Journal of King Saud University – Computer and Information Sciences 34 (2022) 6793–6807

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities

Bela Shrimali [a,*], Hiren B. Patel [b]

[a] LDRP Institute of technology and Research, Kadi Sarva Vishwavidyalaya, Gandhinagar, Gujarat, India
[b] Vidush Somany Institute of Technology and Research Kadi Sarva Vishwavidyalaya, Gandhinagar, Gujarat, India

ARTICLE INFO

Article history:
Received 18 March 2021
Revised 2 August 2021
Accepted 2 August 2021
Available online 12 August 2021

Keywords:
Blockchain
Consensus
Cryptocurrency
Smart contract
Internet of Things

ABSTRACT

Blockchain is a chain of blocks where each block contains a set of transactions that are digitally signed by its verifier and stored across the distributed network so that all the legitimate stakeholders can access/verify them. Due to the attributes of Blockchain such as decentralization, immutability, auditability, transparency, and cryptographic security, it offers various benefits to different domains such as cryptocurrency, financial sectors, private/public segments, insurance, healthcare, supply chain management, Internet of Things, etc. However, the technology is in its early stage and still, there is a range of concerns that are yet to be addressed before its wide adoption. Through this paper, we intend to cover extensive study on the Blockchain that includes taxonomy, application/use-cases, consensus mechanisms, prospective research, future directions, and related technologies. This paper also aims to discuss the opportunities, benefits, and challenges of Blockchain technology and to assist the research community in understanding the same.

Contents

* Corresponding author.
E-mail address: bela_ce@ldrp.ac.in (B. Shrimali).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2021.08.005
1319-1578/

1. Introduction

Different kinds of agreements, contracts, and financial transactions are maintained and recorded in a fixed structure in our traditional business, social and political systems. Day by day, due to digitization and rapid growth in Internet technologies, we are moving towards a world where transparency is a mandatory expectation by end-users. In today's digital era, either in business or in any other communication, the participated stakeholders want to transact without any intermediary and expect trust and reliability through technology design. A Blockchain has been claimed as miraculous technology to fulfill these objectives. Initially, it is used with the cryptocurrencies such as Bitcoin (Nakamoto, 2008) and Ethereum (Wood et al., 2014). Bitcoin is introduced by Satoshi Nakamoto in 2008 (Nakamoto, 2008). He discusses the role of bitcoin as a cryptocurrency and Blockchain as its underlying technology. Blockchain has been highly appreciated for decentralized, peer-to-peer communication.

The emergence of Blockchain has made a tremendous impact on business and IT industries. Over the past few years, large companies such as IBM (IBM Home Page, 2016) makes efforts to provide more powerful, reliable, and cost-efficient platforms for it. The technical improvement in Blockchain from 1.0 to 4.0 has made it more suitable for industrial applications. More scalable, programmable, the optimized data structure for blocks and transactions, new consensus methods generates a huge demand of Blockchain all over real-world applications. Fig. 1 depicts the evolution of Blockchain Technology.

The evolution in the Blockchain has grown up exponentially from 1.0 to 4.0. The evolution originated with Blockchain 1.0 which was limited to store and transfer of value (e.g. Bitcoin, Ripple, Dash) followed by Blockchain 2.0 where its environment is programmable via smart contracts such as Ethereum and Cardano and Blockchain 3.0 in which the technology became applications-centric that reaches to daily lives by facilitating various industries such as healthcare, education, agriculture, e-commerce and many more. Examples of these enterprise Blockchains are Hyperledger, R3 Corda, and Ethereum Quorum. Next, Blockchain 4.0 removes almost all the limitations in the previous Blockchain. In Blockchain 4.0, it utilizes a distributed environment suffering from major issues like scalability and limited transaction per second. It has handle scalability, throughput, and latency. An example of it is RChain.

Business industries started striving to reshape their business models to gain benefit from this new technology. The Blockchain can be used by its three types of implementation environment (Michael et al., 2018):

1. Permissioned Blockchain (Vukolić, 2017): This environment provides proprietary (aka private or closed) networks that define and decide the participants and their roles. This is particularly developed by industries for their private commercial use.
2. Permissionless or public Blockchain (Bozic et al., 2016): This is an open-source environment that anyone can access, use and participate in. E.g. Bitcoin Blockchain (Nakamoto, 2008; Bitcoin Home Page, 2009)
3. Hybrid or Consortium Blockchain (Li et al., 2017): There is also a third category knows as hybrid or consortium Blockchain. It is derived from two of the basic Blockchain types mentioned above. In consortium blockchain, the control over the data read and write is defined for the number of participants. It is used by groups of organizations/firms, who collaborate with each other on some projects. Hence, they participate in the environment with restricted access to carry out their task and thus, get the advantages of technology within the consortium.

The comparison of these Blockchain environments is depicted in the Table 1. The comparison shows that a permissionless environment is highly scalable compare to permissioned and hybrid environment. In the case of security and immutability, permissioned environment is more secure and less vulnerable to any kind of attack. All three environments are transparent. But, permissioned and hybrid environments are fast in throughput compare to permission-less. Whereas, anonymity is purely maintained by permission-less environment in comparison to the other two. In permission less environment any participated node can participate in the mining process and can be a miner. Wherein, permissioned and hybrid environment, only selected nodes can participate in mining and they are called validators.

By facilitating with different environment, Blockchain technology provides various benefits as follow:

- Transparency: Transactions stored on the Blockchain are transparent to all the participated users. Blockchain uses the distributed ledger (a shared copy of document) kept by individual parties and can only be updated by the consensus mechanism, which means that the file can only be updated if all the legitimate parties agree to do so.
- Enhanced security: There are many ways by which Blockchain is more secure than the other record management systems. Transactions are added after the consensus by all permitted parties. Once everyone agrees upon the transaction, it is encrypted and securely linked with the previous block. Secured hashing mechanisms attached with each block are used to secure the blocks that hold the number of transactions. And hence, it is practically infeasible to temper a block as it requires modifications to other blocks in the chain too.
- Enhanced traceability: Tracking of data/process is easy with Blockchain. Transactions are visible to all parties which lead to traceability for any operation. If enterprise deals with the supply chain, the tracking of the product is easy through this technology.
- Fast and Efficient: In a traditional system, the paperwork is time-consuming, tedious, and prone to human errors. By automating it with Blockchain, the process becomes more fast and efficient and operates without any third-party intervention.
- Cost-effective: For any business, profit/cost-effectiveness is important. With this technology, it doesn't need any intermediary or third party; hence, it becomes cost-effective.

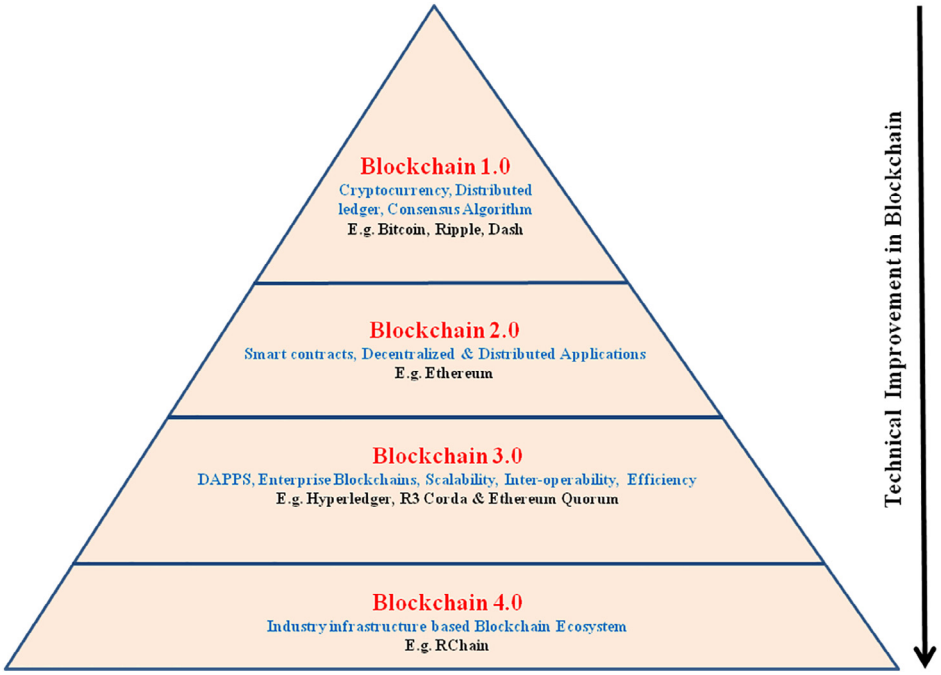

Fig. 1. Evolution of Blockchain technology.

Table 1
Types of Blockchain.

Blank	Public/ Permissionless	Private/ Permissioned	Consortium
Governance Type	Public	Single Node	Set of Nodes
Throughput	Slow	Fast	Fast
Node's Identity Disclosure	Not revealed	Revealed	Revealed
Energy Efficiency	No	Yes	Yes
Protocol	PoW,PoS,PoET		PBFT, PoA, Tendermint
Permission	Without Permission		With Permission
Example	Bitcoin, Ethereum, Ripple		Multichain, Hyperledger, Tendermint, Quorum
Attack (Double Spending)	Yes	Difficult	Yes
Transaction Validation	Any Node can be Miner		List of Authorized Nodes (Validators)
Scalability	High	Low/Medium	Low/Medium
Infrastructure	Decentralized	Decentralized	Distributed
Censorship/ Regulation	No	Yes	Yes

Along with features, it is important to identify and discuss the research challenges and issues. Many of the challenges have been already studied and addressed in Blockchain (Manoj and Krishnan, 2020; Saad et al., 2019; Lin and Liao, 2017; Sankar et al., 2017; De La Rosa et al., 2017; Aras and Kulkarni, 2017; Lu, 2018; Gao et al., 2018; Mingxiao et al., 2017). However, few unfolded challenges and limitations are needed to be studied further. In this paper, we present a survey of Blockchain technology, discussing its key concepts, architectural design, state-of-the-art use-cases/applications as well as research challenges. Our aim with this paper is to provide a better understanding of the basic fundamentals, taxonomies, and design challenges of its architecture and protocols to identify important research directions in this interesting technology.

The remainder of this paper is organized as follows. In Section 2, we provide an overview of Blockchain technology, the architecture of Blockchain, its design principles, and compare it with other related technologies. In Section 3, we describe, discuss and compare the consensus protocols of Blockchain. In Section 4, we summarize the current research topics and challenges in Blockchain. Finally, the paper concludes in Section 5.

2. Overview of Blockchain

This section presents a general overview of Blockchain including its definition, architecture, related technologies, and applications.

The main idea behind Blockchain is not a new one. Stuart Haber and W. Scott Stornetta (Haber and Stornetta, 1990) in the year 1991 worked on a cryptographically secured chain of blocks for timestamping the document system where they wanted the system to be tempered-proof (Haber and Stornetta, 1990). For the same, they used cryptographic hash function (Becker, 2008) and Merkle tree (Becker, 2008) to store the secured collection of certified documents in one block. However, this technology became popular and known after it was introduced and used in cryptocurrency such as Bitcoin, introduced by Nakamoto (2008) in 2008. Bitcoin was introduced as the first electronic payment system without third-party intervention using decentralized and distributed peer-to-peer networks. The term "Block" and "chain" used separately by Satoshi Nakamoto. That later on collectively used after being popular. The term "Block" signifies the collection of information including transactions and other related information

and "chain" signifies the connection/link between these blocks using cryptographic hash code. These cryptographically linked blocks made this technology more secured. The wide use and success of Bitcoin motivated other industries to make use of this. Officially, Blockchain can be defined as.

- As per NIST (Yaga et al., 2019), Blockchain is distributed digital ledger of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.
- An open distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way (Lakhani and Iansiti, 2017).
- A decentralized, distributed, and public digital ledger that is used to record transactions across multiple nodes to make the record and block tamperproof (Economist, 2015).
- A Blockchain is a transactional database–based record on a mutual distributed cryptographic ledger shared amongst all nodes participating in a system (Mainelli and Smith, 2015).

So, Blockchain, in a simple term, is a technology that provides accessible and verifiable data control over the distributed or decentralized environment to every participated node in a fast and convenient way. There is no single or centralized authority to validate/verify the nodes. Rather, to participate in a network, a node has to validate itself by solving a mathematical puzzle called a proof of work. A node that succeeds in a proof of work can introduce a block. We will see the block and its content in detail in the next subsection called architecture. Now subsequent subsection describes its architecture.

2.1. Architecture

Blockchain is a technology where multiple parties involved in communication can perform different transactions without third-party intervention. Verification and validation of these transactions/communications are carried out by special kinds of nodes called miners. The valid transactions are included in the data structure called a block. Execution of the current transaction depends on the previously committed transactions. In this way, this technology is helpful to avoid/restrict double-spending in the cryptocurrency system. The architecture of Blockchain is shown in Fig. 2. It depicts the block structure and its chain. We can see that the chain of blocks is created by the hash of the previous block. A block is divided into two components:

- Block header
- List of transactions

1. The block header is comprising of three components. The first component is the hash code of the previous block which links the current block with the previous one. The second component is comprising of mining statistics that are used to create the block. And the last component is the Markle tree root (that is nothing but the hash code of the current block) which is the base for verifying the integrity of all transactions residing in the block. To generate a hash code of the current block, we use the hash code of the previous block. Hence, if an attacker tries to modify the block contents, he/she has to modify all the hash code of the rest of the chain which is practically difficult to carry out. Thus, it makes the Blockchain tampered proof. The mining statistics include nonce, timestamp (that is recorded time), and mining difficulty (Economist, 2015). Merkle tree includes the hash chain of data blocks where transactions are hashed and attached with leaf nodes and non-leaf node includes the cryptographic hash of its child nodes of Merkle tree (Nakamoto, 2008). Fig. 3 depicts the description of Merkle tree.
2. The second component of the block is a list of valid transactions. The number of transactions in a block depends upon the block and transaction size.
   Authorization and authentication of the transactions are done by asymmetric cryptography. Once a transaction is included in the chain, it cannot be removed or altered. Blocks are chained together, where each block includes a hash of the previous block, and a chain of blocks (Blockchain) is created. Block will be accepted in the chain if it is valid and has proof of work, which is a computationally difficult hash generated by the mining procedure. As it has a secure hashing technique (E.g. SHA-256) with secure hash pointers pointing to the previous hash, it ensures that, if any of the blocks is modified, all succeeding blocks will have to be recomputed. Following are some taxonomy related to block and Blockchain. Fig. 4 depicts how the longest chain is accepted and added into the Blockchain and other shorter chains are rejected.
3. Orphan block: Miners try to mine blocks on their own with the list of transactions that are yet to be added. Once a block is mined by a miner, it broadcasts to all other nodes in the network for verifications.

Out of so many blocks in the network, the block with the highest consensus will be accepted to be added into the network. Other block(s) are considered as orphan block(s) and discarded later by the network. Orphan blocks have some transactions which have already been included in the valid block just added but may have some transactions which have not been considered yet. Such transactions are to be taken care of in further mining processes.

- Fork: All chain other than the valid one is called a fork. Sometimes a newly mined block gets connected to the orphan chain and hence not becomes part of the longest chain. Such connected blocks create a fork.
- Genesis block: The first-ever block created in the system is called the genesis block. In the case of the Bitcoin network, the Genesis Block is the first-ever block mined by creator Satoshi Nakamoto. The Genesis Block can also be called block 0 of any Blockchain system. It is the ancestor that every other block in the chain will follow (Home Page, 2012).

2.2. State-of-the-art

In this section, we present the state-of-the-art implementations of Blockchain. We first discuss the key technologies currently used for Blockchain. Then, we survey the popular Blockchain use cases and applications.

2.2.1. Related key technologies

Following are a few of the Blockchain underlying technologies, each of which shares certain aspects with Blockchain:

- Distributed Ledger Technology (DLT): Ledger plays an important role in commerce to record the information such as the valuation, properties traceability, financial transactions, etc. In the traditional approach also, ledgers have been very important. Due to the wide use of computers and digitization, ledgers have been shifted from papers to digital forms. In a simple computerized system also, ledgers have been validated and maintained by third parties. The distributed approach enables

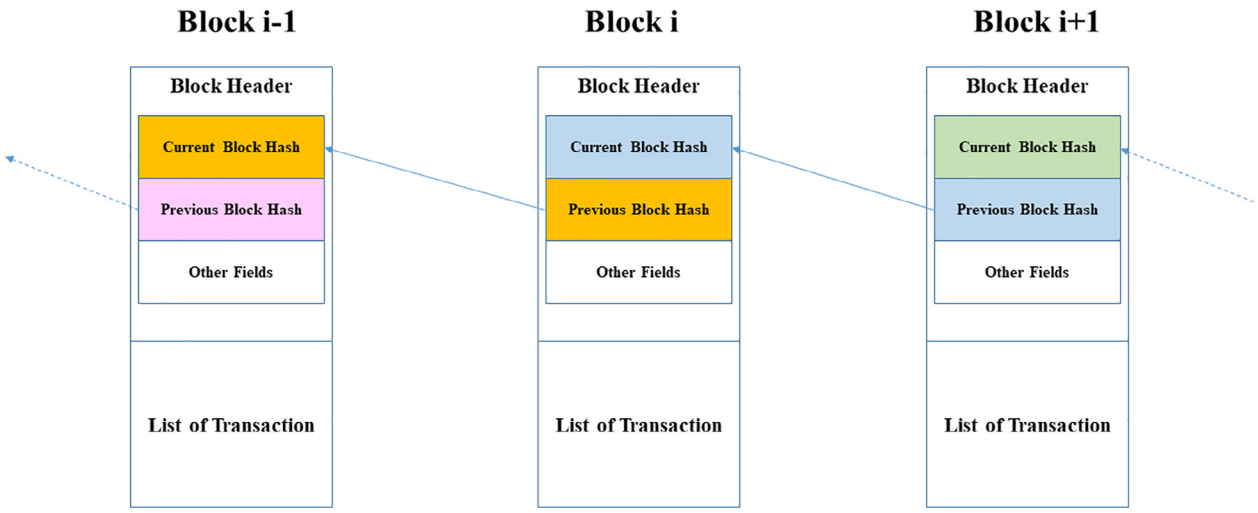

Fig. 2. Blockchain architecture.

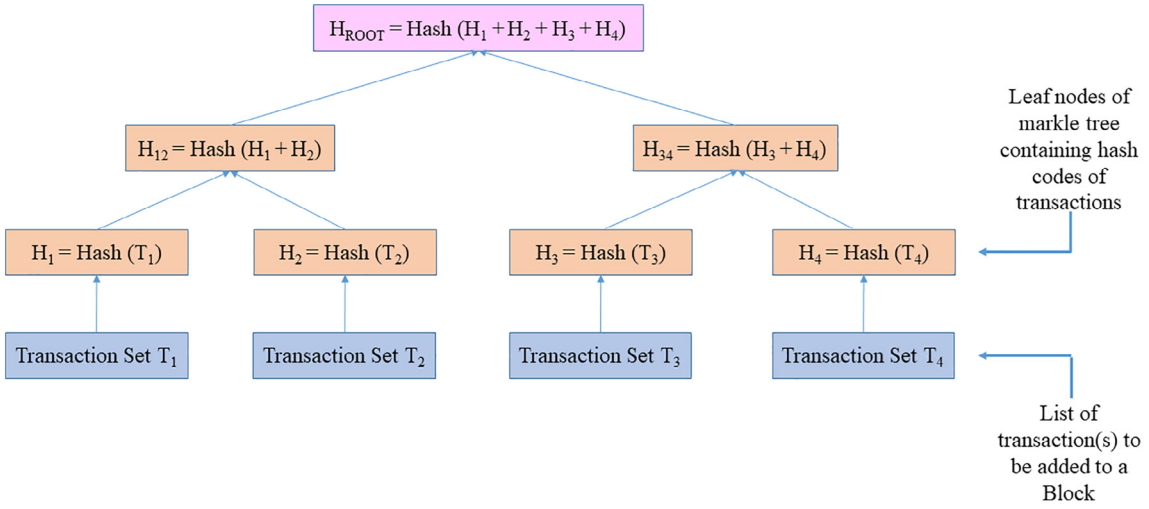

Fig. 3. Merkle tree.

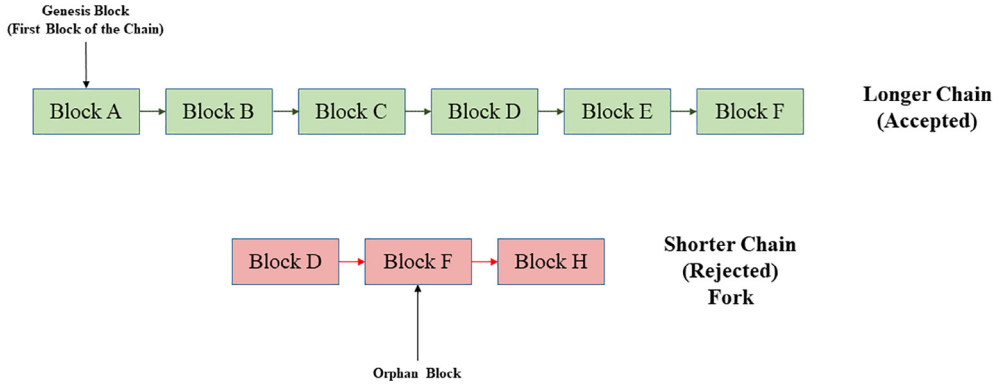

Fig. 4. Accepting/Rejecting a Chain.

the collaborative formation of digital distributed ledgers with the properties and capabilities of creation and modification by multiple parties involved. A distributed ledger is basically a database asset that can be mutually shared across multiple networks, institutions, and over geographical locations (Walport, 2016). All participants within a network can have their own identical copy of the ledger. Any changes/updates to the ledger are reflected in all copies within the predefined time interval. The ledger is kept secured and accurate through the use of cryptographic algorithms such as digital signatures and hash func-

tions. The control over the ledger for modification or creation is defined by the mutual agreement called consensus. This will define who can do what within the shared ledger.

- Smart Contract: Smart contract is treated as a computer algorithm that allows to carry out mutual understanding in form of an agreement between multiple stakeholders without the intervention of any of the involved parties or third party. It is a contract in which the terms of the agreement between the buyer and the seller are written in the line of code that executes according to pre-defined requirements (Home Page, 2019a). In simple term, the smart contract is a self-executable line of code which is implemented/maintained/regulated on terms and agreements made between two or more parties. Distributed ledgers are applied and executed through smart contracts. Blockchain technology relies on smart contracts to implement business logic on the shared ledger.
- Cryptographic techniques: Security is a prime concern in almost every application that runs on the Internet. Following are the two major concerns of security in Blockchain.

1. Users' authentication and validation of transactions.
2. Tamper-proof chain of blocks.

For both of these, it uses different cryptographic techniques. For 1, it uses a digital signature using public-key cryptography for authentication and to prevent non-repudiation. Normally, an asymmetric key encryption algorithm such as RSA is used for it. Particularly, in Bitcoin, it uses Elliptic Curve Digital Signature Algorithm (ECDSA). To create an immutable chain of blocks, it uses a Secured Hash Algorithm (SHA) that efficiently generates computationally verifiable hash code. As described earlier, blocks contain two parts, block header, and transactions. Block header contains a hash pointer that points to the hash of the previous block. Change/tempering in one block is to be reflected in all blocks and this is how Blockchain becomes tempered-proof. In summary, Blockchain leverages distributed ledger technology to achieve the successful execution of smart contracts using secured cryptographic methods. Using these technologies offers unique benefits and imposes distinct challenges to meet its requirements. The implementation of secured distributed ledgers with embedded smart contracts will turn into many efficient blockchain applications.

2.2.2. Use-cases

After the Bitcoin revolution and popularity, industries were/are keen to use Blockchain technology to build distributed and secure systems for inventory (Palamara, 2018), manufacturing (Polkowski et al., 2018), supply chain (Osei et al., 2018), IoT (Zhou et al., 2018), finance (Gandhi et al., 2019), governance, and many more. After discussing the permission-less and permissioned Blockchain previously, in this subsection, we will discuss different applications and use cases of public/ permission-less Blockchain over the private/ permissioned Blockchain.

- Public/ Permission-less Blockchain: It is an open environment of Blockchain where anyone can join, participate and leave the network without permission. Public Blockchain protocols based consensus algorithms are open source and permissionless (Home Page, 2019b). Few examples of public Blockchain are Bitcoin (Nakamoto, 2008), Ethereum (Wood et al., 2014), Monero (Logo and van Saberhagen, 2014), Dash (Duffield and Diaz, 2015), Litecoin (Gibbs and Yordchim, 2014), Dodgecoin (Dinh et al., 2018) and other (Home Page, 2019b). Very popular applications and use cases of Blockchain in this category are Bitcoin and Ethereum. Here, we discuss them along with some more cryptocurrencies like litecoin, Bitcoin Cash, Cardano, and Polkadot in brief.
  - Bitcoin: It is a Blockchain-based decentralized digital currency that enables instant payments to anyone, anytime and anywhere in the world (Home Page, 2019c). This is a peer-to-peer currency transfer system where bitcoin is generated during the mining process when each time miners mine the new block. The number of bitcoins created per block is set to decrease gradually, with a 50% reduction for every 210,000 blocks, or approximately 4 years to handle inflation. Thus, the miners' rewards get reduced as time progresses. So, in the Bitcoin network, to maintain the reward prize and the interest of miners, it increases the transaction fee. It uses public-key cryptography to create and verify the digital signature. Bitcoin doesn't require any account or email address to log in Bitcoin wallet. Only bitcoin address is used for transactions and hence, the user remains anonymous. It uses FORTH-like language as a Bitcoin script to validate the Bitcoin transaction (SandipChakraborty, 2018). The consensus algorithm used for the bitcoin network is Proof of Work (PoW). It is discussed in detail in the next section.
  - Ethereum: Ethereum is another popular Blockchain platform. It actually facilitates developers to build and deploy decentralized applications. It uses Ether as a decentralized digital currency, also known as ETH (URL, 2019a). Ether does not only serves as a cryptocurrency but also enables the Ethereum network by paying for transaction fees and computational logical services. A decentralized application (or Dapp) serves a particular purpose to its users. For example, Bitcoin is a Dapp that provides its users a peer-to-peer electronic money transfer system enabling online Bitcoin payments. As it is decentralized, the network is not controlled by any individual or central entity. Any centralized services can be decentralized using Ethereum. Ethereum is also used by organizations to build Decentralized Autonomous Organizations (DAO) which is nothing but a fully autonomous, decentralized organization with no centralized owner. It uses a programming code, on a collection of smart contracts implemented on the Ethereum Blockchain. This code will replace the centralized control and change the rules and structure of a traditional organization. Ethereum is also being used as a platform to present other cryptocurrencies. Because of the ERC20 token standard defined by the Ethereum Foundation, other developers can issue their own versions of this token and raise funds with an initial coin offering (ICO). In this fundraising strategy, the issuers of the token set an amount they want to raise, offer it in a crowd sale, and receive Ether in exchange. Billions of dollars have been raised by ICOs on the Ethereum platform in the last two years, and one of the most valuable cryptocurrencies in the world, EOS, is an ERC20 token (URL, 2019b).
  - Litecoin: Litecoin (Bhosale and Mavale, 2018) is a new cryptocurrency with fast transaction ability. As the name suggests, Litecoin is Lite in processing and can be mined in the desktop machine with less processing power. It was introduced by Charles Lee in Oct. 2011. Bitcoin uses the cryptographic hash SHA-256 algorithm wherein, Litecoin uses a newer algorithm called Scrypt. Around 84 million Litecoins are in circulation in the market, wherein, 21 million Bitcoins are there in the market. Litecoin transaction processing time is about 2.5 min compared to about 10 min for that of Bitcoin (Bhosale and Mavale, 2018).

- Cardano: Cardano (Houben and Snyers, 2018) is a permissionless Blockchain environment. Currency exchanges in this platform require a special wallet and interface as it deal with numerous transactions. It facilitates the open-source decentralized cryptocurrency called Ada (ADA). which can be used to send and receive digital funds. It is used in the Cardano platform, just like the currency "ether" uses in the Ethereum platform. Cardano also provides a distributed environment for decentralized applications and smart contracts like Ethereum. Cardano established with a vision to enhance security, scalability, and interoperability with conventional financial systems and regulations, by understanding, learning, and analyzing the Bitcoin and Ethereum (Investopedia, 2019a).
- Bitcoin Cash: Bitcoin cash is a cryptocurrency introduced in August 2017. Compared to Bitcoin, Bitcoin Cash increased the size of blocks and allow more transactions to improve scalability (Investopedia, 2019b). Like Bitcoin, Bitcoin Cash also uses the same consensus mechanism, hashing algorithm and other technicalities (Houben and Snyers, 2018).
- Polkadot: Polkadot is a distinct proof-of-stake cryptocurrency. Its main role is to deliver interoperability among other blockchains. Its mechanisms/protocols are designed to link permissioned and permissionless blockchains (Investopedia, 2019c). It allows the parallel Blockchain to work together with their own tokens for particular applications. In Ethereum, developers can create just decentralized applications with their own security measures, wherein Polkadot, developers can create their own blockchain with inbuilt security facility (Investopedia, 2019c). A Dot is used as a token in this cryptocurrency. The Polkadot architecture has three main layers viz. Parachains, Relay chains, and Bridges. Parachains represent the heterogeneous blockchains, relay chains control and manage transactional consensus and delivery, while the bridges work as a connector between the parachains to their consensus (Qasse et al., 2019).

- Private/ Permissioned Blockchain: It is a close environment of Blockchain where pre-define nodes can join and operate as per permission defined for them. Many organizations can participate and every organization would have different rights. Write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary level. Private Blockchains are a way of taking advantage of Blockchain technology by setting up groups and participants who can verify transactions internally. Retail, insurance, supply and logistics, healthcare, government, and public sectors are huge application/use cases of permissioned blockchain by industries. Here, we will discuss two successful use cases of permissioned Blockchain.

1. Project Ubin (Ubin URL, 2019): Project Ubin is a collaborative project of the Singapore government with the industry to explore the use of DLT (Ethereum) for clearing and settlement of payments and securities. Ethereum has shown potential in making financial transactions and processes more transparent, strong, and at a lower cost. The project is the joint venture of the Monetary Authority of Singapore (MAS) and the industry to understand the technology and use the potential benefits from the practical implementation. The project is implemented in two phases:
   (a) Phase I: Phase I identified what components of finance need to be included and whatnot. They have decided to start with inter-bank payments using Blockchain technology. The consortium includes Bank of America Merrill Lynch, Credit Suisse, DBS Bank, The Hongkong And Shanghai Banking Corporation Limited, J.P. Morgan, Mitsubishi UFJ Financial Group, OCBC Bank, R3, Singapore Exchange, UOB Bank, and BCS Information Systems as a technology provider to the project (Ubin URL, 2019).
   (b) Phase II: Reimagining Real-Time Gross Settlement (RTGS) on multiple DLT platforms is emphasized in phase II. Also, decentralized inter-bank payment and settlements with liquidity savings mechanisms are successfully introduced with three different DLT platforms (Quorum, Hyperledger Fabric, and R3 Corda). Moreover, It also fulfilled the objectives like Digitalization of Payments, Decentralized, Processing, Payment Queue, Privacy of Transactions, Settlement, and Finality.

   Project Ubin focuses on new methods to conduct cross-border payments using central bank digital currency as future work in the next phase (Ubin URL, 2019).
2. We.trade (We-trade Homepage, 2019): It is a digital platform for trade built on the IBM Blockchain Platform using Hyperledger fabric (Androulaki et al., 2018) that offers banks' customers access to a simple user interface, leveraging innovative Smart Contract and opening up potential new trading opportunities. It enables accurate trading posture information, settlement control, risk coverage, track and trace options. Near-real-time exchange of information, digitization of transactional financing and other complex processes, continual business and compliance readiness, scalability, and security are benefits of implementing trading on Blockchain.

2.2.3. Applications

Blockchain emerges as a new opportunity for this digital world. There are various fields where it can be applied. This section covers the two very important real-world applications of Blockchain.

1. Blockchain with 5G industrial automation: The Internet of Things (IoT) and 5-Generation network (5G) are the need of this era. Particularly when there is a diversity of consumers and a variety of digital applications. The 5G- enabled IoT (5G-IoT) will connect trillions of IoT devices communicating with each other in a real-time manner without any third-party interventions which enable the deployment of an application having a massive number of devices without worrying about network traffic or network related issues. However, the 5G-enabled IoT devices environment suffers from privacy and security issues because of having a centralized system that is more vulnerable to attackers. To resolve the same, Blockchain integration comes out as a promising technology as it offers a secure, transparent, reliable, and tempered-proof environment for 5G-enabled IoT due to its distributed and peer-to-peer network architecture (Surati et al., 2021). Many researchers (Liu et al., 2019; Zhang et al., 2019; Xiaoding et al., 2021; Jia et al., 2021; Wu et al., 2020) have proposed and claims the methods for integration of Blockchain with 5G industrial-IoT for the enhancement of performance in terms of security, privacy, immutability, and transparency.
2. Blockchain in 5G Healthcare: Healthcare is one of the most important industries that directly influences human lives. 5G brings so many opportunities for the digital healthcare industry. Remote surgeries, telesurgeries, and remote medical practices are being possible through 5G. Wherein, issues of privacy, security, and immutability can be resolve with the integration of Blockchain in 5G healthcare. Many researchers (Khujamatov et al., 2020; Srinivasu et al., 2021; Chamola et al., 2020; Wazid et al., 2020; Hewa et al., 2020) have discussed, proposed, and claims the deployment possibilities for integration of Blockchain with 5G healthcare to resolve the issues of security, privacy, immutability, and transparency.

3. Distributed consensus in Blockchain

Blockchain is a typical illustration of distributed computing in which decentralized consensus is a primitive issue as there is no centralized authority to obtain a common agreement. Various algorithms (as shown in Fig. 5) have been proposed over the last three decades to address the issue of consensus with a variety of assumptions. Putting in simple words, the consensus is about multiple entities/members/servers agreeing on the same value(s). According to Wikipedia (Wikipedia, 2019), consensus usually refers to general agreement among the members of a group or community. Wikipedia defines common agreement, collaboration, cooperation, democratization, inclusiveness, and participation as the key components for Consensus. To us, the consensus in Blockchain is basically a decision of the game of harmonization among multiple untrustworthy entities through a message-passing mechanism to achieve reliability and fault-tolerance in a multi-agent system. Unlike voting, where the majority elects a leader who in turn takes decisions, consensus, on the other hand, is a process of reaching a common agreement (proposed by a member of a group of members) that is applicable to all the members in communication. Many of the consensus algorithms work on the simple principle of "'collect/ validate/ order/ record/ discard"' transactions and sending the consistent and confirmed settlements (after the mining process) to the shared distributed public ledger which is accessible to all or to the authorized entities. The state-of-the-art theoretical implication of these algorithms is an area where much work can be carried out. In this section, we aim to describe various consensus algorithms being used by various platforms of Blockchain technology.

There are various properties (Watanabe et al., 2015) of distributed consensus algorithm viz. (i) termination - some value is generated as the outcome of consensus mechanism by an authorized entity (ii) validity - if the same value is being proposed by all entities then authorized entities agree on it (iii) integrity - every authorized entity must agree on one value which has previously proposed by some authorized entity (iv) agreement - every authorized entity must agree on the same value. To reach a common agreement or value, these properties must be satisfied. Consensus should be achieved even under various types of faults in the distributed system such as crash fault, network partitioned fault, or byzantine faults.

As shown in Fig. 5, the algorithms are classified into two broad categories viz. permissioned Blockchain and permission-less Blockchain. Most of the digital currencies available in the market work under the category of permission-less Blockchain where anyone can become part of the chain without requiring any authentication or other barrier. Users can simply create their personal addresses and start interacting with the Blockchain network without any censorship. Decentralization, anonymity, and transparency are the key issues in permission-less Blockchain. Bitcoin (Nakamoto, 2008) is an example of permission-less Blockchain and Proof of Work (PoW) (Vukolić, 2015), Proof of Stake (PoS) (Zheng et al., 2017), Proof of Activity (PoA) (Bach et al., 2018), Proof-of-Location (PoL) (Migliorini, 2018), Proof-of-Importance (PoI) (Bozic et al., 2016) and Proof-of-Elapsed-Time (PoET) (Bach et al., 2018) are few of the consensus mechanisms in the category of permission-less Blockchain.

Permissioned blockchain, on the other hand, is a closed or private network where users are not allowed to join without permission/authorization/censorship. Users are expected to know each other in this category of Blockchain. Permissioned Blockchain is used for any organization such as private corporate or consortium group where some authoritative entities are only permission to participate. Unlike permission-less algorithms where the miners need to use power, time, and/or Cryptocurrency, permissioned Blockchain avoids the mining (computational) overhead. However, the consensus among the users is a primitive challenge that could be handled through the concept of state machine replication. The major challenge in achieving the distributed consensus in permissioned Blockchain is a fault such as a crash fault, network fault, and byzantine fault. Ripple (Gomez et al., 2019) is an example of permissioned Blockchain. Varying decentralization, transparency, anonymity, and governance are the key challenges in permissioned Blockchain.

It works in two networking scenarios viz. synchronous environment and asynchronous environment. In the synchronous environment, the communication system must run under a common time clock with finite delay (mostly known as apriori). RAFT (Mingxiao et al., 2017), Paxos (Lamport et al., 2001) and Byzantine Fault Tolerance (BFT) (Cachin and Vukolić, 2017) are the consensus mechanisms used in permissioned Blockchain under synchronous environment.

In an asynchronous environment, such as the Internet, there is no bound on delay and hence time constraint should not be there. Obviously, the latter is more complex in nature as there are many different dynamic issues for considerations such as safety and liveliness which will be discussed during the discussion on individual

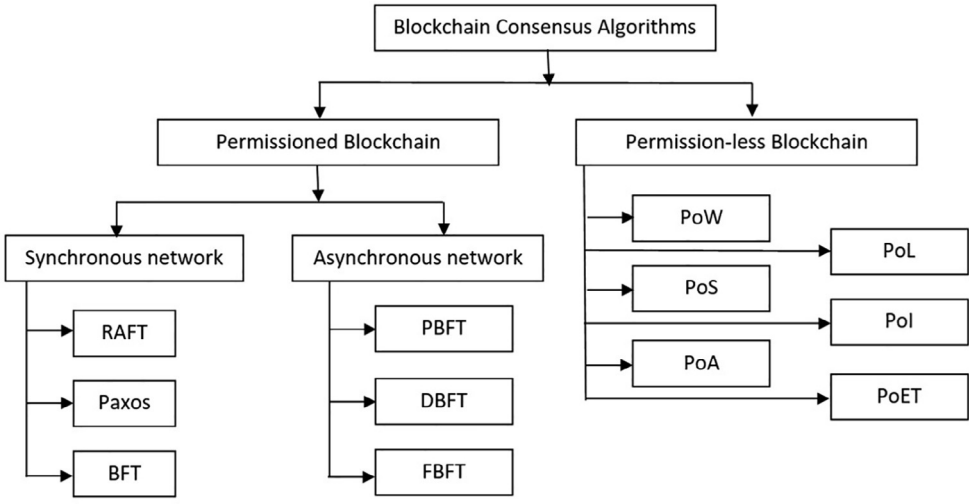

Fig. 5. Classification of Consensus Algorithms.

algorithms in the category. Practical BFT (PBFT) (Abraham et al., 2017). Delegated BFT (DBFT) (Nguyen and Kim, 2018) and Federated Byzantine Fault Tolerance (FBFT) (Nguyen and Kim, 2018) are the consensus mechanisms used in permissioned Blockchain under asynchronous environment. In the subsequent discussion, we study each of these algorithms in detail. We have mainly three algorithms under the category of permissioned Blockchain in synchronous network scenario viz. RAFT (Baliga, 2017) and Paxos (Lamport et al., 2001) which address crash and network fault and BFT (Abraham et al., 2017) which is Byzantine Fault Tolerance algorithm. Paxos (Lamport et al., 2001) works on a simple idea of proposing a proposal (having a unique number) from multiple proposers and acceptors either accept or decline the proposal based on its number. The higher proposal number is accepted whereas the other lower numbered proposals are discarded. The proposer getting a majority of the vote shall be elected as a leader who will be making decisions on behalf of the group. The final outcome is communicated to all the nodes in the network sometimes also known as learners.

3.1. Permissioned Blockchain

Permissioned Blockchain consensus mechanisms are divided into two broad categories based on the environment they work viz. (i) synchronous (ii) asynchronous Before we start understanding the protocols under the synchronous or asynchronous environment, we need to understand the idea of State Machine Replication (SMR) which is very helpful to achieve consensus in permissioned blockchain. The smart contract can be represented through a finite state machine (FSM). A crowdfunding application is a nice example of a contract presented through FSM. Rather than running the (smart) contract on each machine/node of the network, it is recommended to run it on a (sub) set of nodes and the network makes sure that the same state is broadcasted to other nodes of the network through a certain consensus mechanism. A typical state machine is comprising of a set of states (ST) with each state having a set of inputs (IN), set of outputs (OUT), transition function (ST X IN -> ST), output function (ST X OUT -> ST) and a start state (E.g. ST1). Through distributed SMR, state machines are synchronized across multiple servers to avoid any possible breakdown.

1. Synchronous Network Environment: Under this category, there are different protocols. We discuss here them one by one.
   - PAXOS: There are various types of faults in distributed consensus. Crash fault, network or partitioned faults, and Byzantine faults. Byzantine faults are further subdivided into malicious behavior nodes, hardware faults, and software errors. To handle crash and network faults, PAXOS (Lamport et al., 2001) and RAFT (Huang et al., 2019) are used whereas to address Byzantine faults (including crash and network faults), BFT (Hackfeld, 2019) and PBFT (Castro et al., 1999) are used. The idea behind the working of PAXOS is simple. Out of total nodes in the network, one or more nodes propose a value (in the form of the proposal with a unique and constantly incrementing number) which is propagated to the entire network. These nodes are known as proposers. Other nodes (known as acceptors) either accept or reject the proposal based on comparing the number associated with the current proposal with that of the received proposal. The third category of the node knows as the learner, learns the value chosen by acceptors through the majority voting principle.
   - RAFT: Primarily designed to act as an alternative to Paxos, along with the factors such as fault- tolerance and performance, RAFT mainly works on the idea of dividing the main problems into sub-problems and addressing individual sub-problem independently. Collaboratively, all nodes of the system select a leader and other nodes become followers of the leader. While selecting a leader, concept of majority voting is applied among the available candidates for leadership. The leader maintains and replicates the state transition (e.g. logs) among the followers. The leader keeps on informing all followers about its existence by sending a special message (called heartbeat). Followers do not issue any request on their own but simply respond to leaders' requests. Failing to receive a heartbeat from a leader (after a certain timeout), followers start a process of re-electing the leader. In case of failure or crash of a leader node, a new leader is selected (after a predefined timeout) with voting. When a failed node is recovered, it becomes the follower. Like Paxos, RAFT follows the concepts of majority voting, that is, as far as N/2 + 1 nodes are working (or in other words N/2–1 are failed nodes), it is resistant to Byzantine fault tolerance. The issue with RAFT is that the leader is supposed to be correct (or honest) as all the other nodes blindly follow the leader.
   - BFT (Byzantine Fault Tolerance): The basic issue with the distributed system is to achieve reliability by agreeing upon a common consensus among various decisions taken by multiple actors of the system. This issue is momentous when there are faulty or misbehaving actors in the system which may jar the system with inconsistency. Therefore, fault tolerance is necessary for the facet of achieving consensus. To understand the concern, the Byzantine Generals Problem was described in (Lamport et al., 2019) where there are multiple army generals (one being the commander and the other being the lieutenants) communicating through a message-passing system. Various cases have been discussed by considering one or more lieutenants either loyal or traitor, including a case where the commander is also considered as loyal or traitor. The problem can be formalized as Consensus can be achieved in a system with 3 N nodes (generals) where maximum N nodes (generals) are faulty (traitor). In other words, with 66.66% (2 N/3) honest/regular/loyal nodes and 33.33% (N/3) dishonest/faulty/traitor nodes, a system can achieve consensus. Byzantine Fault Tolerance is a system which remains tolerance towards node's failure belonging to the Byzantine faults.
2. Asynchronous Network Environment

- PBFT (Practical BFT): Introduced by Castro et al. (1999), PBFT was designed for Internet type of asynchronous communication environment where there is no upper limit (in term of time) concerning when the response to a particular request will be received. It was intended to address the issues raised in the BFT mechanism (such as failure to return a result, respond with incorrect/deliberately misleading results, etc). PBFT works on the principle of state machine replication where one node is primary (master/leader) (which is selected in a round-robin fashion) and other nodes are secondary (slave/backup/follower). Like BFT, to function PBFT properly, dishonest/faulty/traitor nodes should not be greater than (N/3) where N is the total number of nodes in the network. In other words, PBFT requires 3F + 1 replicas so as to tolerate F faulty nodes. PFBT works in four phases. In the first phase, the client sends a request to the primary node which in turn broadcasts the request to secondary nodes in the second phase. All the nodes (primary and secondary) respond to the client after performing the service request in the third phase. In the last phase, the request is considered to be successful if M + 1 replies are having identical results where M is the maximum number of faulty nodes.

PBFT aims to address the concerns in an energy-efficient way

i.e. without going for multifarious mathematical computations. PBFT also intends to provide transaction finality i.e. once transactions have been agreed upon (or finalized), unlike PoW, they do not need multiple confirmations. Further, as all nodes in the network take part in decision making (by responding to the request) it leads to low reward variance. However, PBFT is prone to be vulnerable to Sybil attack and it does not scale well because of heavy communication cost.

- DBFT (Delegated BFT): DBFT (Hackfeld, 2019) is claimed to be designed to address the challenges of scaling and performance which are the primary concerns for Blockchain implementation. In DBFT, the number of faulty nodes should not be greater than [(N-1)/3] where N is the number of active nodes. All active nodes (consensus nodes) are divided into small groups and each group selects their leader (delegate) by voting. All such delegates work to reach consensus and create new blocks whereas other nodes receive and verify blocks. There will be one overall leader from this group of delegates who is the decision-maker. If a group disagrees with its delegate it can elect a new delegate. For validating a block, the speaker sends a message to each delegate and the delegates having enough credentials (for example some gas money) verify each block. Misbehaving delegate may lose their gas money. For behaving regularly, the delegate gets rewards in form of transaction fees. If 2/3 of delegates agree with the speaker, the block is validated and added to the chain. If only 1/3 of delegates agree with the speaker, then the speaker can be replaced. Hence, the speaker cannot manipulate the process of validating the block for its personal gain because of the delegates. And delegate cannot manipulate because of its electing nodes otherwise it will be replaced.
- Federated Byzantine Fault Tolerance (FBFT): This variant of BFT is used in the Blockchain platform pertaining to payment protocol. Examples of such protocols are Ripple (Armknecht et al., 2015) and Stellar (URL, 2019c). As financial transactions are critical to performing, FBFT should be a confrontation with any type of fault/attack. In FBFT, the consensus is achieved through quorum slices. System-level quorums (slices) are formed and such slices unite the system together. FBFT promotes open membership to the network leading to organic network growth. Unlike permissioned-less protocol such as PoW and PoS, FBFT results in less computational and financial needs.

3.2. Permissionless Blockchain

- Proof of Work (PoW) (Vukolić, 2015): It is a consensus mechanism (used in Bitcoin (Nakamoto, 2008), Litecoin (Gibbs and Yordchim, 2014), Ethereum (Bogner et al., 2016), etc) where a compute-intensive mathematical problem is given to solve. For instance, a hash problem could be: Given Out and In1, compute In2, such that Out = Hash (In1 ——In2). Another way to represent the mathematical problem is through Integer/Prime factorization where a number is represented using the multiplication of two other prime integers. For example, 589 can be represented as the multiplication of two prime integers 19 and 31. Hence, given 589, finding out its prime multiplicands is a challenging task but given the multiplicands, it's very easy to compute the multiplication. The primitive property of such a problem is that it is difficult to solve but easy to verify (the correct solution). Fig. 6, demonstrates the working of PoW. In connection to Blockchain, the problem is floated across various stakeholders of the chain, and the (special) member (also called miner or a group of miners) who solves the problem first, is allowed to mine the block and claims the subsequent mining reward too. Bitcoin PoW uses SHA-256. Here, the miners are required to do some work to compute a number Nonce such that it satisfied the equation:

$$\text{Hash of Block} = \text{Hash}\,(\text{Hash of Previous Block} \,\|\text{Merkle Root}\|\text{Nonce}).$$

where all other variables are given to miners except Nonce. Here, an important aspect to note is the introduction of difficulty which is nothing but making the compute-intensive mathematical problem moderately complex to solve. The difficulty is adjusted based on various factors such as (i) expected time to mine the last certain block(s) (ii) actual time required to mine the last certain block(s), (iii) number of users in the network (iv) current power and (v) network load. The difficulty level satisfies the economical aspects of the Blockchain and helps controlling the inflation of the cryptocurrency. Lower/easy difficulty raises issues such as Sybil attack, DoS attack, Spam, and other vulnerabilities. Higher/hard difficulty raises issues of speed of block generation and de-motivation for miners. Hence,

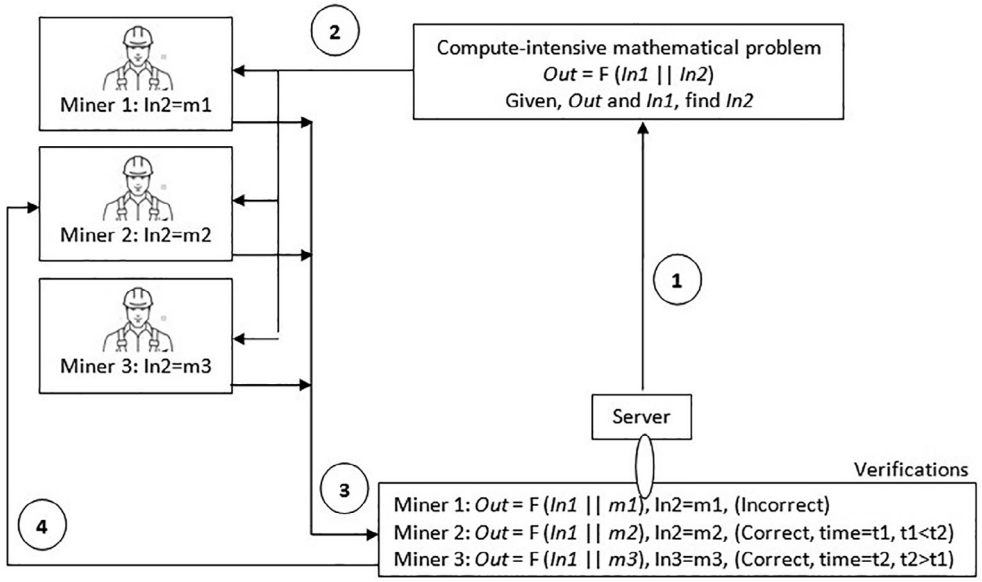

Fig. 6. Working of PoW Mechanism [1]: Server drafts Compute-intensive mathematical based on predefined difficulty. [2]: The Compute-intensive mathematical problem is floated across the network [3]: Miners try to solve the problem and submit the results to server for verification. [4]: Based on (i) solution proposed and (ii) time to solve the problem, the server selects a miner to mine the block, and accordingly, a mining reward is given to the chosen miner.

difficulty should be adjusted deliberately. However, due to the inherent nature of PoW, fix the number of miners having more computational resources may lead to an issue known as Monopoly or 51% attack problem. Further, it incurs huge computational power resulting in enormous electrical power leading to an increase in cost due to specialized hardware.

- Proof of Stake (PoS) (Zheng et al., 2017): PoS was primitively created as an alternative to PoW. Unlike PoW, where the miners are supposed to solve a compute-intensive mathematical puzzle to achieve distributed consensus, here in PoS, the miner (in fact, the block creator) is (randomly) selected based on the stake or minted coins (cryptocurrency such as Ether in Ethereum Ethereum Home page, 2020) it possesses. The Ether is locked during the process of adding the block into the network. And when the block is successfully added, the locked Ether is released. In case of any illegitimate attempt while adding the block, the penalty may be imposed and deducted from the already locked Ether. Moreover, there is no competition among the miners in PoS. Additionally, there is no (mining) reward in PoS but the block creator charges some transaction fees (as a reward) to add the block into the network. However, an obvious question may arise that the miner with a higher stake may behave maliciously but it may not be empirically achievable. For a block creator to add a spurious block into the network, it has to have more than or equal to 51% of the total cryptocurrency stake of the network which is practically very unlikely. A 51% attack ensues when a miner governs 51% of the computational power of the network which is improbable. It is detrimental for a block creator to attack the network where it possesses a 51% stake. Yet experts are skeptical regarding PoS as, without the penalty facet, PoS seems to be easy to attack. Some researchers (URL, 2019d; URL, 2019e) debate that PoS is not a perfect decision for a distributed consensus protocol. The major benefit of PoS is energy-saving due to the avoidance of compute-intensive resources.
- Proof of Activity (PoA) (Bach et al., 2018): PoA is a hybrid approach to achieve distributed consensus to ensures that the transactions are legitimate and common consensus is achieved. PoA lies somewhere between PoW and PoS. The mining process of PoW is used to generate blocks but to add the block into the network it switches to PoS type of approach is used where the validators put their stake to get itself selected for mining the block. The new block comprises a header and the miner's reward address. A new random group of validators is chosen (based on the header details) that sign the new block. Depending on the stake, a signer is selected. Indirectly PoA inherits the benefits of PoW and PoS. As far as the security of PoA is concerned, the attacker needs to have both (i) mining power in terms of computation and (ii) sufficient minted coins in terms of stake, hence adding an extra line of defense.
- Proof-of-Location (PoL) (Brambilla et al., 2016): PoL verifies one's location and the locations are encoded into blocks. PoL is useful for location-dependent functionalities. Proof of Location services (Researchly Page, 2016a,b,c; URL, 2016a) work on open-source maps and verifiable and tamper-proof geospatial data.
- Proof-of-Importance (PoI) (Bozic et al., 2016): Founded by a group called NEM (New Economic Movement) (URL, 2016b), the Proof of Importance (PoI) consensus mechanism decides the eligible nodes who can add a block to the chain, through a process called harvesting (such as mining). Nodes with a higher importance score (of their reputation) will have a greater chance of being selected to add a block. The node should have at least 10,000 vested XEM to become eligible for harvesting. Unlike PoS (the rich get richer), where only one parameter (the stake) was considered for selecting the node that can add the block into the chain, PoI considers overall support of the network to count the score with multiple parameters such as vesting, transaction partners, and number & size of transactions in the last 30 days. PoI has several benefits such as no hardware needed, inexpensive due to less resource-intensive, and keeps the process of harvesting fair, transparent and correct (in terms of offering incentives).
- Proof-of-Elapsed-Time (PoET) (Bach et al., 2018): Invented by Intel in 2016, it is a consensus mechanism used in permissioned Blockchain which is based on a simple lottery scheme with a sole purpose to offer an equal chance to every participating node in the network for adding a block. It avoids the usage of a compute-intensive mining process hence it is highly efficient and low power consuming. The functionality of this algorithm is simple. Every node goes to sleep mode for a random period of time. The node who wakes up first, adds the block and intimate to the rest of the network. Here, two factors are to be taken into consideration. First, the genuine process of generating randomness and second, no one cheats and wakes up before its time.

Summary and comparisons of various popular consensus protocols on the basis of different parameters such as strength, weakness, scalability, and many more in Table 2.

4. Research challenges and prospective future directions

Blockchain is identified and adopted widely. Extensive research and development from both academia and the industry are at their peak. However, there are still major challenges to be overcome before it's all over adoption. Many areas need to be concentrated. Many existing issues have not been fully addressed, while new challenges keep emerging from adopted applications by industries.

4.1. Research challenges Blockchain

In this section, we discuss the major research challenges and directions that we believe are important to explore. Swan (Swan, 2015) listed seven technical challenges and limitations for the full-fledged adaptation of Blockchain technology in the future are:

1. Throughput: The throughput of this technology reflects by the number of transactions added per defined time. If the Bitcoin network is considered then the throughput is up to 7 tps (transactions per second). Compare to other transaction processing networks like VISA and Twitter having 2000 tps and 5000 tps respectively, Blockchain technology also needs to improve its throughput capacity (Home Page, 2019c).
2. Latency: Secure and tamper-proof blocks are the major concern of current Blockchain technology. To avoid double spending and unauthorized transactions, most of the time is spent on verification and validation. Block creation and confirmation of transactions consume lots of time due to security concerns. So, currently, latency is a major concern in Blockchain.
3. Size and bandwidth: The size of a Blockchain depends on the number of blocks created. In Bitcoin, the size of one block is 1 MB, and it is created every ten minutes (Home Page, 2019c). Hence, there is a limitation in the number of transactions that can be included in the block. If the Blockchain includes/handles more transactions, the size and bandwidth issues of Blockchain can be resolved.
4. Security: Currently, Blockchain has a possibility of a 51% attack. There are many cases where even a single entity can have full control over a majority of the network. This can be considered a security concern and challenge. So, to overcome this problem, more research on security algorithms is required.

Table 2
Consensus protocols comparisons.

Protocol	PoW	PoS	PBFT	PoET	PoL
Type	Permissionless	Permissionless	Permissioned	Permissioned blockchain, with and without permissions	Permissionless
Performance	Low	Good	Good	Average	Average
Process of adding Block	Mining	Harvesting	Based on the total decisions submitted by all nodes	Random selection	Mining
Selection Criterion for Head Node	Voting	Polling	Voting	-	Voting
Strength	Most suitable for the untrusty environment	Complex and unnecessary calculations not required	Prone to be vulnerable to Sybil attack	Similar to Proof of Work but utilizes less electricity	Allows users to secure a specific GPS location and thus authenticate themselves on the network
Weakness	High cost of computing resources	Only miners with large stakes get chances	Extremely high-performance requirements for the network	Average	Average
Computing power efficient/Cost effective	Less	High	Less	High	High
Scalability	High	High	Low	High	High
Example	Bitcoin, Ethereum, Litecoin	NXT, Tezos, Ethereum	Hyperledger, Stellar, and Ripple	Intel	FOAM, Platin

5. Wasted resources: Mining procedure in the permissionless environment requires lots of compute-intensive mining work by miners. Many a time, due to the consensus protocol and time constraints, some of the mining work fails. Thus, time and mining resources are wasted. This issue of wasted resources is required to be resolved to have more efficient mining in Blockchain.
6. Usability: Blockchain applications should have user-friendly APIs. It has been found that the Bitcoin API for developing services is difficult to use (Home Page, 2019c). Development of a more developer-friendly API for Blockchain is required to make it more popular among developers.
7. Versioning, hard forks, multiple chains: A small chain and/or multiple chains with less number of nodes have more chances of attack. Another issue arises when chains are split for administrative or versioning purposes.

Along with these challenges, we also discuss other important challenges from the review study in the following sub-sections.

4.1.1. Real-time block analysis

In a distributed shared asynchronous environment, a block is introduced by miners through authenticating oneself. Along with the transactional data, the block also contains metadata in a block header that includes a time stamp, version, hash of the previous block, and nonce. Analysis of this block is the process of identifying, inspecting, verifying, and representing metadata of the block to discover useful information about the relevancy of the previous block, transactions, nonce, and timestamp. Blocks are introduced huge in numbers. Real-time analysis of block will reduce the chances of fork and attack. But to perform block analysis, real-time/on-time is a major challenge due to its anonymous and asynchronous environment.

4.1.2. Scalability

With the increased popularity of cryptocurrency and Blockchain technology, the number of transactions is increasing day by day resulting in the dense Blockchain. At present, Bitcoin Blockchain has exceeded 100 GB storage (Zheng et al., 2018). The Blockchain methodology needs all transactions to be stored for validation of every transaction. Moreover, due to the restriction on block size and complexity of algorithm to generate the new block, the bitcoin Blockchain cannot proceed/work for a real time environment, it limits itself to process only 7 transactions/s (Zheng et al., 2018). Also, as the capacity of blocks is very small, many small transactions might be delayed since miners prefer those transactions with a high transaction fee. However, large block size would slow down the propagation speed and lead to Blockchain branches. So scalability problem is quite complex. There are a number of efforts proposed to address the scalability problem of the Blockchain, which could be categorized into two types:

4.1.3. Storage optimization of Blockchain

According to IBM Blockchain storage documentation (Mencias et al., 2018), Blockchain ledger requires 6,912 MB i.e 0.00659 TiB/-transaction/yr for 1000 Transactions Per Block (TPB). So if modest transaction rates are considered, storage for Hyperledger Blockchain ledger is in the terabyte or multi-terabyte size. based on different considerations with the total size of the ledger and the total number of transactions stored, bitcoin is averaging close to 555 bytes per transaction (BPT) or 1889 TPB and Ethereum is close to 2 KB per transaction or 512 TPB. Blockchain also has off-chain storage to store other data. Off-chain storage is the personal storage of the node that participate. In chain, the storage is a crucial entity as the number of transactions increased and needs to use efficiently. A novel cryptocurrency scheme was proposed in Bruce (2014) to solve the problem of bulkiness. Their scheme removes the old transaction records from the network and used a database named account tree to hold the balance of all non-empty addresses. Thus, nodes do not need to store every transactions to check whether a transaction is valid or not. VerSum (van den Hooff and Kaashoek, 2014) was introduced to handle light weight clients. VerSum allows lightweight clients to outsource expensive computations over large inputs. It ensures that the computation result is correct by comparing results from multiple servers.

4.1.4. Redesigning Blockchain

Bitcoin-NG (Next Generation) was introduced in Eyal and Sirer (2014). The next-generation decouples conventional block into two

parts: key block for leader election and microblock to store transactions. In this method also miners are competing to become a leader. The leader would be responsible for microblock generation until a new leader appears. Bitcoin-NG also extended the heaviest (longest) chain strategy where only key blocks count and micro blocks carry no weight. In such a way, Blockchain is redesigned and the tradeoff of block size and network security has been handled.

4.1.5. Security and privacy

One of the key strength of Blockchain technology is distributed way of storing, creating, and validating data. Blocks are tempered proof because of their authentication method. There is various consensus algorithm mentioned earlier that allow miners to validate and introduce the block in the network. One of the famous consensus algorithms called proof of work needs a hash power to join the network and for the same miners are combine to join the network to mine more blocks. Such miners collectively create mining blocks that holds a maximum hashing power. Once, if, in a network it holds 51% of computing power, it can control overall Blockchain and affect the security of Blockchain. Also, (if someone/group have more than 51% computing/hash power)/ (51% attack) can decide block permission, can cause double spending by modifying transaction data, it can stop miners mining available block and can stop the verification of transaction (Lin and Liao, 2017).

4.2. Prospective future directions

Being an emerging technology, Blockchain has been explored by main organization and sectors for their possible adoption. In this section, we intend to make an exhaustive review which would help the research community to find out the possible integration of Blockchain technology with existing computation domains.

4.2.1. Big data management

Big data management is about generating and processing huge amounts of data which is in size gigabytes, terabytes, or more. Authors of Zyskind et al. (2015) introduced a decentralized personal data management system for user's authentication and access control mechanisms without requiring a trusted third party. Decentralization could be an appropriate approach to deal with Big data management. In Azaria et al. (2016), authors propose an approach to handle electronic medical records in a flexible and granular way. Secure data exchange without the need for a trusted third party was introduced by Chen and Xue (2017). Authors use immutable call logs through a set of network protocols to achieve security. The research in Yuan and Wang (2016) introduces an intelligent transportation system that stored data such as maintenance, resale, and traffic accidents, etc. in an immutable and irrevocable ledger with traceability.

4.2.2. Smart contract

Initially, the concepts of Blockchain were derived from cryptocurrency viz. Bitcoin. The usage of cryptocurrency required transparency and security. However, issues such as trust are to be resolved between two non-trusting parties especially when they do not interact directly. In real life situations, there are mutual agreements between the two such non-trusting parties which are notarized and can be produced in case of any legal dispute. Manual agreements and the court of law require a lot of documentation and time. Hence, smart contracts (primitively a set of codes having few ifs and buts) are introduced with the same motto to serve the same way, but with minimal documentation and quick response time, and of course without a trusted third party. An open-source platform for decentralized applications like (Wood et al., 2014) and hawk (Kosba et al., 2016) are being more popular platforms for smart contracts. However, smart contracts lack some implementation issues such as scalability and performance which are addressed by Alharby and Van Moorsel (2017). A defeasible logic framework has been introduced by Idelberger et al. (2016) to implement a logic-based smart contract that investigates different combinations for leveraging logic programming languages to operate smart contracts. A decentralized smart contract system viz. Hawk (Kosba et al., 2016) provides security and transparency through cryptographical protocols such as zero-knowledge proofs. Researchers (Atzei et al., 2017) has also worked on testing the vulnerability of Ethereum smart contracts by implanting deliberate attacks on Ethereum.

4.2.3. Artificial intelligence (AI)

Recent developments in Blockchain technology are creating new opportunities for artificial intelligence (AI) based applications for add-on privacy, security, and transparency. AI makes computers work as human intelligence. To make a machine work as intelligent as humans, AI models used to analyze, classify, and make a prediction of data. Deep learning and machine learning, areas of AI used the data to make the decisions. These models improve/learn/train themselves with the new data. This secure data used by AI models make the decentralized artificial intelligence. For example, in an application like Robotic processes automation, a logic written on smart contracts can control the misbehavior and operations/data. Authors of Ghassemi Toosi and Sai (2019) have shown how machine learning (such as linear regression and binary classification) techniques can be used to identify pattern-based frauds (on wallets with a high degree of cohesiveness) on the Blockchain. Access control mechanism has been introduced by Outchakoucht et al. (2017) in a distributed infrastructure for the Internet of things (IoT) environments. They have tested the same on an online learning mechanism of machine learning (reinforcement learning) algorithms in order to provide a dynamic, optimized, and self-adjusted security policy. Intelligent software agents have been used by Somdip (2018) to monitor the activity of stakeholders in the Blockchain networks to detect anomalies such as collusion. Authors introduced techniques of the supervised machine learning algorithms and algorithmic game theory to stop the majority attack from taking place in Blockchain. In Kurtulmus and Daniel (2018) authors proposed the DanKu protocol that utilizes the anonymous and distributed nature of smart contracts and the intelligent problem-solving aspect of machine learning. It also introduces a new method for crowdsourcing funds for computational research. The protocol potentially created a new marketplace where no middlemen are required. It further democratized machine learning models, and increase the opportunity in acquiring these models.

4.2.4. Internet of Things (IoT)

As the IoT has grown up at a rapid rate, the devices and sensors are communicating in the network. Important data like location, humidity, temperature, and human sensitive data are shared in a network. A permissioned Blockchain with IoT can make the tempered proof data in the network. With permissioned Blockchain, the partners automate the tempered proof process without building any centralized IT infrastructure. There are many IoT applications where Blockchain can play a vital role. In Healthcare applications, patient data transmit through IoT devices can be written using Blockchain can make the system non-vulnerable. Same way, in supply chain management, when data is passed through to permission Blockchain, IoT enabled packages to have different status information like time, dispatch time, temperature, and all. A smart contract will define the conditions to be met during the shipping of packages. This way, without creating any central infrastructural burden, Blockchain can make the application more

secure. In the same way, there are many fields of IoT where Blockchain can be applied. In Dorri et al. (2017), authors proposed (local and private) Blockchain-based smart home a framework to gain security goals of confidentiality, integrity, and availability. A study was made by Danzi et al. (2018) to investigate the synchronization between IoT devices and the Blockchain. They further learn the impact of the communication link quality, protocols' execution performance, and Blockchain parameters on the synchronization process. In clinical trials where trusting the third-party is inevitable, authors of Danzi et al. (2018) worked in the direction of (a) the characterization of the population of potential participants in the trial and (b) the effective recruitment of patients, to protect the interests of both the investigator (i.e., the utility of the data) and the participants (i.e., the privacy of the data). In Lin et al. (2018), Blockchain and IoT used together for agriculture purposes. They used IoT with Blockchain to insure more secure and fast access to data. The use of Blockchain also reduces human intervention to the system.

5. Conclusion

Started its journey from cryptocurrency, Blockchain technology is being explored in various fields such as smart contract, insurance, asset traceability, healthcare, IoT, supply chain management, financial transactions, electronic voting, logistics, manufacturing, etc. Through this comprehensive study, we have explored various dimensions of Blockchain technology containing its taxonomy, architecture, applications, use-cases, consensus mechanisms, prospective research directions, and future options. Nevertheless, being relatively infant technology, many concerns such as security, privacy, efficiency, scalability, energy consumption, interoperability, regulatory concerns, etc. are yet to be deeply investigated for its overall adoption. Based on our study, we identified and discussed a number of research opportunities in the various application domains. This study is expected to help the research community to understand various aspects such as research challenges and future directions of Blockchain technology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abraham, I., Malkhi, D., et al., 2017. The blockchain consensus layer and BFT, Bull. EATCS 3 (123).

Alharby, M., Van Moorsel, A., 2017. Blockchain-based smart contracts: A systematic mapping study, arXiv preprint arXiv:1710.06372.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, 1–15.

Aras, S.T., Kulkarni, V., 2017. Blockchain and Its Applications–A Detailed Survey. Int. J. Comput. Appl. 180 (3), 29–35.

Armknecht, F., Karame, G.O., Mandal, A., Youssef, F., Zenner, E., 2015. Ripple: Overview and outlook, in: International Conference on Trust and Trustworthy Computing, Springer, 163–180.

Atzei, N., Bartoletti, M., Cimoli, T., 2017. A survey of attacks on ethereum smart contracts (sok), in: International conference on principles of security and trust, Springer, 164–186.

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A., 2016. Medrec: Using blockchain for medical data access and permission management, in: 2016 2nd International Conference on Open and Big Data (OBD), IEEE, 25–30.

Bach, L., Mihaljevic, B., Zagar, M., 2018. Comparative analysis of blockchain consensus algorithms. In: 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, pp. 1545–1550.

Baliga, A., 2017. Understanding blockchain consensus models. Persistent 2017 (4), 1–14.

Becker, G. 2008. Merkle signature schemes, merkle trees and their cryptanalysis, Ruhr-University Bochum, Tech. Rep.

Bhosale, J., Mavale, S., 2018. Volatility of select crypto-currencies: A comparison of Bitcoin, Ethereum and Litecoin, Annu. Res. J. SCMS, Pune 6.

Bitcoin Home Page, 2009. https://bitcoin.org/en/blockchain-guide, accessed:31/05/2019.

Bogner, A., Chanson, M., Meeuw, A., 2016. A decentralised sharing app running a smart contract on the ethereum blockchain. In: Proceedings of the 6th International Conference on the Internet of Things, pp. 177–178.

Bozic, N., Pujolle, G., Secci, S., 2016. A tutorial on blockchain and applications to secure network control-planes. In: 3rd Smart Cloud Networks & Systems (SCNS), IEEE, pp. 1–8.

Brambilla, G., Amoretti, M., Zanichelli, F., 2016. Using blockchain for peer-to-peer proof-of-location, arXiv preprint arXiv:1607.00174.

Bruce, J., 2014. The Mini-Blockchain Scheme: White Paper, White Paper.

Cachin, C., Vukolić, M. 2017. Blockchain consensus protocols in the wild, arXiv preprint arXiv:1707.01873.

Castro, M., Liskov, B., et al., 1999. Practical Byzantine fault tolerance, in: OSDI, vol. 99, 173–186.

Chamola, V., Hassija, V., Gupta, V., Guizani, M., 2020. A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. IEEE Access 8, 90225–90265.

Chen, J., Xue, Y., 2017. Bootstrapping a blockchain based ecosystem for big data exchange. In: IEEE international congress on big data (bigdata congress), IEEE, pp. 460–463.

Danzi, P., Kalor, A.E., Stefanovic, C., Popovski, P.P. 2018.Analysis of the communication traffic for blockchain synchronization of IoT devices, in: 2018 IEEE International Conference on Communications (ICC), IEEE, 1–7.

De La Rosa, J.L., Torres-Padrosa, V., El-Fakdi, A., Gibovic, D., Hornyák, O., Maicher, L., Miralles, F., 2017. A survey of blockchain technologies for open innovation. In: Proceedings of the 4th Annual World Open Innovation Conference, pp. 14–15.

Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J., 2018. Untangling blockchain: A data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. 30 (7), 1366–1385.

Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P., 2017. Blockchain for IoT security and privacy: The case study of a smart home. In: IEEE international conference on pervasive computing and communications workshops (PerCom workshops), IEEE, pp. 618–623.

Duffield, E., Diaz, D., 2015 Dash: A privacycentric cryptocurrency, GitHub.

Economist, T. 2015. Blockchains: The great chain of being sure about things, Edición impresa 31.

Ethereum Home page, 2020. https://ethereum.org/, accessed: 13/01/2020.

Eyal, I., Sirer, E.G., 2014. Majority is not enough: Bitcoin mining is vulnerable. In: International conference on financial cryptography and data security, Springer, pp. 436–454.

Gandhi, H., More, R., Patil, N., 2019. A blockchain in banking application, Global J. Res. Anal. 8 (4).

Gao, W., Hatcher, W.G., Yu, W., 2018. A survey of blockchain: techniques, applications, and challenges, in: 2018 27th International Conference on Computer Communication and Networks (ICCCN), IEEE, 1–11.

Ghassemi Toosi, F., Sai, A.R., 2019. Using Artificial Intelligence To Detect Fraud On The Blockchain.

Gibbs, T., Yordchim, S., 2014. Thai perception on Litecoin value. Int. J. Soc. Behav. Educ. Econom. Bus. Ind. Eng. 8 (8), 2613–2615.

Gomez, M., Bustamante, P., Weiss, M.B., Murtazashvili, I., Madison, M.J., Law, W., Mylovanov, T., Bodon, H., Krishnamurthy, P., 2019. Is Blockchain the Next Step in the Evolution Chain of [Market] Intermediaries? Available at SSRN 3427506 (3427506), 3–22.

Haber, S., Stornetta, W.S. 1990. How to time-stamp a digital document, in: Conference on the Theory and Application of Cryptography, Springer, 437–455.

Hackfeld, J., 2019. A lightweight BFT consensus protocol for blockchains, arXiv preprint arXiv:1903.11434.

Hewa, T., Braeken, A., Ylianttila, M., Liyanage, M. 2020. Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT, in: GLOBECOM 2020–2020 IEEE Global Communications Conference, IEEE, 1–6.

Home Page, 2012. https://www.investopedia.com/terms/g/genesis-block.asp, accessed: 30/07/2019.

Home Page, 2019a. https://www.scalablockchain.com/, accessed: 4/08/2019.

Home Page, 2019b. https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/, accessed:14/04/2019.

Home Page, 2019c. https://en.bitcoin.it, accessed: 13/03/2019, 2019.

Houben, R., Snyers, A. 2018. Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion.

Huang, D., Ma, X., Zhang, S., 2019. Performance analysis of the raft consensus algorithm for private blockchains, IEEE Trans. Syst. Man Cybern.: Syst.

IBM Home Page, 2016. https://www.ibm.com/blockchain, url:https://www.ibm.com/blockchain, accessed: 12/12/ 2019.

Idelberger, F., Governatori, G., Riveret, R., Sartor, G., 2016. Evaluation of logic-based smart contracts for blockchain systems, in: International Symposium on Rules and Rule Markup Languages for the Semantic Web, Springer, 167–183.

Investopedia, 2019a. https://medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-cardano-a6ce4033985c, accessed: 20/06/2021.

Investopedia, 2019b. https://www.investopedia.com/terms/b/bitcoin-cash.asp, accessed: 23/06/2021.

Investopedia, 2019c. https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/, accessed: 27/06/2021.
Jia, B., Zhang, X., Liu, J., Zhang, Y., Huang, K., Liang, Y., 2021. Blockchain-enabled Federated Learning Data Protection Aggregation Scheme with Differential Privacy and Homomorphic Encryption in IIoT, IEEE Trans. Ind. Inform.
Khujamatov, K., Reypnazarov, E., Akhmedov, N., Khasanov, D., 2020. Blockchain for 5G Healthcare architecture, in: 2020 International Conference on Information Science and Communications Technologies (ICISCT), IEEE, 1–5.
Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C., 2016. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: IEEE symposium on security and privacy (SP), IEEE, pp. 839–858.
Kurtulmus, A.B., Daniel, K., 2018. Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain, arXiv preprint arXiv:1802.10185.
Lakhani, K.R., Iansiti, M., 2017. The truth about blockchain. Harvard Bus. Rev. 95, 118–127.
Lamport, L. et al., 2001. Paxos made simple. ACM Sigact News 32 (4), 18–25.
Lamport, L., Shostak, R., Pease, M., 2019. The Byzantine generals problem, in: Concurrency: the Works of Leslie Lamport, ACM, 203–226.
Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., Zhang, Y., 2017. Consortium blockchain for secure energy trading in industrial internet of things. IEEE Trans. Ind. Inf. 14 (8), 3690–3700.
Lin, I.-C., Liao, T.-C., 2017. A survey of blockchain security issues and challenges. IJ Netw. Secur. 19 (5), 653–659.
Lin, J., Shen, Z., Zhang, A., Chai, Y., 2018. Blockchain and IoT based food traceability for smart agriculture. In: Proceedings of the 3rd International Conference on Crowd Science and Engineering, pp. 1–6.
Liu, D., Alahmadi, A., Ni, J., Lin, X., Shen, X., 2019. Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain. IEEE Trans. Industr. Inf. 15 (6), 3527–3537.
Logo, M., van Saberhagen, N., 2014 Monero (cryptocurrency), WikiZER.
Lu, Y., 2018. Blockchain: A survey on functions, applications and open issues. J. Ind. Integr. Manage. 3 (04), 1850015.
Mainelli, M., Smith, M. 2015. Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology), J. Finan. Perspect. 3 (3).
Manoj, M., Krishnan, S.S.R. 2020. Decentralizing Privacy Using Blockchain to Protect Private Data and Challanges With IPFS, in: Transforming Businesses With Bitcoin Mining and Blockchain Applications, IGI Global, 207–220, 2020.
Mencias, A.N., Dillenberger, D., Novotny, P., Toth, F., Morris, T.E., Paprotski, V., Dayka, J., Visegrady, T., O'Farrell, B., Lang, J., et al., 2018. An optimized blockchain solution for the IBM z14. IBM J. Res. Dev. 62 (2/3), 1–4.
Michael, J., Cohn, A., Butcher, J.R., 2018. Blockchain Technol. 1, 7.
Migliorini, S., 2018. Enhancing blockchain smart-contracts with proof-of-location. In: 10th International Conference on Geographic Information Science.
Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C. 2017. A review on consensus algorithm of blockchain, in: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE, 2567–2572.
Nakamoto, S., 2008. Bitcoin:A peer-to-peer electronic cash system. Decentral. Bus. Rev., 21260
Nguyen, G.-T., Kim, K., 2018. A Survey about Consensus Algorithms Used in Blockchain, J. Inf. Process. Syste. 14 (1).
Osei, R.K., Canavari, M., Hingley, M., 2018. An Exploration into the Opportunities for Blockchain in the Fresh Produce Supply Chain.
Outchakoucht, A., Hamza, E., Leroy, J.P., 2017. Dynamic access control policy based on blockchain and machine learning for the internet of things. Int. J. Adv. Comput. Sci. Appl. 8 (7), 417–424.
Palamara, P., 2018. Tracing and tracking with the blockchain.
Polkowski, Z., Nycz, M., Borah, S., 2018. Blockchain Implementation In Business. Sci. Bull. Econ. Sci. 17 (3), 187–196.
Qasse, I.A., Abu Talib, M., Nasir, Q., 2019. Inter blockchain communication: A survey. In: Proceedings of the ArabWIC 6th Annual International Conference Research Track, pp. 1–6.
Researchly Page, 2016a. http://researchly.leobosankic.com/cryptos/fysical/, accessed:12/07/2019.
Researchly Page, 2016b. http://researchly.leobosankic.com/cryptos/xyo/, accessed:1/07/2019.
Researchly Page, 2016c. http://researchly.leobosankic.com/cryptos/foam//, accessed:12/08/2019.
Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., Mohaisen, A., 2019. Exploring the attack surface of blockchain: A systematic overview, arXiv preprint arXiv:1904.03487.
SandipChakraborty, P.J., 2018 Blockchain architecture, design and use case, nptel lecture series.
Sankar, L.S., Sindhu, M., Sethumadhavan, M., 2017. Survey of consensus protocols on blockchain applications, in: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 1–5, 2017.
Somdip, D. 2018. A proof of work: Securing majority-attack in blockchain using machine learning and algorithmic game theory, Ph.D. thesis, Modern Education and Computer Science Press.
Srinivasu, P.N., Bhoi, A.K., Nayak, S.R., Bhutta, M.R., Woźniak, M., 2021. Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network. Electronics 10 (12), 1437.
Surati, S., Shrimali, B., Patel, H., 2021. Introduction of Blockchain and 5G-enabled IoT Devices, chap. 4. Springer International Publishing, Cham, pp. 83–105.
Swan, M., 2015. Blockchain: Blueprint for a new economy. O'Reilly Media Inc.
Ubin URL, 2019. https::://www.mas.gov.sg/singapore-financial-centre/smart-financial-centre/project-ubin.aspx, accessed: 12/05/2019.
URL, 2016a. http://researchly.leobosankic.com/cryptos/platin/, accessed:12/09/2019.
URL, 2016b. https://nem.io/, accessed:12/09/2019.
URL, 2019a. https://www.blockchain.com/learning-portal/ether-basics, accessed 05/05/2019.
URL, 2019b. https://blockgeeks.com/guides/ethereum/, accessed: 27/06/2019.
URL, 2019c. https://fortune.com/2014/07/31/stripe-launches-bitcoin-challenger-gives-it-away-for-free/, accessed: 13/09/2019.
URL, 2019d. https://download.wpsoftware.net/bitcoin/pos.pd/, accessed: 15/12/2019.
URL, 2019e. https://blog.ethereum.org/2014/07/05/stake/, accessed: 3/11/2019.
van den Hooff, N.Z.J., Kaashoek, M.F., 2014. Versum: Verifiable computations over large public logs. In: ACM SIGSAC Conference on Computer and Communications Security, pp. 1304–1316.
Vukolić, M., 2015. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication, in: International workshop on open problems in network security, Springer, 112–125.
Vukolić, M., 2017. Rethinking permissioned blockchains, in: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 3–7, 2017.
Walport, M., 2016. Distributed ledger technology: beyond block chain (a report by the uk government chief scientific adviser), UK Government.
Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J.J., 2015. Blockchain contract: A complete consensus using blockchain. In: IEEE 4th global conference on consumer electronics (GCCE), IEEE, pp. 577–578.
Wazid, M., Bera, B., Mitra, A., Das, A.K., Ali, R., 2020. Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services. In: Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, pp. 37–42.
We-trade Homepage, 2019. https://we-trade.com/, accessed: 12/05/2019.
Wikipedia, 2019. https://en.wikipedia.org/wiki/wikipedia:what-is-consensus, accessed: 3/01/2020.
Wood, G. et al., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151 (2014), 1–32.
Wu, Y., Dai, H.-N., Wang, H., 2020. Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. IEEE IoT J. 8 (4), 2300–2317.
Xiaoding, W., Garg, S., Lin, H., Jalilpiran, M., Hu, J., Hossain, M.S., 2021. Enabling secure authentication in industrial iot with transfer learning empowered blockchain, IEEE Trans. Indu. Inform.
Yaga, D., Mell, P., Roby, N., Scarfone, K., 2019. Blockchain technology overview, arXiv preprint arXiv:1906.11078.
Yuan, Y., Wang, F.-Y., 2016. Towards blockchain-based intelligent transportation systems, in: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), IEEE, 2663–2668.
Zhang, K., Zhu, Y., Maharjan, S., Zhang, Y., 2019. Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things. IEEE Network 33 (5), 12–19.
Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., 2017. An overview of blockchain technology: Architecture, consensus, and future trends. In: IEEE international congress on big data (BigData congress), IEEE, pp. 557–564.
Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H., 2018. Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. 14 (4), 352–375.
Zhou, Q., Yang, Y., Chen, J., Liu, M., 2018. Review on Blockchain Application for Internet of Things. In: International Conference on Cloud Computing and Security, Springer, pp. 724–733.
Zyskind, G., Nathan, O., et al., 2015. Decentralizing privacy: Using blockchain to protect personal data. In: IEEE Security and Privacy Workshops, IEEE, pp. 180–184.