IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 2, 2021, accepted March 19, 2021, date of publication April 13, 2021, date of current version April 28, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3072849

A Survey on Blockchain Technology: Evolution, Architecture and Security

MUHAMMAD NASIR MUMTAZ BHUTTA[1], AMIR A. KHWAJA[1], ADNAN NADEEM[2], (Member, IEEE), HAFIZ FAROOQ AHMAD[3], MUHAMMAD KHURRAM KHAN[4], (Senior Member, IEEE), MOATAZ A. HANIF[5], HOUBING SONG[5], (Senior Member, IEEE), MAJED ALSHAMARI[1], AND YUE CAO[6], (Member, IEEE)

[1]Information Systems Department, College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2]Faculty of Computer and Information System, Islamic University of Madinah, Medina 42351, Saudi Arabia
[3]Computer Science Department, College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al-Ahsa 31982, Saudi Arabia
[4]Center of Excellence in Information Assurance, King Saud University, Riyadh 12372, Saudi Arabia
[5]Security and Optimization for Networked Globe Laboratory (SONG lab), Embry-Riddle Aeronautical University, Prescott, AZ 86301, USA
[6]School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

Corresponding authors: Muhammad Nasir Mumtaz Bhutta (mmbhutta@kfu.edu.sa) and Muhammad Khurram Khan (mkhurram@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research (DSR), King Faisal University, Saudi Arabia, under Grant 186218.

ABSTRACT Blockchain is a revolutionary technology that is making a great impact on modern society due to its transparency, decentralization, and security properties. Blockchain gained considerable attention due to its very first application of Cryptocurrencies e.g., Bitcoin. In the near future, Blockchain technology is determined to transform the way we live, interact, and perform businesses. Recently, academics, industrialists, and researchers are aggressively investigating different aspects of Blockchain as an emerging technology. Unlike other Blockchain surveys focusing on either its applications, challenges, characteristics, or security, we present a comprehensive survey of Blockchain technology's evolution, architecture, development frameworks, and security issues. We also present a comparative analysis of frameworks, classification of consensus algorithms, and analysis of security risks & cryptographic primitives that have been used in the Blockchain so far. Finally, this paper elaborates on key future directions, novel use cases and open research challenges, which could be explored by researchers to make further advances in this field.

INDEX TERMS Evolution of blockchain, blockchain architecture, smart contracts, blockchain applications, development frameworks, blockchain security.

I. INTRODUCTION

The concept of secured chain of blocks is not a new idea. It was presented by Stuart Haber *et al.* in 1991 as a means to digitally timestamp electronic documents to protect against tempering [2]–[4]. However, it gained popularity in the recent years when used in Blockchain technology to store transactions of a crypto currency called "Bitcoin" [1].

The Blockchain 1.0 technology is associated with Cryptocurrencies, especially Bitcoin. Bitcoin uses Blockchain as a way to solve the long-existing problems of double spending of digital cash and processing of digital transactions in a decentralized way without the need of any trusted third party. In a layman term, Blockchain is defined as the chain of digital blocks connected and associated with each other as an open distributed ledger. Initially, it was used to store only transactions of digital currencies, but later it started to use in other applications beyond currency and payments [7].

There are also different types of Blockchains based on their usage and distinct attributes: 1) Public blockchains 2) Private blockchains and 3) Consortium blockchains. Public blockchains are truly decentralized and allow anyone to join the network and engage in managing them. While in private blockchains only invited people from a single organization can join the network and manage them. The consortium Blockchain also called "Federated Blockchain" is between public and private Blockchain, in terms of permissions and management. Invited people from multiple organizations are

The associate editor coordinating the review of this manuscript and approving it for publication was Jenny Mahoney.

TABLE 1. Comparison of Recent Blockchain Survey Articles with this SURVEY PAPER.

Topic	Details of Topic	Addressed in Previous Survey Papers	Addressed in this Article
Preliminaries	Preliminary Concepts related to understand Blockchain	[20]	✓
Evolution	Blockchain 1.0 (Cryptocurrency) , Blockchain 2.0 (Smart Contracts) Blockchain 3.0 (Blockchain Applications)	[15][29]	✓
	Types of Blockchain (Public, Consortium, Private, Hybrid)	[8][13][16]	✓
Architecture (Components and Working)	Blockchain 1.0 (Cryptocurrency) Components and their Working	[8],[9],[11],[12],[13],[14] [15],[16],[17] [18], [19], [20], [21], [23], [24], [25], [26], [27], [28]	✓
	Blockchain 2.0 (Smart Contracts) Components and their Working	[8][13]	✓
	Blockchain 3.0 (Blockchain Applications) Components and their Working	[9][12],[22],	✓
Development Frameworks	Application Development Frameworks	[9][17]	✓
Security and Privacy	Open Research Issues and Challenges	[8] [11][15][16][17]	✓
Characteristics	Decentralization, Disruptive Technology, Scalability, Computation	[8] [9][11][16][18]	✓
Scalability	Scalability in terms of changing its structure or divide in multiple committees	[48][67][73][160]	✓

allowed to join this Blockchain. These different types of blockchains are described in detail later in this paper. The main strength of the applicability of Blockchain to such wide domains is in its characteristics or features like decentralization, pseudonymity, transparency, democracy, immutability, auditability, fault tolerance and security. The success of Blockchain technology also heavily depends on the availability of the application development frameworks (ADFs).

As one of the present technologies that have managed to attain huge fame, there are still numerous open issues in security and privacy associated with Blockchain innovation.

A. CONTRIBUTION OF THIS SURVEY AND COMPARISON WITH RELATED SURVEY ARTICLES

This paper mainly contributes to the existing knowledge in two broad ways. First, the Blockchain evolution and architecture in cryptocurrencies is reviewed as well as architecture and research developments pertaining to Smart Contracts (Blockchain 2.0) and Blockchain-based applications or ecosystems in general (Blockchain 3.0) beyond financial transactions. Second, we also present a comparative analysis of existing Blockchain frameworks, consensus algorithms, security risks, and future perspectives in this single paper. Recently, many survey articles have attempted to review the Blockchain technology in varying degrees of depth with a specific scope. However, based on the literature review, no paper has addressed detailed aspects of various versions of Blockchain technology, review of consensus algorithms, and security issues together in a single survey paper. This lack of comprehensiveness motivates us to contribute through this survey of Blockchain evolutions, architecture, consensus, and security in-depth in this paper.

Many survey articles are written in the recent past with only a focus on cryptocurrencies [8], [9], [11]– [21], [23]– [28], or only consensus algorithms [20], [26], [157], [170]. Some articles have superficially discussed smart contracts [8], [13] and Blockchain applications architecture [9], [12], [22]. Some survey articles have also presented different Blockchain applications [26], [151] while major review focus has been on Blockchain applications with other technologies like IoT and smart cities [8], [9], [14], [21]– [25]. The Blockchain security is also reviewed in some survey articles including [11], [15], [16], [29], [152].

However, on the other side, the contribution of this survey is as follows: preliminary technical concepts and characteristics and issues are discussed to enable the reader to understand the Blockchain concepts effectively. The architecture of all versions of Blockchain including cryptocurrencies, smart contracts, and generic applications, is reviewed in detail to guarantee the flow of understanding in a holistic manner. The design and working of components of all versions of Blockchain are presented with a clear distinction for different versions. The research related to consensus algorithms, development frameworks, and security is then reviewed in detail in this paper.

Ultimately the goal of this survey is to acquaint the researchers with inner technical details and research advancements of all versions of Blockchain technology. The similarities and differences of research areas addressed in this survey in comparison to previous survey articles are highlighted in Table 1.

B. ORGANIZATION OF THE SURVEY

The organization of the survey is as follows and shown in Figure 1: Section 2 discusses the background concepts as preliminaries for better understanding of core of this paper followed by characteristics of Blockchain. This section also highlights the challenges and issues of Blockchain technology. Section 3 presents evolution and types of Blockchain technology in detail. In section 4, we review existing

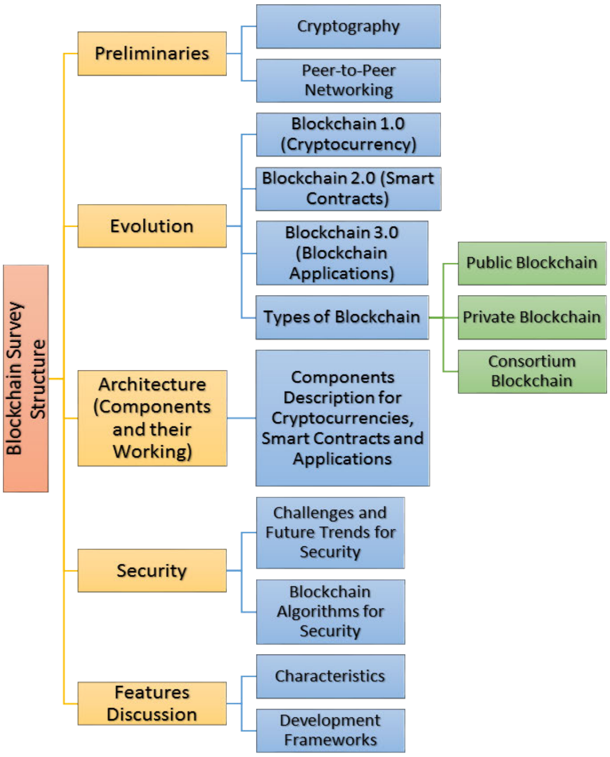

Blockchain Survey Structure
Preliminaries
Cryptography
Peer-to-Peer Networking
Evolution
Blockchain 1.0 (Cryptocurrency)
Blockchain 2.0 (Smart Contracts)
Blockchain 3.0 (Blockchain Applications)
Types of Blockchain
Public Blockchain
Private Blockchain
Consortium Blockchain
Architecture (Components and their Working)
Components Description for Cryptocurrencies, Smart Contracts and Applications
Security
Challenges and Future Trends for Security
Blockchain Algorithms for Security
Features Discussion
Characteristics
Development Frameworks

FIGURE 1. Structure and Contribution of this survey.

architectures and components of Blockchain in relation to cryptocurrencies, smart contracts and Blockchain applications in general. The research advancements in consensus algorithms are highlighted separately in section 5. A detailed discussion in research advancements and open research issues related to Blockchain security is included in Section 6. Section 7 describes the open research issues learned from the literature review to carry out in future and finally, Section 8 concludes the survey.

II. BACKGROUND, CHARACTERISTICS AND CHALLENGES

This section first presents the basic concepts of Blockchain technology and then discusses the characteristics and issues of technology.

1) PRELIMINARY CONCEPTS

a: PEER-TO-PEER (P2P) NETWORK

P2P network is a distributed network architecture to share resources among participants. The participants make their resources (processing power, link capacity, printers and storage capacity etc.,) available to be shared with other participants. Each participant node (peer) in such network acts in roles of both (client and server). At one time, peer A (acting as client) can directly request services and/or contents from other peer B (acting as server) of the network without any intermediate entities. Later, peer A may act as a server for a content or service request from peer B acting as client [1].

b: CRYPTOGRAPHY

The mathematical art of making communication secure is cryptography. It is commonly used in most modern security protocols [2]. In cryptography, a mathematical value called 'key' plays a central role. There are two types of modern cryptography:

- Symmetric key cryptography in which same key is used by sender and receiver for cryptographic operations.
- Asymmetric key cryptography in which, each communicating party has two different keys called public and private keys used for different cryptographic operations in different ways [2].

There are multiple operations performed in cryptography for provision of different security services like confidentiality (keeping information private to communicating parties), integrity (ensuring information remains in its original form), authentication (validating the identity of source) and non-repudiation (ensuring integrity and authentication) [2].

c: ENCRYPTION/DECRYPTION

Encryption is used for provision of confidentiality of security service. Encryption is a process to encode the plaintext (intelligible data) into cipher text (unintelligible data or ununderstandable data). The decryption is the reverse process to convert cipher text into plaintext. Encryption and decryption process can be implemented by using symmetric or asymmetric cryptography [3].

d: HASH

Hash is one-way mathematical function to protect the integrity of data. It works by calculating a fixed-sized unique value called "hash value" for every variable input. The hash function is one-way, which means original data cannot be calculated back from the unique output [3]. Its security strength lies on one-way characteristic, which is used to protect the integrity of data [3].

e: HASH CHAIN

A hash chain is generated by successively applying the hash function on a piece of data. For example, a hash value h_1 is generated by applying a hash function $f(x)$ on data x. The h_1 is input to the other hash function '$f(h_1)$' to calculate second hash value h_2 in the chain and so on. These calculated hash values $h_1, h_2, \ldots, h_n$ make a chain of hashes of length n. Because, hash functions are irreversible so h_1 cannot be computed from h_2 and then h_2 cannot be computed from h_3 and so on [4]. Hash chains have many applications for protection of data integrity and play a key role in Blockchain.

f: MERKLE TREE

Merkle trees also called hash trees provide efficient and secure verification of data by arranging the data and corresponding hash values in the form of a tree. In the tree structure, every leaf node is labelled with the hash value of some data and every non-leaf node contains the hash value of its child nodes. Figure 2 shows an example of a Merkle tree

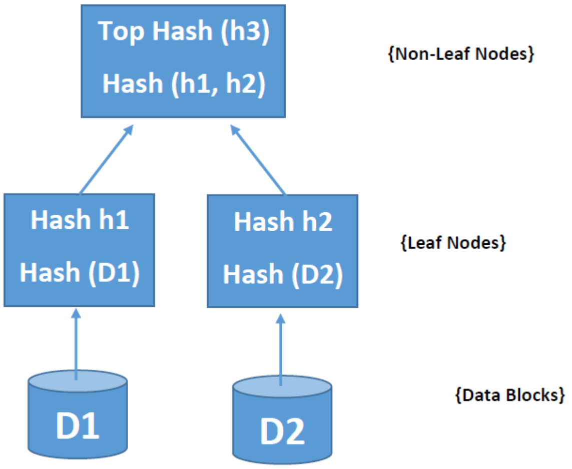


FIGURE 2. An Example of Merkle Tree (Binary Hash Tree).

in which data blocks represented as D1 and D2 are input to leaf nodes (hashes of D1 and D2) of Merkle Tree. From the hashes h_1 and h_2, another hash is calculated and is added as the parent node of child nodes [5].

g: DIGITAL SIGNATURES & TIMESTAMP

Digital signatures are used as a proof of authorship along with the contents. The signatures are usually applied using public key cryptography in which, a signer uses its private key to sign a document and a recipient can verify the signatures using signer's public key. Digital signatures are considered authentic, unforgeable, non-reusable and non-repudiated. It means that digital signature cannot be shifted for any other document/contents and one cannot deliberately claim the signature except the original signer and even original signer cannot repudiate it [3], [40]. Timestamp is the time at which event occurrence is recorded by a computer, rather than the time of event itself. Usually, it records the date and time of the day at which event occurred and is accurate to a small fraction of second. This timestamp's data is recoded in a consistent manner along with the actual data for easy comparison of two different records to track progress over time [6].

2) BLOCKCHAIN CHARACTERISTICS

This section synthesizes key Blockchain characteristics from literature. In doing so, the paper highlights variation in terminology for some of these characteristics which is quite natural for a technology considered in its infancy. The section attempts to unify the terminologies for various characteristics. The benefits and any possible issues related to each characteristic are also discussed. In addition, current issues with the Blockchain technology are identified and key research challenges are highlighted.

Following key characteristics have been identified for the Blockchain technology:

a: DECENTRALIZATION

Decentralization is perhaps the most important characteristic of the Blockchain. The Blockchain ledger exists on multiple computers, often referred to as nodes. These nodes form a Blockchain network with several of these nodes working in a P2P manner, validating access to the information without a centralized authority [50], [70] and [12]. The Blockchain system uses distributed system structure for recording, storing, updating, transmission, verification, maintenance, and several other processes related to the information in the Blockchain network [16], [71]. This decentralization characteristic eliminates the need for powerful central authorities and instead transfers control to the individual user making the system fair and considerably more secure. Information recording is performed, and the transactions are validated, using a set of rules and algorithms, called consensus protocols, among the Blockchain nodes to ensure that information is consistent and incorruptible [70] and [72]. Consensus is achieved when enough devices agree about what should be recorded onto a Blockchain. Chain nodes may use a pure mathematical method (asymmetric cryptography) to establish trust among each other without control of any central authority or regulatory agency to manipulate the data unilaterally [71]. Each distributed node in this network is relatively independent, have equal rights and obligations, and does not affect the entire network if there is a node level corruption, guaranteeing improved reliability and robustness of the Blockchain system [71]. Due to complex consensus mechanism required to edit or manipulate multiple copies of information recorded on the Blockchain; it can be certain that the information is genuine. Multiple copies of distributed information on the Blockchain also prevents the risk of information being lost or destroyed due to dependency on a centralized location. Moreover, removing a centralized body collecting, recording, maintaining, and, in general, unrestricted access to information, also improves privacy of users as well as eliminates misuse of the information. Finally, lack of reliance on a centralized body for executing and validating transactions can significantly reduce intermediary costs and improve performance bottlenecks at the central servers [71], [72].

b: TRANSPARENCY

Transactions on Blockchain ledger are completely transparent where anyone can see the details and history of any transaction. This level of transparency is unique to Blockchain technology and provides a high level of accountability and integrity to the information, ensuring that nothing is unduly altered, deceitfully added, or removed. This high level of transparency is unprecedented, especially for large financial systems. This level of transparency is achieved because a Blockchain network has several validating peer nodes without a centralized authority [12] as well as the fact that the holdings and transactions of each public address are accessible and open to viewing to anyone [70], resulting in traceable and transparent transaction records. Xinyi *et al.* [71] used the term openness to refer to the same concept. According to Xinyi *et al.* [71], the technical foundation of Blockchain is open source where any node can develop appropriate applications through an open interface to query data of Blockchain resulting in the data content and the operating rules of the whole system to be highly public and transparent with no deception between nodes [71]. Same transparency rules apply on any updates to any data in the Blockchain [16]. Zheng *et al.* [72] and Ferrag *et al.* [42] used the term auditability for high visibility, easy tracking, and verification of the transactions. In addition to significant importance of this characteristic for financial auditability of large companies, another key area where transparency characteristic has found its applicability is in healthcare and clinical trials data transparency. In healthcare, Blockchain technology can be used by individual patients to easily view all their claims, medical history, transactions, and overdue payments. Clinical trials data has traditionally been held from researchers, doctors, and patients, resulting in a lack of trust and credibility of findings [55]. Blockchain based methods were suggested to trace the existence of documents containing pre-specified end points in clinical trials [45]. Use of smart contracts were also proposed to act as a trusted administrator to address data manipulation issues common in clinical trials [55]. Supply chain management malpractices as well as obscurity of product history is also shown to benefit from the transparency characteristic of Blockchain [30], [43] and [161]. Non-fraudulent public elections and increasing voters' trust in the electoral process is also suggested to benefit from the transparency characteristic [53].

c: AUTONOMY

All transactions are usually based on trust which guarantees that the parties involved can depend on each other in fulfilling their commitments. Blockchain technology provides a system where trust is no longer an issue. This "trust free" system means that the Blockchain system can function in a P2P manner without a reliable third party required to ensure trust [70]. Some have called such systems "trustless" [32], [61] and [69]. However, this term has a negative connotation and implies that there is trust missing among the parties transacting using a Blockchain system [47]. Blockchain uses cryptography to completely replace third party as the governor of trust. Using the privacy and unforgeability of asymmetric cryptography, the Blockchain system protects message contents and verifies the sender identity, ensuring reliable transactions in the Blockchain system [71]. Complex distributed consensus algorithms are used by participating nodes on the Blockchain network to unanimously and securely add or update data to the distributed ledger of Blockchain, while solving the problem of ownership confirmation in transaction process as well as maintaining the system integrity [71]. These Blockchain transactions are accomplished without intervention of a third party to ensure trust due to the use of the failsafe consensus protocols providing the basis for the trust [16]. Elimination of these "middlemen" to ensure trust results in decreasing the overall cost of transactions.

d: SECURITY

Blockchain systems are inherently secure as these systems use asymmetrical cryptography consisting of set of public keys visible to anyone and a set of private keys visible only to the owner. These keys are used to ensure the ownership of transaction as well as the un-tamperability of the transaction [42] and [71]. Security in the Blockchain system is related to the integrity, confidentiality, and authorization of transactions [70]. The distributed nature of Blockchain system requiring P2P consensus mechanism eliminates single point of failure for data [70] versus that which is centrally stored and is far more vulnerable to being compromised.

e: IMMUTABILITY

Immutability is also called un-tampereability [71], persistency [72], and unforgeability [50], and immutability for Blockchain [16], [42], [70] and [12] means that once data is added to a Blockchain, it cannot be altered or tampered with. The data blocks in a Blockchain structure are time stamped and each block is encrypted with hash algorithm, making the entry of data permanent and tamper-proof unless consensus of majority of the nodes of the whole system [16], [71] and [12]. The transactions can be viewed by anyone anytime, however, once validated and added to the Blockchain, these transactions cannot be changed or deleted, making them irreversible and immutable [56]. Any change, no matter how small, will generate a different hash and can be detected right away, making the shared ledger immutable [70]. This feature has a great benefit for financial transactions and financial audits since either as a provider or recipient of data it proves that the data has not been changed. This characteristic also generates trust in the Blockchain system. However, immutability for Blockchain has its own issues and challenges and some have now started to question the benefits of immutability [39] and [40].

f: TRACEABILITY

Data traceability is to track the source, destination, and sequence of various updates the data goes through in between nodes. Needed for data integrity and higher levels of trust on the information, data traceability also has several other benefits of better data governance, conformity with regulations, understanding impact of change, and improvement of data quality among others [46]. Blockchain technology provides support for data traceability as information added or updated in a Blockchain system is time stamped. Time stamp technology is used to add time dimension for each data block and the hash values stored in each block correctly identifies the current and parent block [71]. Data traceability has high impact in the areas of financial transactions, clinical trials [72], and supply chain management [49] and [62].

g: ANONYMITY

Anonymity characteristic of Blockchain supports privacy, which is defined to be protected from unauthorized intrusion or observation. Anonymity is achieved by authenticating transactions without revealing any personal information of parties involved in the transaction. The data is exchanged between nodes using a defined algorithm establishing trust, hence the information of the nodes does not need to be revealed or verified and the information transfer can be carried out anonymously [31]. Users in a Blockchain system can interact with generated Blockchain addresses to keep their real identities hidden [16] and [72]. However, Blockchain cannot guarantee perfect privacy due to its inherent nature of distributed and public environment [72] and, hence, that is why some researchers have used the term pseudonymity [70] to define this characteristic of the Blockchain where anyone can create a Blockchain address and it is not possible to connect that address to a person without information from other sources [34].

h: DEMOCRATIZED

In a Blockchain system, decisions are made democratically by all nodes using P2P approach [70]. Consensus algorithms are used by all decentralized nodes to allow specific nodes for adding new blocks to an existing Blockchain as well as to ensure the block is appropriately appended to the shared ledger and its copies across the Blockchain nodes are synchronized properly [12], [70], [71]. All nodes participating in this decision process are relatively independent, possess equal rights and obligations, share data, and jointly maintain information in the Blockchain resulting in low maintenance cost overheads [71]. Nodes can vote based on their computing power, accepting valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them [54] and [72].

i: INTEGRITY

Blockchain systems, by design, are inherently resistant to changes in data. Data integrity is the assurance that the data in the Blockchain remains accurate and consistent over its entire life cycle [12]. This feature is achieved due to the decentralized and virtually immutable shared ledgers across the Blockchain network which means once a data block is agreed upon to be added to a Blockchain, the transaction record of that block cannot be edited or modified. This data is permanently preserved in the Blockchain system with multiple copies of it in various nodes across the Blockchain network, effectively guaranteeing the reliability and integrity of data [71].

j: INTEGRITY

Blockchain systems, by design, are inherently resistant to changes in data. Data integrity is the assurance that the data in the Blockchain remains accurate and consistent over its entire life cycle [12]. This feature is achieved due to the decentralized and virtually immutable shared ledgers across the Blockchain network which means once a data block is agreed upon to be added to a Blockchain, the transaction record of that block cannot be edited or modified. This data is permanently preserved in the Blockchain system with multiple copies of it in various nodes across the Blockchain network, effectively guaranteeing the reliability and integrity of data [71].

k: PROGRAMMABILITY

Blockchain technology is open source and users can develop applications through a common application programming interface [16] and [50]. The flexible script coding system can be used to create advanced smart contracts or other decentralized applications [71]. The SDN controllers of the nodes are used to provide programming interface for network management [42]. Li *et al.* [15] proposed a Blockchain-based data sharing system, called MeDShare, for cloud service providers consisting of user layer, data query layer, data structuring provenance layer, and existing database infrastructure layer. All Blockchain systems provide some programming language to implement transaction logic [70]. Ferrag *et al.* [42] suggest that these APIs should be as user friendly as possible. Examples of programmable blockchains consist of Ethereum, Tron, and Cardano among others.

l: FAULT TOLERANCE

Blockchain is inefficient and redundant by design to provide high levels of immutability and fault tolerance, both of which are important Blockchain characteristics [52]. Since Blockchain network uses P2P architecture, each node is considered equal to every other node and every node can act both as a client or as a server which gives the network an extremely high margin of error for nodes coming and going offline, for network transport issues, etc. [52]. Blockchains are designed to be Byzantine Fault Tolerant, which means the network will come to a consensus even if some nodes are down or not acting correctly. A consensus protocol is considered fault tolerant if it can recover from failure of a node participating in consensus [33]. Fault tolerance of the Blockchain system can recover from either fail-stop faults where some nodes fail to participate in the consensus protocol due to software or hardware reasons or Byzantine faults where nodes start to misbehave due to either software bugs or malicious attacks [33].

m: AUTOMATIC

Smart contracts on the Blockchain can automatically perform transaction generation, decision making, and data storage [70]. All nodes in the system can automatically transact and verify data using specific consensus protocols [50]. The Blockchain is maintained and validated automatically through a protocol without manual intervention [50]. However, just like any other computer program, smart contracts can also suffer from bugs and errors with no easy way to fix or update these contracts [51]. In addition, smart contracts can also be attacked by hackers just like any other software application.

3) CHALLENGES AND ISSUES

Even though Blockchain technology has gained fast momentum and has become the focus of research community, it is not devoid of issues and challenges that need to be addressed for this technology to become mainstream and to be deployed widespread. Some of the Blockchain issues and challenges are as follows:

4) SCALABILITY

Blockchain systems, as these exist today, suffer from scalability issues [66] and [12]. These scalability issues rise from limitations of low throughput, high transactional latency, and increasingly high resource needs [12]. The storage space requirements for the Blockchain will continue to increase as the number of transactions increase. For example, in September 2017, the Bitcoin size was about 158 GB with bootstrap time of approximately four days for adding a new node [12]. Such large storage requirements may eventually result in few large businesses to take control of majority of the nodes and may cheat whereas the other nodes are not able to detect this fraud [36]. These large blockchains, ever growing bigger with new data nodes, may become unwieldy in terms of loading, computing, and synchronizing data and may bring big problems to client running the Blockchain based system [16]. On-chain scaling and off-chain scaling (state channels) are some of the suggested techniques to address the scalability issue, but these are in very early stages and unproven techniques [12]. Edge computing is another suggested approach to address high computational resources and storage requirements distributed at the network edge, offloading the Blockchain and mining computation from the power-limited nodes [12]. Kim *et al.* [48] provide a survey of various scalability solutions consisting of on-chain, off-chain, sidechain, child-chain, and inter-chain-based solutions [48]. Authors in [156], discuss Blockchain scalability challenges and then classify the existing scalability solutions in two layers. The first layer focuses on changing the Blockchain structure in terms of its size and second layer divides the Blockchain in multiple committees.

5) PERFORMANCE ISSUES

Blockchain systems suffer from performance issues such as throughput bottleneck, transactions latency, and storage constraints [68]. For example, smart contracts in the current Blockchain systems are executed serially by miners and validators, which significantly limit the throughput [68]. Bitcoin transactions usually are verified in one hour, which is acceptable but not good enough [16]. Lightning Network [60] is a proposed solution to this problem that uses Hashed Timelock Contracts (HTLCs) with bi-directional payment channels allowing secure payments routing across multiple P2P payment channels. Blockchain community needs to explore utilization of today's concurrent multicore and cluster architecture to address these performance issues [68]. In [154] authors have performed a systematic study of performance evaluation of Blockchain exiting solutions using empirical evaluation methods including experimental analysis and benchmarking. They also suggest recommendations to optimize performance of Blockchain-based systems.

6) COST OF DECENTRALIZATION

Even though decentralization is considered one of the most important characteristics of Blockchain, it is not without a cost. For example, there is the open issue of consensus algorithms balancing between security and resource efficiency regarding adaptively controlling the replication factor in shards [67]. Moreover, append-only chains with historical data, such as spent transactions, will continue to grow to sizes that ordinary nodes will eventually run out of storage and the Blockchain network may by controlled by few powerful nodes [67]. One of the possible solutions is to investigate pruning out-of-date blocks that need to be forgotten without compromising its immutability [37]. However, except for some experimental work [35] and [59], the data pruning problem remains an open issue [67]. Another important aspect of cost is the monitory cost of using public Blockchain.

7) IRREVERSIBLE BUGS

Due to the immutability of the Blockchain, if deployed smart contracts have any bugs, there is no direct way to fix these bugs [68]. There is no easy way to patch a buggy smart contract without reversing the Blockchain which is a significantly daunting task [51]. Even if there is a way to update the defect, when a new version of an existing contract is deployed, there is no way to automatically transfer data stored in the previous version and the data needs to be manually updated in the new contract which makes it quite unwieldly [68]. Hence, properly designing safe smart contracts using software engineering principles and verification before deployment is critical [38] and [51].

8) ENERGY INEFFICIENT

The Blockchain proof of work (PoW) consensus approach for Bitcoin is an energy inefficient approach since the power spent to reach consensus using the PoW approach is almost 15.77-Terawatt hour, which is 0.08% of world's electricity consumption [63]. Most of this power is spent in computing the irreversible SHA256 hashing function [63]. Furthermore, the resource-intensive design of the Blockchain system to verify its transactions and the inefficient use of scarce energy resources for these financial activities is a serious threat for the global climate due to the greenhouse gas emissions [65].

9) ATTACKS ON BLOCKCHAIN INTEGRITY

Despite high security characteristic of the Blockchain systems, these systems are still prone to several security and data integrity attacks. These attacks may consist of PoW consensus related such as 51% majority manipulation [41], consensus delay due to distributed denial of service [44] and [58], selfish mining, pollution log, Blockchain forking, orphaned blocks, de-anonymization, and block ingestion [64], double spending attacks [58], and liveness attacks [89].

10) CENTRALIZATION ASPECTS

Even though Blockchain is inherently mostly decentralized, there are still centralized aspects such as cryptocurrency exchanges that may result in vulnerability for hackers'

TABLE 2. Unified Blockchain Characteristics and Related Issues.

Unified Terminology	Mapped Terminology in Literature	Related Issues/Challenges
Decentralization	Decentralization [16] [51] [71] [72] [12] [74]	- Complex security control - Resource inefficiency - High resource needs - Long and out-of-date chains pruning - Low performance due to transaction latency & throughput bottlenecks - Energy inefficient - Scalability
Transparency	Transparency [51][71][12] Auditability [42] [74] Openness [72]	- Privacy concerns - Opposite of anonymity
Autonomy	Autonomy [16] Trustlessness [72] Trust-Free [71]	- Few large corporations overtaking decision making based on computing power
Security	Security [72][42][71]	- Various types of attacks
Immutability	Immutability [42][16][71][12] Persistency [74] Unforgeable [51] Untamperability [72]	- Irreversible bugs in smart contracts - Cumbersome deployment of smart contracts patches - Hinderance in some application domain such as health care privacy of patients
Anonymity	Anonymity [16] [51][72] [74] Transactional Privacy [42] Pseudonymity [71]	- Lack of transparency about actual users involved in transactions
Democratized	Democratized [71] Persistency [74] Collective Maintainability [72] Synchronized through Consensus [12]	- Low performance due to large number of nodes involved in decision making - Few large corporations overtaking decision making based on computing power
Integrity	Integrity [12] Reliable Database [72] Data Reliability & Integrity [42][71]	- Various types of attacks
Programmability	Programmability [42][71] [72] Open Source [16] Openness [51] Blockchain-Based Control [12]	- Non-friendly user interface
Fault Tolerance	Fault Tolerance [33][42][53]	- Duplication of data at multiple nodes resulting in high storage requirements - Overhead of synchronizing all nodes for any updates
Automatic	Automatic [71] Independence [51]	- Irreversible bugs in smart contracts - Cumbersome deployment of smart contracts patches - Prone to hacks and attacks as any other computer software

attacks. Hackers can attack the single point of cryptocurrency exchanges to gain access [57]. These hacks have given rise to consideration for decentralized exchanges that do not store funds in a centralized location but rather promotes P2P cryptocurrency trading which are more resistant to such hacking attacks.

11) IMMUTABILITY HINDERANCE

Immutability feature of Blockchain may cause hinderance in the use of Blockchain in some applications. If used in the healthcare domain, for instance, the immutability feature may hinder implementation of the privacy laws which requires that an individual has a right to request their personal health data to be erased and not visible to others [40]. This is a sensitive issue and application of Blockchain for healthcare cannot be done without addressing this legal obligation [40]. A summary of characteristics, mapping of related terminologies in literature and relevant issues are shown in the Table 2.

III. EVOLUTION AND TYPES OF BLOCKCHAIN

In this section, we classify Blockchain technology evolution in three versions.

12) EVOLUTION

The Blockchain 1.0 technology as part of Bitcoin is associated with an unknown company identified by a tag ‘‘Satoshi Nakamoto’’ from 2008 [1]. Bitcoin used Blockchain 1.0 as a way to solve the long-existed problems of double spending of digital cash and processing of digital transactions without the need of any trusted third party as described below:

13) TRANSACTION PROCESSING

For long time, the financial institutions have been relying on trusted third parties for processing electronic payments. These third parties provide mediation for disputes between merchants and customers. These third parties spend time to provide additional information to customers and reversing the transactions if required. It can increase the cost per transaction and limit the transactions carried out for a merchant within a specific time however, there is no other mechanism to make payments over communication channel without a trusted third party. Blockchain provides a way to the willing parties to make transaction directly with each other without any existing trusted third party. The money of stakeholders is protected by providing a cryptographic proof instead of any already existing trusted party [1].

14) DOUBLE SPENDING PROBLEMS

The online payment system has been there for long time with inherent problem of double spending. The double spending problem is a potential flaw in online payment systems where same digital money can be spent more than one time to make different transactions. This becomes possible by exploiting the implementation details of saving money in the form of duplicated file or by providing falsified information [7].

Blockchain in cryptocurrencies is used as a public ledger to store all the transactions happening. Transactions are stored as a data structure in Blockchain called Blocks (described in detail in section 4 in this paper). New blocks are constantly added as transactions happen, thus continuously expanding the Blockchain.

Cryptocurrencies are considered the first application of Blockchain and have already been functional as a digital payment system on the Internet. With the ability of programming cryptocurrency as a network of decentralized trading of all resources, it had already been extended into Blockchain 2.0 to take advantage of more robust functionality of digital money.

Blockchain 2.0 was the next big tier in the development of Blockchain industry and is termed as ''Smart Contracts''. It is a concept for the decentralization of markets in general and support for transfer of many different kinds of assets like stocks, bonds, loans, mortgages, smart properties etc., beyond digital currency [7]. It was developed as a way to automatically enforce the rules agreed between interested parties like traditional business contracts. With the advancement in technology, it was realized that Blockchain can revolutionize all industries rather than just markets, payments, financial services and economies. This gave birth to Blockchain 3.0 called Blockchain Applications beyond financial markets in areas including government, health, literature and culture and so on [7].

Blockchain 3.0 is a platform to develop distributed and secure applications for all industries beyond the monetary markets. It supports a universal and global scope and scale by interconnection with the web technology. It is being seen as platform to contribute for the development of ''Smart World'', especially for resource allocation of physical-world and human assets [8], [9].

A. TYPES OF BLOCKCHAIN

Blockchains are classified into multiple types based on their usage and distinct attributes. All types of Blockchain examples are presented in all versions of Blockchain including cryptocurrencies like Bitcoin, smart contracts like Ethereum, and Blockchain applications like health sector.

1) PERMISSIONLESS OR PUBLIC BLOCKCHAIN

In permissionless or public Blockchain, system participants do not need any permission to join the network [10]. This Blockchain is truly decentralized as participants can participate in consensus process, read and send transactions and maintain the shared ledger [9]. New blocks can be published, accessed and validated by all participants thus they can maintain a copy of the complete Blockchain [8].

Public blockchains are secure in formation and operation. Though any participant can join the network and add transactions as blocks, these blocks are verified by computationally expensive consensus processes like puzzle solving or stacking one's own cryptocurrency. The tampering of the contents of blocks is protected by hashes and decentralized consensus. Also, a large number of nodes can be anonymous in Blockchain to protect their privacy [8].

Besides many benefits, public blockchains also have many open research issues as well. The challenges of achieving efficiency are influenced by the large number of participants and computationally expensive consensus mechanisms [10].

2) PERMISSIONED OR PRIVATE BLOCKCHAIN

Permissioned or private blockchains are designed for a single organization. Participants are allowed to join the network by invitation and play specific role to maintain the Blockchain in decentralized manner [10]. The private blockchains are different from public blockchains as only authorized entities are allowed to join the network and maintain the blocks [9].

Permissioned blockchains are considered more secure and efficient than public ones as only known participants join the network and tampering is similarly protected by hashes and consensus of participants as in the case of public blockchains. However, nodes in private blockchains are not anonymous [9]. The open research issues in private blockchains are related to tampering of blocks and network being hacked by internal authorized participants.

3) CONSORTIUM BLOCKCHAIN

Consortium blockchains are also private blockchains but are meant for multiple organizations. Only invited and trusted participants are allowed to join and maintain the network. The consensus process in this type is relatively slow as compared to private blockchains, but faster than public blockchains [10]. For security, consortium blockchains handle information in more protected way for alteration as compared to private blockchains. The hacking is also protected better in this type of Blockchain based on better security measures due to participants from multiple organizations [10].

IV. ARCHITECTURE OF BLOCKCHAIN

4) ARCHITECTURE OF BLOCKCHAIN 1.0 (CRYPTOCURRENCIES)

Blockchain 1.0 is a distributed ledger to store the digital cash transactions between two parties efficiently. The transactions are stored as a growing list of records called "Blocks". These blocks are resistant to any modification in them and are verifiable in a permanent way. A group of users joined together by a P2P network typically manages the verification of the ledger records. In order to make any changes within blocks, a consensus is required between more than half of the users of the network. This section discusses the details of design, working and open research issues of these components of Blockchain including blocks, network and consensus.

5) BLOCK

A block is the data structure in Blockchain 1.0 to store transaction records. As shown in the Figure 3, it consists of two parts: 1) Block Header and 2) Block Body. The block header contains following fields:

- Block Version: specifies the rules for block validation.
- Merkle Tree Root Hash: it stores the hash value of all transactions in the block.
- Time Stamp: stamps the current time in seconds according to universal time since January 1, 1970.
- nBits: threshold for a valid block hash.
- Nonce: a mathematical value starts with 0 and increases with calculation of every hash.
- Parent Block Hash: points to the previous block.

The block body contains the transactions and transaction counter. The maximum capacity of block to store the transactions is determined by the block size and size of each transaction contained in it.

6) NETWORK

In general, there are two types of nodes in a Blockchain network: 1) Full node 2) Lightweight node. However, authors in [1] have further categorized these nodes based on their functionalities which is illustrated in Figure 4.

a: FULL NODE

The full node is a fully functional node in the Blockchain network that performs role of the server. The full node has the capability to store copy of Blockchain nodes data and history of Blockchain. In case of a transaction in Blockchain network, full node is responsible to maintain consensus among other nodes by applying consensus algorithm and verify the transaction. It also participates in future policy and decision making.

b: PRUNED NODE

This is a kind of reduced function nodes as compared to the archival node. It is easier to understand from recalling the blocks in Blockchain architecture [74]. The pruned nodes in the Blockchain have a set limit of block storage. These nodes keep the blocks information from the starts, but when they reach the set limit, they only retain the header of blocks and chain placement.

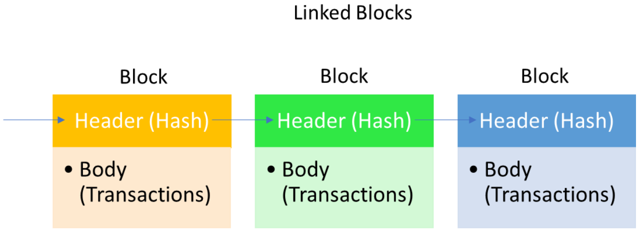


FIGURE 3. Blocks in the Blockchain architecture [74].

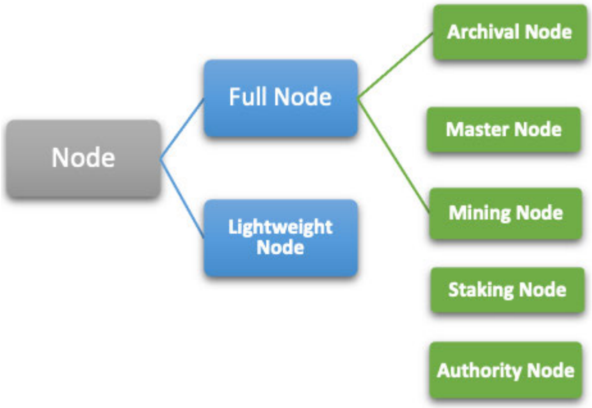


FIGURE 4. Categorization of Blockchain nodes [73].

c: ARCHIVAL NODE

It is a fully capable node in terms of space utilization. They can be seen as full server that can host all Blockchain. These nodes have the capability to add blocks in the Blockchain, validate blocks, and enforce consensus essential for a Blockchain transaction.

d: MINER NODES

All of the transactions are validated through special nodes, called 'miners' [75]. Miner nodes perform the required tasks to add a block in the network as long as all other nodes agree. After this consensus the transaction is stored in a decentralized node. In a public Blockchain these nodes can earn by validating the transaction.

e: STAKING NODE

Cryptocurrency Blockchain has a concept of staking node. This node determines based on rules and chance (proof of luck [76]) that which node will create next block in the Blockchain to get rewarded. The proof of work algorithm [77] decides which node will be rewarded. Cryptocurrency node such as raspberry pi cryptocurrency node [78] can also be considered as an example of this node.

f: AUTHORITY NODE

Nodes in the Blockchain network that will implement consensus algorithm or Proof-of-Authority are generally recognized as authority nodes in the network [73].

g: MASTER NODE

Master node in Blockchain network keeps full record of the transaction and validate them. Master nodes are also considered as back-end nodes of the network, which provide proof-of-stakes for cryptocurrency network [79]. Master nodes can also be considered as wallet running on millions of computers enabling the Blockchain up and running at real-time.

h: LIGHTWEIGHT NODE

A lightweight node is also considered as simple payment verification node [73]. According to authors in [80], lightweight nodes are becoming increasing feasible for Blockchain deployment because of their less resource consumption. Authors in [80] highlight the issue of reward for lightweight node and nothing for full node who serve lightweight client in Blockchain network. The authors suggest that smart contract can provide fair deployment environment. They suggest a unifying mechanism SmartLight that integrates payment routine to reward full node for serving lightweight client in the Blockchain network.

i: CONSENSUS

The Consensus is required to validate transaction and to update ledger. The first consensus algorithm used in Blockchain 1.0 was Proof-of-Work.

7) PROOF-OF-WORK (PoW)

PoW is considered as main achievement of Bitcoin to reach consensus in a distributed decentralized Blockchain network that could consists of 1000 of nodes. Consensus algorithm decides how agreement is made between Blockchain nodes to append a new block in the chain and the verification process. To add a block and earn reward in PoW algorithm, the initiator node applies cryptographic algorithm to produce a winning value less than the set value of network. In case of more than one node producing value, then this situation is dealt by analyzing the maximum value of PoW, which represents the higher amount of work done by the node. This node then allows to add a block and earn reward. This method is more suitable for scalable Blockchain network. However, it has few drawbacks including the cost of equipment's for node to perform mining, low transaction rate and its vulnerability to be attacked. More consensus algorithms are described in detail in section 6 of this paper.

8) ARCHITECTURE OF BLOCKCHAIN 2.0 (SMART CONTRACTS)

The concept of Smart Contracts is also not new and existing in literature since 1994. It is defined as "a computerized transaction protocol that executes the terms of a contract". The vision was to translate contractual clauses (collateral, bonding, etc.) into code and implement them in the form of software or hardware to self-enforce them with minimal role of trusted intermediaries [23].

In terms of Blockchain, smart contract automatically enforces agreements between two or more parties without a trusted intermediary. These smart contracts are implanted as computer programs in Blockchain softwares like Ethereum and Hyperledger. Participants join the network depending upon the type of Blockchain and can request the execution of a particular contract for a transaction in the Blockchain P2P network. The history of these transactions is stored in Blockchain similar to digital currencies. The state of the contract and assets of participants are determined by the sequence of transaction in the Blockchain [142].

The correct execution of smart contracts does not rely on a trusted third party similar to cryptocurrencies. Consensus protocols [157] are there to resolve any potential conflict between contractual parties. There are different consensus algorithms available for conflict resolution depending on the platform [142].

1) Block

The blocks in smart contracts contain programming code for recording transaction for a particular contract. The further details of the design of blocks are same as for cryptocurrencies as discussed in section 4A.

2) Network

The types of nodes present in smart contract P2P network are same as described in section 4A. The permissions for nodes to join the network are dependent on type of Blockchain implementation from public, private or consortium choices.

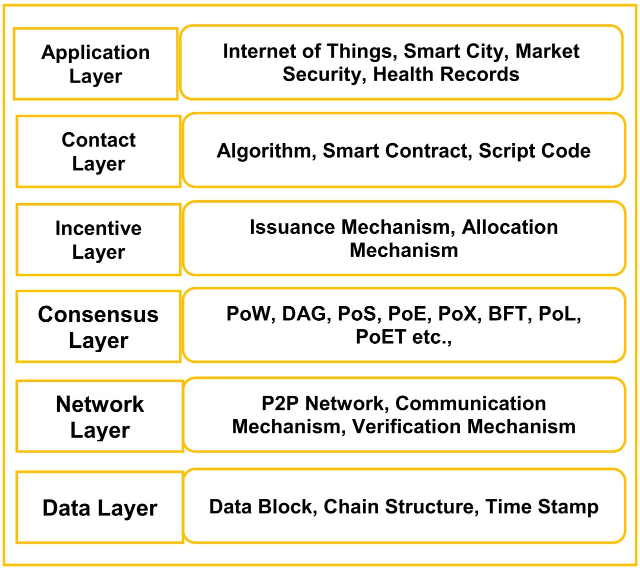
3) Consensus

The consensus mechanism in smart contracts is used to resolve any dispute between participants and recording transactions for a particular contract. Different available platforms or frameworks for smart contracts (see section 7 for more details) implement different consensus algorithms (details of different consensus algorithms are available in section 6).

9) ARCHITECTURE OF BLOCKCHAIN 3.0 (BLOCKCHAIN APPLICATIONS)

Besides financial market, the Blockchain technology has been adopted in many industries for development of distributed applications e.g., games, user-generated content networks, internet of things (IoT), smart hardware, supply chain, source tracing and economy sharing credits etc. Blockchain technology provides many features to these distributed applications including better performance in terms of low latency and high throughput, simpler identity management and enabling them for offline transactions and flexible maintainability for system upgrades and easy bug recovery [10]. There are some novel applications of Blockchain and some are briefly reviewed, for example, authors in [153] claim that fusion of Blockchain technology in existing deployed cloud solution can reform cloud data centers in terms of their performance enhancement and security. Authors in [171], recently proposed the use of Blockchain for identity authentication issues in the smart grid through a secure and mutual authentication protocol. Similarly, in [173] authors first highlight the potential security threat on smart grid infrastructure and then propose a Blockchain-based lightweight authentication protocol for the smart grid. Authors in [172] propose an efficient medical data storage and sharing mechanism using double Blockchain. From double blockchain, they mean two blockchains first one for data storage and second for data sharing between hospitals and healthcare organizations. Applications use Blockchain for their different needs e.g., verifying the identities, keeping track of manufactured items in the form of chain of item etc.

A general Blockchain architecture is presented in the literature as a layered architecture to develop distributed applications as shown in Figure 5 [9].



Application Layer	Internet of Things, Smart City, Market Security, Health Records
Contact Layer	Algorithm, Smart Contract, Script Code
Incentive Layer	Issuance Mechanism, Allocation Mechanism
Consensus Layer	PoW, DAG, PoS, PoE, PoX, BFT, PoL, PoET etc.,
Network Layer	P2P Network, Communication Mechanism, Verification Mechanism
Data Layer	Data Block, Chain Structure, Time Stamp

FIGURE 5. **A general Blockchain Layered Architecture [9].**

- Blockchain based business applications represent application layer.
- The contact layer show programming approaches available for Blockchain.
- The nodes participating in managing applications get incentives according to mechanisms listed in incentive layer.
- The consensus layer makes various consensus algorithms available for Blockchain applications.
- The network layer is composed of data propagation and data verification mechanisms along with distributed networking mechanisms.
- The timestamped data blocks are part of data layer. Chain structure, Merkle tree, cryptography and hash functions are used to manage security of these blocks.

10) BLOCKCHAIN FRAMEWORKS

Blockchain has been gaining widespread attention globally but the success of the technology depends on the availability of the application development frameworks. There are a number commercial as well as open-source application development frameworks (ADFs) available currently. The most common and widely use is Bitcoin. This section describes a number of important ADFs for developing commercial grade Blockchain applications [94], [95].

11) BITCOIN

Bitcoin has been the seminal research work to lay the foundation of Blockchain-based P2P digital currency systems [144]. Major contribution of the research on Bitcoin is the implementation of the concept of direct digital payments without relying on trusted third-party financial system. Digital signatures coupled with network timestamps transactions by constructing hashing chain exploit hash-based PoW. These interconnected blocks generate immutable distributed database records that cannot be changed without redoing the PoW. Bitcoin holds major shares in cryptocurrency world today, but there are a number of other platforms available.

12) ETHEREUM

Ethereum has been developed as open-source public Blockchain platform to implement decentralized applications (DApps) [102]. Ethereum facilitates users to develop fairly complex applications of different capabilities to perform arbitrary operations and hence it can be used to develop DApps other than Cryptocurrencies. DApps actually exploit smart contracts, a small immutable program stored in Ethereum network, to represent resources such as currency, land and house. The central component of this platform is Ethereum virtual machine (EVM) to run DApps for complex algorithms. The code for DApps is written in a contract-oriented programming language Solidity [103].

13) HYPERLEDGER

Hyperledger fabric has been introduced as permissioned Blockchain distributed operating system by IBM [85]. This hyperledger fabric is unique in a sense that it's a first programmable framework Blockchain system that allows user to run distributed application independent of native cryptocurrency. The authors in [85] firsts identified the limitation of order-execute architecture such as sequential execution, non-deterministic code & confidentiality of execution. Hyperledger fabric introduces execute-order-validate Blockchain architecture as shown in Figure 6. This proposal from the IBM became popular in Blockchain community. However, authors in [86] highlighted concerns in hyperledger fabric or Blockchain technology. The first is that they cannot use permission-less Blockchain, secondly lack of proven use cases and limited number of programmers that can develop applications using this hyperledger fabric.

The core theme behind Hyperledger project is to develop open-source Blockchain technology framework and the code base to be used by a large number of users from the different industries for heterogeneous application requirements [104]. The Hyperledger project is managed by the Linux foundation in cooperation with many industrial giants such as IBM, Hitachi, Fujitsu, NEC, Intel, and many more. The Linux Foundation adopts modular umbrella approach for

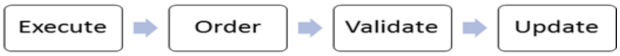


FIGURE 6. Execute-order-validate architecture [104].

Hyperledger project. At the top level, the Linux Foundation and Hyperledger provide support to build the infrastructure. Technical, legal, and marketing support is included in this infrastructure development task. Furthermore, below the infrastructure layer, is the Hyperledger's development and implementation of Fabric, Iroha, Sawtooth, Burrow, Grid, and Indy frameworks to cope with heterogeneous application requirements. The third layer in the Hyperledger project is tool support. A number of tools have been developed for these frameworks such as Composer, Explorer, Caliper, Cello, Quilt and Ursa. These tools have been developed based on a specific framework but gradually they are being modified to achieve portability to other frameworks. Composer provides an environment to facilitate block chain technology application development. Composer models business network and consolidates data from conventional systems. Explorer module can be used to develop web applications with user-centric interfaces to view status of the Blockchain application.

14) TRON

TRON is another open-source platform to realize decentralized Internet and associated infrastructure for Blockchain applications [106]. The main claim to propose TRON protocol is to provide support of high throughput, high scalability, and high availability for all DApps in the TRON ecosystem. The architectural design of the TRON consists of three layers, namely storage, core, and application layers. The TRON protocol is language neutral as it uses Google Protobuf. Core layer consists of a number of modules such as smart contracts, account management, and consensus. TRON has a stack-based virtual machine implementation with optimized instruction set. Solidity programming language can be used to develop DApps. A distributed storage protocol comprising of Block Storage and State Storage has been developed for the TRON. Google's LevelDB, an open-source on-disk key-value graph store, has been selected as storage to achieve high performance for the applications. All newly created fork chains can be stored for a certain period of time into a full-node memory database namely KhaosDB.

15) MULTICHAIN

MultiChain is a platform for designing and implementing private Blockchain applications. It helps easy to develop and deploy applications within an organization or between organizations in financial sectors [107]. Fundamentally, as a private Blockchain technology, it copes with the issues of mining, privacy and openness by managing user permissions at global level. In MultiChain, no one but participants can view the Blockchain's activity with full control over transactions. Moreover, proof of work is not needed for mining which minimizes the costs. MultiChain is available on Windows, Linux and Mac servers with a simple API and command line interface. Scalability is one prime requirement for many block chain applications and MultiChain addresses this issue by controlling the block size. Special metadata is used in network transactions to grant privileges to participants in MultiChain. All privileges are granted to the miner of the first "genesis" block and this user acts as the first administrator with sole authority for delegating privileges.

16) OPENCHAIN

OpenChain is one of the most popular open source Blockchain frameworks with focus to achieve interoperability with existing applications by supporting highly scalable Blockchain application developments [108], [109]. Interoperability essentially means that OpenChain presents unique decentralized application gateway for pluggable integration with existing applications' backend [109]. This is a significant technology achievement with the capability to promote mainstream adoption of Blockchain applications development and deployment. In order to achieve high scalability, OpenChain exploits multi-threading and data parallelization through OPEN Blockchain Load Balancing Protocol and ORapid consensus. In OpenChain, Scaffold, a new technology concept, constitute payment schema for an application, which is transformed into OPEN state in the Blockchain application [108]. OpenChain supports heterogeneous Blockchain platform and hence an application deployed on OpenCahin is essentially deployed on other Blockchain platforms with their own consensus algorithm through OPEN cluster. At the start of the transaction processing in the OpenChain, ORapid consensus technique has the capacity to handle fairly high volume of the transactions. However, while the number of transactions increases to the limit of the techniques, OpenChain executes OPEN Blockchain Load Balancing Protocol to dispatch transactions toward other blockchains and hence archives data parallelization at very large scale.

17) QUORUM

Quorum is permissioned Blockchain open-source platform supported by J P Morgan, one of largest financial institutions on the globe [110]. Indeed, the support of J P Morgan for the Blockchain technology Quorum is based on the Ethereum codebase, but unlike Ethereum it provides permissioned Blockchain platform with enhanced contract privacy and high-performance applications [111]. The baseline functional model of Quorum is very similar to Ethereum, but with substantial difference in the Network and peer permissions management, greater transaction and contract privacy, voting-based consensus mechanisms and performance.

18) IOTA

IOTA is open source Blockchain platform for Internet of Things (IoT) to facilitate secure communication and payment [112]. It is a Blockchain platform for IoT which employs DAG (Directed Acyclic Graph). Figure 7 illustrates

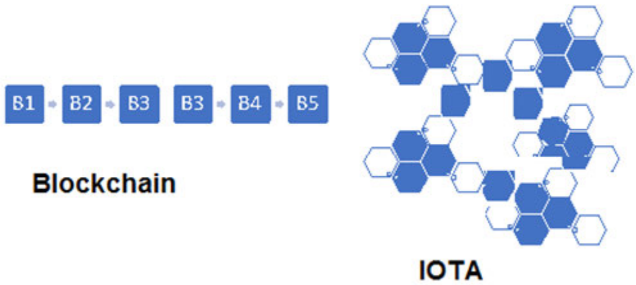


FIGURE 7. IOTA vs Bitcoin technology [24].

both IOTA DAG and Bitcoin Blockchain based technology [23].

19) EXONUM

Exonum is an open-source application development framework for developing heterogeneous domain such as legal, financial and governmental fields [113] and [114]. The framework targets permissioned Blockchain applications in these domains and its core has been developed in Rust programming language based on service-oriented architecture. Java Binding tool for Exonum facilitates application services development on the Exonum framework for permissioned blockchains.

Few more promising Blockchain frameworks are proposed recently including Corda and Ripple. In the presence of a large number of frameworks, it is challenging to select one appropriate to satisfy application requirements. Though there can be a number of criteria but we opt the criteria given in the Table 3 to meet the users' needs [115].

A comparison of various development frameworks in terms of different characteristics and properties is shown in Table 3.

V. CONSENSUS MECHANISMS

The consensus mechanism is used for validating the transaction and to reach a consensus in effect of a transaction on ledger update. There have been various consensus models proposed in literature and are implemented by different Blockchain platforms. According to authors in [87], Quorum is the first Blockchain platform to employ different consensus model. In this section, we review, classify and compare various consensus algorithms used and proposed for Blockchain technology.

Figure 8 shows our classification of Blockchain consensus model based on the review of literature. As it can be seen from Figure 8 that consensus models are classified in eight major categories and some of them have further types based on minor variations of their working.

A. PROOF OF WORK (PoW)

Proof of Work is termed as one of pioneering consensus models for Blockchain technology. The main idea in PoW is to compete for generating new block in the Blockchain based on computational power. This algorithm requires miner to perform a computation and produce a value. The wining value is less than the predefine value set by the network. In PoW, there is a possibility of forking (i.e., two nodes produce wining value), which is dealt by the network by proof of work through the nodes. Research community has proposed different variations of PoW algorithms, which are highlighted in our classification in Figure 8.

1) PROOF OF WEIGHT

Proof of Weight consensus [145] model is based on Algorand consensus that has an additional feature of "weight" in the core idea of PoW. These weights are relative to the values produced by nodes to represent their contribution in the network. The main idea is to prevent problem of "double spending" forking by adding the feature of relative weight.

2) PROOF OF REPUTATION

Proof of reputation [146] consensus mechanism builds the reputation of a node based on its participation, transactions and assets. The node with the highest reputation value generates a new block and this block is validated by voting in the Blockchain. This mechanism allows degradation in the reputation of nodes in case of misconduct in the past and also adds to the security of the Blockchain.

3) PROOF OF SPACE

Proof of space [147] is a flavor of PoW where a node that requests service must dedicate the ample amount of disk space as compared to do the computation in PoW. Information is sent to the verifier node as a proof that ample amount of space is allocated against a service request.

4) PROOF OF HISTORY

Proof of history consensus mechanism requires node to provide a proof of history [147]. It creates a historical record to provide evidence that an event is occurred at specific time. This provides as alternative of trusting the timestamp on the transaction.

5) PROOF OF BURN

Proof of burn [148] consensus mechanism is based on the concept of burning coins to compete to mine the upcoming block in the Blockchain. Burning coins here means sending the digital currency to an address where it is irretrievable. The nodes burn more coins to increase their chances of getting selected in the lottery.

In comparison to PoW, Directed Acyclic Graph (DAG) [144] is proposed as promising Blockchain consensus technology for Internet of Things Blockchain framework namely IoTA. DAG has a prominent feature of scalability as the blocks are added in parallel in the Blockchain in DAG. It allows to add a block immediately into the ledger as they process previous transaction. DAG also deal with the issue of "double spending" by using effective algorithms.

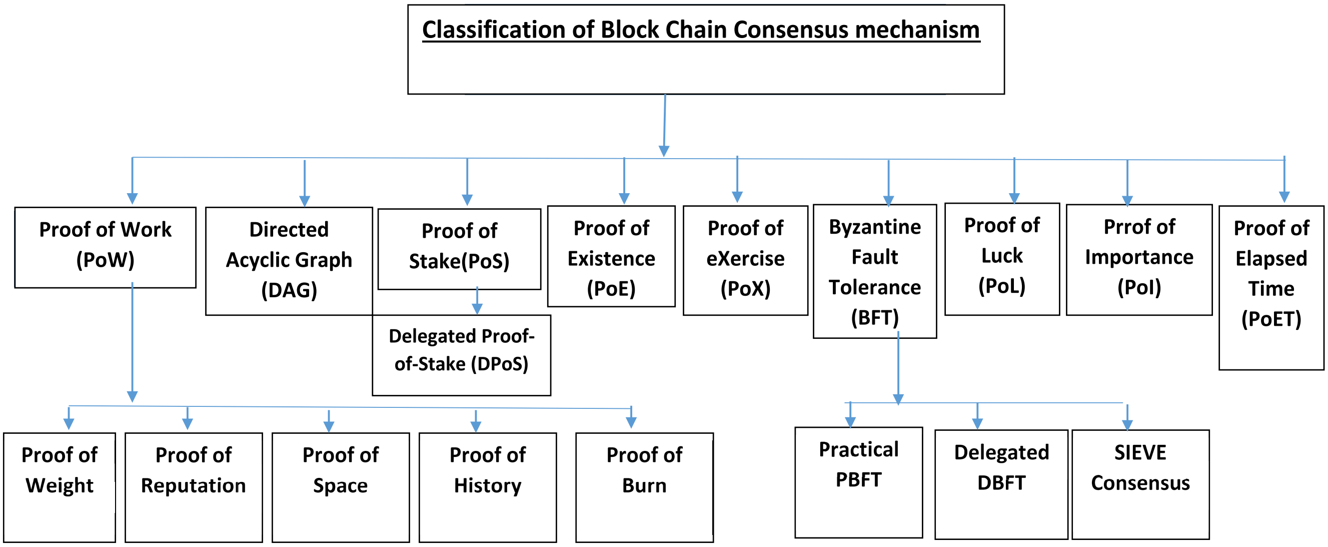


FIGURE 8. Classification of Blockchain consensus mechanisms.

TABLE 3. Comparative analysis of the Characteristics of Various Frameworks.

Framework	License(a)	Development Community (b)	Support model	Enterprise Activity	Enterprise Regulatory Compliance	Roadmap	Ease of programming	Reliable Backing
Ethereum	✓	✓	×	✓	×	✓	✓	×
Hyperledger	✓	✓	×	✓	✓	✓	×	✓
Tron	✓	✓	×	✓	✓	✓	✓	✓
MultiChain	✓	✓	✓	✓	✓	✓	✓	✓
Open Chain	✓	✓	✓	✓	✓	✓	✓	✓
Quorum	✓	✓	✓	×	✓	✓	✓	✓
IOTA	✓	✓	✓	×	×	✓	×	×
Exonum	✓	✓	✓	✓	×	✓	×	×

✓Means It Is Open Source But Some License Fee May Be Involved Under Certain Conditions

B. PROOF OF STAKE (PoS)

The main advantage of Proof-of-Stake is that it does not require its node to purchase expensive equipment to perform mining. In PoS, a node can perform mining or validating a block based on proofing its stake i.e., number of coins. PoS suggests purchasing cryptocurrency and uses the same to buy chances of block creation [88], [89].

1) DELEGATED PROOF OF STAKE (DPoS)

A variation of PoS algorithm is proposed in [96] called Delegated Proof-of-Stake. It is suggested to use voting from stakeholders to elect the witness node, which will create block in the chain. The witness node gets payment for block creation, but if the selected witness node cannot produce block, then it will not be allowed in future voting process.

C. PROOF OF EXISTENCE (PoE)

PoE is proposed as a system to verify the existence of certain documents at specific time by timestamp of transaction. It could be used to provide data ownership information without disclosing the actual data. This PoE model is helpful in proving existence of copyright documents e.g., a patent.

D. PROOF OF eXercise (PoX)

Another alternate to the PoW is proposed by authors in [99] called Proof-of-exercise (PoX). In PoX, an exercise is a matrix based on real world scientific problem. The miners will solve matrix-based problems given by employee in the system. They suggest DNA and RNA sequencing and data comparison as an example of matrix solving problems.

E. BYZANTINE FAULT TOLERANCE (BFT)

In case of loss of system service or failure because of Byzantine fault in Blockchain require consensus [20]. The nodes in the network should reach to consensus even some nodes fail to respond and maintain consistency of this information in the Blockchain network. It is a challenge considering the distributing system.

1) PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

Authors in [93] propose "Practical Byzantine Fault Tolerance", an algorithm to deal with Byzantine faults. To efficiently survive Byzantine faults in asynchronous network, the authors in [93] propose first state-machine replication protocol. They consider distributed file system and implement Byzantine fault tolerance.

2) DELEGATE BYZANTINE FAULT TOLERANCE (DBFT)

NEO whitepaper presents a variation of standard Byzantine Fault Tolerance called delegated byzantine fault tolerance [97]. It is currently used by the NEO Blockchain core library. They suggest it as a novel mathematical model that can verify consensus behavior using a discrete model. This can deal with untrustworthy participants better than other algorithms.

3) SIEVE CONSENSUS

Sieve [149] is considered a type of Practical Byzantine Fault Tolerance (PBFT) consensus to deal with non-deterministic chain code execution. Different output can be produced in non-deterministic chain code execution by replicas. Sieve can analyze the output in case of minor divergence detected in small number of replicas.

F. PROOF OF LUCK (PoL)

Authors in [98] have considered the limitations of PoW and proposed a new consensus model called Proof-of-Luck to reduce the required computational power for a transaction and increase its throughput. This algorithm is based on TEE (trusted execution environment). It mainly consists of two functions PollRound and PollMine. A luck value a random number between 0 and 1 is assigned to each block as it is mined. A cumulative luck value is calculated through summation of all luck values within each block of the chain. Miner will prefer to append their block to the chain with highest luck value.

G. PROOF OF IMPORTANCE (PoI)

This algorithm is used by NEM (XEM) [101]. This cryptocurrency introduces the concept of harvesting which is similar to mining. This algorithm uses the concept of network theory to define rating of each account mainly based on vested and unvested coins. PoI relies on a number of days' coins are in the account of a node in the network to estimate ‘‘importance’’. It allows 10% of current unvested amount vests every day. It is also calculated based on the rank of account within the network considering the number of vested coins held.

H. PROOF OF ELAPSED TIME (PoET)

This consensus mode uses lottery-based election model to randomly select the new leader for adding block in the Blockchain. Trusted Execution Environment (TEE) is used to ensure secure environment for this process of election. The major steps in the process of election of leader are as follows:

- Validator and miner nodes run TEE by Intel SGX.
- Every validator node requests a wait time
- The node with the shortest wait time wins the election to become a leader node.

Since it relies on specialized hardware, it is the main drawback of utilizing this consensus mechanism [90], [91]. Table 4 shows the comparison of consensus algorithms based on key parameters such as the prominent feature of consensus model, its fault tolerance and scalability.

VI. BLOCKCHAIN SECURITY

This section reviews various security issues and related research developments in detail.

A. CHALLENGES AND FUTURE TRENDS RELATED TO SECURITY

Blockchain utilizes a P2P network instead of a central authority such as a central bank to carry out financial transactions [122]. The fact that Blockchain is decentralized implies that an individual can verify and undertake financial transactions in real-time. Over the recent past, researchers have managed to invent several Blockchain applications. Nevertheless, Bitcoin has been exposed to a wide variety of privacy and security issues. For instance, after an individual links a public key with a person's identity, he can browse previous transactions on the Blockchain and examine all transactions related to the specific public key. Therefore, the main challenge is balancing the privacy and security of an individual and accountability [163]. Authors in [162] study Blockchain-based identity management systems.

According to [118], it is estimated that Blockchain technology firms will earn a revenue of more than six billion by the year 2020. However, these earnings may be affected by the vulnerabilities that are present in the Blockchain security and this factor is yet to be tackled by the distributed ledger technology (DLT) [123].

The Internet of Things (IoT) usually enables a smart workforce, such as an interaction between human beings and machines, as well as machine to machine interaction [124]. Evidence indicates that although there are numerous benefits of IoT and Blockchain technologies, there are several challenges that still exist. These challenges are related to tackling the security factors and dealing with privacy concerns. In addition to privacy and security concerns, other challenges that face IoT and Blockchain technology include interoperability, legal issues, lack of standards, access control, regulatory issues, developmental issues, and emerging IoT economy issues.

Evidence indicates that most of the challenges associated with Blockchain technologies tend to be interrelated. In [123], authors argue that the security challenges associated with IoT and Blockchain technologies can be examined from the perspective of Bitcoin, which enables transactions to occur in a decentralized manner [125]. In [155], authors have performed a systematic exploration of Blockchain attack surfaces. First, they highlight various attacks on a Blockchain-based system and then explored the relationships between these attacks. Now we briefly present the most common vulnerabilities and attacks in the Blockchain system.

TABLE 4. Comparison of Consensus Algorithms.

Consensus Algorithm	Main Feature	Fault Tolerance	Power Consumption	Scalability
Proof-of-Work (PoW)	Computational Power	Low	High	High
Proof-of- Stake (PoS)	Stake (amount of coins)	<51% stake [29]	low	High
Delegated Proof-of- Stake (DPoS)	Voting to elect witness node	<51% validators	low	high
Proof-of-Elapsed Time (PoET)	Lottery based election	Yes	high	
Byzantine Fault Tolerance (BFT)	Reach consensus even some node failed to response	33% nodes being faulty	Low	low
Delegated Byzantine Fault Tolerance (DBFT) [22]	Reach consensus with untrustworthy participants	<33 % replicas [29]	medium	low
Proof-of-Importance	Estimate importance based on no of days coins in	Unknown	Low energy saving	Fair
Proof-of-Luck	Cumulative luck value	Not applicable	Reduce computational power	Does not scale well
Proof-of-eXercise (PoX)	Miner will solve matrix-based problem	Not applicable	Partial energy saving	Un known
Proof-of-Existence (PoE)	Use timestamp of transaction to verify existence of document	Not applicable	Unknown	Unknown
Directed Acyclic Graph (DAG)	Consensus for IoT Blockchain	Not applicable	High	Very high

B. 51% VULNERABILITY

Blockchain depends on a disseminated agreement mechanism to create a common trust. Nonetheless, the mechanism of consensus has a vulnerability of 51%, which attackers might exploit to manage the whole Blockchain. Most notably, in blockchains based on PoW, in case a miner's hashing control is accountable to above 50% of the entire hashing control of the whole Blockchain, then a launch of 51% might occur. Therefore, the concentration on mining power on a small number of mining pools might lead to uncertainties of unintended situations, for example, a pool being in charge of over half of the entire computing control. After the *ghash.io* pool in January 2014 reached 42 percent of the entire computing control of Bitcoin, many minors willingly left the pool, and a press announcement was issued by ghash.io to give the Bitcoin community reassurance of its avoidance in getting to the threshold of 51%. In blockchains based on PoS, there is a probability of an attack of 51% if the coin's figures being in possession by one miner is above 50% of the whole Blockchain.

Through the launch of the 51% attack, the information on Blockchain might be arbitrarily manipulated and modified by an invader. Specifically, vulnerability can be exploited by an invader to perform the attacks given below:

1) Overturn operation and start twofold spending strike (similar coins are used numerous times).
2) Eliminate and adjust transactions ordering.
3) Obstruct normal operations of mining for additional miners.
4) Hamper the operation's confirmation of ordinary transactions.

C. PRIVATE KEY SECURITY

When utilizing Blockchain, the private key of the user is considered as credentials of recognition as well as security, which the user generates and maintains rather than intermediary agencies. For instance, when building a cold storage holder in Bitcoin Blockchain, the private key must be imported by the user. A vulnerability scheme in Elliptic Curve Digital Signature Algorithm (ECSA) was discovered by which, an invader might get the private key of the user as randomness cannot be generated by it during the process of signing. It will be hard to recover the private key of the user the moment it gets lost. In case criminals steal the private key, the Blockchain account of the user will deal with the danger of others tampering with it. Because Blockchain does not rely on a centralized intermediary trusted organization, in case the private key of the user is stolen, it will be complex to trace the conduct of the criminal and salvage the Blockchain's modified information.

D. CRIMINAL ACTIVITY

Users of Bitcoin might possess numerous addresses of Bitcoin, yet the address is not related to their actual identity in real life. Hence Bitcoin is vulnerable to illegitimate activities through certain intermediary platforms of trading that assist Bitcoin. Because the procedure is anonymous, user's conduct is difficult to trace, therefore they avoid legitimate sanctions.

E. MONEY LAUNDERING

A Dark Wallet is an application of Bitcoin that might cause the transaction of Bitcoin to be totally private. Information on transaction might be encrypted and user's legitimate coins are mixed with chaff money by the Dark Wallet. This makes money laundering easier.

F. UNDERGROUND MARKETPLACE

Inside the secretive marketplace, Bitcoin is always utilized as the legal tender. For instance, Silk Road is an international nameless marketplace that functions as unknown services, and Bitcoin is applied as its currency of exchange. The majority of merchandise being traded in the Silk Road are illegal drugs or certain items that are regulated within the ordinary world. Because global dealings make up for Silk Road major proportion, the underground market transaction is made more convenient by Bitcoin, which could lead to harm the safety of the society.

G. DOUBLE SPENDING

Though the consensus mechanism of Blockchain can authenticate transactions, it is still challenging to evade dual spending. Double spending means that consumers can use the same single digital token multiple times. For instance, an invader could control race invasion for dual payments. It is relatively easy to execute this method of attack in blockchains based on PoW since the invader might take advantage of the intermediary period between double transactions' launch as well as confirmation to initiate an attack quickly. Before the subsequent operation is mined as null, the invader has by now gotten the output of the initial transaction, leading to dual spending.

H. TRANSACTION PRIVACY LEAKAGE

It is easy to trace the behavior of the user in Blockchain, the Blockchain platform takes actions to guard the user's transaction secrecy. Zcash and Bitcoin apply one-time financial records to keep the received cryptocurrency. Furthermore, the user is required to give every transaction a private key. Thus, the invader cannot deduce if the cryptocurrency in a dissimilar transaction is acknowledged via the equivalent user. Users could include a few chaff coins (known as "mixis") in Montero during transaction initiation such that the invader might not deduce the connection of real coins used via the deal.

I. COMPUTATION AND MINING NODES

In the majority of present applications, nodes are simple, and the capabilities of computation are not high. Specifically, the client of Blockchain requires to remain simple to meet the reduced needs of computation. Conversely, the services of security, generally require high computation capability. Furthermore, the minor nodes of Blockchain require high power of computation. Nonetheless, the required high power of computation for the nodes contributes to the system cost. An enhanced method involves decreasing the computation need for mining and associating the powers of the mining node towards its trustworthiness or its reputation within the platform. Additionally, simpler schemes of cryptocurrency might be built to decrease the need for computation for data encryption and signing.

J. SCALABILITY

Blockchain technology is scaling better compared to contemporary centralized methods. Though, there are reports of reduced levels of performance of the technology because higher number of nodes. This remains a main challenge, particularly with applications of network safety, where numerous users require service and there is a fast scaling of the network. Also, the system dynamicity contributes to issues of scaling because there is need for nodes to regularly send transaction updates. The Hyperledger and Ethereum platform possess their individual scalability promises. Nonetheless, the operation experiments reveal that the two platforms continue to improve in certain aspects related to scalability.

K. TIME CONSUMPTION

Offering services of security require fast capabilities of processing, particularly within the existing networks, where billions of dollars can be the cost of milliseconds. Besides, mining as well as accomplishing consensus still consume time in blockchains.

L. CONFIDENTIALITY, INTEGRITY AND AUTHENTICATION

There is a considerable need for elevating privacy and security issues concerning the attributes of various IoT elements. Researchers argue that the current technology can be used to authorize, authenticate, and audit data that has been generated by these devices. Blockchain can create new foundations for both social and economic systems. Blockchain can also be described as more than just a foundation for the circulation of cryptocurrency, and it also provides a secure means of exchanging various services, goods, and transactions [131].

A decentralized strategy can provide numerous benefits in terms of information authenticity, neutrality, security, and fault tolerance. Peers in the blockchain network must contain some functionalities such as storage, routing, mining, and wallet services. Nevertheless, researchers argue that scalability and storage capacity of Blockchain has been questioned over the years. The main reason is that the chain in this technology has been expanding at a rate of one megabyte per block every ten minutes in Bitcoin [132]. Furthermore, evidence indicates that numerous copies have been stored within the nodes in the network. Manual processes have been optimized and transformed by IoT to ensure that they fit in the digital era through making resolutions from limited logs of Blockchain without dissemination of consensus. Authors in [175], proposed a covert communication

TABLE 5. Cryptographic Primitives used for Security in Blockchain.

S. No	*Name*	*Function*
1	Hash	Maps casual size information to a string of fixed size.
2	Digital Signature	Source verification
3	Zk-SNARK in Zerocash	Breaks bitcoins and gives them anonymity
4	Zero-Knowledge (Range) Proofs	Protect privacy and anonymity of transaction

system for Bitcoin, which uses Blockchain as a covert communication channel to transmit covert messages for Bitcoin. Similarly, in [176], the authors provide a scheme and theoretical support for covert communication over Blockchain using a special Bitcoin address using the tool Vanitygen.

M. COMMUNICATION OVERHEAD

The nodes in blockchain are forced to dispatch transactions regularly to revise the Access Control List or amend the information on the provenance. Conversely, the technology of Blockchain is a P2P network, where considerable operational cost is due to the traffic of the network and the processing abilities of the system. The blocks and transactions require broadcasts. Therefore, the added overhead to the network is imperative as well as a challenge. The processing and storage overhead present a challenge in adapting blockchains applications of security [133].

Evidence indicates that most of the security problems are due to the three major areas, network links, authentication, and transactions. Therefore, technologies that allow incorrect connections, and their expansion with other technologies could raise numerous security concerns. A summary of risks and related causes is shown in Table 5.

N. CRYPTOGRAPHIC PRIMITIVES

Despite the fact that numerous works of literature are dedicated to the privacy and security of Blockchain issues, there is a lack of systematic evaluation of the cryptographic primitives in blockchains. Evidence indicates that there are a number of strategies that can be used to deal with these hurdles.

Blockchain technology utilizes a decentralized architecture which implies that all devices must be connected to a network in order to corporate and interact using predefined protocols. Recent research efforts have managed to significantly improve Blockchain technology in terms of security. For instance, every person who accesses the Blockchain network is provided with a distinct identity that is directly linked to his account. Such a mechanism ensures that only the account owner performs transactions and other operations.

Analysts argue that Blockchain technologies offer decentralized privacy and security, but they use a huge amount of energy despite being exposed to computational overhead and delays. Such challenges are the main factors that are actively being tackled by experts since they are not favorable for most resource-constrained IoT devices connected to the blockchain. To solve these problems, experts have attempted to develop numerous approaches that are specifically geared towards resource utilization.

The blockchain-based smart homes work in three basic tiers which are known as an overlay network, cloud storage, and smart home. The system requires that every smart home will be equipped with a highly capable device called a "miner." Such a device will have the capability of handling various forms of communications that take place within and outside the home. The miner node in the Blockchain can audit and managing all forms of communication. Researchers claim that this Blockchain-based smart home framework is capable of examining security issues such as integrity, confidentiality, and availability.

Authors in [134], suggest Bitcoin technologies provide weak anonymity, and they propose a system that can safeguard the privacy of the user in Bitcoin.

O. BLOCKCHAIN ALGORITHMS FOR SECURITY

In Blockchain, privacy is a significant issue. For example, the address of Bitcoin payer can be seen by anyone and every transaction's content in the Blockchain of Bitcoin. This can be counter by various advanced cryptographic primitives such as:

1) HASH FUNCTIONS

The hash function has two basic requirements, which are known as collision-resistance and one-way functionality. The key use of hash is to ensure data integrity for online or offline transactions. A hash function could be used to ensure that a file is downloaded from the online source is authentic. In blockchain applications, the hash functions could be used in the generation of address, PoW, bridge mechanism, generation of random or pseudo numbers (PNG), generation of the blocks, and message digest in signatures (MDS). The use of hashes in Blockchain gain popularity in cryptocurrency applications. The most commonly used hash function in blockchains is SHA256 [141].

2) DIGITAL SIGNATURE

The concept of digital signature was built in 1976 by Hellman and Diffie when they first developed the public key cryptography [141]. As a basic primitive of public-key cryptography, the applications of digital signature are used for the authentication of source, integrity, and non-repudiation [141]. The

Digital signature algorithm (DSA) ensures that the message legitimate signatures cannot be forged.

3) ZCASH, zk-SNARK

Miers *et al.* proposed Zerocoin to offer the anonymity of Bitcoin through breaking coins traces [141]. Nonetheless, the e-cash result could not sustain full-edge nameless payments, because Zerocoins utilize fixed value coins. Also, nameless coins have to be transferred by someone into coins that are nameless before payment. On the other hand, in transactions, metadata or amount cannot be hidden. Therefore, Zerocash was proposed to handle these problems. Particularly, Zerocash offers anonymity and data transaction privacy with nameless coins. Furthermore, Zerocash extensively decreases transaction's size with a coin to below a kilobyte and reduce the period of verification of a transaction below 6 minutes.

4) ZERO-KNOWLEDGE (RANGE) PROOFS

A normal concept to protect the confidentiality and anonymity of a transaction is to make them unlikable. The system of electronic cash needs to authenticate if the online payer possesses classified information similar to the address from where the cash is coming to process the transaction. It is pertinent to mention that the zero-knowledge proof was created to handle this situation.

5) MONERO RING SIGNATURE

Monero employs ring signature technology to preserve the privacy of users. Moreover, the ring signature is a type of digital signature in which a group of potential signatories is combined together to produce a distinct signature that can use to authorize a transaction [23].

VII. FUTURE PROSPECTS

This survey paper has covered architecture of cryptocurrencies, smart contracts and general Blockchain based applications. Blockchain has a great potential to revolutionize the way of doing businesses and making payments across the world without consideration of geographical boundaries and trusted intermediaries. Blockchain has also has phenomenal potential in establishing transparent, democratic and secure fabric for other industries of the world. Many aspects of all versions of Blockchain are going to remain hot research topics including consensus mechanisms, network management in terms of efficiency. Some key findings and future research directions are discussed below in this section.

The business and research community has shown incredible interest in adopting Blockchain technology in the last decade. Consensus algorithms play a vital role in ensuring consistent operations of Blockchain application. The important future direction in terms of consensus algorithms is the transition from PoW to new algorithms such as PoS. Ethereum has already started working on it and will be looking towards the implementation and performance analysis aspect of this transition. Another interesting future prospect is how new Cryptocurrencies like NEM and EOS will motivate business to build Blockchain solutions using new consensus algorithms.

For the Blockchain technology to become mainstay technology of the future for varying domains, it must resolve several current issues. First, the Blockchain technology needs to become scalable and must solve the limitations of low throughput, high latency, and increasingly high storage demands. For example, it needs to investigate significantly improving transaction execution performance by exploiting high concurrency of multicore and cluster architectures. The resource inefficiency and monopoly by large organizations with powerful nodes can be addressed by investigating controlling chain sizes by pruning out-of-date and unneeded blocks without affecting immutability. The efficient deployment of updated smart contracts without much overhead is another issue for the research community to solve. Finally, the Blockchain community must eventually address environmental effects from the high energy consumption of a large number of nodes participating in reaching consensus, which may become a serious global climate issue.

Microsoft and Intel have already joined hands to support enterprise Blockchain [158] and the alliance believes that enterprise Blockchain success needs to cater the performance, confidentiality and governance issues [116]. ADFs essentially need to integrate support for these issues to have wider acceptability in various business domains. Blockchain technology has given rise to autonomous trust management in a decentralized way between two concerned parties in the form of smart contracts while artificial intelligence (AI) paves the way for intelligent decision-making for machines at par with humans, and even in some cases with more efficiency [117]. Integrated capabilities of Blockchain and AI have great potential for emerging applications in various domains. For instance, trust of Blockchain and decision making of AI in healthcare and autonomous vehicles will result in excellent match for highly useful applications [170-173, 120]. Consequently, future ADFs will be required to provide inherent support for such functionalities.

In future, there are two major challenges in promoting Blockchain security. One is to balance the privacy and security of an individual and accountability, mainly due to DLT. The other is to address security and privacy issues brought by the IoT, such as interoperability, legal challenges, lack of standards, rights issues, regulatory issues, developmental issues, and emerging IoT economy issues, etc.

Prospects of future Blockchain projects are discussed by authors in [158] including future development directions and future trends. There are a number of novel use cases where this technology could excel in the future including energy trading [165], vehicle life cycle tracking [164], smart grid [160], and Blockchain for tax management system etc.

VIII. CONCLUSION

Blockchain is a transformational technology, which provides a basis to develop distributed and secure applications for all industries beyond the monetary markets. Due to its vast and rapid applications development, it is envisaged that Blockchain will do for trusted transactions what the internet did for communications. After the first appearance of Bitcoin in 2008, the concept of Blockchain has got considerable attention by the research and scientific community. On the basis of detailed and comprehensive analysis of the Blockchain evolution, frameworks, architectures, security and privacy characteristics, this paper has presented a survey of relevant works and elaborated on their contributions and limitations with a critical comparative analysis. The paper has provided a perspective to describe the Blockchain architectures in relation to cryptocurrencies, smart contracts and other applications. The research advances in consensus algorithms are also highlighted with some key development and application frameworks. A detailed discussion with respect to future and open research avenues is also performed, which could help to pave the way for researchers to explore the key challenging areas in the Blockchain field.

REFERENCES

[1] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," in *Proc. 1st Int. Conf. Peer Peer Comput.*, Linkoping, Sweden, 2001, pp. 101–102.

[2] J. R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Indianapolis, IN, USA; Wiley, 2008.

[3] B. Schneier, *Applied Cryptography, Protocols, Algorithms and Source Code in C*, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.

[4] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[5] C. R. Merkle, "Method of providing digital signatures," U.S. Patent 4 309 569, Sep. 5, 1979.

[6] A. P. Bernstein and E. Newcomer, *Principles of Transaction Processing*, 2nd ed. Burlington, VT, USA: Morgan Kaufmann, 2009.

[7] M. Swan, *Blockchain, Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[8] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.

[9] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey on blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8642861, doi: 10.1109/COMST.2019.2899617.

[10] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53019–53033, 2018, doi: 10.1109/ACCESS.2018.2870644.

[11] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019, doi: 10.1109/COMST.2018.2863956.

[12] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019, doi: 10.1109/COMST.2019.2894727.

[13] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[14] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[15] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.

[16] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, Sep. 2017, doi: 10.6633/IJNS.201709.19(5).01.

[17] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018, doi: 10.3390/s18082575.

[18] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/IJWGS.2018.10016848.

[19] I. Ahmed and M. A. Shilpi, "Blockchain technology a literature survey," *Int. Res. J. Eng. Technol.*, vol. 5, no. 10, pp. 1490–1493, Oct. 2018. [Online]. Available: https://www.irjet.net/archives/V5/i10/IRJET-V5I10284.pdf

[20] W. Wang, D. T. Hoang, Z. Xiong, D. Niyato, P. Wang, P. Hu, and Y. Wen, "A survey on consensus mechanisms and mining management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[21] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2016, pp. 1–6.

[22] M. Atzori. *Blockchain-Based Architectures for the Internet of Things: A Survey*. Accessed: 2017. [Online]. Available: https://ssrn.com/abstract=2846810

[23] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[24] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[25] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[26] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.

[27] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.

[28] T. Neudecker and H. Hartenstein, "Network layer aspects of permissionless blockchains," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 838–857, 2018.

[29] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey on attacks on Ethereum smart contracts," in *Proc. 6th Int. Conf. Princ. Secur. Trust*, vol. 29, Apr. 2017, pp. 164–186.

[30] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *Int. J. Res. Eng. Technol.*, vol. 5, no. 9, pp. 1–10, Sep. 2016.

[31] Anonymous, "New kid on the blockchain," *New Scientist*, vol. 225, no. 3009, p. 7, Feb. 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0262407915603219, doi: 10.1016/S0262-4079(15)60321-9.

[32] A. Banafa, "IoT and blockchain convergence: Benefits and challenges," *IEEE IoT Newslett.*, vol. 10, Jan. 2017. [Online]. Available: https://iot.ieee.org/newsletter/january-2017.html

[33] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 2017, no. 4, pp. 1–14, 2017. [Online]. Available: https://ieeexplore.ieee.org/ielx7/6287639/6514899/09184895.pdf

[34] H. Berg. *How is Blockchain Verifiable by Public and Yet Anonymous?* Accessed: May 11, 2019. [Online]. Available: https://www.quora.com/How-is-Blockchain-verifiable-by-public-and-yet-anonymous

[35] J. Bruce. *The Mini-Blockchain Scheme Rev 3*. Accessed: May 12, 2019. [Online]. Available: http://cryptonite.info/files/mbc-scheme-rev3.pdf

[36] V. Buterin. *A Next Generation Smart Contract and Decentralized Application Platform*. Accessed: May 13, 2019. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[37] R. Dennis, G. Owenson, and B. Aziz, "A temporal blockchain: A formal analysis," in *Proc. Int. Conf. Collaboration Technol. Syst. (CTS)*, Orlando, FL, USA, Oct. 2016, pp. 430–437.

[38] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, and R. Hierons, "Smart contracts vulnerabilities: A call for blockchain software engineering?" in *Proc. Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, Campobasso, Italy, vol. 20, Mar. 2018, pp. 19–25.

[39] M. Dunjic. (Jun. 3, 2018). *Blockchain Immutability. Blessing or Curse?* Blog Article. Accessed: May 11, 2019. [Online]. Available: https://www.finextra.com/blogposting/15419/Blockchain-immutability–blessing-or-curse

[40] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K.-R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.

[41] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur.* Christ Church, Barbados: Springer, Mar. 2014, pp. 436–454.

[42] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[43] K. Francisco and D. Swanson, "The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency," *Logistics*, vol. 2, no. 1, p. 2, Jan. 2018, doi: 10.3390/logistics2010002.

[44] J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," *Perform. Eval.*, vol. 104, pp. 23–41, Oct. 2016.

[45] G. Irving and J. Holden, "How blockchain-timestamped protocols could improve the trustworthiness of medical science," *FResearch*, vol. 5, p. 222, Mar. 2017. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4866630/

[46] A. Javed. *Managing Data Traceability: Impact and Benefits*. Accessed: May 11, 2019. [Online]. Available: http://www.xorlogics.com/2017/04/10/managing-data-traceability-impact-and-benefits/

[47] P. Kasireddy. *ELI5: What do we Mean by 'Blockchains are Trustless'?* Accessed: May 10, 2019. [Online]. Available: https://medium.com/preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6

[48] S. Kim, Y. Kwon, and S. Cho, "A survey of scalability solutions on blockchain," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Jeju Island, South Korea, Oct. 2018, pp. 1204–1207.

[49] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Softw.*, vol. 34, no. 6, pp. 21–27, Nov. 2017.

[50] Y. Lu, "Blockchain: A survey on functions, applications and open issues," *J. Ind. Integr. Manage.*, vol. 3, no. 4, Dec. 2018, Art. no. 1850015.

[51] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 254–269.

[52] D. Massessi. *Blockchain Consensus and Fault Tolerance in a Nutshell*. Accessed: May 12, 2019. [Online]. Available: https://medium.com/coinmonks/Blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03

[53] T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in *Proc. 18th Annu. Int. Conf. Digit. Government Res.*, Staten Island, NY, USA, Jun. 2017, pp. 574–575.

[54] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[55] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," *FResearch*, vol. 5, p. 2541, Oct. 2016, doi: 10.12688/f1000research.9756.1.

[56] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, Mar. 2018.

[57] S. Russolillo and E.-Y. Jeong, "Cryptocurrency exchanges are getting hacked because it's easy," *Wall Street J.*, Jul. 2018. Accessed: May 12, 2019. [Online]. Available: https://www.wsj.com/articles/why-cryptocurrency-exchange-hacks-keep-happening-1531656000

[58] S. Sayadi, S. Ben Rejeb, and Z. Choukair, "Blockchain challenges and security schemes: A survey," in *Proc. 7th Int. Conf. Commun. Netw. (ComNet)*, Hammamet, Tunisia, Nov. 2018, pp. 1–7.

[59] J. Sidhu, "Syscoin: A peer-to-peer electronic cash system with blockchain-based services for E-business," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Vancouver, BC, Canada, vol. 3, Jul. 2017, pp. 1–6.

[60] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *Proc. 19th Int. Conf. Financial Cryptogr. Data Secur.*, San Juan, Puerto Rico. Berlin, Germany: Springer, Jan. 2015, pp. 507–527.

[61] M. Swan, *Blockchain: Blueprint for a New Economy*. Newton, MA, USA: O'Reilly, 2015.

[62] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manage.*, Dalian, China, Jun. 2017, pp. 1–6.

[63] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," in *Proc. IEEE 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, New York City, NY, USA, Oct. 2017, pp. 469–474.

[64] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, Madrid, Spain, May 2017, pp. 458–467.

[65] J. Truby, "Decarbonizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies," *Energy Res. Social Sci.*, vol. 44, pp. 399–410, Oct. 2018.

[66] M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Secur.*, Zurich, Switzerland, vol. 29, Oct. 2015, pp. 112–125.

[67] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[68] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019.

[69] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[70] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, Feb. 2019.

[71] Y. Xinyi, Z. Yi, and Y. He, "Technical characteristics and model of blockchain," in *Proc. 10th APCA Int. Conf. Control Soft Comput. (CONTROLO)*, Jun. 2018, pp. 562–566.

[72] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE 6th Int. Congr. Big Data*, Honolulu, HI, USA, Jun. 2017, pp. 557–564.

[73] J. Evans. (Jan. 10, 2019). *Blockchain Nodes: An in Depth Guide*. Nodes.com. Accessed: Mar. 13, 2019. [Online]. Available: https://nodes.com/

[74] Pluralsight. (Jan. 19, 2019). *Blockchain Architecture*. Pluralsight.com. Accessed: Mar. 13, 2019. [Online]. Available: https://www.pluralsight.com/guides/Blockchain-architecture

[75] E. J. A. Kroll, "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries," in *Proc. 12th Workshop Econ. Inf. Secur. (WEIS)*. Washington, DC, USA: Georgetown Univ., 2013, p. 11.

[76] M. Milutinovic, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. 1st Workshop Syst. Softw. Trusted Execution*, New York, NY, USA, Dec. 2016.

[77] E. J. Becker, "Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency," in *The Economics of Information Security and Privacy*. Springer, 2013, pp. 135–156.

[78] Raspnode. (Jun. 10, 2015). *DIY Raspberry Pi Cryptocurrency Node*. Raspnode. Accessed: Mar. 14, 2019. [Online]. Available: http://raspnode.com/

[79] L. Hertig. (Nov. 18, 2018). *Hidden Blockchain Opportunities (2): Masternodes & Enterprise Blockchain Hosting*. Plesk.com. Accessed: Mar. 18, 2019. [Online]. Available: https://www.plesk.com/blog/product-technology/hidden-Blockchain-opportunities-2-masternodes-enterprise-hosting/

[80] D. Gruber, W. Li, and G. Karame, "Unifying lightweight blockchain client implementations," in *Proc. Workshop Decentralized IoT Secur. Standards (DISS)*, San Diego, CA, USA, 2018.

[81] S. Omohundro, "Cryptocurrencies, smart contracts, and artificial intelligence," *AI Matters*, vol. 1, no. 2, pp. 19–21, Dec. 2014.

[82] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[83] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, "Untrusted business process monitoring and execution using blockchain," in *Proc. Int. Conf. Bus. Process Manage.* Cham, Switzerland: Springer, 2016, pp. 329–347.

[84] P. E. O'Neil, "The escrow transactional method," *ACM Trans. Database Syst.*, vol. 11, no. 4, pp. 405–430, Dec. 1986.

[85] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and S. Muralidharan, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Lisbon, Portugal, Apr. 2018, doi: 10.1145/3190508.3190538.

[86] A. Davies. (Aug. 18, 2018). *Pros and Cons of Hyperledger Fabric for Blockchain Networks*. DevTeam.Space. Accessed: Mar. 19, 2019. [Online]. Available: https://www.devteam.space/blog/pros-and-cons-of-hyperledger-fabric-for-Blockchain-networks/

[87] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017.

[88] P. Vasin. (2018). *Blackcoin's Proof-of-Stake Protocol V2*. Accessed: Mar. 20, 2019. [Online]. Available: https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper. pdf

[89] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake Blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA. Cham, Switzerland: Springer, 2018.

[90] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (poet)," in *Proc. Int. Symp. Stabilization, Saf., Secur. Distrib. Syst.* Cham, Switzerland: Springer, 2017.

[91] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," 2018, *arXiv:1805.02707*. [Online]. Available: http://arxiv.org/abs/1805.02707

[92] K. Driscoll, B. Hall, H. Sivencrona, and P. Zumsteg, "Byzantine fault tolerance, from theory to reality," in *Proc. Int. Conf. Comput. Saf.* Berlin, Germany: Springer, 2003.

[93] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Operating Syst. Design Implement.*, New Orlin, LA, USA, 1999.

[94] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. Int. Conv. Inf. Commun. Technol., Electron. Microelectron.*, Zagreb, Croatia, 2018.

[95] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Elsevier Future Gener. Comput.*, vol. 88, pp. 173–190, Nov. 2018.

[96] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," 2018, *arXiv:1801.10228*. [Online]. Available: https://arxiv.org/pdf/1801.10228.pdf

[97] D. Larimer, "DPOS consensus algorithm—The missing white paper," Steemit, New York, NY, USA, White Paper, 2018.

[98] V. N. C. P. L. E. Z. Igor and M. Coelho, "Delegated Byzantine fault tolerance: Technical details, challenges and perspectives," NEO, Shanghai, China, Tech. Rep., Mar. 2019, sec. 8. [Online]. Available: https://neoresearch.io/assets/yellowpaper/yellow_paper.pdf

[99] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. 1st Workshop Syst. Softw. Trusted Execution*, Trento, Itlay, Dec. 2016.

[100] A. Shoker, "Sustainable blockchain through proof of exercise," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, Oct. 2017.

[101] NEM. (2018). *Investor Harvesting: Proof-of-Importance*. NEM (XEM). Accessed: Apr. 22, 2019. [Online]. Available: https://nem.io/xem/harvesting-and-poi/

[102] (2019). *Vitalik Buterin*. Accessed: May 23, 2019. [Online]. Available: http://Blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[103] (2019). *TRON: Advanced Decentralized Blockchain Platform*. Accessed: May 23, 2019. [Online]. Available: https://tron.network/static/doc/white_paper_v_2_0.pdf

[104] *An Introduction to Hyperledger*. Accessed: May 23, 2019. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf

[105] *Hyperledger Publications*. Accessed: May 23, 2019. [Online]. Available: https://www.hyperledger.org/resources/publications

[106] *TRON*. Accessed: May 23, 2019. [Online]. Available: https://ipfs.io/ipfs/QmWh3LEWUQN8LsoHerQecmwfACXAPNKE9wigx6t9dLitmE/tron/Tron-Whitepaper-1031-V18-EN.pdf

[107] G. Greenspan. (2019). *MultiChain Private Blockchain*. Accessed: May 23, 2019. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf

[108] *OPEN Chain: Scalability Through Data Parallelization*. Accessed: May 23, 2019. [Online]. Available: https://s3.amazonaws.com/openmoney/OPEN_Chain_-_Scalability_Through_Data_Parallelization_-_Google_Docs.pdf

[109] *OPEN Chain*. Accessed: May 23, 2019. [Online]. Available: https://drive.google.com/file/d/0B7ljBZOyjFLkYi0teUN6T3NweU1FUjVnaUVVc2M2SXE2UTI0/view

[110] *Smart Quorum*. Accessed: May 23, 2019. [Online]. Available: https://smartquorum.com/download/WhitePaperSmartQuorum.pdf

[111] A. Baliga, I. Subhod, P. Kamat, and S. Chatterjee, "Performance evaluation of the quorum blockchain platform," 2018, *arXiv:1809.03421*. Accessed: May 23, 2019. [Online]. Available: http://arxiv.org/abs/1809.03421

[112] S. Popov. (2018). *The Tangle*. Accessed: May 23, 2019. [Online]. Available: https://docs.iota.org/

[113] Y. Yanovich, I. Ivashchenko, A. Ostrovsky, A. Shevchenko, A. Sidorov. (2018). *Exonum: Byzantine Fault Tolerant Protocol for Blockchains*. Accessed: May 23, 2019. [Online]. Available: https://bitfury.com/content/downloads/wp_consensus_181227.pdf

[114] *Exonum*. Accessed: May 23, 2019. [Online]. Available: https://exonum.com/doc/version/latest/

[115] *6 Blockchain Frameworks to Build Enterprise Blockchain & How to Choose Them*. Accessed: May 23, 2019. [Online]. Available: https://dreamztechusa.com/blog/6-Blockchain-frameworks-build-enterprise-Blockchain-choose/

[116] D. B. Black. (2019). *Microsoft and Intel Detail the Deep-Seated Problems With Blockchain*. Accessed: May 23, 2019. [Online]. Available: https://www.forbes.com/sites/davidblack/2019/05/13/microsoft-and-intel-detail-the-deep-seated-problems-with-Blockchain/#4a90d9c36b06

[117] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[118] R. Martin. *5 Blocked Security Risks and How to Reduce Them*. Accessed: Nov. 29, 2018. [Online]. Available: https://igniteoutsourcing.com/Blockchain/Blockchain-security-vulnerabilities-risks/

[119] D. He, K.-K.-R. Choo, N. Kumar, and A. Castiglione, "IEEE access special section editorial: Research challenges and opportunities in security and privacy of blockchain technologies," *IEEE Access*, vol. 6, pp. 72033–72036, 2018.

[120] Q. Wang, X. Li, and Y. Yu, "Anonymity for bitcoin from secure escrow address," *IEEE Access*, vol. 6, pp. 12336–12341, 2018.

[121] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, 2018.

[122] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Comput. Sci.*, vol. 132, pp. 1815–1823, Jan. 2018.

[123] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.

[124] J. Baumann and A. Lesoismier, "Cryptocurrencies outlook 2018. Stairway to heaven," Swiss Borg, Lausanne, Switzerland, Tech. Rep. 25, 2017.

[125] A. Narayanan, J. Bonneau, E. Felten, M. A. Andrew, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*. Princeton, NJ, USA: Princeton Univ. Press, 2016.

[126] P. D. DeVries, "An analysis of cryptocurrency, bitcoin, and the future," *Int. J. Bus. Manage. Commerce*, vol. 1, no. 2, pp. 1–3, 2016.

[127] E. Teo. (Accessed: Mar. 4, 2009). *How Do Cryptocurrencies Work?* [Online]. Available: https://skbi.smu.edu.sg/sites/default/files/skbife/HowDoCryptocurrenciesWorkErnieTeo.pdf

[128] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Math. Found. Comput.*, vol. 1, no. 2, pp. 121–147, 2018.

[129] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[130] A. Chakravorty, T. Wlodarczyk, and C. Rong, "Privacy preserving data analytics for smart homes," in in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2013, pp. 23–27.

[131] A. Dorri, S. S. Kanhare, R. Jurdak, and P. Gauravara. *Blockchain for IoT Security and Privacy: The Case Study of a Smart Home*. Accessed: Mar. 2017. [Online]. Available: https://www.researchgate.net/publication/312218574_Blockchain_for_IoT_Security_an_Privacy_The_Case_Study_of_a_Smart_Home

[132] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[133] S. He, Q. Wu, X. Luo, Z. Liang, D. Li, H. Feng, H. Zheng, and Y. Li, "A social-network-based cryptocurrency wallet-management scheme," *IEEE Access*, vol. 6, pp. 7654–7663, 2018.

[134] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, "Cryptographic primitives in blockchains," *J. Netw. Comput. Appl.*, vol. 127, pp. 43–58, Feb. 2019, doi: 10.1016/j.jnca.2018.11.003.

[135] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[136] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

[137] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed E-cash from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2013, pp. 397–411.

[138] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," 2018, *arXiv:1802.06993*. Accessed: Mar. 27, 2019. [Online]. Available: http://arxiv.org/abs/1802.06993

[139] F. Alkurdi, I. Elgend, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "Blockchain in IoT security: A survey," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf.*, 2018, pp. 1–4.

[140] X. Lia, P. Jianga, T. Chenb, X. Luoa, and Q. Wenc, Dept. Comput., Hong Kong Polytech. Univ., Hong Kong Center Cybersecurity, Univ. Electron. Sci. Technol. China, Chengdu, China, Tech. Rep. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17318332

[141] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019.

[142] N. Atzei, M. Bartoletti, T. Cimoli, S. Lande, and R. Zunino, "SoK: Unraveling Bitcoin smart contracts," in *Proc. Int. Conf. Princ. Secur. Trust*, 2018, pp. 217–242.

[143] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," in *Proc. Int. Symp. Stabilization, Saf., Secur. Distrib. Syst.*, 2017.

[144] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph based blockchain for Internet of Things: Performance and security analysis," 2019, *arXiv:1905.10925*. [Online]. Available: https://arxiv.org/abs/1905.10925

[145] P. Compare. *What is Proof of Weight, a Web Article Published by Coincodex*. Accessed: 2019. [Online]. Available: https://coincodex.com/article/2617/what-is-proof-of-weight/

[146] Q. Zhuang, Y. Liu, L. Chen, and Z. Ai, "Proof of reputation: A reputation-based consensus protocol for blockchain based systems," in *Proc. Int. Electron. Commun. Conf. (ACM IECC)*, Okinawa, Japan, Jul. 2019, pp. 131–138.

[147] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Proc. 35th Annu. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 2015, pp. 585–605.

[148] R. Smith. (2019). *Proof of Burn | Consensus Through Coin Destruction, Article Published by Coin Central*. [Online]. Available: https://coincentral.com/proof-of-burn/

[149] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 2017, no. 4, p. 114, 2017.

[150] *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Dec. 21, 2019. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[151] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: Problems and recommendations," *IEEE Access*, vol. 7, pp. 176838–176869, 2019, doi: 10.1109/ACCESS.2019.2957660.

[152] M. S. Siddiqui, T. Ali, A. Nadeem, W. Nawaz, and S. S. Albouq, "BlockTrack-L: A lightweight blockchain-based provenance message tracking in IoT," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 4, pp. 463–470, 2020.

[153] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain meets cloud computing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2009–2030, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2989392.

[154] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," *IEEE Access*, vol. 8, pp. 126927–126950, 2020, doi: 10.1109/ACCESS.2020.3006078.

[155] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1977–2008, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2975999.

[156] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020, doi: 10.1109/ACCESS.2020.3007251.

[157] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020, doi: 10.1109/COMST.2020.2969706.

[158] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020, doi: 10.1109/TEM.2019.2926471.

[159] Y. Zou, T. Meng, P. Zhang, W. Zhang, and H. Li, "Focus on blockchain: A comprehensive survey on academic and application," *IEEE Access*, vol. 8, pp. 187182–187201, 2020, doi: 10.1109/ACCESS.2020.3030491.

[160] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 3–19, Jan. 2021, doi: 10.1109/TII.2020.2998479.

[161] S. E. Chang and Y. Chen, "When blockchain meets supply chain: A systematic literature review on current development and potential applications," *IEEE Access*, vol. 8, pp. 62478–62494, 2020, doi: 10.1109/ACCESS.2020.2983601.

[162] Y. Liu, D. He, S. M. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *J. Netw. Comput. Appl.*, vol. 166, Jun. 2020, Art. no. 102731.

[163] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.

[164] T. A. Syed, M. S. Siddique, A. Nadeem, A. Alzahrani, S. Jan, and M. A. K. Khattak, "A novel blockchain-based framework for vehicle life cycle tracking: An end-to-end solution," *IEEE Access*, vol. 8, pp. 111042–111063, 2020, doi: 10.1109/ACCESS.2020.3002170.

[165] T. Li, W. Zhang, N. Chen, M. Qian, and Y. Xu, "Blockchain technology based decentralized energy trading for multiple-microgrid systems," in *Proc. IEEE 3rd Conf. Energy Internet Energy Syst. Integr. (EI)*, Changsha, China, Nov. 2019, pp. 631–636, doi: 10.1109/EI247390.2019.9061928.

[166] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017.

[167] S.-J. Horng, S.-F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "B-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013.

[168] Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, "On emerging family of elliptic curves to secure Internet of Things: ECC comes of age," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 3, pp. 237–248, Jun. 2017.

[169] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah, and R. Baliyani, "A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3527–3542, Nov. 2016.

[170] S. Wan, M. Li, G. Liu, and C. Wang, "Recent advances in consensus protocols for blockchain: A survey," *Wireless Netw.*, vol. 26, no. 8, pp. 5579–5593, Nov. 2020, doi: 10.1007/s11276-019-02195-0.

[171] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efcient mutual authentication protocol for smart grid under blockchain," *Peer Peer Netw.*, vol. 13, no. 6, pp. 1–3, Nov. 2020.

[172] Z. Lejun, P. Minghui, W. Weizheng, S. Yansen, C. Shuna, and K. Seokhoon, "Secure and efficient medical data storage and sharing scheme based on double blockchain," *Comput., Mater. Continua*, vol. 66, no. 1, pp. 499–515, 2020.

[173] W. Wang, H. Huang, L. Zhang, Z. Han, C. Qiu, and C. Su, "BlockSLAP: Blockchain-based secure and lightweight authentication protocol for smart grid," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Guangzhou University, China, Jan. 2021, pp. 1332–1338.

[174] W. Wang and C. Su, "CCBRSN: A system with high embedding capacity for covert communication in bitcoin," *ICT Systems Security and Privacy Protection* (IFIP Advances in Information and Communication Technology), vol. 580, M. Hölbl, K. Rannenberg, and T. Welzer, Eds. Cham, Switzerland: Springer, 2020.

[175] L. Zhang, Z. Zhang, W. Wang, R. Waqas, C. Zhao, S. Kim, and H. Chen, "A covert communication method using special bitcoin addresses generated by vanitygen," *Comput., Mater. Continua*, vol. 65, no. 1, pp. 597–616, 2020.

MUHAMMAD NASIR MUMTAZ BHUTTA received the B.C.S. degree (Hons.) from International Islamic University, Islamabad, Pakistan, in 2004, and the M.Sc. and Ph.D. degrees from the University of Surrey, U.K., in 2007 and 2012, respectively. He is currently working as an Assistant Professor with King Faisal University. He is an active researcher with numerous publications in international conferences and journals. He has contributed to several research projects, including three research projects funded from EADS Astrium U.K., ESA, and ESPRC U.K. He is also focusing on technical and management aspects of Cyber Security for the IoT, smart cities, and blockchain.

AMIR A. KHWAJA received the bachelor's degree in computer engineering from NED University of Engineering and Technology, Karachi, Pakistan, and the M.S. and Ph.D. degrees in computer science from Arizona State University, Arizona, USA. Since 2014, he has been an Assistant Professor with the College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia. Prior to that he had 21 years of semiconductor industry experience. He worked for 20 years at Intel Corporation, USA, in various capacities, such as a CAD Software Developer, an XScale and Atom Mobile System-on-a-Chip (SoC) Validation Architect, a Validation Program Manager, and a Senior Engineering Manager. He worked as a Principal Engineer and Senior Manager for one year at Qualcomm, San Diego, California, USA, leading the successful completion of the validation of Qualcomm's Femtocell SoC product. He has also worked as an Adjunct Faculty with Arizona State University and the University of Phoenix. He is currently serving at Qualcomm.

ADNAN NADEEM (Member, IEEE) received the Ph.D. degree from the Institute for Communication Systems, U.K., in 2011. He has been an Associate Professor and the Coordinator of MS Security Technology Program with the Faculty of Computer and Information System (FCIS), Islamic University of Madinah, KSA, since 2016. He is currently with the Federal Urdu University of Arts Science and Technology, Pakistan. For the last five years, he earned several research grants. He has published more than 50 articles in international conferences and journals, including a patent accepted and sealed by the Government of Pakistan. He has mainly worked on network layer security, QoS and reliability issues of mobile Ad Hoc, and sensors networks. He is currently focusing on Blockchain technology and the IoT applications and security. He received the 5th HEC Outstanding Research Award 2013/14 for his article published in the IEEE COMMUNICATION SURVEY & TUTORIALS. During his pedagogical journey, he has received several awards and achievements, including the Foreign Ph.D. Scholarship, Associate Fellowship of Higher Education Academy (AFHEA), U.K., in 2009, and the Best Paper and Best Track Paper Award in the ICICTT 2013 and ICEET 2016 conferences, respectively. He received Nishan-e-Imtiaz for his outstanding research from Federal Urdu University, Pakistan, in August 2016. He received the Best Academic Advisor and Best Researcher Award from FCIS, Islamic University of Madinah, in 2018.

HAFIZ FAROOQ AHMAD received the Ph.D. degree in distributed computing from Tokyo Institute of Technology, Tokyo, Japan. He is currently an Associate Professor with the College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al Ahsa, Saudi Arabia. He is the pioneer for Semantic Web Application Firewall (SWAF) in cooperation with DTS Inc., Japan, in 2010. He contributed in agent cites project, a European funded research and development project for agent systems. He initiated Scalable fault tolerant Agent Grooming Environment (SAGE) Project and proposed the concept of decentralized multi agent systems SAGE back, in 2002. He has more than 100 international publications, including a book on security in sensors. His research interests include semantics systems, machine learning, health informatics, and Web application security. He has been awarded a number of national and international awards, such as the Best Researcher Award of the Year 2011 by NUST, the PSF/COMSTECH Best Researcher of the Year 2005, and the Star Laureate Award, in 2004.

MUHAMMAD KHURRAM KHAN (Senior Member, IEEE) is currently working as a Professor of cybersecurity with the Center of Excellence in Information Assurance, King Saud University, Saudi Arabia. He is the Founder and the CEO of the Global Foundation for Cyber Studies and Research, Washington DC, USA, an independent and non-partisan cybersecurity think-tank. He has published more than 400 papers in the journals and conferences of international repute. In addition, he is an Inventor of ten US/PCT patents. His research interests include cybersecurity, digital authentication, the IoT security, biometrics, multimedia security, cloud computing security, cyber policy, and technological innovation management. He is a Fellow of the IET, U.K., the BCS, U.K., and the FTRA, South Korea. He is the Vice Chair of IEEE Communications Society Saudi Chapter. He is a Distinguished Lecturer of the IEEE. He is the Editor-in-Chief of *Telecommunication Systems* (Springer-Nature) with its recent impact factor of 1.73 (JCR 2020). He has edited ten books/proceedings published by Springer-Verlag, Taylor & Francis, and IEEE. He is on the editorial board of several journals including, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, *IEEE Communications Magazine*, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, *Journal of Network & Computer Applications* (Elsevier), IEEE ACCESS, *IEEE Consumer Electronics Magazine*, *PLOS One*, and *Electronic Commerce Research*.

MOATAZ A. HANIF received the master's degree in cybersecurity engineering from Embry-Riddle Aeronautical University. He is currently a Computer Engineer and AI Enthusiast. He has participated in several publications in the Blockchain field and is currently working in the cybersecurity field as IR Team Lead.

HOUBING SONG (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in August 2012, and the M.S. degree in civil engineering from the University of Texas, TX, USA, in December 2006.

In August 2017, he joined the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, FL, where he is currently an Assistant Professor and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab). From August 2012 to August 2017, he served on the Faculty of West Virginia University. In 2007, he was an Engineering Research Associate with the Texas A&M Transportation Institute. He is the author of more than 100 articles. His research interests include cyber-physical systems, cybersecurity and privacy, the Internet of Things, edge computing, AI/machine learning, big data analytics, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking. His research has been featured by popular news media outlets, including IEEE GlobalSpec's Engineering360, USA Today, U.S. News & World Report, Fox News, Association for Unmanned Vehicle Systems International (AUVSI), Forbes, WFTV, and New Atlas.

Dr. Song is a Senior Member of ACM and an ACM Distinguished Speaker. He was a recipient of the Best Paper Award from the 12th IEEE International Conference on Cyber, Physical and Social Computing (CPSCom-2019), the Best Paper Award from the 2nd IEEE International Conference on Industrial Internet (ICII 2019), the Best Paper Award from the 19th Integrated Communication, Navigation and Surveillance technologies (ICNS 2019) Conference, the Best Paper Award from the 6th IEEE International Conference on Cloud and Big Data Computing (CBDCom 2020), and the Best Paper Award from the 15th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2020). He has been serving as an Associate Technical Editor for IEEE COMMUNICATIONS MAGAZINE, since 2017, an Associate Editor for IEEE INTERNET OF THINGS JOURNAL, since 2020, and IEEE JOURNAL ON MINIATURIZATION FOR AIR AND SPACE SYSTEMS (J-MASS), since 2020, and a Guest Editor for IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (J-SAC), IEEE INTERNET OF THINGS JOURNAL, *IEEE Network*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE SENSORS JOURNAL, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, and IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS. He is the editor of six books, including *Big Data Analytics for Cyber-Physical Systems: Machine Learning for the Internet of Things* (Elsevier, 2019), *Smart Cities: Foundations, Principles and Applications* (Hoboken, NJ: Wiley, 2017), *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications* (Chichester, UK: Wiley-IEEE Press, 2017), *Cyber-Physical Systems: Foundations, Principles and Applications* (Boston, MA: Academic Press, 2016), and *Industrial Internet of Things: Cybermanufacturing Systems* (Cham, Switzerland: Springer, 2016).

MAJED ALSHAMARI received the B.Sc. degree in computer information systems from King Faisal University, Saudi Arabia, and the M.Sc. and Ph.D. degrees in information systems from University of East Anglia, Norwich, U.K. Prior to that, he has been an Assistant Professor, since 2011. Since 2012, he has been the Dean of the College of Computer Sciences and Information Technology, King Faisal University. Since 2017, he has been an Associate Professor with the College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia. He has been leading a number of academic and scientific funded projects related to usability, HCI, and HIS. His research interests include HCI, information systems developments, and big data.

YUE CAO (Member, IEEE) received the Ph.D. degree from the Institute for Communication Systems (ICS) (formerly known as Centre for Communication Systems Research), University of Surrey, Guildford, U.K., in 2013. Further to his Ph.D. study, he had conducted research as a Research Fellow with the University of Surrey, and as an Academic Faculty with Northumbria University, Lancaster University, U.K., and Beihang University, China. He is currently a Professor with the School of Cyber Science and Engineering, Wuhan University, China. His research interests include intelligent transport systems, including e-mobility, V2X, and edge computing.