An Extensive Survey on Consensus Mechanisms for Blockchain Technology

Jalpa Khamar and Hiren Patel

Abstract Blockchain technology is a cryptographic technique that enables users to maintain their data in a decentral way with a non-editable form without an arbitrator. Originally motivated from the underlying platform of bitcoin cryptocurrency, researchers found blockchain to be very useful in many application domains, including smart contracts, insurance, banking, finance, and many other sectors. As multiple stakeholders try to add a block (containing the data or transactions) into the chain, there is a need for a mechanism to come to an agreement on which stakeholder's block should be added. Such a mechanism is known as consensus mechanism which is a primary factor of significance because it decides the correctness of data to be added as well as trustworthiness of the node which is attempting to add the block. An efficient consensus mechanism achieves security, higher precision, and better performance. In this research, we aim to study various consensus mechanisms in blockchain technology with their strengths and challenges. We discuss factors affecting the consensus mechanism and provide our suggestions for drafting an effective consensus mechanism.

Keywords Blockchain · Consensus · Bitcoin

J. Khamar (✉)
LDRP Institute of Technology and Research, Research Scholar, Kadi Sarva Vishwavidyalaya, Gandhinagar, India
e-mail: khamarjalpa7@gmail.com

H. Patel
Vidush Somany Institute of Technology and Research, Kadi Sarva Vishwavidyalaya, Gandhinagar, Gujarat 382015, India
e-mail: hbpatel1976@gmail.com

K. Kotecha et al. (eds.), *Data Science and Intelligent Applications*,
Lecture Notes on Data Engineering and Communications Technologies 52,
https://doi.org/10.1007/978-981-15-4474-3_40

1 Introduction

The primitive concepts of carrying out some computation work or burn some of your wealth in any form before you add the block to the chain was first introduced by a group of researchers in 1991 [1]. However, the idea of blockchain was mostly not in use until it was first referred by Satoshi Nakamoto [2] in 2009 which was the birth of bitcoin cryptocurrency.

The blockchain is a decentralized, distributed ledger uses to record transactions between two parties in a secure, transparent, and immutable manner [3]. Data is recorded in blocks that are needed to be verified by network participants (also known as peers or nodes) before it is finally added on to the chain. The dynamically run-time updated blockchain ledger is available on a distributed peer-to-peer network across all stakeholders, which makes it possible for all participants to verify; hence, a group of malicious people cannot just add any random data block to the chain. Once fixed numbers of participants (not knowing each other and situated geographically apart, i.e., located decentralized) verify/confirm the transactions in the block, the block is ready to be added into the chain. Once a block is added to the chain, it is immutable, i.e., it cannot be altered, tampered, or deleted. The added block is visible to every node of the network, i.e., the block is transparent to the entire network. Any node of the network can verify the integrity of any block which results in auditability property of the blockchain. The blockchain, therefore, enables us to securely record, store, and transfer data without the need for a central authority to process and verify it. All the transactions occur in a scattered way that expels the need to authorize the transactions by mediators [4]. Blockchain has some key characteristics (as mentioned above), such as decentralization, transparency, immutability, and auditability [5].

In the case of bitcoin [2], individuals can make electronic money transactions without the need for a bank or involvement of any trusted third party; enabling each user to directly interact with others without any extra cost to be paid on the transactions. Although bitcoin is the most distinguished application of blockchain, the primeval concept can be applied to disparate application areas beyond cryptocurrencies.

In recent times, blockchain has also gained its popularity among researchers as the notion behind blockchain can be used in variety of domains. Many researchers have been working in different application areas such as study of digital currency based on blockchain [6], some are working on blockchain applicability in non-digital currency such as application of blockchain in smart city [7], medical information security management [8], and also in underlying blockchain technology such as scalability of consensus algorithms [9], smart contracts [10], difficulty control in mining [11] to name a few.

The rest of the paper is organized as follows. Section 2 discusses the background theory of blockchain technology. Section 3 depicts various types of blockchain. Different consensus mechanisms are studied in Sect. 4 followed by challenges and opportunities conversed in Sect. 5. Different tools and technologies related to blockchain technology have been conferred in Sect. 6. The paper has been concluded by a list of references used.

2 Basics of Blockchain

Blockchain technology has taken the world by surprise, with the hundreds of businesses and flourishing projects around the world. Although it seems a relatively new concept, blockchain, as well as decentralization, have been around for quite some time; these technologies have received attention in recent years. To explain how blockchain works, we must define the fundamental concept of it. The blockchain is a distributed ledger (data structure) which contains information about transactions or events. This is replicated and shared among network participants [12]. The blockchain can also be used as a generic term to refer to purely distributed peer-to-peer systems as a whole instead of referring to a software unit that is part of a purely distributed system [13]. Blockchain is an sequential list of blocks where each block contains a small list of transactions. Each block in a blockchain is "chained" to the previous block, by containing a hash of the representation of the previous block as seen in Fig. 1. So, historical transactions in the blockchain cannot be deleted or modified without invalidating the chain of hash. Combined with computation and incentive constraints block creation schemes, this can in practice prevent falsification and revision of the information stored in the blockchain. The first generation of blockchains, like bitcoin, provided a large public book to store cryptographically signed financial data transactions [14].

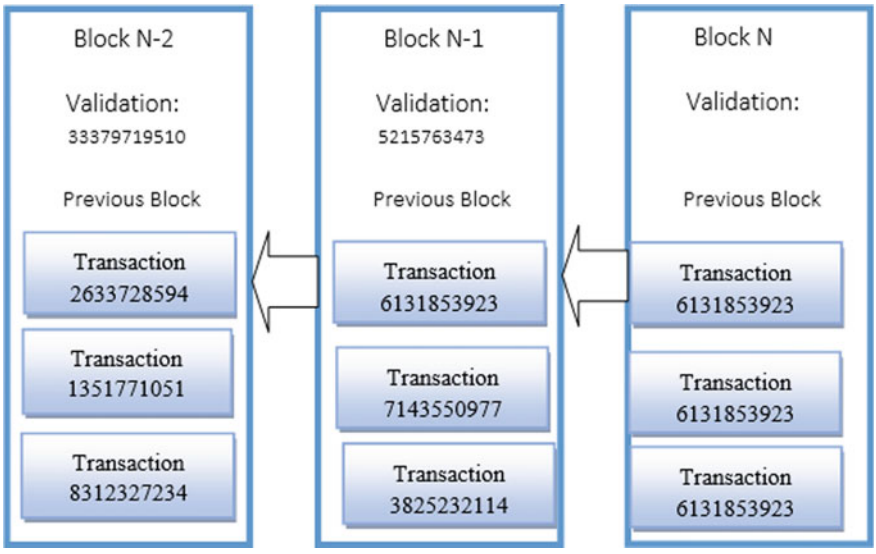

Fig. 1 Chain of blocks in blockchain

3 Types of Blockchain

Before we introduce the words such as permissioned blockchain or permissionless blockchain, we need to understand the specific application domain of the blockchain in form of centralized or decentralized monitoring mechanism. There are few applications in which a closed group of users are permitted to access the chain and hence it required a centralized approach to the chain. For such type of application, permissioned (or sometimes referred to as private) blockchain is used. Examples of permissioned blockchain are Ripple [15] Corda [16], Hyperledger Fabric [17]. In contrast to it, permissionless (sometimes referred to as public) blockchain mechanism is an approach where any number of participants may join the network. There is no central authority or restrictions for getting someone registered to the network. All the participants are able to access the database and store a local copy, and according to their computing power, they can update it. Bitcoin [2] and other cryptocurrencies such as Ethereum [18] are examples permissionless blockchain. There is also a hybrid category named consortium blockchains which is open to the public but not all data is available to all participants. Users have limited rights and blocks are validated based on predefined rules. Consortium blockchains are, therefore, "partly decentralized". R3 consortium [19] is an example of a consortium blockchain. In all such category, to validate transaction authenticity, to put the legitimate transactions in a block, to verify the block, and to add the verified block to the chain, there is a need for some work (in terms of computation or other) to be carried out. In a permissionless blockchain, the proof of work (PoW) [20] is one of such compute-intensive algorithms. And the process of adding such block to the network is often called mining. The next paragraph discusses the mining process followed by the significance of the consensus mechanism in the mining process.

4 The Consensus Mechanisms

In real world, consensus is termed as an agreement. Consensus among dishonest nodes in blockchain is achieved through Byzantine Generals Problem [21]. In Byzantine Generals Problem, a group of Generals each having a commando over them, decides to attack or to retreat. All the messages between then is passed through any messenger. It is not necessary that every time this messenger will be loyal; it may be betrayer. So, loyal Generals need to reach to a common consensus knowing the existence of betrayer. Since blockchain does not rely on any central authority, distributed nodes are required to agree to the validity of transactions and for these consensus mechanisms play a vital role in blockchain. We present a taxonomy of different consensus mechanisms in the blockchain by classifying them on the basis of the different environment of blockchain.

4.1 Permissionless Blockchain

4.1.1 Proof of Work

Proof of work (PoW) is a consensus algorithm which was firstly used in the bitcoin [2]. In PoW, by performing some form of computational work, consensus is achieved [22], For instance, in decentralized network, some value has to be selected to store or record the transactions. It can be done by selecting any random value. However, selecting random value is vulnerable to attacks, so to avoid attacks, nodes need to perform lots of computation in different forms (e.g., adding nonce to the original value). By using node's own computational power, it can be decided which transaction is to be added to the blockchain.

4.1.2 Proof of Stake

Proof of stake (PoS) consensus requires the node with larger amount of stake (e.g., coin, mileage, speed, etc.) to validate the data [23]. The stakeholders having more coins are more likely to add a new block to the existing blockchain [24]. PoS consumes less power as compared to PoW. In PoS, at the establishment of blockchain network, tokens are distributed to all the validating nodes. During regular time intervals, a specific node is selected to commit the new block. But if any node having more stakes, it has more power and it can commit the new block. Usually, PoS requires considerably less computational work, so the cost of executing PoS is substantially lower. Main problem with the PoS is "nothing at stake" problem. In the PoW blockchains, reward is given to the longest chain, so the miners are awarded to mine one single chain. But with PoS, there is little to prevent a miner from mining on numerous PoS chains and the cost of mining is very low. Therefore, a PoS miner operating on various chains can make it difficult for the network to reach consensus.

4.1.3 Delegated Proof of Stake

There are many peoples in delegated who have to vote for a delegation, which also includes some "witnesses" who are miners who review the transactions and maintain the chain [25]. A person having more stakes has more power to vote for the witness. After the review, the witnesses, therein check the transactions and create blocks, including the valid ones. The list of witnesses is always mixed. The witnesses will have to produce blocks consecutively in the list one at a time with a build up speed of 2 s per block. If a witness does not produce his or her block, it may be removed from the delegation. Whenever a witness creates a block to attach to the chain, he receives a reward.

4.1.4 Proof of Activity

The objective of the PoA protocol is to have a decentralized cyptocurrency network whose security is based on a combination of proof of work and proof of stake [26]. In general, PoW protocols give decision-making authority to entities performing computational tasks, while PoS protocols confer decision-making power to entities that hold a stake in the system. While we argue that proof of stake-based protocols offer significant benefits, proof of stake is neither problem-free nor effective in mitigating all the key risks that successful cryptocurrency faces.

4.1.5 Proof of Luck [27]

Proof of luck is an example of an Intel SGX-based consensus protocol, where all participants choose a random number (good luck) and a large number of wins (lucky ones). The lucky block is then used as the next block in the blockchain. Random number selection takes place in the SGX environment so it cannot be duplicated. Each CPU can only select one random number per block. To execute it, after all the ledgers from all the miners are synchronized, each miner will create for themselves a new block to append to their current chain, then a random number ranged from 0 to 1 will be assigned for each created block, which could be considered a lucky value. All of the nodes will have to agree that the chain with the total largest lucky value would be the main chain. As a result, proof of luck is considered to be fair for all the miners. Furthermore, it would be very difficult to make attacks, like double-spending attack, because the attacker should be very lucky to perform their illegal actions successfully.

4.1.6 Proof of Importance

The proof of importance is a modified version of the proof of stake, where instead of taking into account only the balances of the nodes, to determine the next winning node; to solve the upcoming block, it considers the aspects, including the reputation specified by a function defined by the particular system and the number of node transaction [28]. Therefore, this consensus method considers the productive network activity of the nodes that is more effective than the only equilibrium of nodes [29]. NEM is a cryptocurrency that uses PoI for consensus.

4.1.7 Proof of Elapsed Time

PoET is designed to achieve distribution consensus in a lottery type function. It was originally designed with the aim of create a fair mechanism to distribute mining rights within permits networks [30]. PoET complies with a four-stage process flow. First, each validator requests a timeout period randomly distributed from a reliable enclave.

Second, the validator with the shortest waiting time wins the elections and is given the leadership for the transactional block in question. A function is used to create a timer for the transaction block that is guaranteed to have been created by the enclave. Then, another function is used to verify the origin of the timer. The enclave comes in the form of a secure CPU instruction set, ensuring equity in the randomness of the selection among all participants. This is achieved through low-level implementation, using Intel software protection extensions (SGX) [31]. This facilitates the PoET algorithm by providing a random distribution of leadership across a population of participants fairly. A certificate of execution provides verification of a claim from participants to the leadership, providing a low cost of participation. This offers a strong incentive for participation in the network, since the algorithm is perceived as fair and accessible.

4.2 Permissioned Blockchain

Synchronous Mechanisms:

RAFT Raft algorithm is considered as a consensus algorithm for private blockchains [32], which is applied more to ad hoc networks such as the intranet. Compared to PBFT and Paxos, the Raft algorithm is highly efficient and simple, and it is widely used in distributed systems. A Raft is a leader-based algorithm that uses leader selection as an integral part of the consensus protocol. Book entries in a Raft-based system are transferred in only one direction from the leader to other servers. A network is called split when more than half of the nodes are outside the control of the current leader. Host failure and communication interruption caused by packet loss are the main reasons for network separation. If the network splits up, the blockchain network with the Raft algorithm will restart the new leader election process.

Byzantine Fault Tolerance Byzantine fault tolerance is commonly considered with respect to Byzantine General Problem [33]. With regard to Byzantine General Problem, Byzantine fault tolerance is reached when loyal generals reach a majority agreement on their strategy. Typical Byzantine defects are the most difficult to treat, as no restriction or hypothesis is made around the behavior that a node can exposure.

Asynchronous Mechanisms:

Practical BFT The Practical Byzantine Fault Tolerance (PBFT) [34] is one of the most well-established BFT algorithms. In PBFT, there are two kinds of nodes: A leader node, and some validating peers (nodes); and these peers will execute some rounds for appending a block to the chain. Specifically, it relies on three cycles of message exchange; pre-prepare, prepare and commit phase before reaching an agreement. This ensures that $3f + 1$ nodes can reach consensus also in the presence of Byzantine knots; this turned out to be optimal.

Delegated BFT DBFT is a variant of PBFT. This fault tolerant algorithm divides client within peer-to-peer system into two types; ordinary node and bookkeepers [35]. An ordinary node does not participate in consensus, and it just votes the nodes which are supported by bookkeeper nodes. The selected bookkeeper nodes participate in consensus. A random bookkeeper node broadcast its transaction to the entire network. If 66% of other bookkeeper nodes agree about the validity of transaction, then it is committed and next round of consensus is started.

5 Challenges and Opportunities

Blockchain is currently the subject of numerous research and development activities, both by academics and industry. However, there are still major challenges ahead of the mass penetration and adoption of the market. In this section, we highlight the major challenges in different domains which can be resolved by using blockchain.

Blockchain for enterprise [36]: In the enterprise, blockchain as participants are already known, the scalability issue is easy to solve as compared to public blockchain. However, to reach scalability, we must first keep in mind the usage context and the performance measures, we want to optimize: the transactions throughput, validation latency, and number of participating nodes, number of validation nodes, energy costs, calculation costs, storage fees or other criteria. In overall, scalability is an active area of research; we can mention some initiatives such as: fragmenting a global ledger into smaller sub-ledgers which are running by a subset of nodes, removing old transactions in order to optimize the storage using a blockchain hierarchy. Though we have techniques like ring signature, zero knowledge proof, homomorphic encryption which provide privacy in public blockchain, by incorporating these techniques, privacy can be achieved for enterprise blockchain.

Healthcare industry [37]: Healthcare industry has a unique concern with regard to privacy and security in order to protect the medical information of patients. Interoperability is also a major issue in health sector. The main limitation that prevents interoperability is the use of centralized storage of data in medical applications and institutions. Centralized storage of data is a problem for healthcare providers because they store all records in a central database. Data portability and mobility is a growing demand in the health sector as patients become more mobile. Due to smart devices, sensors and other Internet features, devices become more predictable so the ability to carry this data is also important.

Security threats [38]: The 51% attack is a technique that occurs when an attacker has possession of 51% of the hash power. Formation of chain of blocks, which is separated from real version of chain initiates this attack. This chain becomes the real chain for execution. This allows the double-spending attack [39]. Since the blockchain policy abides by the longest chain rule [2], if attackers can get 51% of the hash power or more, they will be able to manage the longest chain by persuading network nodes to follow their chain. However, for double-spending attack, it is not

strictly necessary to obtain 51% of the hash power; it will work with the less than half of the hash power, but the success probability is less [40]. The stronger the blockchain network, the attack will become more expensive. Thus, cryptocurrencies with a high network hash are supposed to be more secure against the attack of 51%.

6 Blockchain Implementation

The expansion of blockchain platforms has introduced different architectures to satisfy the application requirements in an evolving communal ecosystem. In this section, we present a profane evolution of some of the blockchain architectures. We provide a retrospective analysis of these architectures and provide information on current problems for future areas of research.

Hyperledger fabric: Hyperledger fabric [41] (github.com/hyperledger/fabric) is an implementation of a distributed ledger platform for the execution of smart contracts, which exploits technologies, with a modular architecture allowing plug-in implementations of various functions. This is one of the many projects being incubated as part of the Hyperledger project. A developer version of the Hyperledger framework (called "v0.5-developer-preview") was released in June 2016. (Github.com/hyperledger/fabric/wiki/Fabric-Releases) The distributed ledger protocol is peerly managed. The fabric distinguishes between two types of peer: A validation peer is a node in the network responsible for executing the consensus, transaction validation, and general ledger. A non-validating peer is a node which serves as a proxy for connecting the clients (issuing transactions) to the validators. A non-validation the peer does not execute transactions but can verify them.

Ethereum: Basically, Ethereum is a "global computer" as a platform gives users the ability to run distributed applications in a decentralized environment way [42]. This means that applications running on Ethereum are available anywhere and anytime. Ethereum blockchain has two types of accounts: Externally account owned and contract account to specify an authorized SHS person. During installation, external property account was created automatically by default. Smart contract account can be configured with the processing policies transactions. Ethereum can be developed by using Turing-complete language such as solidity.

Corda: Corda is a distributed ledger platform for the collection and processing of financial data agreements. The Corda platform supports intelligent contracts that meet the definition of Clack, Bakshi, Braine. Corda provides framework for running smart contracts. It is a unique approach for data distribution and transaction semantics while retaining the functions of distributed ledgers, who initially lured institutions to projects like R3, namely reliable execution of financial arrangements in an automatable and enforceable manner [43].

Quorum [44]: Quorum was developed by JP Morgan [45] as an authorized implementation of Ethereum in the general ledger. Ethereum is a public blockchain without permission that can be used across several areas to implement decentralized applications. It supports Turing-complete intelligent contracts and can be used to build

general purpose blockchain applications in several areas. Being public and without authorization, its security is assured by the proof of work consensus algorithm. PoW consensus algorithm adds deliberate cryptographic difficulty to prevent Sybil attacks on Ethereum blockchain.

7 Conclusion

Blockchain technology has been a buzz in the computing era for the last few years due to its attractive characteristics such as immutability, distributed, transparent, and no central arbitrator. The data and transactions stored on blockchain are tamper-proof. Any node in the network can verify the correctness. The smart contract is an excellent application of blockchain, which is being used by many different domains. The transactions are packed into a block and every block is added to the chain after certain verification. The process of adding a block into the network is sometimes called mining where mutual agreement in terms of consensus mechanism plays a major role. In this research paper, we have studied the background theory for blockchain technology along with their types and classifications. Further, we have discussed various consensus mechanisms in detail with their detail analysis. We also have explored challenges and opportunities in the domain of blockchain consensus. In the future, we would like to propose a novel consensus mechanism, which would take criterion such as performance, a number of miners in the network, practical consideration (such as node/link failure), nodes credibility, etc., into consideration.

References

1. Haber S, Stornetta WS (1990) How to time-stamp a digital document. In: Proceedings of the 10th annual international cryptology conference on advances in cryptology, pp 437–455(11–15 Aug)
2. Nakamoto S (2008) Bitcoin a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
3. Helo P, Hao Y (2019) Blockchains in operations and supply chains: a model and reference implementation. Comput Indust Eng 136:242–251. ISSN: 0360-8352. https://doi.org/10.1016/j.cie.2019.07.023.(http://www.sciencedirect.com/science/article/pii/S0360835219304152
4. Litke A, Anagnostopoulos D, Varvarigou T (2019) Blockchains for supply chain management: architectural elements and challenges towards a global scale deployment. Logistics 3(1):5
5. Kouhizadeh M, Sarkis J (2018) Blockchain practices, potentials, and perspectives in greening supply chains. Sustainability 10(10):3652
6. Danezis G, Meiklejohn S (2015) Centrally banked cryptocurrencies
7. Biswas K, Muthuk kumarasamy V (2016) Securing smart cities using Blockchain technology. In: 18th IEEE international conference on high performance computing and communications, 14th IEEE international conference on smart city and 2nd IEEE international conference on data science and systems, HPCC/SmartCity/DSS, pp 1392–1393 (12, 14 Dec)

8. Liu PTS (2016) Medical record system using Blockchain, big data and tokenization. In: 18th international conference on information and communications security, ICICS (29 Nov–2 Dec, pp 254–261
9. Vukoli M (2016) The quest for scalable Blockchain fabric: proof-of-work vs BFT replication. In: IFIP WG 11.4 international workshop on open problems in network security, iNetS, pp 112–125
10. Idelberger F, Governatori G, Riveret R, Sartor G (2016) Evaluation of logic-based smart contracts for Blockchain systems. Cham, Switzerland, pp 167–83
11. Kraft D (2016) Difficulty control for Blockchain-based consensus systems. Peer-to-Peer Netw Appl 9:397–413 (201601-01)
12. Tama BA et al (2017) A critical review of Blockchain and its current applications. In: International conference on electrical engineering and computer science (ICECOS), IEEE
13. Drescher Daniel (2017) Blockchain basics. Apress, Berkeley, CA
14. Swan M (2015) Blockchain: blueprint for a new economy. O'Reilly, Sebastopol, US
15. Schwartz D, Youngs N, Britto A (2014) The ripple protocol consensus algorithm. Ripple Labs Inc White Pap 5:8
16. Brown RG, Carlyle J, Grigg I, Hearn M (2016) Corda: an introduction. R3 CEV 1:15
17. Sousa J, Bessani A, Vukolic M (2018) A byzantine fault-tolerant ordering service for the hyper ledger fabric Blockchain platform. In: 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN), IEEE, pp 51–58
18. Baliga A (2017) Understanding Blockchain consensus models. Persistent
19. Guo Y, Liang C (2016) Blockchain application and outlook in the banking industry. Fin Innov 2(1):24
20. De Angelis S (2018) Assessing security and performances of consensus algorithms for permissioned Blockchains
21. Lamport L, Shostak R, Pease M (1982) The byzantine generals problem. In: ACM Trans Program Lang syst 4:382–401
22. Bach LM, Branko M, Mario Z (2018) Comparative analysis of Blockchain consensus algorithms. In: 41st international convention on information and communication technology, electronics and microelectronics (MIPRO), IEEE
23. Yuan Y, Wang F-Y (2016) Towards Blockchain-based intelligent transportation systems. In: IEEE 19th international conference on intelligent transportation systems (ITSC), IEEE
24. Ray J (2018) Proof of stake FAQ. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
25. Nguyen GT, Kyungbaek K (2018) A survey about consensus algorithms used in Blockchain. J Inf process syst 14(1)
26. Bentov I et al (2014) Proof of activity: extending bitcoin's proof of work via proof of stake. ACM SIGMETRICS Perform Eval Rev 42(3):34–37
27. Milutinovic M et al Proof of luck: an efficient Blockchain consensus protocol. In: proceedings of the 1st workshop on system software for trusted execution, ACM
28. Salimitari M, Chatterjee M (2018) An overview of Blockchain and consensus protocols for IoT networks. Preprint at arXiv:1809.05613
29. Proof of Importance. https://nem.io/technology/. Accessed 05 Apr 2018
30. Maple C, Jackson J (2018) Selecting effective Blockchain solutions. In: European conference on parallel processing. Springer, Cham
31. Costan V, Devadas S (2016) Intel SGX explained. https://eprint.iacr.org/2016/086.pdf
32. D Huang, X Ma, S Zhang (2019) Performance analysis of the Raft consensus algorithm for private Blockchains. IEEE Trans Syst Man Cybern: Syst
33. Castro M, Liskov B (1999) Practical byzantine fault tolerance. http://pmg.csail.mit.edu/papers/osdi99.pdf
34. De Angelis S et al (2018) PBFT vs proof-of-authority: applying the cap theorem to permissioned Blockchain
35. NEO White paper (2014) http://docs.neo.org/en-us. Accessed 10 Feb 2018
36. Hamida EB, Brousmiche KL, Levard H, Thea E (2017) Blockchain for enterprise: overview, opportunities and challenges. In: The thirteenth international conference on wireless and mobile communications, nice, France, (ICWMC 2017). https://hal.archives-ouvertes.fr/hal-01591859

37. McGhin T, Choo KK, Liu CZ, He D (2019) Blockchain in healthcare applications: research challenges and opportunities. J Netw Comput Appl 135:62–75. ISSN: 1084-8045. https://doi.org/10.1016/j.jnca.2019.02.027
38. Sayeed S, Marco-Gisbert H (2019) Assessing Blockchain consensus and security mechanisms against the 51% attack. Appl Sci 9(9):1788
39. Jimi S (2018) Blockchain: how a 51% attack works double spend attack. https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474. Accessed 1 May 2018
40. Rosenfeld M (2014) Analysis of hashrate-based double spending. Preprint at arXiv:1402.2009
41. Cachin C (2016) Architecture of the hyperledger Blockchain fabric. In: Workshop on distributed cryptocurrencies and consensus ledgers, vol 310
42. Aung YN, Tantidham T (2017) Review of ethereum: smart home case study. In: 2nd international conference on information technology (INCIT), IEEE
43. Brown RG et al (2016) Corda: an introduction. R3 CEV 1:15
44. Baliga A et al (2018) Performance evaluation of the quorum Blockchain platform. Preprint at arXiv:1809.03421
45. Chase JPM (2018) A permissioned implementation of ethereum. https://github.com/jpmorganchase/quorum. Accessed 20 Feb 2018