Computers and Electrical Engineering 90 (2021) 106897

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions

Bharat Bhushan [a,*], Preeti Sinha [b], K. Martin Sagayam [c], Andrew J [d]

[a] Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh-201310, India
[b] System Engineer, Tata Consultancy Services, Noida, Uttar Pradesh-201309, India
[c] Department of Electronics and Communication Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil nade-641114, India
[d] Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil nade-641114, India

ARTICLE INFO

Keywords:
Blockchain
Data privacy
Security
Anonymity
Cryptocurrency
Survey

ABSTRACT

Blockchain is a distributed, decentralized public ledger that has gained massive momentum recently. Currently, security services such as privacy, confidentiality, resource provenance, access control, authentication and integrity assurance are managed by centralized controllers. However, this centralization faces numerous security and privacy challenges. Blockchain solve such challenges as it helps to create an attack resistant, digital data storage as well as sharing platform by employing linked block structures for data verification and trusted consensus mechanism for data synchronization. The goals of this paper are to provide an in-depth survey of blockchain technology, to provide insights into the blockchain security threats, to highlight the privacy necessities for current applications, to outline their challenges and give an insight on how these challenges can be resolved by the blockchain technology. Furthermore, we summarize the future research challenges associated with the usage of blockchain based security services to spur further investigation in this field.

1. Introduction

A ground breaking innovation named blockchain is stamping the dawn of an emerging era. Blockchain is a distributed, shared and secured ledger that helps to track and record resources without the need of any centralized authority. Originally invented as the Bitcoin's underlying infrastructure (the first ever decentralized cryptocurrency), the potential application of blockchain has advanced far beyond financial assets and cryptocurrencies [1]. It facilitates communication and exchange of resources among two parties in a peer-to-peer (P2P) network where majority of the distributed decision are made by a centralized authority. Resources can be intangible (e.g. intellectual copy rights, digital documents and copyrights) or tangible (e.g. lands, cars, houses and money). In general, a blockchain network can track anything that has a value to mitigate the overall monitoring cost and the security risks involved [2,3].

The traditional database approaches employ concurrency control scheme and assumes a trusted environment to order transactions. In contrast, blockchain technology can guarantee security and resolve numerous traditional vulnerabilities by providing a consensus,

* Corresponding author.
E-mail addresses: bharat_bhushan1989@yahoo.com (B. Bhushan), andrewj@karunya.edu (A. J).

https://doi.org/10.1016/j.compeleceng.2020.106897
Received 15 July 2019; Received in revised form 24 October 2020; Accepted 26 October 2020
Available online 1 November 2020
0045-7906/

provably secure and distributed solutions. Moreover, blockchain assumes the node to behave in a byzantine or arbitrary manner and therefore blockchain based systems are capable of tolerating byzantine failure and offering enhanced security as compared to incumbent database systems [4]. Fig. 1 presents the difference between the access control guarantees in a traditional centralized architecture and the blockchain network architecture. The access control schemes of a traditional centralized architecture are shown by Fig. 1 (a) and that of a blockchain network architecture is shown by Fig. 1 (b). Blockchain has capability to distort the status of third-party brokers in these applications as it sustains low cost and provides security services such as provenance, integrity, privacy, authentication and confidentiality. The transparency and immutability of blockchain helps to reduce the need for manual intervention and also mitigates human errors arising because of conflicting data. Blockchain technology helps to remove duplicate efforts thereby streamlining business processes in data governance and also automate device management enabling convenient data synchronization among Internet of Things (IoT) devices [5].

Blockchain have several promising applications including security trading and settlement [6], banking and insurance [7], asset and finance management [8] and several others. Owing to the widespread adoption of blockchain technology, there have been several previously published surveys that have reviewed blockchain in varied degrees of depth and scopes. Most of the in-depth surveys or review articles on blockchain technology focusses on cryptocurrencies, consensus schemes, integration with IoT and emphasize mainly on the security challenges faced by various blockchain based applications [9–12]. These do not cover a broad aspect of blockchain technology and represent only its partial potential as a data processing platform. Furthermore, the aforementioned surveys only consider either few selected topics or a particular issue only. To the best of our knowledge, this is the first survey that brings forth a wider, detailed view of blockchain focussing especially on security threats, privacy challenges, application areas and future research directions. This up-to-date survey addresses the state-of-the-art blockchain technology, trade-offs in selecting the most suited consensus protocols, security threats, privacy services, blockchain based security standards and open research challenges. In summary, the major contribution of our work is as follows.

- This work presents an in-depth survey of blockchain technology and also explores state-of-the-art by categorizing the system into four facets: distributed ledger, cryptography, forks and consensus protocol. The goal is to enable the new readers to get the required familiarity with blockchain and its underlying technologies.
- This work presents a systematic survey that covers the blockchain security threats along with their attack vectors, cause and the proposed countermeasures.
- This work redefines the data privacy concept in blockchain. It investigates the data privacy requirements, its necessity to the current applications, current challenges faced in providing an efficient privacy service and how blockchain effectively comes to the rescue.
- Finally, this work identifies several critical open challenges that restricts the practicality of blockchain and provides a roadmap of encouraging research opportunities, challenges and avenues for which future research is required.

The remainder of the paper is organized as follows. Section 2 presents the overview of the architecture, classification, characteristics and open source implementations of blockchain technology. Section 3 describes the state-of-the-art and key concepts related to blockchain technology. Section 4 explores various types of blockchain security threats. Section 5 presents a detailed description of four key blockchain based security standards namely P2P network, smart contract, asymmetric encryption and distributed ledger. Numerous open challenges and future research directions are explored in Section 6 followed by conclusion in Section 7.

2. Overview of Blockchain

In order to execute sequential and successful money transfer, a financial system requires a ledger for recording the transaction history and verifying them. In 1494, the Italian mathematician Lucca Pacioli developed a double entry bookkeeping system that records the destination and source of each account simultaneously. Further, it introduces the account verification scheme to enhance the reliability of accounting [13]. In contrast to the traditional centralized bookkeeping approaches, a distributed, decentralized and tamper proof architecture named blockchain is proposed where every peer node maintains the shared copy of the ledger. S. Nakamoto introduced first generation of blockchain technology, restricted only to money transactions to avoid cheating or misbehaving and was

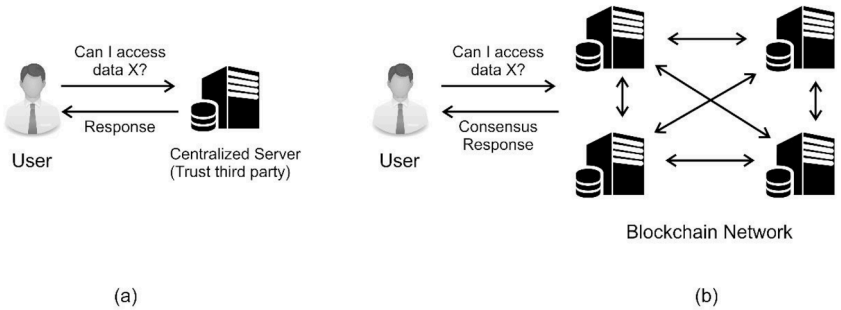

Fig. 1. Access Control guarantees provided by traditional centralized architecture and blockchain network architecture

initially launched as a part of cryptocurrency named Bitcoin [14]. A brief introduction to blockchain and its appealing characteristics along with its open source implementations and privacy requirements are presented in this section with an objective to introduce the researchers to the key principles of the blockchain technology.

2.1. Blockchain architecture

Blockchain can be viewed as a log with its records arranged in the form of timestamped blocks. These blocks are identified by its cryptographic hash and every block references the hash of its previous block. This creates a chain of blocks in blockchain as depicted in Fig. 2.

In order to understand the working of a typical blockchain network, we consider a set of nodes (clients) operating on a single blockchain to form a P2P network. The sequence of steps involved are enumerated as below.

- Step 1: Users use their private/public keys to interact with the blockchain. These users make their public key addressable on the network and use their private keys for signing their transactions. The signed transactions are then broadcasted to the one-hop peers. The asymmetric key cryptography helps to maintain integrity, authentication and non-repudiation within the network.
- Step 2: The neighbouring peers verify validity of the transaction, discards invalid transactions and relays the valid ones further. The validity of the transaction is verified using the application dependent rules (certain conditions that must be satisfied by every database transaction) programmed into the client.
- Step 3: The validated transactions that are collected within the agreed time frame, are mined (i.e., packed into a timestamped candidate block). Based on the consensus strategy, the mining nodes are selected to broadcast these timestamped blocks to the entire network.
- Step 4: The nodes verify that the suggested block is referenced via hash of its preceding block and holds valid transactions. if it holds true, the block is appended to the chain else discarded.

Every node in the network follows the above listed repeating steps in order to guarantee the authenticity and timestamped network activity of the shared blockchain. The blockchain majorly comprise of a network of nodes and a database for record maintenance. A blockchain database is fault-tolerant, distributed, shared and append-only type that is maintained by P2P network nodes. A block is a data structure comprised of a block header and several transaction records. A typical block header consists of time stamp, Merkle root, hash value of the preceding block, a nonce and other related information. A Merkle tree is a hash tree where the hash of a data block labels every leaf node and the cryptographic hash of the child labels the non-leaf nodes. Although, all the blockchain users are capable of accessing the blocks but they cannot delete or alter the content. Each block holds the hash of the previous block and are connected to each other forming a chain like structure. Moreover, each block has a timestamp, several verified transactions and "*nonce*" for performing cryptographic operations. The communicating parties in a blockchain network are capable of interacting with each other without the need of any third-party and the recorded interactions provides the desired level of security. The network nodes check for the validity of the interactions and performs mining to construct a new valid block transaction.

2.2. Classification of blockchain

Although, the concept of blockchain was first implemented using bitcoin, its use cases have the potential to go far beyond the cryptocurrencies. The classification of blockchain is categorized into two different classes as explored in the subsections below.

2.2.1. Permission based

Based on the control of participants or how a blockchain is restricted to access new block contents and create new blocks, it can be categorized into permissionless or permissioned. Anyone is free to join the network and engage in new block creation in permissionless blockchains. Whereas, only the authorised or predefined nodes can do so in a permissioned blockchain. The major differences between these two types of blockchains are presented below.

- Permissionless blockchain: It permits any node having a valid pseudonym (account address) to join and quit the network without any authorization. Further, such nodes can use the common rules to receive, send, and validate blocks. Bitcoin network is a perfect example for this where the users are capable of performing transactions using bitcoin. Owing to its adherence to the public governance nature, permissionless blockchain is also called as permissionless blockchain. It is assumed that permissionless

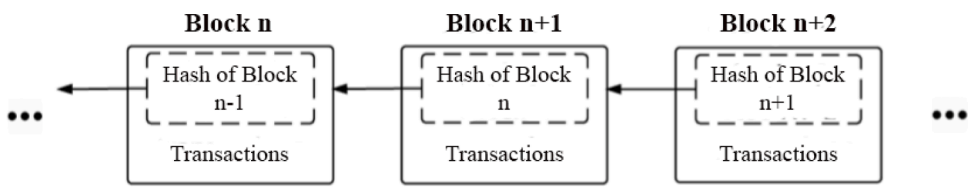

Fig. 2. Chain of blocks in a blockchain

blockchain operate under zero trust operational environment which brings forth the need for efficient consensus schemes to avoid malicious users from compromising the network [15].

- Permissioned blockchain: Prior to participation in the network operations, permissioned blockchains requires proper authorization of the participants. The consensus body and network governance cab be subsidiaries of either a consortium of entities or a single private entity. The effective network governance and identity revealing requirement in permissioned blockchains make it ideal for multiparty or internal business applications. Furthermore, owing to the limited size of its consensus body, permissioned blockchains facilitates the deployment of more effective consensus protocols that possesses higher transaction capability [16].

Table 1 presents the difference between the two categories of permission based blockchains.

2.2.2. Participation based

Blockchain can be categorized into three on the basis of the participants: public, private and consortium blockchain. Most of the projects today rely on public blockchain as it grants access to numerous users and nodes. It resembles a P2P system and is fully decentralized in approach. However, private or consortium blockchain is preferred ahead of them owing to their access control mechanisms. These three types of blockchains are discussed in the subsections below.

- Public blockchain: Bitcoin or Ethereum is the most widely accepted example of a public blockchain. The participants in a public blockchain can engage in the consensus process by reading and submitting the transactions if they are valid. Digital coins are the states in a Bitcoin and the transaction moves these coins from one address to another.
- Consortium blockchain: The most widely accepted example of a consortium blockchain is Hyperledger [9] in which a predefined set of nodes controls the consensus process. These are partly private and operates under a group leadership instead of a single leader. The right to read may be restricted to few participants or public.
- Private blockchain: Essentially, an inverse of public blockchain is a private blockchain that keeps the read permissions public and write permissions centralized to a single organization. One entity in a private blockchain rules the entire system whereas other blockchain members share the authority among them. The infrastructure in private blockchains are centralized resembling common distributed databases where the data belonging to a single owner is replicated on multiple nodes. Corporate users use private blockchains due to its management by a trusted party and the use of shared encrypted database. There is broad flexibility for management and governance within such blockchain architecture.

Table 2 presents the difference between the three categories of participant based blockchains.

2.3. Blockchain open-source implementations

Owing to the existence of numerous blockchain open source implementations, choosing the most appropriate out is a challenging task. However, the most popular of these are Hyperledger [17], Ethereum [18], and Bitcoin [19]. Table 3 compares these open source implementations on the basis of mining technique employed, smart contract, crypto token, participation model, computational level, language, confidentiality, turing complete nature, virtualization technology, advantages and disadvantages.

3. State-of-the-Art

The aforementioned sections present an overview of blockchain in terms of its architecture, classification, characteristics and open source implementations. In this section, we introduce the state-of-the-art concepts and mechanisms involved in a blockchain system (distributed ledger, cryptography, forks and consensus), which will further help the readers to gain an insight of the previously discussed concepts.

Table 1
Comparison of permissionless and permissioned blockchain

Distinguishing features	Permissionless blockchain [15]	Permissioned blockchain [16]
Participation	Facilitates free join and exit	Authorized participation
Transparency	Open	Open / Closed
Governance	Public	Consortium / Private
Consensus Techniques	PoW, PoS	BFT
Number of Readers	High	High
Number of Writers	High	Low
Number of Untrusted Writers	High	Low
Network Size	Huge (greater than thousands)	Limited (tens to hundreds)
Network Synchronization	Asynchronous / Partially synchronous	Partially / Fully synchronous
Network Connectivity	Loosely connected	Fully connected
Transaction Capacity	Low	High
Throughput	Low	High

Table 2
Comparison of public, consortium and private blockchain

Distinguishing Features	Public Blockchain	Consortium Blockchain	Private Blockchain
Infrastructure	Highly-decentralized	Decentralized	Distributed
Governance type	Consensus is public	Set of participants manage the consensus	Single owner manages the consensus
Security	Proof of Stack	Proof of Work	Pre-approved participants
Asset	Native	Native	Any
Participation in consensus process	No authentication needed	Authentication needed	
Throughput	Low	High	
Consensus Algorithm	Without permission	With permissions	
Identity	Pseudo-anonymous	Approved participants	
Data Immutability	Possible but blockchain rollback is not possible	Possible along with rollback	
Network Scalability	High	Medium to low	
Transaction Processing Speed	Slow	Fast	
Access	Public read/write	Restricted	

Table 3
Comparison of various blockchain open-source implementations

Distinguishing Features	Hyperledger [17]	Ethereum [18]	Bitcoin [19]
Mining Technique	PBFT	PoW or PoS	PoW
Smart contract	Yes	Yes	No
Crypto Token	Application level tokens	Ether native token that supports decentralized computing platform	Bitcoin native token that supports the cryptocurrency ecosystem
Participation Model	Permissioned	Permission less	Permission less
Business Logic Support	Fully programmable	Fully programmable	Very limited scripting
Computation level	Chaincode	Both high-level and low-level	Low-level (Virtual Machine)
Language	Golang, Java, node.js	Solidity and serpent	C++
Confidentiality	Guaranteed	Not guaranteed	Not guaranteed
Turing complete	Yes	Yes	No
Virtualization technology	Yes (Docker)	No	No
Advantages	Faster than other implementations as involves no specific mining technique	Scalable and requires less computations	Scalable in terms of users and number of nodes
Disadvantages	Scalability issue as does not accommodate more than 20 nodes	Requires wealth or stake for mining	Time consuming and computationally expensive

3.1. Distributed ledger

It is a data structure replicated over all network nodes and comprises of an ordered list of transactions grouped and chained together in a block. The entire update history made to the initial state of a blockchain is recorded by the ledger. User account model similar to the traditional banking systems is adopted by this cryptocurrency application. Systems may have several ledgers connected to each other in a general purpose blockchain where as in large enterprises, separate ledgers are designated for each department. Moreover, ownership of a ledger varies from being strictly controlled by single authority to being public or completely open. The target applications of different types of ledger are detailed in the subsections below.

3.1.1. Cryptocurrency and general applications

Cryptocurrency is the most widely adopted blockchain technology. Numerous competing currencies such as Dodgecoin or Litecoin [20] emerged after the enormous success of Bitcoin and adopted a similar data model. Ethereum is a cryptocurrency different from Bitcoin due to its account-based model opposed to transaction-based model of Bitcoin. Apart from asset management and cryptocurrency, several ledgers support smart contracts or user defined computations. Derivatives of Ethereum such as Monax, Parity, Quorum, Hydrachain and Dfinity allows users to write their own business logic that can executed on the top of the ledger. Ethereum have numerous applications ranging from complex investment funds to crowdfunding campaigns.

3.1.2. Digital assets

It is the real-world entities that issues digital assets and its exchange and existence are recorded by blockchain in contrast to the cryptocurrency that directly derive their values from the blockchain. Corda, Multichain and BigchainDB offer ledgers for tracking and storing the history of assets. These use transaction-based data models that are centred around assets. Private settings are the target of these systems where numerous organizations trade assets between them. IOTA [21] issues their own assets and offers a platform for

exchange of micro-payments. It adopts account-based data models and facilitates zero-fee micropayment thereby easing exchanges among IoT devices.

3.2. Cryptography

Heavy cryptographic techniques are used by the blockchain systems to guarantee ledger's integrity (ability to detect blockchain's data tampering). In public setting that has no pre-established trust, therefore in a public blockchain, a ledger must be capable of avoiding the double spending problems thereby making integrity protection a necessity. It is also needed in private blockchains as sometimes an authenticated node in a private blockchain can also behave maliciously. Integrity protection schemes are implemented at two levels in a blockchain system. In the first scheme, *Merkle Hash tree* is used to protect the global state that stores the root hash in a block. In the second scheme, the blocks are linked using a chain of *cryptographic hash pointers* (contents of $(n+1)^{th}$ block is the hash of n^{th} block) thereby making the blocks immutable after it is attached to the blockchain. This immediately invalidates all the subsequent blocks if there is any kind of modification encountered in block *n*. Blockchain offers an efficient and secured data model by combining the hash pointers and the Merkle tree as it makes it capable of tracking all the changes made to the global states. The key concepts related to cryptography is detailed in the subsections below.

3.2.1. Identity management

Public key certificate of a user uniquely identifies them within a blockchain. Initially, the user generates an elliptic curve based key pair and then derives the hash as its identity which serves as the account number or transaction address in a crypto-currency system. Users sign the transactions using private key in order to claim the transaction ownership. There exists an additional access control layer that provides certificate authority service or membership provider service. These services can be utilized by the administrator for implementing arbitrary policies to control the blockchain access. A typical enterprise system and a private blockchain have similar user key management issues which calls for the integration of existing solutions. However, public blockchains requires more usable and secure protocols owing to its momentary impact of losing private keys and sheer scale.

3.2.2. Trusted hardware

These are employed by the distributed systems in the recent past for performance improvement at the cost of security. During the manufacturing process, an Endorsement Key (EK) is burnt into every device and these key pairs are used to derive various short-term keys. Prior to the loading of the code pieces, the hardware performs hashing and signs the code to measure them. A certificate authority is required by these protocols for maintaining and endorsing revoked and known certificates. Several attestation techniques such as direct anonymous attestation does not require a certificate authority for offering hardware anonymity.

3.2.3. Transactions Privacy

Blockchain technology majorly focuses on protecting transactions without considering the privacy aspect. The first blockchain that provides transaction unlinkability is *Zerocoin* that facilitates trading between a special coin (called Zerocoin) and Bitcoin. These Zerocoins makes use of cryptographic mixer to hide linkability between corresponding Bitcoin and Zerocoins. The efficiency of the cryptographic operation of Zerocoin is improved by *Zerocash* that acts as a standalone blockchain. The transactions of Zerocash such as merge and split transactions are based on non-zero proofs and are fully private.

3.2.4. Advanced signatures

Multi-signature scheme is adopted by bitcoin in which a minimum number of signatures are mandatory in order to redeem a transaction. These schemes are resilient to adversaries by virtue of distributing the signing capabilities or decryption to a class of users. Multi-signature scheme is also adopted by Lightning Network, a wing of bitcoin that supports instant payment confirmation. Goldfeder et al. [22] proposed to extend the bitcoin's ECDSA signature for enforcing security policies that ensured secure bookkeeping, shared wallet control, personal wallet security and secure delegation of authorities. Several other advanced signature schemes can be successfully employed without significantly altering the current design. A collective signature is produced in Cosi after the end of four

Table 4
Comparison of various blockchain systems

Blockchains	Language of Smart contract	Execution Platform	Data Model	Consensus Mechanism	Applications
Litecoin	C++, Golang	Native	Transaction-based	PoW	Crypto-currency
Ethereum	Serpent, Solidity	EVM	Account-based	PoW	General applications
Monax	Solidity	EVM	Account-based	Tendermint	General applications
Parity	Serpent, Solidity	EVM	Account-based	Trusted validators	General applications
Quorum	Golang	EVM	Account-based	Raft	General applications
HydraChain	Serpent, Solidity	EVM, Python	Account-based	Trusted validators	General applications
Dfinity	Serpent, Solidity	EVM	Account-based	Threshold relay	General applications
Corda	Kotlin, Java	JVM	Transaction-based	Raft	Digital assets
Multichain	C++	Native	Transaction-based	Trusted validators	Digital assets
BigchainDB	Python	Native	Transaction-based	Trusted validators	Digital assets
Sawtooth Lake	Python	Native	Key-value	PoET	General applications

rounds of communication. The generated signature is organized as a Schnorr signature tree and must be verified by all the group members. The network message size is reduced in PBFT as it is not compulsory for the nodes to verify individual signatures from all the other nodes.

Table 4 groups and compares various blockchain systems supporting distributed ledger on the basis of their target applications.

3.3. Forks

The distributed nature of blockchain technology coupled with the need for consent of entities makes it impossible to update rules in the network. In case of unanimous consensus between nodes, the network asserts a single blockchain with verified transactions to be correct. However, in many cases the network fails to reach a unanimous consensus in terms of the future state of the blockchain. This gives rise to 'forks' where a single blockchain is split into multiple but still valid chains. The variations in the implementation and software of blockchain is known as fork. Forks in a blockchain can be divided into two types: soft forks and hard forks. The variations or changes in soft forks are backward compatible with non-updated nodes. Whereas, this is not the case in hard forks in which the non-updated nodes may reject the blocks after these changes thereby splitting the blockchain network to create multiple versions of itself. Table 5 compares the two above discussed forking schemes in terms of various parameters.

3.4. Consensus

The current and historical states that a blockchain maintains is reflected by the ledger content and any updates within the ledger must be accepted by all the involved parties. Lack of trust between the nodes (Byzantine behaviour) is the key property of blockchain and the consensus protocols must be capable of handling these byzantine failures. Blockchain systems comprise of huge number of consensus protocols ranging from communication bounded protocols such as Practical Byzantine Fault Tolerance (PBFT) to computation bounded protocols such as PoW. Amidst the two extremes, there exists numerous hybrid protocols that aims to improve the performance of PBFT and PoW. Some of the major consensus protocols are explored in the subsections below.

3.4.1. PoW

PoW is the first public consensus mechanism established in bitcoin. The miners use cryptographic hash to deduce answers to cryptographic puzzles in PoW protocols. The solution to the PoW problem is appended to the new block and broadcasted throughout the network thereby allowing all other nodes to verify the correctness of the newly published block. This process is incentive based and the overall concept is called mining. Even though, PoW effectively handles the cyber-attacks, it falls prey to 51% attack in which the adversaries takes control of 51% of the overall processing power. Further, PoW is also susceptible to *non-finality problem* which means that a block is not confirmed to a blockchain until several other blocks joins to extend them.

3.4.2. Proof of Stake (PoS)

The best-known alternative of PoW mechanism is PoS, in which the validators for new block creation is randomly determined and the probability of a node to validate the next new block is determined on the basis of the assets / stakes it owns. PoW involves hugely expensive mining techniques as it is energy intensive and consumes more electric power. Therefore, PoS is proposed to avoid the high computational puzzle solving and consequently mitigate the mining cost.

3.4.3. Delegated Proof of Stake (DPoS)

DPoS is a variant of PoS in which only a predefined number of delegates possess the block generation and validation capability. Also, the representatives have the ability to change the network specifications such as block intervals and block size. Therefore, it can be inferred that DPoS is delegated democratic whereas PoS is directly democratic. Furthermore, DPoS takes less time for block validation and transaction approval as it considers lesser entities to authenticate the block. This consensus protocol is adopted by bitshares blockchain.

Table 5
Difference between soft fork and hard fork

Features	Soft Fork	Hard Fork
Backward compatibility	Yes	No
Hashpower requirement	Demands 51% of mining power	Hashpower has no meaning
Network splits	Do not lead to networks splits and nodes continue to transact safely	Nodes that fail to fork are split
Parallelism of chains	Parallel chain does not exist	Both older and new blockchains operate parallelly and follow their respective protocol sets.
Divergence	Temporary divergence because of the non-updated nodes that does not follow the new consensus rules.	Permanent divergence as the non-updated nodes is unable to validate the blocks mined by updated ones.
Implementation type	New features such as segregated witness and check sequence verification is deployed	New protocols giving rise to compatibility is deployed.
Fund retrieval	Retrieving funds from the attacker's child DAO is not possible	Funds can be retrieved without the attacker's consent

3.4.4. PBFT

PBFT is a duplication algorithm that can endure Byzantine Generals Problem (BGP) in an asynchronous environment. It works under the assumption that, out of all the network nodes, at least one-third is honest. PBFT enables the node to sustain a common stake and consequently guarantees consistent action in every consensus round. It is implemented in Hyperledger version 0.6 and ensures that if the block is appended once, it cannot be modified or replaced. In contrast to the probabilistic nature of PoW, PBFT is deterministic in nature. In spite of several improvements over the original protocols, PBFT-based communication bounded protocols face the problem of scalability. For overcoming this limitation, Ripple choose to partition networks into small federates or groups and each group run a local consensus protocol. It makes use of fully trusted collaborative subnetworks within a bigger network. Owing to its small network size, these protocols are not susceptible to scalability issues.

3.4.5. Proof of Burn (PoB)

In PoB, the validators create a block and get rewarded after they burn their own assets/coins by delivering to un-spendable, public and verifiable addresses. It is an alternative for both PoS and PoW consensus mechanism. Spending coins can be considered as an investment in PoB as after doing so, the user can claim their stakes in the chain and establish themselves as a n authorized validator. Furthermore, there is no energy consumption requirement in PoB as seen in PoS and PoW. The Slimcoin is based on PoB where the nodes destroy their own base currencies in order to be able to propose a new block.

3.4.6. Proof of Authority (PoA)

PoA is a consensus protocol especially designed for permissioned blockchain that requires the participants to confirm their identity before receiving the block publishing authority. PoA is different from PoS as it considers participants as stake instead of having some assets or coins. It works under the assumption that the authorities are trusted and pre-selected to publish a block. Parity uses PoA that considers several pre-defined nodes as trusted authorities capable of proposing new blocks. Further, it relies on round-robin scheduling mechanism to assign a time window in which every authority node can propose blocks.

Table 6 presents the comparison of various consensus protocols for blockchain systems.

4. Blockchain security threats

Huge range of attacks emerged with the advancement of blockchain technology. These attacks or risks might arise due to internal participants or external entities. The growing blockchain popularity brings forth new privacy and security protection demands on data transmission and storage. The current blockchain security threats can be broadly classified into four: double spending threats, network threats, mining pool threats and wallet security threats. These categories are explored in the section below along with their attack vectors, causes and the proposed countermeasures.

4.1. Double-spending threats

This type of attack takes place if a consumer uses a single cryptocurrency for multiple transactions. Various ways of launching the double spending attacks are detailed in the subsections below.

4.1.1. Race attack

This attack is launched when an adversary rapidly sends two or more conflicting transactions into the bitcoin network. In PoW-based blockchains, this attack can be implemented easily. Adversaries sends a transaction directly paying the merchant who accepts the payment and ships the product without waiting for confirmation. Meanwhile, the adversary sends another conflicting transaction which the bitcoin nodes accepts genuinely and considers the coins sent to the merchant as invalid. Adversary exploits the timeframe between the initiation and confirmation of two transactions thereby quickly launching the double spending attack. *Proposed Countermeasures:* A peer upon receiving a new transaction, checks about the prior use of the transaction coins in the blockchain and its

Table 6
Comparison of consensus protocols

Consensus Protocols	Nature	Adversary Tolerance	Type of Consensus	Transactional finality	Description
PoW	Public	< 25 % Computing power	Competitive	Probabilistic	Pure PoW is used by Bitcoins however, it leads to scalability issues.
PoS	Public	< 51 % Assets/ stakes	Competitive	Probabilistic	Probability of a node to validate the next new block is determined on the basis of the assets / stakes it owns.
DPoS	Public	< 51 % Validators	Collaborative	Probabilistic	Only a predefined number of delegates possess the block generation and validation capability.
PBFT	Private	< 33 % Faulty replicas	-	Immediate	Original PBFT is used by the Hyperledger.
PoB	Public	< 25 % Computing power	Collaborative	Economic	It is an alternative for both PoS and PoW consensus mechanism where spending coins is considered as an investment.
PoA	Public	-	Collaborative	Immediate	Works under the assumption that the authorities are trusted and pre-selected to publish a block.

memory pool. Peers add these coins in their memory pool and forward them to the entire network only if it is not found in prior transactions. The scheme basically focusses on detecting the double spending attack instead of preventing them.

4.1.2. 51 % Attack

For maintaining the mutual trust in a blockchain network, it relies on distributed consensus mechanism which itself is vulnerable to 51% attack. Such attack can be launched whenever a user or group of miners gain control of more than half the hash power in PoW. Adversary in such situation gains enough power to destroy the network and launch attacks such as self-reverse transactions, modify, exclude and double spending. Such attack is considered as the most threatening scenario as attackers can perform any kind of extreme network operations. *Proposed Countermeasures:* As the security model of a bitcoin relies on more than half of the total hash rate within the network, preventing a mining pool or even a single miner from achieving the half of the total hash rate within the network prevents this attack.

4.1.3. Finney attack

In such attacks, the adversaries' pre-mine a transaction into blocks, invalidates them and releases them to the public network at the expense of the same coins. This is a fraudulent double spend scheme that requires the miner's participation after the block is mined. *Proposed Countermeasures:* As one-confirmation vendor can cause Finney attack; in order to avoid this, vendors must release the product only after several confirmations. However, this cannot prevent double spending attack, but it reduces the risk involved thereby making the adversary to spend a greater number of coins.

4.1.4. Vector 76 attack

It is a type of confirmation attack where the adversaries utilize privately mined blocks for performing double spending attack. This is an integration of the finney attack and the race attack such that for reversing a transaction, only one confirmation is needed. These can be launched when a cryptocurrency wallet exchange service accepts direct incoming connections. *Proposed Countermeasures:* This can be prevented by waiting for multi-confirmation, inserting network observers and notifying the merchant regarding the existence of double attack problem.

4.2. Network threats

The peer to peer nature of the blockchain network requires all nodes to use the blockchain protocols to provide network services. Considering the bitcoin network, there are two types of nodes namely the *users* and the *miners*. The former node type creates transactions and submits them into the bitcoin network whereas the latter generates blocks and accepts incoming TCP connection in a blockchain. Various types of network threats are detailed in the subsections below.

4.2.1. Transaction malleability attack

It is the inherent flaw of the bitcoin protocol. In a typical transaction malleability attack, adversaries trick its target to believe that a particular transaction has failed and then again asks to repeat the same transaction by changing the transaction hash ID before its confirmation on the bitcoin network. Such attack is considered as an alternative double spending attack in which the adversaries are not the transaction issuing authority. *Proposed Countermeasures:* A Bitcoin Improvement Proposal 62 (BIP 62) is an effective countermeasure proposed to counter the malleability issue as it involves multiple transaction verification metrics for validation of a new transaction.

4.2.2. Sybil attack

This attack focusses weakening the reputation system by introducing forged identities in a P2P network. Adversaries in a sybil attack subverts the reputation system by creation of numerous pseudonymous identities and then utilizing them to gain huge influence. As sybil attack is possible to launch in almost every condition except under unrealistic and extreme resource assumption among entities, PoW cannot prevent such attacks. *Proposed Countermeasures:* A two-party decentralized mixing protocol that addresses timing-based inference attacks, DoS attacks and the sybil attack simultaneously.

4.2.3. Eclipse attack

In such type of attack, an attacker is capable of controlling a huge number of IP addresses and monopolizing all the connections towards a single victim node. Utilizing this, the attacker can force network partition between a specific miner and the public network. If the attacker succeeds in this, it can launch a huge range of attacks including selfish mining, adversarial forks, N-confirmation and Zero-confirmation double spending attacks.

4.3. Mining pool threats

Group of miners work collaboratively to create mining pools to pool their resources for contributing to the block generation and sharing the block based on the added processing power. Various attack vectors exploit the pool vulnerabilities to launch both external and internal attacks on a mining pool. The various types of mining pool threats are detailed in the subsections below.

4.3.1. Selfish mining attack

Eyal et al. [23] first introduced the selfish mining attack where a dishonest miner selectively releases blocks instead of acting like a regular miner and immediately publishes them to the network. Such attack is launched with a primary motive to obtain unfair reward and confuse the honest miners leading them to waste resources in an incorrect direction. Selfish miners upon discovering a new block keeps it private and if there arise any competition with the honest miners, these selfish miners win the race by publishing their private branch. *Proposed Countermeasures:* Freshness Preferred (FP) scheme to prevent selfish mining attack uses unforgeable timestamps within the block header to identify the recently mined blocks. This approach decreases the selfish mining motives as the withheld blocks lose the race against the freshly mined blocks. Therefore, if dishonest miner releases private block chain list, the remaining honest miners weighs their validity against the hashed timestamp and the reported network timestamp.

4.3.2. Block Withholding Attack (BW)

In this type of mining pool attack, the blocks are discarded thereby preventing the dishonest miners from publishing a mined block for sabotaging the pool revenue. Typically, a mining pool comprise of two types of users namely the regular miners and pool managers. The task of the pool manager is to forward the unsolved tasks to the regular miners who generates the PoW and submit it to the pool manager who broadcasts this newly generated block to the entire network. In this kind of attack, the pool manager uses some of its miners and infiltrates a victim pool by registering itself as a regular miner of that pool. The adversary sends the partial PoW received from the infiltrating miners to the victim pool and discards the full PoW received from the same infiltrating miners thereby not contributing to the victim's revenue. However, the mining power of the attacker is reduced in this scenario but he enjoys additional revenue by other pool infiltrations.

4.3.3. Fork-After Withholding attack (FAW)

Kwon et al. [24] presented another variation of BW attack where the reward of the adversary is always greater than or equal to the BW attacker owing to its more practical nature. FAW integrates the components of both BW attack and the selfish mining attack as the adversary divides his computing power between infiltration mining and innocent mining.

4.4. Wallet security threats

Private key based authentication schemes are used by blockchain based currencies even though the password authentication is the most commonly used user authentication schemes. In order to make transactions or to access coins in a blockchain, users need to possess private as well as the public keys. Wallets in general can be of two types namely *cold / offline* (disconnected from internet) and *hot / online* (connected to internet). Various types of wallet security threats include *vulnerable signature, flawed key generation, lack of address control creation and pre-image attack*.

5. Blockchain based Security

Whenever an adversary intends to double spend a cryptographical coin or plunder a cryptocurrency, the attacker must generate the block using a long term blockchain ledger. Legitimate network nodes do not accept the blocks from the adversary if they are not capable of mining or generating blocks at a faster rate than other nodes. Attacker is capable of merging the newly generated block into a long-term blockchain if it achieves more than half of the overall computing power. However, technically it is not that easy for the adversary to do so. Blockchain integrates four key technologies namely P2P network, smart contract, asymmetric encryption and distributed ledger. These technologies power blockchain to emerge as a new information processing generation which is intelligent, efficient, fair, open, reliable and secure. These technologies are explored in the subsections below.

5.1. P2P Network

In a distributed P2P application, peers cooperate and self-organize to complete tasks such as uploading data, delivering messages, and forwarding files. Blockchain adopts a fault-tolerant, load balanced and decentralized P2P network architecture instead of a employing the traditional client-server model. Based on the network architecture and design, these P2P networks are categorized into *Unstructured, Hybrid* and *Structured*. Several works showed that real networks resemble a small-world model having small average feature path length and large aggregation coefficient. The blockchain network is also operated and designed as per the small-world model where the network nodes can be divided into series of recording and non-recording nodes on the basis of their recording capability. The network stability is dynamically ensured by the small-world model under various changing node conditions. It also enhances the overall robustness of the blockchain network and preserves transaction data consistency and integrity. Moreover, miners and users in a blockchain P2P system may collude with each other or exhibit selfish actions. He et al. [25] proposed to integrate a secure pricing strategy and validation method into the incentive mechanism. The proposed architecture focuses on providing satisfying rewards to the users as a compensation for their consumed resource. Such incentive mechanism is introduced to meet the diverse user requirements in distributed and dynamic P2P environments.

5.2. Smart contract

Smart contract is basically a type of agreement among various parties that can be executed with the help of a computer code. The

code ensures trust less execution as it executes without giving any opportunity to the parties to back out. One of the most important characteristics of blockchain systems is smart contracts as it is capable of implementing trusted transactions without the need of any third-party involvement. Smart contracts contributed to the growth of the blockchain technology beyond the scope of cryptocurrencies and made it applicable for huge range of applications such as supply chain, IoT, healthcare, and business process management. Taking the security perspective into account, smart contracts possesses similar characteristics to the blockchain data. Smart contract specifies the trigger conditions for contract execution, participant obligations, participant rights and the corresponding results. After addition with the smart contract, the blockchain begins to execute accurately and objectively without any impact. Smart contracts security depends on the contract code and the blockchain security is seriously impacted if there occurs any issue in the contract code's implementation logic. The template of the smart contracts has been tested and professionally reviewed for the purpose of verification.

5.3. Asymmetric encryption

It is the basic technique to enforce blockchain security that makes use of two different keys: private and public key. The two major contribution of asymmetric encryption for blockchain is digital signatures and data encryption. Apart from verification and transaction signature, asymmetric cryptography can also be useful for encryption of the recorded blockchain data. The token is held by the public key and is visible to everyone whereas the private key can be used to authorize actions. Aitzhan et al. [26] proposed an effective tool called multi-signature technology. It is important for the data recorded within a block to be verified by network nodes in the blockchain. Blind signature technology is employed to achieve the security goals and prevent the information disclosure. Digital signatures can be used to sign transactions in a safer manner and is also used by many cryptocurrencies. These can be used in multi-signature wallet and contracts as it requires digital signatures from different private keys before initiating any execution action.

5.4. Distributed ledger

Basic operations permitted by the traditional database are querying, changing, adding and deleting data. In contrast, the blockchain permits only two operations namely querying and adding. Traditional databases can be categorized into two: *distributed* and *centralized*. Data is distributed in the original database by the distributed database model to enhance the concurrent access and storage capacity. The blockchain is a type of distributed ledger employing varied data structures and storage methods. These power the blockchain technology to achieve data provenance and ensure security as well as data authenticity. Fischer et al. [27] proposed that a deterministic consensus protocol cannot guarantee all the three properties (*Consistency, Fault-tolerance* and *Liveness*) in a distributed system. The distributed systems choose fault tolerance in all cases owing to its criticality and choose any one among the liveness and safety depending on the assumptions and the system requirements. Existing protocols assumed the replication environment to be free from adversaries. However, distributed ledger technology helps the network to achieve consensus without the need of any third-party even in a byzantine environment.

6. Blockchain challenges and future directions

Apart from huge range of benefits that the blockchain technology provides, there exists few challenges that restricts its practicality for numerous security applications discussed in aforementioned sections. Some of these challenges are detailed in the subsections below.

6.1. Privacy and anonymity

The major advantage and property of using blockchain technology is that it provides pseudo-user anonymity which is very much needed as the public blockchains are susceptible to attacks owing to its open nature. A permissioned blockchain enables secure interaction among entities that works for a common purpose but do not trust each other. There are several limitations in permissioned blockchains such as its inability to handle huge volume of transactions, need for the smart contract to be written in domain-specific language, incompetence to support non-deterministic transactions and limited performance due to sequential execution of transactions. The majority of existing schemes can only provide some level of anonymity therefore further investigation is required for developing a fully anonymized approach that fulfils the requirement of various security applications.

6.2. Computation and mining nodes

The employed security services and the mining process associated with the blockchain technology requires huge computations in signature generation, encryption and decryption process. To this end, several research works are devoted to resource allocation strategy in the block mining process. Also, in order to reduce the computational needs for encrypting and signing the data, development of a simple cryptographic scheme needs to be investigated further.

6.3. Compatibility

For varied application requirements and scenarios, there exist numerous transaction structures such as the Ethereum's ACCOUNT architecture and Bitcoin's UTXO (Unspent Transaction Output) architecture. The Bitcoin's UTXO is an integral cryptocurrency

component linked by a digital signature chain. The working of Ethereum ACCOUNT architecture is similar to the traditional banking world where a global state maintains the account and transactions effect the state of these accounts independently. Wang et al. [28] proposed Ethereum based identity management framework supported by simple credit management scheme to solve the issue of third-party dependencies. However, none of the proposed schemes to the best of our knowledge consider an effective privacy preserving mechanism under this transaction structure. Ethereum is the most accepted platform for decentralized applications owing to its programmable system. But, compatibility of the privacy preserving schemes with the ACCOUNT architecture is a challenge and needs further investigation.

6.4. Communication overhead and storage

Owing to the highly dynamic nature of the current applications, there is need of change in provenance data and access lists frequently. Therefore, the node is forced to broadcast frequent transactions in order to modify the provenance information or update the ACL. In contrast, the blockchain technology incurs significant overhead in terms of system processing capabilities and network traffic as it is a peer-to-peer network. These processing and storage overhead bring forth additional challenges in adoption of blockchain for various security applications. This issue deteriorates even further when blockchains are deployed in supply chain or any other similar data intensive application. Several proposed solutions rely on offloading the transaction activity of the main blockchain by the use of payment channel networks. However, this obscures the data transparency and compromises privacy. This brings forth the need to come up with more effective solutions in this regard.

6.5. Querying over data stored in blocks

Existing blockchain based applications focus on reducing fraud, increasing tamper resistance, lowering operational costs and enforcing contracts. However, blockchain supports limited query ability and can be labelled as unforgeable and distributed database that focus on data storage [29,30]. Blockchain ensures data integrity with the help of consensus protocols and hash chain technique. These cryptographically guaranteed security schemes powered by provenance and decentralization properties of blockchain underlines its potential to revolutionize traditional database systems. With the exponential increase in adoption of blockchain technology for data intensive applications such as intellectual property rights management, supply chains and finance, there is a rise in user requests to query the stored data. In order to execute such queries, the system ask all the peer nodes to traverse all records and generate the final query result. This random record retrieval process makes the query processing extremely time consuming. Even though, blockchain brings forth numerous security benefits, efficient record searching and tracing data transactions in the current blockchain systems is yet to be solved.

7. Conclusions

Owing to its security features and decentralized nature, blockchain has gained much significance in the field of information systems recently. For future interactive systems including supply chain systems and IoT, it promises to play a crucial role as it brings forth a completely new way of updating, sharing and storing data. However, emerging blockchain applications may be hindered due to rapidly increasing privacy protection needs. In this context, we presented a comprehensive survey on blockchain technologies and its utilization in providing distributed security services such as integrity, provenance, privacy, confidentiality and entity authentication assurances. We laid out four concepts (distributed ledger, cryptography, fork and consensus) behind blockchains to analyse its state-of-the-art. We classified the current blockchain security threats and explored the blockchain security standards that are capable of mitigating these attacks. At the end, we outline the challenges that hinders the practicality of blockchain for various security applications. Testing the applicability of various blockchain approaches in real-time large-scale environment and resolving the outlined challenges can serve as future research directions. We hope that our survey would be beneficial towards the implementation and design of future blockchain systems that is usable for the real-world and scalable for large scale applications.

Declaration of Competing Interest

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

References

[1] Yuan Y, Wang F. Blockchain and cryptocurrencies: model, techniques, and applications. IEEE Trans Syst, Man, Cybern: Syst 2018;48(9):1421–8. https://doi.org/10.1109/tsmc.2018.2854904.
[2] Ali MS, Vecchio M, Pincheira M, Dolui K, Antonelli F, Rehmani MH. Applications of blockchains in the internet of things: a comprehensive survey. IEEE Commun Surv Tutor 2019;21(2):1676–717. https://doi.org/10.1109/comst.2018.2886932.
[3] Bhushan B, Khamparia A, Sagayam KM, Sharma SK, Ahad MA, Debnath NC. Blockchain for smart cities: A review of architectures, integration trends and future research directions. Sustain Cities Soc 2020;61:102360. https://doi.org/10.1016/j.scs.2020.102360.
[4] Muzammal M, Qu Q, Nasrulin B. Renovating blockchain with distributed databases: an open source system. Futur Gener Comput Systs 2019;90:105–17. https://doi.org/10.1016/j.future.2018.07.042.
[5] Huang K, Zhang X, Mu Y, Wang X, Yang G, Du X, Guizani M. Building redactable consortium blockchain for industrial internet-of-things. IEEE Trans Ind Inf 2019;15(6):3670–9. https://doi.org/10.1109/tii.2019.2901011.

[6] Morkunas VJ, Paschen J, Boon E. How blockchain technologies impact your business model. Bus Horiz 2019;62(3):295–306. https://doi.org/10.1016/j.bushor.2019.01.009.
[7] Ikeda K, Hamid M. Applications of blockchain in the financial sector and a peer-to-peer global barter web. Adv Comput Blockchain Technol: Platf, Tools Use Cases 2018:99–120. https://doi.org/10.1016/bs.adcom.2018.03.008.
[8] Fu Y, Zhu J. Big production enterprise supply chain endogenous risk management based on blockchain. IEEE Access 2019;7:15310–9. https://doi.org/10.1109/access.2019.2895327.
[9] Xiao Y, Zhang N, Lou W, Hou YT. A survey of distributed consensus protocols for blockchain networks. IEEE Commun Surv Tutor 2020. https://doi.org/10.1109/comst.2020.2969706. 1–1.
[10] Bhushan B, Sahoo C, Sinha P, Khamparia A. Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions. Wirel Netw 2020. https://doi.org/10.1007/s11276-020-02445-6.
[11] Fernandez-Carames TM, Fraga-Lamas P. Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. IEEE Access 2020;8:21091–116. https://doi.org/10.1109/access.2020.2968985.
[12] Sengupta J, Ruj S, Bit SD. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J Netw Comput Appl 2020;149:102481. https://doi.org/10.1016/j.jnca.2019.102481.
[13] L. Pacioli, Summa de Arithmetica geometria proportioni: et proportionalita... Paganino de Paganini, 1994.
[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[15] Neudecker T, Hartenstein H. Network layer aspects of permissionless blockchains. IEEE Commun Surv Tutor 2019;21(1):838–57. https://doi.org/10.1109/comst.2018.2852480.
[16] Qiu C, Yao H, Yu R, Jiang C, Guo S. A service-oriented permissioned blockchain for the internet of things. IEEE Trans Serv Comput 2019. https://doi.org/10.1109/tsc.2019.2948870. 1–1.
[17] Hyperledger GitHub implementation, https://github.com/hyperledger/fabric-sdk-py, (accessed June 13, 2020).
[18] Ethereum GitHub implementation, https://github.com/ethereum/goethereum, (accessed June 13, 2019).
[19] Bitcoin GitHub implementation, https://github.com/bitcoin/bitcoin, (accessed June 13, 2019).
[20] "Global decentralized currency," https://litecoin.org/.
[21] "Openchain: Next generation blockchain," https://iota.org/.
[22] Goldfeder, S., Felten, E.W., Kroll, J.A., & Narayanan, A.R. (2014). Securing Bitcoin wallets via threshold signatures.
[23] Eyal I, Sirer EG. Majority is not enough. Commun ACM 2018;61(7):95–102. https://doi.org/10.1145/3212998.
[24] Kwon Y, Kim D, Son Y, Vasserman E, Kim Y. Be selfish and avoid dilemmas. Proceed 2017 ACM SIGSAC Conf Comput Commun Secur - CCS 2017;17. https://doi.org/10.1145/3133956.3134019.
[25] He Y, Li H, Cheng X, Liu Y, Yang C, Sun L. A blockchain based truthful incentive mechanism for distributed P2P applications. IEEE Access 2018;6:27324–35. https://doi.org/10.1109/access.2018.2821705.
[26] Aitzhan NZ, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans Dependable Secure Comput 2018;15(5):840–52. https://doi.org/10.1109/tdsc.2016.2616861.
[27] Fischer MJ, Lynch NA, Paterson MS. Impossibility of distributed consensus with one faulty process. J ACM 1985;32(2):374–82. https://doi.org/10.1145/3149.214121.
[28] Wang S, Pei R, Zhang Y. EIDM: A ethereum-based cloud user identity management protocol. IEEE Access 2019;7:115281–91. https://doi.org/10.1109/access.2019.2933989.
[29] Wang H, Ma S, Dai H, Imran M, Wang T. Blockchain-based data privacy management with Nudge theory in open banking. Futur Gener Comput Syst 2020;110:812–23. https://doi.org/10.1016/j.future.2019.09.010.
[30] Liu D, Ni J, Huang C, Lin X, Shen XS. Secure and efficient distributed network provenance for iot: a blockchain-based approach. IEEE Internet Things J 2020;7(8):7564–74. https://doi.org/10.1109/jiot.2020.2988481.

Bharat Bhushan is currently working as an assistant professor in the Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, India. He received his B.Tech. in Computer Science and Engineering in 2012, M.Tech in Information Security in 2015, and is currently working towards the Ph.D. degree at Birla Institute of Technology, Mesra, India.

Preeti Sinha is currently working as system engineer in Tata Consultancy Services, India. She received the B.Tech. degree in computer science and engineering in 2016, and M.Tech degree in Information Security from Birla Institute of Technology, Mesra, India in 2018. From 2017 through 2018, she worked as a software engineer at NVIDIA, Hyderabad, India.

K. Martin Sagayam is working as Assistant Professor in the Department of ECE, Karunya Institute Technology and Sciences, India. He received his Ph.D in the research field of Signal, Image processing and machine learning approaches in 2018, Master degree in Communication Systems in the year 2012 and B.E degree in Electronics and Communication Engineering in the year 2009.

Andrew J is currently serving as a faculty member in the Department of Computer Science and Engineering at Karunya Institute of Technology and Sciences, India. He is currently pursuing his Ph.D. degree from VIT University, Vellore. He has received his bachelor of engineering degree and master of engineering degree from Anna University in the year 2011 and 2013.