ones that can involve smart homes [10] or insurance companies, do not need a structure based on a chain of blocks. An insurance company is interested in a tamper-proof log of events but cannot cope with the slow performance of a permissionless public blockchain nor is willing to disclose all of its data. At the same time permissioned blockchains do not help more than any type of database that results in better performance level without chaining. Since trust is placed in a Trusted Third Party, the immutability is guaranteed by this entity rather than by the blockchain properties. Hence, a permissioned blockchain is vulnerable to attacks directed on TTP, as well as other types of databases. Furthermore, these use cases are not applicable on a permissionless blockchain because it is not acceptable that sensitive data can be managed by a network where participants do not trust each other and there is no central authority that can certificate the participants identity. An example of permissioned blockchain is the MultiChain [11], a platform that can be used within an organization or between multiple organizations. As already explained, the permissioned blockchain does not need complex mechanisms of distributed consensus and therefore obtains better performances regarding the data insertion on the blockchain and the transaction verification phase. In this case, IoT devices are called hardware “oracles”, which give information about the physical world. MultiChain allows creating different assets and exchanging them within the blockchain, so as to offer a good flexibility. This type of blockchain can be applied to different areas, yet, in the IoT eco-system there is no evidence of the advantage of this technology compared to solutions based on traditional databases. Indeed, the use of a TTP always available makes the structure used by the blockchain completely unnecessary.

4. Scalability Issues

In blockchain–based systems the transaction management mechanism is decentralized, secure and solves the problem of double spending without the presence of a central authority. At the same time, those systems must cope with scalability issues, avoiding the risk of damaging the quality of the offered core services. For examples, the Bitcoin networks process an average number of seven transactions per second regardless the increasing number of involved nodes and transactions. This is sufficient to conclude that a permissionless blockchain is not a feasible solution, for IoT eco-systems where the number of involved devices requires optimal scalability. In permissioned blockchains, scalability problems are less critical since the system does not provide a total decentralization and therefore there are fewer limitations on the speed of transactions validation [12].

A solution that has been proposed for executing transactions between IoT devices in a scalable fashion, is IOTA [13], a cryptocurrency that does not need to be mined because all the money is generated in the genesis transaction. IOTA was designed to keep the system decentralized allowing the processing of a large amount of transactions. This goal is achieved using a system called the Tangle, a structure based on a DAG (directed acyclic graph), that allows for parallel executions of transactions. There is no reward for the transactions validation; the only incentive is the need to validate at least two transactions before being able to perform one. There are no miner and no one has to spend a large amount of computational resources. In order to guarantee from node collusion, IOTA uses a special validator, called Coordinator, which deals with periodically validating the transactions. This component serves to avoid double spending and to gain certainty about a transaction. This solutions means that there exists a a trusted third party that needs to have a global vision of the whole system actually making the Tangle completely different from a permissionless blockchain and actually vulnerable both from a security and from a performance point of view.

In [14], Slepak and Petrova shows that decentralization, distributed consensus and scalability are conflicting features and that a decentralized consensus system, when it scales, tends to centralization, in the sense that the transaction processing depends on a few nodes, which can join to form a central authority within the network. The IoT eco-system absolutely requires scalability, hence, either decentralization or distributed consensus needs to be sacrificed. As these two properties are strictly linked in blockchain based systems, it is convenient to study other possibilities that better adapt in the IoT context.

5. Conclusions

Many studies and many projects have proposed blockchain based solutions for securing data in IoT systems [15]. In this paper we have analyzed the main features and characteristics of blockchain based systems, both in the permissionless and in the permissioned flavor, and we have tried to map them onto the requirements of the IoT eco-systems (e.g., resource constraints and high scalability). Our analysis show that, while the capability of a permissionless blockchain to achieve eventual consensus in a completely decentralized way provides a very high resilience to faults and a very high level of system availability that would be extremely desirable in the IoT eco-system, the energy and computational costs of the POW are incompatible with most IoT systems. At the same time, the reduced resource constraints imposed by a permissioned blockchain also weakens the main characteristics of a blockchain based system and, with the introduction of an always available trusted third party, make a solution based on relational or noSQL databases feasible and more capable from the performance point of view. Moreover, in those applications that employ IoT devices in a trustless network (like smart homes), the blockchain can not be used due to the impossibility of the system to scale. Anytime there is a trusted network, the blockchain loses its main characteristics and becomes a simple chain-structured database whose usefulness has to be proved on a case-by-case basis. Again, this means that other types of databases are likely to be more suitable for applications such as smart homes or supply chains. It is our conclusion that, at present, there is no significant proof that blockchain technology is a good match for the IoT eco-system.

References

1. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303, doi:10.1109/ACCESS.2016.2566339.
2. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in Internet of Things: Challenges and Solutions. *arXiv* **2016**, arXiv:1608.05187.
3. Zhang, Y.; Wen, J. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 983–994.
4. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 26 May 2018).
5. Aa, V.V. Bitcoin Developer Guide. 2018. Available online: https://bitcoin.org/en/developer-guide (accessed on 26 May 2018).
6. Peck, M.E. Blockchain world—Do you need a blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectr.* **2017**, *54*, 38–60, doi:10.1109/MSPEC.2017.8048838.
7. Greenspan, G. The Blockchain Immutability Myth. 2017. Available online: https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/ (accessed on 28 May 2018).
8. Madeira, A. The DAO, The Hack, The Soft Fork and The Hard Fork. Available online: https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/ (accessed on 28 May 2018).
9. Wang, G.; Tang, J. The NoSQL Principles and Basic Application of Cassandra Model. In Proceedings of the 2012 International Conference on Computer Science and Service System, Nanjing, China, 11–13 August 2012; pp. 1332–1335. doi:10.1109/CSSS.2012.336.
10. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623. doi:10.1109/PERCOMW.2017.7917634.
11. Greenspan, G. MultiChain Private Blockchain, White Paper. Available online: http://www.multichain.com/download/MultiChain-White-Paper.pdf (accessed on 22 October 2018).
12. Xin, W.; Zhang, T.; Hu, C.; Tang, C.; Liu, C.; Chen, Z. On Scaling and Accelerating Decentralized Private Blockchains. In Proceedings of the 2017 IEEE 3rd International Conference on Big Data Security on Cloud (Bigdatasecurity), IEEE International Conference on High Performance and Smart Computing (Hpsc), and IEEE International Conference on Intelligent Data and Security (ids), Beijing, China, 26–28 May 2017; pp. 267–271. doi:10.1109/BigDataSecurity.2017.25.
13. Popov, S. The Tangle. Available online: https://iota.org/IOTA_Whitepaper.pdf (accessed on 22 October 2018).
14. Slepak, G.; Petrova, A. The DCS Theorem. *arXiv* **2018**, arXiv:1801.04335.
15. Conoscenti, M.; Vetrò, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6. doi:10.1109/AICCSA.2016.7945805.