IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 15, 2021, accepted November 18, 2021, date of publication November 19, 2021,
date of current version November 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3129697

A Survey of IoT and Blockchain Integration: Security Perspective

ELHAM A. SHAMMAR[1], AMMAR T. ZAHARY[1,3], (Member, IEEE), AND ASMA A. AL-SHARGABI[2,3], (Member, IEEE)

[1]Department of Information Technology, Faculty of Computer and Information Technology (FCIT), Sana'a University, Sana'a, Yemen
[2]Department of Information Technology, Collage of Computer, Qassim University, Buraydah 51452, Saudi Arabia
[3]Department of Computer Science, Faculty of Computing and IT, University of Science and Technology, Sana'a, Yemen

Corresponding author: Elham A. Shammar (el.shammar@su.edu.ye)

ABSTRACT Blockchain has recently attracted significant academic attention in research fields beyond the financial industry. In the Internet of Things (IoT), blockchain can be used to create a decentralized, reliable, and secure environment. The use of blockchain in IoT applications is still in its early stages, particularly at the low end of the computing spectrum. As a result, the future roadmap is hazy, and several challenges and questions must be addressed. Several articles combining blockchain technology with IoT have recently been released, but they are limited to shallow technological potential discussions, with very few providing an in-depth examination of the complexities of implementing blockchain technology for IoT. Therefore, this paper aims to coherently and comprehensively provide current cutting-edge efforts in this direction. It provides a literature review of IoT and blockchain integration by examining current research issues and trends in the applications of blockchain-related approaches and technologies within the IoT security context. We have surveyed published articles from 2017 to 2021 on blockchain-based solutions for IoT security, taking into consideration different security areas and then, we have organized the available articles according to these areas. The surveyed articles have been chronologically organized in tables for better clarity. In this paper, we try to investigate the vital issues and challenges to the integration of IoT and blockchain, and then investigate the research efforts that have been conducted so far to overcome these challenges.

INDEX TERMS Blockchain, IoT, security.

I. INTRODUCTION

Since its inception in 1999, when Kevin Ashton coined the term of IoT, IoT has evolved from a simple concept to one of the most powerful business development drivers. Integrated with cloud computing, big data, and machine learning, IoT has become the establishment stone upon which data-driven digital services are built. These days, IoT devices range from wearable devices to hardware development platforms. In 2018, the number of Internet-connected devices used worldwide were approximately 7 billion [1]–[3]. In 2019, the number of IoT connected devices reached 5 billion, and this number will continue to grow to reach 29 billion in 2022 [4]. The National Intelligence Council and McKinsey Global Institute have announced that everyday objects such as furniture, food packages, paper documents, etc., will represent nodes of the Internet by 2025. They shed the light on the future that will be created by integrating technologies that interact with the human environment [5]. In 2025, the number is expected to rise to 35 billion [6]. Others predict that by 2025, the number of IoT devices may reach 50 billion [7]. This remarkable development is a driving force behind the convergence of the physical and digital worlds that promises to create an unprecedented IoT market of 19 trillion USD over the next decade, with a large proportion of these devices expected to be smartphones [6].

The IoT is widely adopted in many areas of society, including healthcare, agriculture, smart cities, and military. There have also been some cases where information from IoT devices has been used as proof in criminal cases [8]. For instance, Fitbit data (steps walked) were utilized to contradict claims made by the suspect about the victim's movement before the crime [9]. These examples highlight that the data and records of interactions between IoT devices can be used for audit purposes [10].

Things (devices) communicate and exchange data in the IoT without the need for human intervention. Because of the independence and ubiquity of the IoT ecosystem, devices are

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

more vulnerable to attacks. Moreover, as a result of such rich communication, the IoT will reach a tipping point in which the majority of generated data on the Internet will come from billions of devices that are too resource-constrained to efficiently enforce complex security and data privacy policies. Therefore, the solution involves incorporating distributed ledger technologies, such as blockchain, into IoT devices and the use of smart contracts to perform operations based on predefined rules [1]–[3], [11].

Blockchains have attracted significant attention in recent years because of their unique characteristics, such as decentralization, immutability, anonymity, security, and auditability. Owing to these outstanding features, blockchain has been implemented in many non-monetary applications, including the IoT [12]. In IoT, blockchain provides an immutable audit trail of sensor observations by storing sensor data as blockchain transactions. The interactions between IoT devices and other network entities are also stored in the immutable records of blockchain transactions. These transactions are collected into blocks linked together by cryptographic hash functions of each previous block in the chain, which makes it nearly impossible to change formerly stored blocks without being detected. The blockchain can also validate IoT transactions and blocks before adding them to the blockchain using public-key cryptography. Once the block is mined in the blockchain, we are sure that the interactions between the nodes are tamper-proof and securely recorded in the blockchain. Storing data hashes on the blockchain ensures that the integrity of the stored data can be verified by comparing its hash with the hash value stored in the blockchain [13].

This study aims to coherently and comprehensively discuss the current cutting-edge efforts in IoT and blockchain integration. This paper introduces the current advances in research to effectively resolve the challenges and issues of centralized IoT ecosystems using blockchain technology to ensure a decentralized, secure IoT environment. This paper examines recent scientific studies in blockchain-based IoT from a security perspective and clarifies the critical areas of research related to the integration of blockchain and IoT. The roadmap of this paper is as follows: In Section II, the article begins by introducing a view of blockchain technology. It starts with the core concepts of blockchain and how blockchain-based frameworks accomplish decentralization, transparency, and auditable characteristics. Consensus for blockchain-based IoT and blockchain scalability in IoT are discussed in Sections III and IV, respectively. In Section V, the article briefly introduces the IoT and elaborates on the security issues of IoT. In Section VI, the article explains IoT security using blockchain thoroughly by introducing attacks on IoT and the defense mechanisms using blockchain such as intrusion detection systems, firmware updates, and using blockchain to ensure confidentiality, authentication, access control, trust, and reputation in IoT. In Section VII, a discussion of the challenges and trends of integrating blockchain and IoT is presented. We conclude the paper in section VIII.

II. BLOCKCHAIN OVERVIEW

A person, or a group of people, under the name of Satoshi Nakamoto, published a landmark paper [14] on Bitcoin in 2008, which deals with a new decentralized peer-to-peer (P2P) electronic cash system [13]. This paper introduced the concept of blockchain as a new data structure for storing financial transactions, as well as the associated protocol for ensuring the blockchain's validity in the network [1], [11], [15]. People often confuse blockchain with Bitcoin. However, Bitcoin is a cryptocurrency that uses blockchain technology to allow it to trade freely and globally without the oversight of a central guarantor (banks). In other words, Bitcoin is nothing more than a financial application that makes use of blockchain technology [4].

A blockchain is defined as an immutable, permanent, auditable, timestamp, and tamper-resistant ledger of blocks that are used to store and share data in a P2P manner. The data stored in the blockchain can be a payment history, contract, or even personal information [1], [11], [15]. Blockchain technology was initially introduced to solve the problem of double spending in cryptocurrencies [16]. Intriguingly, because of its unique and appealing features such as security, transactional privacy, integrity, authorization, censorship resistance, data immutability, auditability, system transparency, and fault tolerance, blockchain is used in sectors other than cryptocurrencies. Identity management, mobile crowd sensing, Industry 4.0, intelligent transportation, supply chain management, agriculture, smart grids, healthcare, and mission-critical system security are just a few examples [17]. Blockchain technology has received significant attention in terms of security, auditability, and anonymity [1], [18]. According to PwC [10], blockchain is currently one of the most popular research topics in recent years, with startups investing more than 1.4 billion dollars in the first nine months of 2016.

In blockchain, a public ledger stores the digitally signed transactions of users in a P2P network. Asymmetric encryption is used to decrypt the messages. Generally, the user has two keys: a public key for encrypting the messages for other users and a private key for decrypting the messages. From a blockchain perspective, the private key is used to sign the blockchain transaction, whereas the public key represents a unique address. Initially, the user signs a transaction with his/her private key and broadcasts it to his/her peers. When peers receive a signed transaction, they validate and publish it across the network [17]. To ensure high transaction auditability, each node in the network stores a copy of the ledger. Any newly added transactions are verified and confirmed by other network nodes, eliminating the need for a central authority to prevent a single point of failure. All copies are simultaneously updated and validated [1], [11], [15]. The integrity of the blockchain is based on strong cryptography, which validates and chains together blocks of transactions, making it nearly impossible to tamper with any individual transaction without being detected [19]. The primary objective of blockchain is to free people from any form of trust that we are now forced

to place in intermediaries who regulate and manage a large portion of citizens' lives [4].

Special nodes in a blockchain network, called miners, add newly generated transactions to a pool of pending transactions. When the size of the collected pending transactions reaches a predetermined size known as the block size, each miner gathers the pending transactions in a block. To maintain a single history of the blocks and ensure that all entities have the same copy of the ledger so that they do not include any invalid, inconsistent, or contradictory transactions, a consensus among the participants is required to maintain the blockchain architecture and ensure its operation. Consensus provides agreement on the current state of the ledger among untrusted network participants [13]. Once a distributed consensus is reached, a valid transaction is included in a timestamped block by the miner. The block, which is included by the miner, is broadcast back onto the network. The broadcast block is appended to the blockchain after it has been validated and hash-matched with the previous block in the blockchain [17]. The method by which consensus is reached has a significant impact on the security and performance of blockchain networks [13].

According to the required permission attributes and data management, the entity has three options for interacting with the blockchain: *public, private, or consortium*. In *a permissionless blockchain (public)*, all participants contribute to reading, verifying, submitting, and obtaining transaction consensus without any central entity to manage membership or ban illegal readers or writers. Contrary to the permissionless blockchain, the *permissioned blockchain (private)* restricts consensus contributors. Only the selected trustful actors have the right to validate transactions. A central authority must identify, authenticate, and register network devices in a permissioned blockchain. This will prevent the nodes from joining the blockchain network and directly writing to the ledger, as it is possible in a permissionless blockchain. In *a consortium blockchain*, only a pre-selected set of peers is engaged in the consensus process. It can be considered as a partially decentralized network in which the read permission can be opened or restricted to specific peers, whereas the validity of the blocks is affirmed by a small group of previously chosen peers [1], [16].

A blockchain is built up of sequential blocks that can store various types of transactions. The Genesis Block is the name given to the first mined block in the blockchain. Each block in the blockchain consists of two parts, as listed in Table. 1. The first part is called the header and contains information about the block. The block header includes: 1) the block version; 2) the previous block hash; 3) Merkle tree root, shown in Fig.1; 4) timestamp; 5) difficulty (D); and 6) the nonce (N) [4], [20]. The second part is called the body, which represents the transactions or facts (that the database must store), which can be of any type such as monetary transactions, traffic information, health data, system logs, and so on. The block body contains all inputs and outputs of each transaction. The input contains the output of previous transactions, as well as a field containing the signature with the owner's private key, indicating ownership proof of such an asset. The outputs contain the assets to be sent and the recipient's address (the recipient's public key). The recipient will be the only user who is able to spend this asset because only his/her private key can prove the ownership of that asset [4], [20]. The distributed and append-only nature of blockchain improves transaction security and integrity [1], [15], [21]. The blockchain's chaining method (shown in Fig.2) ensures immutability by incorporating the hash of the previous block into the current block [15]. Indeed, if a malicious user wants to change or modify a transaction on a block, he/she must change all following blocks as well, because they are linked with their hashes. Then, he/she must update the blockchain version on each participating node [1], [4], [15], [18], [22], [23].

Consensus mechanisms are an indispensable part of blockchain technology because they ensure the integrity of the blockchain's information while defending against double-spending attacks. The ultimate goal is to reach a consensus in a distributed network of participants who do not need to trust each other without centralized authorities [10]. The basis of these algorithms is the selection of a leader who is in charge of validating the new block and propagating it across the network. The validation process involves all network participants, and when a certain number of nodes agree on a block, the block is added to the network. The main condition is that the majority of nodes are honest. Resolution mechanisms are also present in the event of conflict [4].

The *Proof of Work (PoW)* consensus was first used by Bitcoin and is known as the mining process [24]. In fact, it would be impossible to talk about blockchain without the presence of PoW [4]. With PoW, a group of miners competes with each other to solve a software computer problem with difficulty D and obtain rewards. Miners have to solve a mathematical puzzle that requires considerable computational power, or do a challenge of trial and error, which is difficult to compute but easy to verify. The first miner that solves the puzzle is rewarded for this costly process by winning the consensus algorithm and mining the next block. PoW is the most widely used method of block validation in blockchain systems such as Bitcoin, Ethereum, BitShares, NameCoin, LiteCoin, DogeCoin, and Mone [1], [3], [12], [18]. However, PoW has several flaws that can have serious consequences. PoW has been severely criticized because it is considered too difficult, computationally heavy, and too expensive in terms of energy consumption. In addition, PoW has shortcomings such as high latency and low transaction rates, which reach 10 min, making it unsuitable for many applications. Moreover, in PoW, the blockchain ecosystem is vulnerable to 51% attacks [1], [12], [18]. Several attempts to change the PoW have recently been proposed. For example, Primecoin mitigates power losses by suggesting useful computational intensive tasks such as searching for prime numbers, which can be used for other purposes [4], [10]. However, it is not clear whether underestimating the complexity involved in

TABLE 1. Block data structure [4], [20], [25].

Field	Subfield	Size	Description
Block header	Block size	4 bytes	Size of this block in byte (excluding this field).
	Version number	4 bytes	Mark the block protocol version (indicates the position of this block in the blockchain)
	Parent block hash value	32 bytes	A hash value linking the block to the previous block. To generate block hashes, the blockchain uses the SHA256 hashing algorithm.
	Merkle tree "root"	32 bytes	It is the hash value of all the transactions included in the current block. Thus, transactions cannot be changed without changing the Merkle root hash. One modification in one block payload will change the Merkle root hash value, which invalidates the block.
	Timestamp	4 bytes	The time in which this block is generated.
	Difficulty target	4 bytes	The difficulty target of the proof-of-work calculation for generating this block (it is a measure of finding a successful hash)
	Nonce	4 bytes	It is a counter used in the Proof of Work (PoW) and usually starts with 0 and increases for each hash computation. Simultaneously, this prevents reboot attack
Block body	Number of transactions	1 ~ 9	Number of transactions recorded in this block
	Transaction	Determined by the number of transactions	All transactions that are recorded in this block.

this change will offer security features in the same way as PoW [10].

To address the shortcomings of PoW, *Proof of Stake (PoS)* has been proposed [26]. Proof of Stake (PoS) is the most popular alternative consensus for PoW, which requires fewer CPU computations. There is no mining in PoS. Instead, the miners lock their stakes or assets into the blockchain to mine new blocks. Miners with larger locked stakes are more likely to mine the next block because their weights in the mining blocks are greater. In IoTs, large companies such as Google can buy large parts of the assets, and thus, PoS may eventually lead to centralization [4]. Many blockchain systems use PoS, whereas others transition from PoW to PoS. PoS was originally used by Peercoin and later in Nextcoin, BlackCoin, Nxt, and ShadowCash Crave. Ethereum switches from PoW to PoS [1], [4], [10], [12], [18]. The PoS algorithm provides higher transaction throughput and scales better than PoW, making it more suitable for IoT. Furthermore, dishonest miners are forgiven in PoW, but they are punished in PoS by having to pay their bet. Recently, Ethereum announced the transition from PoW to PoS and a new protocol (Casper) that handles reward and punishment by taking the bets of malicious validators. Nevertheless, PoS is negative in the sense that it encourages enrichment of the rich. Another disadvantage of PoS is that it is less secure than PoW [3], [10].

A variant of PoS is the *Delegated Proof-of-Stake (DPoS)* [27]. To reach a consensus, DPoS requires voting; thus, it is known as a democratic blockchain. In DPoS, users can stake their tokens to vote for certain delegates. The voting weight is proportional to the user's number of coins (for example, if A gets two delegate coins and B gets one coin, A's vote outweighs B's two times). The delegate with the most votes is allowed to create new blocks and receive the bonus, which can be a fixed amount generated through inflation or based on transaction fees [3], [28]. This approach

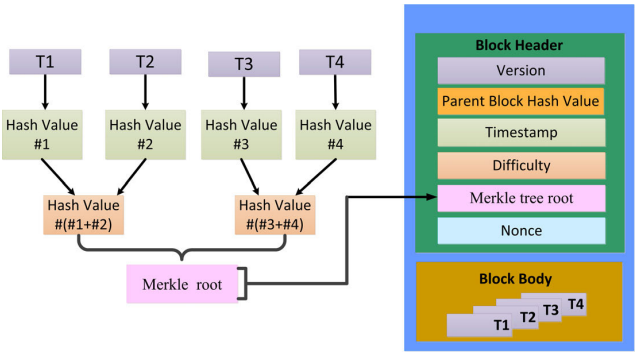

FIGURE 1. Block structure [8].

allows delegates to set the block size, block latency, and confirm transactions in just one second [10]. DPoS is used in BitShares, Monax, Lisk, and Tendermint.

The *Proof of Authority (PoA)* is the successor to PoS, where the auditor's reputation acts as a stake. In PoA, each miner's mining power is determined by its identity in the network rather than the amount of locked assets [29]. All network participants are aware of the identity of the pre-approved group of nodes acting as miners. Miners with a higher reputation have a higher chance of mining new blocks [12]. It is difficult to restore a reputation once it is lost; therefore, it is a better option for a "stake." Although Proof of Authority (PoA) networks have high throughput, they are centralized and controlled by validators [4].

The *Practical Byzantine Fault Tolerance (PBFT)* [30] consensus strategy is based on a replication algorithm to tolerate Byzantine failures [18]. In PBFT, every transaction is validated by every other node in the network [4]. All nodes in the PBFT model are arranged in a sequence such that one node is the primary node or the master node, and the other nodes are referred to as backup nodes. All nodes within the blockchain

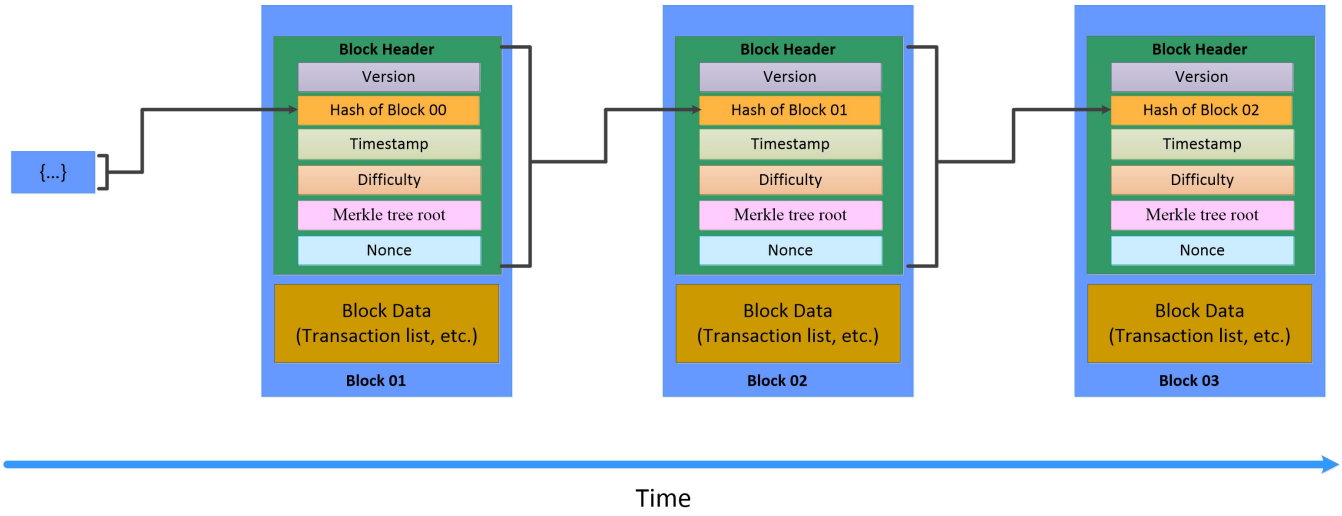

FIGURE 2. Blockchain structure [48].

exchange messages with each other for the honest nodes to reach an agreement on the state of the system through the majority. The final decision is based on a majority rule and can handle up to third malicious byzantine replicas [3]. PBFT is more efficient than PoW, but the model only works well with small consensus group sizes because of the cumbersome amount of communication required between the nodes. Hence, PBFT is optimal for smaller blockchains. Many platforms have implemented PBFT such as the Linux Foundation Hyperledger Fabric [3] and Multichain [10]. Other variants of the PBFT are the *Federated Byzantine Agreement (FBA)* [31] and *Delegated Byzantine Fault Tolerant (dBFT)* [32].

Intel recently developed a new blockchain consensus algorithm known as the *Proof of Elapsed Time (PoET)* [33], which is integrated with Hyperledger. The Proof of Elapsed Time (PoET) was created for the Hyperledger Sawtooth Blockchain project (San Francisco, CA, USA), which is a permissioned blockchain. Proof of Elapsed Time (PoET) is a leader election algorithm designed to run on Intel CPUs in a Trusted Execution Environment (TEE). It achieves consensus by utilizing the TEE of Intel SGX CPUs. Before storing a block in the blockchain, nodes must wait for a random time selected from a trusted enclave. The TimeChecker function validates random time selection. Subsequently, the block can only be appended to the blockchain [12].

Round Robin (RR) consensus permits entities to create blocks in rotation. More specifically, each entity in a given time window can only generate a certain number of blocks, which is determined by a network parameter known as mining diversity, which specifies how many blocks to wait before attempting to mine again [18]. This model ensures that no single participant creates the majority of the blocks, and it benefits from a straightforward approach, lacks cryptographic puzzles, and has low power requirements. Because there is a need for trust between nodes, RR does not work well in permissionless blockchain networks that most cryptocurrencies use. This is due to the fact that malicious nodes could constantly add new nodes to increase the likelihood of deploying new blocks. In the worst-case scenario, they could sabotage the blockchain network's proper operation [34]. A comparison of the discussed consensus mechanisms is presented in Table. 2.

There are many other mechanisms for validating blocks that have not been discussed here, such as the *Leased Proof of Stake (LPoS)* [10] *Proof of Capacity (PoC)* [35], [36] *Proof of Burn (PoB)* [37] *Proof of Importance (PoI)* [38], *Algorand* [39] *RepuCoin* [40], *Ripple* [41], *Stellar* [31], *Proof of Use (PoU)*, *Proof of Hold (PoH)*, *Proof of Stake/Time (PoST)* and *Proof of Minimum Aged Stake (PoMAS)*.

Blockchain introduced a technology in which the concept of a *smart contract* can be materialized. Smart contracts are lines of code or small programs that are stored on the blockchain, like any other transaction, and are automatically executed when predefined terms and conditions are met [3]. In 1993, Nick Szabo defined a smart contract as "a computerized transaction protocol that implements the terms of a contract." Although Bitcoin provides a basic scripting language, it turned out to be inadequate, resulting in the emergence of new blockchain platforms with built-in smart contract functionality [10].

Ethereum [50] is a leader blockchain that supports the use of smart contracts. Smart contracts are now embedded in the vast majority of current blockchain applications, such as Hyperledger [51], in which smart contracts are deployed on the network in packages referred to as chaincode. Smart contracts allow for the definition of functions and terms that go beyond cryptocurrency exchange, such as validating assets in a specific set of transactions involving non-monetary items, making them an ideal component for extending blockchain technology to other areas [10].

Smart contracts offer a range of advantages such as speed, accuracy, transparency, and efficiency, which have promoted

TABLE 2. Comparison between consensus mechanisms [31], [42]–[49].

Consensus Mechanism	Blockchain Type	Energy Saving	Example	Scalability	Mining	Mechanism	Transaction Rate
PoW	Permissionless	No	Bitcoin Ethereum, BitShares, NameCoin, LiteCoin, DogeCoin and Monero	Not scalable	Based on computational power	Proof based	Low 7 transactions per second (TPS)
PoS	Permissioned /Permissionless	Partial	Peer coin Nextcoin, Nxt, BlackCoin, ShadowCash Crave, and Ethereum	Good	No mining Random selection of verifier	Tokens/coins amount of locked assets	High
DPoS	Permissionless	Partial	Bitshares, Monax, Lisk, and Tendermint	High	Democracy	Vote based	High ~million
PBFT and Variants	Permissioned	Yes	Hyperledger Fabric	Medium	No proof of work based mining (Random selection of verifier)	Vote based	High
Proof of Authority (PoA)	Permissioned /Permissionless	Yes	Ethereum Microsoft Azure	High	A validator's identity performs the role of stake	Reputation-based	High
PoET	Permissioned	Yes	Coin desk, Hyperledger Sawtooth	Good	Election of verifier	Lottery	Medium
RR (Round Robin)	Permissioned	Yes	Multichain and Tendermint	Poor	Pseudo-randomly selection Turn base on the interval time	Vote based	High

the emergence of many new applications in a variety of fields. Smart contracts also ensure a greater degree of security, reduce dependence on trusted brokers, and lower transaction costs. Furthermore, the smart contract allows us to convert legal obligations into automated processes [3]. However, the advantages of smart contracts do not come without cost, as they are vulnerable to a variety of attacks that present new challenges. Delegating contract execution to computers introduces some complications because it exposes them to technical issues such as viruses, hacking, bugs, or communication failures. Bugs in smart contract coding are especially dangerous because of the irreversible and immutable nature of the system. Mechanisms for verifying and ensuring the correct operation of smart contracts are required for them to be widely adopted and safely embraced by customers and providers. Formal validation of contract logic and its validity are areas of research where contributions are expected to be made in the coming years [10].

There are many existing blockchain platforms, such as Bitcoin [14], Ethereum [2], [50], [52], Hyperledger [30], [51], Multichain [53], and IOTA [54]. *Bitcoin* is a cryptocurrency and digital payment system based on a P2P network that does not require any central authority. It was launched in 2008 [14] by a person or group of people known as Satoshi Nakamoto in their historical paper [1]. Based on the core concept of blockchain, Bitcoin users do not use real names; instead, they use pseudonyms. Bitcoin relies on three main technical components: transactions, consensus protocols, and communication networks [17]. A conflict (fork) occurs in Bitcoin when multiple miners (in competition) generate blocks simultaneously, and each miner considers its own block a legitimate block to be added to the blockchain. To avoid conflicts between miners and share the same blockchain, Bitcoin uses the longest chain rule [1], [15].

In 2013, a new blockchain platform called *Ethereum* was introduced [50]. Ethereum is a public blockchain that deploys smart contracts to write and execute code in a distributed manner. Ethereum can be considered as a programmable blockchain. In contrast to Bitcoin transactions, where user operations are fixed, the user can create a complex operation using Ethereum, expanding the application of Ethereum beyond cryptocurrencies. In addition to smart contracts, Ethereum is distinguished by the Ethereum Virtual Machine (EVM) as its core. The EVM is a smart contract sandbox environment that isolates code running within it from network access, other processes, or filesystems [4]. To validate the blocks, Ethereum employs a PoW mechanism known as Ethash. There is currently a beta version of Ethereum that uses a PoS-based protocol called Casper. Ethereum can also be used as a private blockchain, in which the participating nodes are pre-selected; thus, a proof-of-work mechanism is no longer required [1]. However, there have been security issues with Ethereum in the past. One of them was the Decentralized Autonomous Organization (DAO) hack in 2016 [55].

DAO is an independent entity that operates through a smart contract and is in charge of transactions, eliminating the need for a central authority. However, an attacker found a bug that allowed him to drain 3.6 million ETH (equivalent to $70 million). Before the smart contract could update the balance, the attacker was able to request the return of the ether several times from the DAO. Furthermore, because Solidity is a young language with little support, modifications can be difficult [2].

Hyperledger [51] is a Linux Foundation project that develops and promotes a variety of business blockchain technologies, including distributed ledger frameworks, smart contract engines, utility libraries, client libraries, graphical interfaces, and sample applications [3]. The goal of Hyperledger is to create a scalable blockchain that will enable organizations to conduct business with anyone without the need for mutual trust. Hyperledger also aspires to go where blockchain has not yet arrived by incorporating new processes into traditional blockchain features for more accurate verification of those involved identities [4]. Some of the frameworks that Hyperledger provides are *Hyperledger Fabric* (contributed by IBM) [51], [56], *Hyperledger Sawtoot*h [33], *Hyperledger Iroha* [57], *Hyperledger Burrow*, *Hyperledger Indy* [3]. Hyperledger also contains open-source tools such as *Hyperledger Composer* [58], *Hyperledger Caliper, Hyperledger Explorer*, *Hyperledger Grid*, *Hyperledger Cello*, *Hyperledger URSA*, and *Hyperledger Quilt/Interledger.js*.

Multichain [53], [59] is a private permissioned blockchain solution based on the use of streams, which act as an independent append-only collection of items, increasing the confidentiality of shared data. Multichain is a stable and simple way to store data with smart contracts. It is distinguished by its adaptability, which allows permission changes and delegations [18]. Multichain is based on the blockchain of Bitcoin, but Multichain is an open-source blockchain platform that natively supports the confidentiality of transactions and supports multi-asset financial transactions and multi-currency. Multichain also supports multiple networks simultaneously on a single server. The consensus mechanism in Multichain is similar to PBFT, with one validator per block and a round-robin algorithm [4], [18].

Blockchain technology has limitations in terms of scalability, cost, and efficiency, which prevents its use in applications that require efficient microtransactions. This limitation has a significant impact on its adoption in emerging IoT applications. Owing to the issues and limitations of blockchain technology, researchers have begun to consider blockchain variants [60]. Sergio Demian Lerner published a paper titled ''Dag Coin: a cryptocurrency without blocks'' in 2015 [61], which introduced the concept of the DAG chain for the first time. A Directed Acyclic Graph (DAG) is one of the most vital variants of blockchain technology. It is a type of graph with directional links. Dag graphs are acyclic with no loops inside the structure, which means that the links cannot be bidirectional [60]. Unlike the blockchain concept, however, DAG does not require miners to authenticate each transaction. Before a new transaction can be successfully recorded on the blockchain network, it needs validation of at least two previous transactions. The nodes that hold transactions are referred to as sites, and the links that connect them are referred to as edges. The rule is that a site is connected to at least two other sites by incoming edges, and sites with fewer than two incoming edges are called unconfirmed and are usually located at the end, which is called the tip of the tangle [2]. DAG has no miners, so there are no miners' fees, which helps to keep authentic transaction fees to a minimum [60], [62]. The Gossip algorithm is used in the DAG network to ensure the final consistency of states between different transactions. Although it cannot guarantee the consistency of the network's states at all times, their final data consistency will be obtained at some point in the future. After a certain period of time, all the nodes in the network will be agreed upon, even if some of them go offline or new nodes join [63]. Owing to its optimized validation, high scalability, efficient provenance, multi-party involvement, and IoT support, DAG has revolutionized blockchain technology and will be useful for any type of IoT-based micro-transaction scenario, including those involving logistics [60].

The DAG structure is well suited for large-scale transaction scenes because of the inherent advantages of parallel processing and multi-thread operations. However, it still has some drawbacks, such as the fact that it does not support strong consistency and that security performance has not been massively validated, which must be corrected and improved gradually [63]. Some distributed ledger systems are based on the DAG structures. For example, *NXT* was the first cryptocurrency to propose switching to a DAG-based blockchain rather than Blockchain's LinkedList structure [60]. Another example is *IoTA* [64], which is a new ledger-based cryptocurrency designed for micropayments. *IoTA* is a popular blockchain protocol for IoT devices. With more users, the IoTA network becomes more scalable, allowing it to process more transactions per second. Other DAG-based distributed ledger systems include Orumesh [60], Byteball [63], Hashgraph [62], and *NANO* (formerly known as *RaiBlocks*) [60]. Table. 3 introduces a comparison between the blockchain platforms mentioned previously.

There are some other blockchain platforms, in addition to the previously discussed platforms, such as *Ripple* [41], *Corda* [65], [66], *HDAC* [67], *Cosmos* [68], *IoTeX* [69], *BigchainDB* [70], *ChainCore* [4], [71], *Domus Tower Blockchain* [72], *HydraChain* [73], [74], *OpenChain* [75].

III. CONSENSUS FOR BLOCKCHAIN-BASED IoT

The use of blockchain in an IoT context may provide several benefits, such as trustworthiness and non-repudiation of data. However, the constrained nature of IoT sensors is incompatible with the high computational power required for blockchain. A naive application of blockchain for IoT results in long delays and a large amount of computational power [79]. The formation of consensus by more than half of the peers for each block is critical to the success of the

TABLE 3. Blockchain platforms comparison [2], [76]–[78].

Features	Bitcoin	Ethereum	Hyperledger Fabric	Multichain	IoTA
Block size	1 MB	Ethereum's block size varies	Hyperledger's block size varies	up to 1 GB	Does not use blocks
Permissioned?	No	Yes	Yes	Yes	Resemble in work
Permissionless?	Yes	Yes	No	No	Yes
Validation Time	10 minutes	15-20 sec	Less than Ethereum	-	Varies from minutes to hours
Consensus Mechanism	PoW	PoW, PoS (Casper)	PBFT	Round robin	Tip Selection Algorithm
Scalability	No	No	Yes	Yes	Yes (high)
Throughput	7 TPS	20 TPS	between 3,000 and 20,000 TPS	based on the calculation it could process over 2 million TPS	7-12 TPS
Vulnerability to attacks	51% attack	51% attack	>1/3 faulty nodes & DoS attack	-	34% attack
Cryptocurrency	Bitcoin	Ether	No native cryptocurrency	Multi-cryptocurrency	mIOTA
Smart Contract	No	Yes (Written in Solidity)	Yes (Written in Go, Java, Node.js)	Not applicable	Not applicable
Data Confidentiality	Yes	No	Yes	Yes	No
User Authentication	No	Digital Signature	Based on Enrolment Certificates	Login Signup Module	Digital signatures
Energy & Computational Cost	High	High	Low	Low	Low

blockchain. Nevertheless, in large-scale systems, this results in a lower transaction rate as the time to reach consensus grows exponentially. Modern business blockchain systems, such as Hyperledger, have addressed this issue by reducing the number of involved peers and limiting verification to trade. However, because block verification is not performed and Byzantine Fault Tolerance is not required, both of these changes may allow malicious trades to occur [80].

Several studies have proposed consensus mechanisms for blockchain-based IoT. In Babelchain [81], a novel consensus protocol called Proof of Understanding (PoU) was proposed, with the goal of adapting PoW for IoT applications. Instead of using miners to solve the hash puzzles, the proposed protocol translates from different protocols to save energy. As a result, the effort is more focused on useful computation while also addressing a critical problem in IoT communications. Instead of agreeing on transaction status, network peers agree on message meanings (format, content, and action). Furthermore, blockchain data, such as learning sets, provide information for learning.

Biswas *et al.* [80] proposed a novel lightweight Proof of Block & Trade (PoBT) consensus algorithm that ensures block security during both the trade validation and block creation phases. The authors employed a lightweight consensus algorithm that incorporates peers based on the number of nodes in a session. This reduces the computational time required by peers and enables higher transaction rates for IoT devices with limited resources. By using a distributed peer system for local and global trade, the memory requirements at the IoT nodes are reduced. The analysis and evaluation of security aspects, computation time, memory, and bandwidth requirements showed a significant improvement in the overall system performance.

Moudoud *et al.* [79] proposed a lightweight consensus for IoT (LC4IoT), which reduces the computational power, storage capacity, and latency. LC4IoT overcomes the challenges of using blockchain in an IoT context and ensures openness. Extensive simulations were performed to assess the consensus. The results showed that the proposed consensus requires little computational power, storage capacity, and latency.

Zhidanov *et al.* [6] proposed a novel consensus algorithm called 'Trinity' based on a combination of PoW, PoA, and PoS. Because the computational resources of mobile devices are currently underutilized, this consensus algorithm motivated the inclusion of mobile devices in the new block generation process. Trinity's underlying concepts are ID-based cryptography and Shamir Secret Sharing, which allow secret key dissemination and reconstruction using only a portion of previously distributed shares.

Niya *et al.* [82] demonstrated a PoS-based blockchain called Bazo, which was specially designed and adapted for IoT data streams. This project includes the creation and implementation of an adaptation layer for IoT data streams. The Bazo system was developed and tested in the real world using LoRa devices, as well as simulated in several scenarios using the NS-3 simulator. Compared to PoW-based

blockchains, Bazo performs better in terms of energy consumption and transaction processing. Sharding and transaction aggregation methods were used to further improve Bazo's performance. Moreover, IoT-blockchain adaptation helpers with a modular and layered architecture are provided to enable wireless devices to send data to the blockchain. The designed architecture is capable of supporting a wide range of hardware and software platforms, as well as network technologies.

Dorri *et al*. proposed a lightweight consensus algorithm in LSB [12]. The proposed lightweight consensus algorithm restricts the number of new blocks generated by Cluster Heads (CHs) during a configurable consensus period. To reduce the computation overhead associated with verifying new blocks that will be added to the public blockchain, LSB employs a distributed trust algorithm. Each CH accumulates evidence about other CHs based on the validity of the new blocks that they generate. The number of transactions in a new block that must be verified gradually decreases as the CHs gain trust in one another.

Because of their limited storage capacity, lightweight IoT devices cannot store the entire blockchain. Kim *et al*. [83] proposed a storage compression consensus (SCC) algorithm that compresses a blockchain on each device to ensure storage capacity. When a lightweight device lacks sufficient storage space, it processes the SCC to compress the blockchain. Although the proposed consensus includes additional processes, it improves the maintenance of lightweight device systems by acquiring free storage capacity. According to the simulation results, the SCC can save 63% on storage. As a result, the proposed SCC can be used to build a blockchain-based storage-efficient lightweight IoT network.

Bai *et al*. [84] proposed a two-layer consensus optimized for IoT requirements: Base-Layer and Top-Layer. The Base-Layer is made up of low-resource devices that are connected to the server as well as users and other nodes. A highly scalable and fully decentralized blockchain that performs basic functions was presented in this layer. Countless blocks are mined and submitted each round, but only one block is selected by the Top-Layer to be recorded. The Base-Layer consensus reduces the mining difficulty and resource consumption to increase the TPS to meet the large-scale IoT environment. Special nodes run a non-Byzantine fault-tolerance algorithm to determine accounting rights in a random form. The two-layer consensus combines the benefits of blockchain and IoT to overcome deficiencies, allowing for greater IoT applications. According to the analysis and evaluation, a consensus has better fault tolerance and increased scalability.

Puthal *et al*. [85], [86] proposed Proof-of-Authentication (PoAh), a novel consensus algorithm that can be incorporated into resource-constrained distributed systems. PoAh not only secures systems, but also ensures system sustainability and scalability. To validate its performance, the proposed consensus algorithm is theoretically evaluated in simulation scenarios and real-time hardware testbeds. While running on limited computer resources (e.g., singleboard computing devices such as the Raspberry Pi), the proposed PoAh has a latency of approximately 3 s.

Dorri *et al.* [87] proposed a tree-chain, which is a scalable, fast, and lightweight consensus algorithm for IoT applications. Tree-chain incorporates a consensus algorithm that does not require validators to solve any puzzles or provide proof of x before storing a new block. The hash function outputs were used to generate randomization among the validators. The tree-chain introduced two levels of randomization among the validators: 1) transaction level, where the validator of each transaction is chosen at random based on the most significant characteristics of the hash function output (known as consensus code), and 2) the blockchain level, where the validator is randomly assigned to a particular consensus code based on a set of criteria. The tree-chain introduced the parallel chain branches, with each validator committing the corresponding transactions to a separate ledger. Furthermore, the tree-chain introduced a load-balancing algorithm that allows overloaded validators to involve new validators, ensuring the blockchain's self-scaling feature. The implementation results show that the tree-chain has a low processing overhead and can be run by low-resource IoT devices. The tree-chain will allow for new fast blockchain applications in resource-constrained scenarios, such as the IoT.

To achieve a lightweight blockchain, Li *et al.* [88] proposed an improved PBFT blockchain consensus mechanism based on a reward and punishment strategy. The authors proposed a blockchain storage optimization scheme based on reward and punishment (RS) erasure code to reduce storage overhead while ensuring blockchain recoverability. Experimental results showed that the strategies proposed in this paper can reduce the consensus delay, communication resources required for consensus, and blockchain storage costs.

Table. 4 provides a brief description of the previously discussed consensus mechanisms.

IV. BLOCKCHAIN SCALABILITY IN IoT

Blockchain has gained popularity as a result of the use of Bitcoin for online transactions that do not require third-party security. However, the most difficult challenge for blockchain providers is the scalability [20]. Scalability issues must be addressed to integrate IoT and blockchain. On the one hand, because of their sheer number, IoT devices will generate transactions at a rate that current blockchain solutions will not be able to handle. However, owing to resource constraints, it is impossible to implement blockchain peers on IoT devices. Both technologies cannot directly be integrated in their current state [89].

To address the issue of scalability, various techniques such as Segwit, Sharding, block size increase, PoS, and off-chain state have been proposed [4]. Segwit, or segregated witness, is a scalability solution that increases the number of transactions in a block while keeping the block size constant. By removing the signature data from the Bitcoin transaction, a segregated witness creates room for new transactions. This signature data is stored in a base transaction block outside the

TABLE 4. Consensus mechanisms for Blockchain-based IoT.

Year	Paper	Name of algorithm	Feature
2016	[81]	Proof of Understanding (PoU)	• A novel consensus protocol that proposed translating from different protocols to save energy instead of using miners to solve hash puzzles. • Network peers agreed on message meaning (format, content, and action) instead of agreeing on the transaction status • Blockchain data, such as a learning set, provide information for learning.
2019	[80]	Proof of Block & Trade (PoBT)	• A lightweight consensus algorithm. • Block security is ensured during both trade validation and block creation phases. • The PoBT reduces the bandwidth required at critical network points. • PoBT also reduces the memory requirements of IoT nodes. • PoBT enables higher transaction rates for IoT devices with limited resources.
2019	[79]	Lightweight consensus for IoT (LC4IoT)	• Secure architecture that overcomes the challenges of using blockchain in an IoT context • The proposed consensus requires little computational power, storage capacity, or latency.
2019	[6]	Trinity	• A combination of Proof-of-Work (PoW), Proof-of-Activity (PoA), and Proof-of-Stake (PoS). • Trinity motivated the inclusion of mobile devices in the new block generation process. • Underlying concepts are ID-based cryptography and Shamir Secret Sharing which allow secret key dissemination and reconstruction using only a portion of previously distributed shares.
2019	[82]	Bazo	• Proof-of-Stake (PoS) based. • The creation and implementation of an adaptation layer for IoT data streams. • Bazo performed better than PoW in terms of energy consumption and transaction processing. • The designed architecture was capable of supporting a wide range of hardware and software platforms, as well as network technologies.
2019	[12]	-	• A lightweight consensus algorithm that restricts the number of new blocks generated by Cluster Heads (CHs) within a predefined consensus period. • A distributed trust algorithm was used to reduce the computational overhead associated with verifying the new added blocks to the public blockchain.
2019	[83]	Storage Compression Consensus (SCC)	• Compresses a blockchain in each device to ensure storage capacity. • When a lightweight device lacks sufficient storage space, it processes the SCC to compress the blockchain. • Although the proposed consensus included additional processes, it improved the maintenance of the lightweight device system by acquiring free storage capacity. • SCC can save 63% in storage. • SCC can be used to build a blockchain-based storage-efficient lightweight IoT network.
2019	[84]	-	• Two-layer consensus (Base-Layer and Top-Layer). • The Base-Layer consensus reduces mining difficulty and resource consumption to increase transactions per second (TPS) to meet the large-scale IoT environment. • Countless blocks were mined and submitted each round, but only one block selected by the Top-Layer can be recorded. • Low-resource devices attached to the server and with users and other nodes form the Base-Layer. • Special nodes, running a non-Byzantine fault tolerance algorithm to determine accounting rights at random, form the Top-Layer with another high-security blockchain. • A two-layer consensus has a better fault tolerance and increased scalability.
2019, 2020	[85], [86]	Proof-of-Authentication (PoAh)	• PoAh not only secured systems but also ensured system sustainability and scalability. • PoAh had a latency of approximately 3 seconds when running on limited computer resources (e.g., single-board computing devices such as Raspberry Pi)
2020	[87]	Tree-chain	• The Tree-chain algorithm includes a consensus algorithm that does not require validators to solve puzzles or provide proof of x before storing a new block. • The hash function outputs are used to generate randomization among the validators. • Tree-chain introduces randomization among the validators at two levels: transaction and blockchain levels. • The Tree-chain is a scalable, fast blockchain instantiation. • The Tree-chain introduces a load-balancing algorithm and parallel chain branches. • It can be run by low-resource IoT devices because of its low processing overhead.
2021	[88]	-	• Improved PBFT blockchain consensus mechanism based on the reward and punishment strategy. • Blockchain storage optimization scheme based on reward and punishment (RS) erasure code. • Reducing consensus delay, communication resources required for consensus, and blockchain storage costs.

chain. This separation of the validation portion allows more transactions to be stored without increasing the block size.

Ethereum developers are working on partitioning schemes such as sharding. In a distributed environment, partitioning leads to the handling of all application requests in a single shard and balances the load among shards; hence, the performance will scale up. However, there are very few applications that can be optimally partitioned in practice. As a result, the system must be able to handle requests from multiple shards. Furthermore, the concept of directed acyclic graphs (DAG) is used in Ethereum, where nodes represent transactions, and edges represent the confirmation direction. Although the problem of balanced graph partitioning is non-deterministic polynomial (NP) complete, methods for partitioning Ethereum blockchain graphs have been developed. These methods are classified as hashing methods, Kernighan Lin (KL) methods, METIS, R-METIS, and TR-METIS methods [20].

Biswas *et al.* [89] proposed a framework that enables the blockchain ledger to scale across all peers by establishing a local peer network. It limited the number of transactions that enter the global blockchain by implementing a scalable local ledger while maintaining peer validation of transactions at both the local and global levels. The results of the implementation testbed showed that significant improvements in the transaction rate and ledger weight were possible. This would improve the scalability of large-scale business transactions in IoT and address the issue of memory requirements for storing blocks. However, the current implementation and evaluation have been carried out in part on virtual machines, with the application written in Node-red.

Dorri *et al*. proposed a tiered structure in LSB [12], in which a single public blockchain was managed by the overlay nodes in a distributed manner, and the devices within each smart home were managed independently by a home-specific Local Block Manager (LBM). An overlay network can have a large number of nodes. To ensure scalability, the authors assumed that the public blockchain is managed by a subset of overlay nodes organized as clusters, in which only the Cluster Heads (CHs) are responsible for managing the public blockchain. Furthermore, the authors proposed a lightweight consensus algorithm that restricted the number of new blocks generated by CHs during a configurable consensus period. The results showed that their approach scaled better and protected against a broader range of attacks.

Shahid *et al*. proposed ''Sensor-Chain,'' a lightweight scalable blockchain framework for resource-constrained IoT sensor devices in [90]. A global blockchain is divided into smaller disjoint local blockchains in the spatial domain such that the required storage space is always less than that of a conventional blockchain. To limit the size of the local blockchains in the temporal domain, a temporal constraint was imposed on their lifespan. A sensor node must maintain no more than one local blockchain in its memory at any given time. The authors compared Sensor-Chain to other approaches by analyzing and testing it in terms of long-run performance and scalability. Experiments showed that it takes up far less storage space than other approaches.

Zhou *et al*. [91] attempted to cover and categorize existing blockchain-scaling solutions. Furthermore, they compared various methods and proposed potential solutions to the scalability problem of blockchain. They described the blockchain performance problem regarding scalability and then classified the existing mainstream solutions into several representative layers. Moreover, to provide a comprehensive explanation, they elaborated on some popular solutions, such as Sharding, Cross-chain, and Sidechain. In addition, based on the drawbacks discovered, the authors summarized several potential research directions and open issues, such as inefficient cross-shard transactions, massive amounts of blockchain data that need to be compressed or pruned, and unfinished protocols to bridge the existing blockchain to cross-chain platforms. Chapter 15 in the Handbook of Research on Blockchain Technology [20] covers chain partitioning-based scalability, DAG-based scalability, and horizontal scalability through sharding.

V. IoT SECURITY

Notwithstanding the benefits provided by IoT services, where IoT technology is successfully implemented on lamps, refrigerators, air conditioners, washing machines, wristwatches, mobile phones, etc., managing IoT communications has become a challenge. A large number of IoT devices can be installed anywhere the end-user wants, leaving them unattended and being a desirable target for others to attack. In addition, manufacturers do not consider the security of these devices because of the large-scale deployment of IoT devices. For bulk-manufactured devices, default usernames and passwords are the same. Many IoT devices are shipped with a pre-programmed key that cannot be changed. In addition, IoT networks are heterogeneous and dynamic in nature, allowing various (untrusted) devices to indefinitely join the network. In the event of a hack, device intentions may differ during connection time, or malicious devices may masquerade as benign [1], [7], [11]. Data integrity is another issue in IoT security. One of the most important IoT applications is the decision support system. The information gathered by the sensors can be used to make timely decisions. As a result, the system must be protected from injection attacks, which attempt to inject false measures and thus influence decision-making [92].

According to Gartner's research, half of all IoT security budgets will address errors, recalls, and safety failures rather than protection by 2022. As a result of the gradual expansion of business associated with this type of always-connected environment, new technological challenges and implications for security, privacy, and interoperability will emerge [4]. Therefore, security is a well-recognized and popular necessity for IoT devices and the widespread use of IoT applications. Because IoT devices have limited resources and are not manufactured with a built-in security principle, they are more vulnerable to attacks. Moreover, given the growth of the

Internet of Things, IoT devices are a major security concern, and their vulnerability opens the door to various types of attacks [7].

A recent example of a distributed denial of service (DDoS) attack, which took down DNS services in Europe and North America, was the attack against DNS provider Dyn in October 2016 using a botnet of Linux-based devices infected with Mirai malware. The unsecured IoT devices (including IP surveillance cameras, residential gateways, and baby monitors) used in this attack, send a large amount of data to Dyn and crash their servers. Mirai DDoS attacks are managed to disrupt major Internet services such as Twitter, Netflix, PayPal, and Amazon. This attack demonstrated that while individual IoT devices may not be powerful, their collaboration as a large-scale botnet enables them to be a threat capable of overwhelming well-prepared defenses of critical Internet services such as the Domain Name System (DNS). However, owing to the limited capabilities of IoT devices and their deployment mode (large-scale and distributed), maintaining and securing each individual IoT device is a challenge. Hence, how can we deter the potential misuse of IoT devices [93], [94]?

Several solutions related to security and privacy have been proposed for IoT environments that provide prevailing security requirements, such as authentication, integrity, and confidentiality. Nevertheless, owing to resource constraints and heterogeneous IoT devices, current solutions cannot meet the security requirements required in the upcoming large-scale IoT paradigm. Although some security-based solutions are secure and efficient, they are generally based on centralized mechanisms. A well-known mechanism of Public Key Infrastructure (PKI) encounters scalability problems in the case of one million nodes [92]. Furthermore, the centralized mechanism faces a single-point of failure problem, which can lead to a catastrophic failure of the entire system and endanger the entire network [85], [86]. A publicly verifiable audit trail without a trusted third party is recommended to solve single-point of failure and non-repudiation problems [4]. Blockchain technology has gained tremendous attention in terms of addressing security, anonymity, traceability, and centralization [92]. Integrated with blockchain technology, IoT systems can benefit from decentralized resource management, lower operating costs, and resistance to threats and attacks [17]. The proliferation of blockchain-enabled IoT will open up new horizons for services and applications for the next generation of cellular and personal wireless networks [95]. Blockchain presents a booming venture that fits the stringent requirements of less capable IoT devices in a typically decentralized structure. Efforts to adopt blockchain to secure communications in IoT using public-key schemes are attracting a lot of interest in the research community [16]. The convergence of IoT and blockchain aims to overcome the major challenges of realizing the IoT platform in the near future [17].

Blockchain is a ''secure by design'' system that can mitigate security risks due to its capabilities such as immutability, auditability, transparency, data encryption, and operational resilience. To overcome security weaknesses in IoT, researchers and developers in the ICT sector have decided to integrate ''security by design'' technology into IoT [4]. Blockchain will change the way we share information in which trust in distributed environments can be built without the need for authorities. Since its inception, IoT has made use of technologies such as cloud computing and big data to overcome its limitations, and we believe that blockchain will be a promising technology [10]. Extending the IoT structure for Device-to-Device (D2D) systems with blockchain provides three key benefits: trust (building trust between parties and devices, and reducing the risk of tampering and collusion), cost savings (removing overhead associated with intermediaries and middlemen), and accelerated transaction rate (reducing settlement time) [89].

In the IoT scenario, blockchain and, more broadly, P2P approaches may play an important role in the development of decentralized and data-intensive applications that run on billions of devices while protecting user privacy [96]. Blockchain technology is expected to be used to keep a ledger of IoT device transaction logs and communications [89]. The blockchain stores all transactions permanently. Thus, by exploring the corresponding transaction ledger for that node, the history of transactions generated by that node can be audited. In a smart home, for example, the homeowner needs to know who has accessed their IoT devices or data. Using blockchain, it is possible to traverse the entire ledger to review previous actions because each transaction retains the ID of its preceding transaction [12].

VI. IoT SECURITY USING BLOCKCHAIN

Moving towards decentralized architectures, blockchain technology has gained tremendous attention in terms of addressing security, anonymity, traceability, and centralization [92]. The security of this technology stems from the use of hash functions to chain blocks to ensure immutability, as well as the use of encryption and digital signatures to secure data. The distributed nature of the blockchain ensures its availability [18]. Enabling blockchain technology in IoT can help to achieve a properly distributed consensus-based IoT system that overcomes security issues. Even if this is an ideal match, it is still a challenging endeavor[97]. Because most existing blockchain schemes are not dedicated to the IoT ecosystem, they are unable to meet the specific requirements of the IoT [98]. IoT environments are resource-constrained with limited capabilities in terms of computation, energy, and storage, which discourages the use of blockchain, which has high computational complexity, limited scalability, high bandwidth overhead, and latency, which is unsuitable for IoT [99].

Filament, which uses blockchain technology, is a notable IoT project in terms of security. It is a hardware and software solution that enables smart contracts and bitcoin-based payments in the IoT. Filament devices include embedded crypto processors that support five protocols: Blockname, Telehash,

smart contracts, Pennyback and Bittorrent protocols. Blockname manages device identity, whereas Telehash, which is an open-source implementation of the Kademlia distributed hash table (DHT), provides secure encrypted communications, whereas smart contracts define how a device can be used [10].

Fakhri and Mutijarsa [100] built IoT systems with and without blockchain and compared the two approaches. MQTT is a communication protocol used in an IoT system that does not use a blockchain. Ethereum was used as a blockchain platform, along with a smart contract, in the other system. The security levels of both IoT systems were evaluated by simulating attacks and observing their security features. The results of the tests showed that the IoT system based on blockchain technology had a higher level of security than the IoT system that did not use blockchain technology.

Sagirlar *et al*. [97] presented a novel hybrid blockchain architecture for IoT, referred to as Hybrid-IoT. In Hybrid-IoT, subgroups of IoT devices, referred to as PoW sub-blockchains, were created. The connection between the PoW sub-blockchains was then made using a Byzantine Fault Tolerance (BFT) interconnector framework, such as Cosmos or Polkadot. The authors' work focused on the formation of PoW sub-blockchains that are guided by a set of metrics, dimensions, and bounds. The performance evaluation validated the PoW sub-blockchain design according to the guidelines of the sweet-spot. The results showed that the guidelines of sweet-spot help to prevent security vulnerabilities.

To provide an IoT network with a scalable and dynamic communication architecture, a dynamic blockchain-based trust system was proposed in [101]. The proposed architecture practically labeled all IoT devices and mapped them as full nodes and lightweight nodes. The authors assessed whether this design could improve security by managing the IDs of IoT devices while making it more difficult for attackers to impersonate IoT nodes. For example, if an attacker wants to join an IoT network by impersonating an ID, the label must first be assigned. If the attacker pretends to be a full node, high-level security verification will either catch him or make the attack extremely costly. It is also difficult if the attacker just wants to pretend to be a lightweight node because all history is recorded and the attacker must fake everything all over again each time they try to attack. However, IoT with blockchain topology should not only manage the ID but also protect the information exchanged in the IoT network.

Chakraborty *et al*. [102] proposed a two-layered architecture for dealing with security in resource-constrained IoT nodes. The goal of the model is to provide a more feasible framework by considering a large number of real-time factors. The selection of efficient cryptography algorithms, in addition to blockchain, plays a significant role in further strengthening the network. The authors concentrated on optimizing the computational load so that the model could meet the feasible deployment conditions. Although dividing the IoT network into layers reduces the computational load at each stage, the load split is not proportional to the amount of work done at each level. Flexibility in monitoring the computational load and distributing workload was introduced at each level. Layer 0 is composed of nodes that are unable to enforce security primitives owing to resource constraints, whereas level N is composed of primary and secondary nodes, with primary nodes handling processing and secondary nodes assisting the primary nodes. Layer 0 nodes are unable to communicate directly with each other because of their inability to enforce security.

Alphand *et al*. [103] proposed IoTChain, an IoT security management platform. IoTChain combined OSCAR architecture elements with the Internet Engineering Task Force (IETF) ACE authorization framework to provide an end-to-end (E2E) solution for secure authorized access to IoT resources. IoTChain is made up of two parts: an authorization blockchain based on the ACE framework and the OSCAR object security model, which has been enhanced with a group key scheme. While OSCAR uses the public ledger to set up multicast groups for authorized clients, the blockchain provides a flexible and trustless way to handle authorization.

CIoTA, a lightweight framework that uses the concept of blockchain to perform distributed and collaborative anomaly detection for devices with limited resources, was proposed by Golomb *et al.* [104]. Through self-attestation and consensus among IoT devices, CIoTA uses blockchain to incrementally update a trusted anomaly detection model. CIoTA continuously trained an anomaly detection model while remaining resistant to adversarial attacks. CIoTA also distinguished between rare benign events and malicious activities by leveraging collective wisdom. One disadvantage of CIoTA is that each IoT model/firmware requires its own chain to be published. As a result, CIoTA in its current form is best suited to large industrial settings and smart cities.

Rathee *et al.* [105] proposed a secure hybrid industrial IoT framework based on blockchain. The authors employed a hybrid industrial architecture in which various branches of a company were located in more than one country. They used a blockchain mechanism to extract information from IoT devices and store the extracted records in the blockchain to maintain transparency among multiple users in various locations. Furthermore, the proposed framework has been tested against the internal communication of blockchain, where IoT devices have been compromised by multiple intruders. The results were analyzed against the conventional approach and validated with improved simulated results that offer an 89% success rate over user request time, falsification attack, black hole attack, and probabilistic authentication scenarios.

Inspired by Chainspace [106], Liu *et al.* [98] introduced a blockchain platform called VChain, which can be used in IoT. VChain is a novel blockchain scheme suitable for IoT, and it is more concrete, secure, and practical than Chainspace. VChain proposed a two-layer BFT-based consensus protocol with the HoneyBadger BFT protocol and a collective signature scheme as building blocks. VChain supported faulty-shard-tolerance and asynchronous network models, which were not possible in Chainspace, while also maintaining high

efficiency. Furthermore, unlike RapidChain, which uses the energy-consuming PoW mechanism for sharding, the sharding strategy presented in VChain is environmentally friendly, making it well suited for IoT. Moreover, VChain inherits the benefits of Chainspace in terms of separating smart contract execution and verification for privacy. The security analysis demonstrated that the basic requirements of the IoT environment, namely liveness, consistency, validity, and auditability, are met.

Abdulkader *et al.* [99] proposed a lightweight blockchain-based cybersecurity (LBC) solution for IoT environments. Their goal was to reduce the high computational cost required in a consensus algorithm to meet IoT requirements. LBC differs from its predecessors in the following ways: blockchain size, managing local and public transactions, separating blockchain in local transactions based on the IoT device requester, and a unique consensus algorithm that reduces the transaction waiting period. Edge block managers (EBMs) and aggregation block managers (ABMs) have been introduced to provide scalability to the proposed scheme. By centrally managing the local blockchain, the EBM aims to overcome the limited capabilities of local IoT resources. ABM is composed of many EBMs that work together to manage the public blockchain in a distributed manner. According to the security analysis, the proposed scheme is resistant to common attacks. Their innovative proposed scheme can also achieve a high throughput while maintaining low latency. The waiting, verification, and block-appending periods were significantly reduced. Their study used a smart home as a case study, but the concept of LBC can be applied to a wide range of applications.

Huang *et al.* [107] proposed B-IoT, a general, scalable, and secure blockchain system for IoT. The proposed blockchain is a low-cost credit-based PoW for power-constrained IoT devices that improves both security and transaction efficiency. To protect the confidentiality of sensitive IoT data, the authors devised a data authority management method for regulating sensor data access. Furthermore, their system was built based on a DAG-structured blockchain rather than a chain-structured blockchain, which allows high throughput. The proposed credit-based PoW mechanism, which reduces power consumption for honest nodes while increasing computing complexity for malicious nodes, contributed to the suitability of DAG-structured for IoT systems. Furthermore, the data authority management method can protect data privacy without impairing system performance, which is useful in IoT systems. The authors built a B-IoT prototype on a Raspberry Pi and conducted case studies of a smart factory. Extensive evaluation and analysis results demonstrated that the proposed credit-based PoW mechanism and data authority management method are applicable to IoT devices. However, their system has some limitations, such as sensor data quality control and storage limitations.

Uddin *et al.* [108] proposed a decentralized architecture for storing IoT data generated by smart homes/cities using blockchain. The architecture includes a secure communication protocol between power-constrained IoT devices and a gateway that employs a sign-encryption technique, which is a lightweight cryptography for IoT devices to ensure the privacy and security of IoT devices. The authors improved Gateway's functionality as a Miner Selector to bridge the gap between power and memory-constraints IoT devices and blockchain. A software agent running on the gateway was proposed to select a miner node based on the miner performance parameters. The gateway chose a small group of efficient miners to speed up block processing. As a semi-trusted center, the network manager increases the dependability and robustness of the proposed blockchain-based smart cities/home monitoring applications. Simulations showed that the recommended miner selection outperforms both the Bitcoin Proof of Works selection and Random Miner Selection. Nevertheless, the selection of miners may introduce the risk of malicious nodes being nominated to process a block. To avoid this selection, the authors must create a trust management system.

Manzoor *et al.* [109] presented a blockchain-based proxy re-encryption scheme to address both scalability and trust issues, as well as to automate payments. After encryption, IoT data are stored in a cloud distributed by the system. The system created runtime dynamic smart contracts between the sensor and the data user to share the collected IoT data, eliminating the need for a trusted third party. An efficient proxy re-encryption scheme was employed to restrict access to the data to the owner and the person presented in the smart contract. The sensor encrypts the data before uploading it to the cloud storage, and then re-encrypts it before sharing. According to the experiment, after the initial request, it took an average of 48.01 seconds to share the encrypted data with the user, with a confidence interval of 2.07 seconds. As a result of the mining of the re-encryption key, incorporating proxy re-encryption into the scheme increased the delay by 60%. The authors tested the architecture's scalability by simultaneously sending multiple requests to the sensor. The entire process was repeated ten times for each scenario before averaging. As the number of transactions increases, the process exhibits a gradual increase in delay. This increase in delay is caused by a scalability issue with the Ethereum blockchain.

Mohanty *et al.* [110] developed an efficient lightweight integrated blockchain (ELIB) model to meet IoT requirements. The presented model was divided into two major levels: smart home and overlay. It generates an overlay network in which highly equipped resources can merge into a public blockchain, ensuring dedicated security and privacy. The ELIB model included three optimizations: a lightweight consensus algorithm, certificateless cryptography (CC), and distributed throughput management (DTM) scheme. The proposed model is deployed in a smart home environment to validate its applicability in various IoT scenarios. A detailed simulation was performed under various scenarios in terms of the processing time, energy consumption, and overhead. The ELIB achieved a total processing time savings of 50%

when compared to the baseline method, with a minimum energy consumption of 0.07mJ. At the same time, it had a minimum packet overhead of 4500 kB owing to the presence of 20 overlay block managers (OBMs).

Hyperledger Fabric introduces a novel framework that separates the execution phase from the consensus phase and implements policy-based endorsements. Kataoka *et al*. [111] proposed a novel method for implementing IoT applications on a fabric blockchain. A smart home was used as the case study during the research. The authors presented a solution to the common security concerns. They also discussed the performance overhead of some transactions and discovered that their application interface built on top of Fabric for IoT had no extra overhead. Furthermore, a comparison with QUORAM-BC demonstrated that their architecture is more efficient, particularly for IoT networks.

A. ATTACKS ON IoT

IoT networks can be attacked from both the outside and inside of the network. External attacks on IoT networks occur when an attacker does not know the network's cryptographic keys and launches an attack from outside the network. On the other hand, to launch an internal attack, it is assumed that the attacker controls a trusted entity on the network. As a result, the attack comes from inside the network. This type of attack is more difficult to detect because it can occur when a trustworthy device goes rogue after gaining network trust. An attacker may have multiple goals, such as sending incorrect information to mislead system decisions or deny system services [1], [21]. If the platform is compromised, the entire system is jeopardized, as proven by recent data breaches involving Facebook, Google, Quora, and Marriott Hotels, just to name a few [3]. Table 5 lists the descriptions of common attacks that can be conducted on IoT networks. In the following subsections, we introduce additional details of these attacks.

1) SYBIL ATTACK

Adversaries can use Sybil attacks to clone multiple bogus identities that appear to act legitimately while carrying out malicious actions, including the distribution of malware and spam, as well as the generation of erroneous readings by devices, resulting in the generation of erroneous reports. To avoid detection, Sybils mimic the behavior of nearby legitimate IoT devices; thus, defense against such attacks is critical in IoT. This attack is applicable to any use case in which information from a specific number of devices is required to elect or make a decision. For example, vehicles transmit multiple pieces of information to a management infrastructure continuously in Cooperative Intelligent Transportation System (C-ITS), such as Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM) in European standards and Basic Safety Messages (BSM) in American standards. These data are related to the activities of the vehicles as well as their surroundings, which are used by the management center to provide and improve a variety of services. For instance, if the management center receives messages from multiple vehicles informing about a traffic jam or an accident, it will immediately disseminate this information to all vehicles in the area and assist them in finding better routes. Using a Sybil attack, an attacker can send incorrect information on behalf of multiple existing or non-existing vehicles to mislead the management center's decisions [1], [21].

To prevent Sybil attacks, Asiri and Miri [21] proposed an IoT trust model that uses permissioned blockchains with smart contracts to evaluate the trustworthiness of IoT devices by recording and validating IoT device identities. Baza *et al.* [112] proposed a Sybil attack detection scheme in VANETs based on proofs of work and location. The scheme was based on the fact that Sybil trajectories are physically bound to one vehicle, and thus their trajectories overlap. Extensive experiments showed that the scheme achieves a high detection rate of Sybil attacks while imposing manageable communication and computation overhead. Abdelatif *et al.* [113] proposed a probabilistic approach for analyzing the security of blockchain protocols based on sharding. The authors investigated the threat of Sybil attacks in these protocols. Their paper's main contribution is a tractable probabilistic approach for accurately computing the failure probability of at least one committee and, ultimately, the probability of a successful attack. Rechained is a scheme proposed by Bochem and Leiding [114] that monetarily disincentivizes the creation of Sybil identities for networks that could operate with intermittent or no Internet connectivity. The authors proposed a new identity revocation mechanism and linked it to the concepts of self-identity and decentralized identifiers.

2) DISTRIBUTED DoS (DDoS)

A denial of service (DoS) or distributed DoS (DDoS) is a type of cyberattack in which multiple devices simultaneously send thousands of malicious requests to a single centralized server. As a result, the server's resources become overburdened, rendering it unable to serve any legitimate requests [115]. A DoS/DDoS attack can be carried out in two ways: i) by exploiting a protocol flaw and ii) by flooding the target. The DDoS attack and, in particular, flooding attacks are among the most dangerous cyber-attacks, and their popularity stems from their high effectiveness against any type of service, as they do not necessitate the identification and exploitation of flaws in protocols or services, but simply flooding them. A DDoS attack on the authentication mechanism causes significant damage, such as system paralysis or allowing non-legitimate users to use the system [1].

Although the first DDoS attack was reported in 1996, the complexity and sophistication of these attacks have increased over time. In the midst of the COVID-19 pandemic, a 2 TBps attack on critical infrastructures, such as finance, was reported in mid-August 2020. It is expected that over the next two years, the number of attacks will be more than double, reaching over 15 million [116]. DDoS attacks

involve two defense mechanisms: 1) defending the network, resources, and other information assets from this disastrous attack and 2) preventing the network from becoming a botnet (bot-force) bondage to launch attacks on other networks and resources [117].

Since its inception, several mitigation schemes have been designed and developed, but the increasing complexity necessitates advanced solutions based on emerging technologies. Blockchain has emerged as a viable and promising DDoS mitigation technology. The inherent and fundamental characteristics of blockchain, such as decentralization, immutability, anonymity, verifiability, integrity, and internal and external trustlessness, have proven to be strong candidates for combating this lethal cyber threat [116]. The use of blockchains for networking purposes is still in its infancy. For example, using blockchain technology to blacklist malicious IoT devices does not scale in terms of mitigating or preventing attacks. DDoS mitigation also relies on anomaly detection, which can take a long time after such attacks occur [93].

Rodrigues *et al.* [118] proposed DDoS mitigation across multiple network domains using blockchain technology to share attack information. Their approach employed blockchain smart contracts to signal white or blacklisted IP addresses across multiple domains, as well as SDN to configure flow rules to prevent DDoS attacks. Javaid *et al.* [119] proposed integrating IoT devices with blockchain to address and mitigate DDoS security issues in the IoT. The integration of IoT with Ethereum not only prevented rogue devices from gaining access to the server but also addressed-DDoS attacks by using static resource allocation for devices.

Banerjee *et al.* [120] presented a comprehensive security abstraction layer for IoT systems based on blockchain. The goal of the proposed layer is to detect and isolate untrustworthy devices. Because trusted devices only communicate with trusted devices, they can effectively prevent common attacks such as man-in-the-middle (MiTM) attacks, DoS attacks, and false data/command injection attacks. Authentication, authorization, and auditing services were provided as part of the system's implementation. The authors also adopted a hardware-based approach, employing dedicated hardware modules to monitor firmware behavior without incurring excessive performance overhead. Chen *et al.* [121] proposed a DDoS attack defense method for IoT devices based on blockchain. This method first extracts the features of network traffic of edge nodes, then analyzes the extracted data features, detects abnormal terminal device behavior, and finally realizes DDoS attack defense by deploying smart contracts in the blockchain network for attack node information and access control strategy.

3) BOTNET DDoS ATTACK

In DDoS, various compromised devices are combined to form a botnet that operates under a single master known as the botnet master [115]. The compromised devices are controlled by attackers for malicious purposes. Modern botnets frequently have a decentralized P2P structure to increase attack success and resilience against defense mechanisms. IoT devices play a critical role and become one of the primary tools used by malicious parties to carry out attacks, where botnets are capable of utilizing IoT devices to pose significant threats to the security and privacy of online services. According to a recent HP study, more than 70% of IoT devices lack adequate password complexity and use unencrypted network services, making them easy targets for attackers [122]. Furthermore, sophisticated security mechanisms cannot be incorporated into these devices. Moreover, even large manufacturers do not build devices from the ground up. The reuse of parts manufactured by unknown vendors who disregard basic security requirements is extremely common. An adversary can inject malicious code into IoT devices through an unprotected communication channel or launch attacks through the backdoor of tampered with or counterfeit devices. A single compromised IoT device may appear insignificant, but the problem becomes severe when a group of compromised devices forms a malicious botnet [123], [124]. According to the Nokia Threat Intelligence Report, IoT botnets were responsible for 78% of malware activities in 2018. Although there have been no reported incidents of adversaries using cloned botnets, these cloned devices will be used for malicious purposes in the near future. According to Bloomberg Businessweek, a tiny chip is being used to infiltrate 30 U.S. companies [125].

The well-known Mirai botnet attack in October 2016 demonstrated how botnets can be used to infect IoT devices and launch a large-scale DDoS attack. The following attacks were carried out using botnets, such as WannaCry,WireX, and Hajime. As a result, botnets are a pressing and dangerous threat to the security of IoT devices [126]. The scale of the Mirai botnet attack was greater than that of any previous similar attempt. The attack was carried out by a botnet made up of approximately one million devices, the majority of which were IP cameras. This Mirai attack employs IoT devices as botnets to generate massive amounts of network traffic, exceeding 1 Tbps. They sent 620 Gbps traffic to the victim, and a subsequent attack on the service provider Dyn took down hundreds of web services for several hours (including GitHub, Twitter, Netflix, etc.). These DDoS attacks not only harm the targeted services, but also the owners of IoT devices; the Krebs attack costs the device owners around $320,000 in excess power and bandwidth consumption. The source code for Mirai, the botnet that attacked Krebs' website, was later released, revealing the simple principle upon which it is based. It searches the Internet for devices that are protected by default usernames and passwords, gains access to these devices, and invites them to join the botnet network. The Mirai attack has highlighted the critical security implications of IoT computing, as insecure devices with default credentials are widely available on the Internet [123]–[125]. Thus, IoT devices must have strong self-protection capabilities to defend against malicious attacks from inside or outside. The authentication mechanism, which is the first gateway to network security, can secure the identity of IoT devices on the network [127].

AutoBotCatcher was proposed by Sagirlar *et al.* [122], whose design was motivated by the fact that bots in the same botnet frequently communicate with one another and form communities. AutoBotCatcher's goal is to detect botnets by dynamically analyzing the communities of IoT devices formed based on network traffic flows. AutoBotCatcher employed the Louvain method to detect communities in mutual contact graphs. To store snapshots of the mutual contact graph, AutoBotCatcher used a permissioned BFT blockchain as a state transition machine, allowing a group of pre-identified parties to collaborate without trust to perform collaborative and dynamic botnet detection by collecting and auditing IoT device network traffic flows as blockchain transactions.

The authors of [123], [124] proposed a novel approach to securing IoT based on a distributed multi-agent system for detecting DDoS attacks carried out by multiple infected IoT devices. The authors used a lightweight agent in each of the multiple IoT installations (e.g., smart homes) to detect security events and collaboratively prevent potential attacks. The methodology was particularly useful for mitigating the effects of distributed DDoS carried out using IoT device botnets, such as the recently discovered Mirai botnet attacks. In their work, it was assumed that all agents behaved predictably. However, this is not the case in a real-world scenario. The model must be modified so that it can function even if a portion of the agents does not follow the plan.

Falco *et al.* [126] developed NeuroMesh, a lightweight IoT security solution that uses hacker tools against hackers, in essence, an IoT vaccine. Their software provided managed security and intelligence to IoT devices by utilizing a ''friendly'' botnet that communicated with distributed systems via a proven existing communication infrastructure, the Bitcoin blockchain. Their goal is to detect anomalies in IoT log files to generate new malware signatures in addition to IP-based blacklists and whitelists. Cui and Guin [125] proposed a novel permissioned blockchain-based framework to ensure the authenticity and traceability of IoT devices in the supply chain. A physically unclonable function (PUF) ensures that each IoT device has a unique identity. The blockchain provides device verification by comparing these unique IDs. This framework aided in defending against potential botnet threats. Ahmed *et al.* [115] used a novel blockchain-based architecture to protect IoT devices from Mirai botnet attacks. The solution was based on segmenting the network into autonomous systems (AS), which communicate via the blockchain network to share malicious node information. When a node's generated traffic exceeds a certain threshold, it is classified as malicious.

4) ON-OFF ATTACK

As the name implies, a malicious node behaves both well and poorly alternatively. This allows it to easily carry out an attack before the trust system becomes aware of it [18]. On-off attacks are classified as selective attacks. Malicious nodes may attack multiservice IoT architectures by performing actions based on the type of service they provide to other nodes in the network. To avoid being rated as a low-trust node, a malicious device can provide both good and bad services at random. On-Off attackers can also behave differently with different neighbors to obtain contradictory trust opinions for the same node. This type of attack is difficult to detect using traditional trust management schemes. To classify a node's behavior, some countermeasures require prior trust knowledge and time. Furthermore, not all malicious devices are misbehaving. Some of them could be faulty devices. In some cases, a malfunctioning node may be misidentified as an attacker. Separating attackers' nodes from broken nodes can aid in the recovery of IoT systems [128].

5) SPOOFING ATTACK

In IoT networks, launching an identity spoofing attack is simple [129]. In contrast to a Sybil attack, in which the attacker attempts to create numerous false or virtual identities, a spoofing attack attempts to spoof the identity of a legitimate user to exploit his privileges [1]. An identity spoofing attacker can pretend to be another legitimate IoT device by using a faked identity, such as the media access control (MAC) or IP address of the legitimate user. The attacker can then gain unauthorized access to the IoT network and launch more sophisticated attacks, such as man-in-the-middle and denial-of-service attacks [129].

6) MESSAGE SUBSTITUTION ATTACK

In a message substitution attack, the attacker intercepts authentic messages in transit and modifies them with their own fake data so that recipients accept the forged messages as if they were sent by the original sender [130].

7) MESSAGE REPLAY ATTACK

Because successful message verification does not certify the correctness of the message's sending time, any message can be selectively captured and replayed at a later time without alteration by the attacker. This can result in objects or servers receiving incorrect information. Message replay attacks are frequently combined with message removal attacks [1], [21].

8) BALLOT STUFFING ATTACK

In contrast to the previous attacks, malicious nodes in this one aim to promote other malicious nodes by providing positive opinions about them, increasing their chances of being trusted [18]. It can improve the reputation of a malicious node by making good recommendations, increasing the likelihood of the bad device being selected as a service provider. This is a type of collusion attack, in that it can work with other bad nodes to boost their reputation [131].

9) BAD MOUTHING ATTACK

Malicious nodes use bad-mouthing attacks to harm the reputation of other well-behaved nodes by making false recommendations against them, thereby lowering their trust score [18]. It can ruin the reputation of well-behaved nodes

TABLE 5. Common attacks on IoT networks [1], [18], [21], [94], [128], [134].

Attack	Category	Description	Research to defend the attack using blockchain
Sybil Attack	External/Internal	The attacker attempts to create numerous false or virtual identities by replicating and impersonating the identities of existing network nodes.	[1], [12], [21], [112], [113], [114]
DoS	External/Internal	Multiple devices simultaneously flood thousands of malicious requests to a single centralized server. Therefore, the server's resources become overburdened, rendering it unable to serve any legitimate requests	[11], [93], [12], [135], [118], [119], [120], [121], [122], [123], [124], [126], [125], [125], [115],
On-off attack	Internal	On-Off attacks put IoT trust security at risk by causing nodes to perform random good and bad behaviors to avoid being classified as a threat.	[18]
Spoofing attack	External/Internal	The attacker attempts to impersonate a legitimate user to gain access to his privileges.	[1]
Message Substitution Attack	External/Internal	The attacker intercepts legitimate messages in transit and modifies them so that recipients accept the forged messages as if they were sent by the original sender.	[1], [137], [22]
Message Replay Attack	External/Internal	Replays previously transmitted messages or inserts fabricated information into them.	[1], [94]
Ballot Stuffing attack	Internal	Malicious nodes seek to promote other malicious nodes by providing favorable opinions about them, thereby increasing their chances of being trusted.	[18], [138]
Bad Mouthing attack	Internal	Forces bad ratings for certain nodes to deny their services or to ruin their reputation within the community.	[94], [18], [132], [18]
Good Mouthing attack	Internal	Forces malicious nodes to have high ratings to appear trustworthy	[94], [132]
Side-channel attack	External/Internal	An adversary can analyze the user's electricity consumption profile or ambient light profile inside the house to track the application's usage patterns. The adversary may plan an attack based on these profiles.	-

(by making bad recommendations against good nodes), lowering the likelihood of good nodes being chosen as service providers [132].

10) GOOD MOUTHING ATTACK

In a good-mouthing attack, the attacker forces malicious nodes to have high ratings to appear trustworthy [18]. Good-mouthing attacks can boost the reputation of bad nodes (by making good recommendations for them), increasing the likelihood of bad nodes being chosen as service providers [132].

11) SIDE-CHANNEL ATTACK

A side-channel attack is one of the most important attacks during data exchange in IoT because it is simple to perform and consumes little power. The first official information on side-channel attacks was published in 1965. Side-channel attacks rely on side-channel information and can be a ciphertext-only attack, plaintext-only attack, or chosen-plaintext attack. Examples of side-channel attacks are timing attacks, power consumption analysis attacks, fault analysis attacks, electromagnetic attacks, and environmental attacks [133]. For example, an adversary may track application usage patterns by analyzing the user's electricity consumption profile or ambient light profile inside the home. The adversary may plan an attack based on these profiles [134].

B. INTRUSION DETECTION SYSTEMS

As the network transits to wireless applications, the threat of attack becomes a critical issue. These attacks can be detected using a variety of intrusion detection techniques. The intrusion detection technique was used to detect network privacy breaches and unauthorized access. Consider a situation in which a temperature sensor and a device containing sensitive data are both connected to the same network. If the sensor is compromised, it can gain access to sensitive files and leak them. It is natural for the user to insist that this sensitive device can only be accessed by trusted devices. However, determining a device's rogue status and the risk it poses to a network is neither natural nor simple, particularly for end-users. As a result, to provide an acceptable user experience, we must automate as much of the risk management process as possible while minimizing the need for user intervention. Thus, proposals to automate and secure home networks using intrusion detection systems (IDS) and intrusion prevention systems (IPS) have been proposed in both research, such as IoT-IDM, and commercial solutions [135]. Table. 6 summarizes some paper contributions to blockchain-based intrusion detection systems.

C. IoT DEVISES FIRMWARE UPDATES

When a device leaves the factory, it comes with the embedded firmware installed by default. This is the first version that

TABLE 6. Blockchain-based IDS.

Year	Paper	Contribution
2018	[139]	• A general architecture for integrating blockchains into collaborative intrusion detection networks (CIDNs). • Interconnected and federated learning systems improve the detection of malicious behavior by joining forces and pooling monitoring data to address the increasing time-to-detection of attacks.
2018	[140]	• Federated learning and blockchain technology integration. • Autoencoder for anomaly detection
2019	[141]	• CBSigIDS, a generic framework of collaborative blockchained signature-based IDSs. • CBSigIDS can provide a verifiable method in distributed architectures without the need for a trusted intermediary. • CBSigIDS can improve the robustness and effectiveness of signature-based intrusion detection systems in adversarial scenarios, according to the evaluation results.
2019	[142]	• A new collaborative intrusion detection (CID) approach using blockchain for multimicrogrid (MMG) systems in smart grids. • A proposal generation method that combines periodic and trigger patterns to generate a CID detection target.
2019	[143]	• Micro-Blockchain-based Geographical Dynamic Intrusion Detection (MBID). • Dynamically configured intrusion detection strategies for vehicles based on location variations. • A novel nested microblockchain structure was proposed. • A control plane was proposed for dynamically configuring IDS strategies within a micro-blockchain.
2020	[144]	• Intrusion detection system based on a multi-agent system, blockchain, and deep learning. • The system was divided into four modules: data collection, data management, analysis, and response. • The experiments showed that the system performs well in a variety of scenarios, including networks of varying complexity and attack types.
2021	[145]	• A deep blockchain framework (DBF) that used a bidirectional long short-term memory (BiLSTM) deep learning algorithm. • The framework has the potential to be used as a decision support system to help users and cloud providers securely migrate data in a reliable and timely manner.
2021	[146]	• A blockchained challenge-based CIDN framework that combines blockchain with a challenge-based trust mechanism. • The framework can assess a node's trustworthiness by analyzing the relationship between the sent challenges and received responses.
2021	[147]	• A blockchain-based federated forest software-defined networking (SDN)-enabled intrusion detection system (BFF-IDS). • The models were hosted on InterPlanetary File System (IPFS) to cope with the limited scalability of blockchain.

adds functionality to the device and allows it to communicate with other devices. If there is a vulnerability in the first version, a new firmware is required to protect the device from attacks. Every firmware should be written by an entity that can be outsourced, or the device vendor can do it in-house. The firmware author is in charge of correcting the error in the previous firmware and creating a new firmware to be sent to the devices. Security begins with the device itself, and to keep the device up to date, its firmware must be updated on a regular and secure basis. This will help to delay attackers' ability to gain control of the devices while patching loopholes or backdoors [136].

Even in the case of serious security flaws, it is uncommon for manufacturers to actively provide firmware updates for IoT devices. As a result, the installed firmware is frequently out of date; even when this occurs, users do not systematically update the firmware of the deployed devices. Users' interactions with IoT devices are limited and usually end after initial installation. Users do not change the device's default settings, including authentication credentials, and do not update the firmware because this is a difficult procedure for novice users. Furthermore, sophisticated security mechanisms have not been incorporated into devices.

Moreover, even large manufacturers do not build the devices from the ground up. The reuse of parts manufactured by unknown vendors who disregard basic security requirements is extremely common [123], [124]. During the CODEGATE sessions, it was said that most IoT device vulnerabilities are caused by vulnerable firmware, emphasizing the importance of firmware integrity and version management. Existing security solutions can only be applied to a limited extent owing to factors such as the low performance of IoT devices, and even if safe firmware is provided, security issues may arise due to attacks such as man-in-the-middle attacks and roll-back attacks [148].

Furthermore, with global IoT deployments, updating devices one by one can be a difficult task [10]. On IoT devices, over–the–air (OTA) firmware updates are common. Even if they are convenient, they are vulnerable to attacks because physical access is not required. Moreover, most frameworks use a centralized architecture to update a potentially large number of devices, which broadens the threat

landscape [149]. Centralized servers are like sitting ducks waiting to be picked off. The attackers are aware that everything that flows from a centralized server can be modified or stolen. This centralized point of control is susceptible to corruption and is vulnerable to a variety of attacks [136]. Several authors have recently proposed using blockchain technology to update software and firmware [150]. Initiatives such as GUITAR and REMOWARE enable real-time network and firmware updates, which are critical for ensuring the long-term security of IoT integration with blockchain [10]. The contributions of some studies on firmware updates are presented in Table. 7.

D. CONFIDENTIALITY

Data confidentiality demonstrates that only authorized entities can access and modify data. Because the data in IoT applications are linked to the physical realm, data confidentiality is critical in many use cases. In addition, data in IoT applications can be accessed not only by users but also by authorized objects. Thus, it is necessary to define an object authentication process [5]. IoT devices are now being deployed on a massive scale. In contrast to endpoint devices, IoT devices have limited resources, are incapable of securing and defending themselves, and are easily hacked and compromised [151]. The confidentiality of the information conveyed by the constraints is a concern for the selection criteria governing IoT device discovery. The use of blockchain technology and smart contracts to implement the overall deployment of the discovery process is a promising solution to this problem. However, owing to the blockchain's design, data within the blockchain are publicly accessible, and smart contracts cannot access data outside the blockchain. On the one hand, this benefits the discovery process through trust decentralization, transparency, and accountability. However, it has serious implications for privacy and confidentiality [152].

Zhou *et al.* [153] proposed a decentralized outsourcing computation (DOC) scheme in which servers perform fully homomorphic computations on encrypted data according to the data owner's request. The servers cannot obtain any plaintext data during this process, and dishonest servers can be detected by the data owner. The authors used the DOC scheme in the IoT scenario to create a BeeKeeper 2.0, a confidential blockchain-enabled IoT system. According to their tests for the BeeKeeper 2.0 system on Hyperledger Fabric and Hyperledger Caliper, the time consumed between the request stage and the recovery stage was no more than 3.3 seconds, which theoretically meets production requirements.

Rondanini *et al.* [152] investigated how to maintain data confidentiality during the discovery process of IoT devices on blockchain, even in the presence of an untrustworthy Oracle. The key concept was to implement the discovery process using smart contracts, with a blockchain network validating smart contract execution to ensure the correctness of the IoT discovery process. Because sensitive data (e.g., device profile and search requirements) are exposed during the evaluation process, the authors proposed homomorphic encryption schemes that support smart contract execution while maintaining the confidentiality of the sensitive data.

Gochhayat *et al.* [160] proposed Yugula, a novel lightweight decentralized encrypted cloud storage architecture that uses blockchain to maintain file confidentiality, eliminate centralized data deduplication, and increase file integrity. In particular, the authors discussed two approaches for file confidentiality with data deduplication: one employed double hashing and the other employed symmetric encryption. Abd El-Latif *et al.* [161] presented a new authentication and encryption protocol based on quantum-inspired quantum walks (QIQW). The proposed protocol was used to create a blockchain framework for secure data transmission between IoT devices. Instead of using classical cryptographic hash functions, quantum hash functions based on QIQW are used to connect chain blocks. The main benefits of the presented framework include assisting IoT nodes in effectively sharing their data with other nodes and having complete control over their records.

E. AUTHENTICATION

Self-organizing networks in the IoT field result in the engagement of various nodes for data communication. The increased number of IoT cyber-attacks poses a significant threat to these connected nodes, necessitating verification of data passing through nodes during communication [162]. Vulnerabilities in providing proper device authentication and data integrity in IoT networks have been demonstrated to have disastrous consequences [163]. Existing IoT device identity authentication relies heavily on an intermediary institution, namely a certificate authority (CA) server, which is vulnerable to a single-point-of-failure attack. Even worse, the critical data of authenticated devices can be tampered with by inner attacks without being detected [127]. This requires the development of an IoT data security architecture capable of accurately authenticating devices by anyone in the network in a decentralized manner and preventing unauthorized modification of stored data [163]. Table. 8 shows the contributions of some studies on IoT authentication using a blockchain.

F. ACCESS CONTROL

Securing access to IoT devices is a difficult task because IoT devices have limited processing, storage, battery life, and networking capacity, requiring a lightweight access control solution with low latency [174], [175]. Authentication, authorization, and auditing are the three components of a complete access control solution. Authentication determines a subject's true identity. Authorization determines whether the subject has the authority to perform operations on the object. Finally, auditing (or accountability) allows for the subsequent analysis of the system's realized activities. These components all play important roles in system security, but the authorization component deserves special attention because it is in charge of enforcing access rules. Some works in the field of access authorization use three well-known and

TABLE 7. IoT devices firmware update using Blockchain.

Year	Paper	Contributions
2016	[154]	• A new firmware update scheme that uses blockchain technology to securely check a firmware version, validate firmware correctness, and download the most up-to-date firmware for embedded devices. • The proposed scheme ensured that the firmware of the embedded device is up to date and is not tampered with. • To determine whether its firmware is up to date, the embedded device sends a firmware update request to nodes in a blockchain network and receives a response. Even if the firmware version is current, its integrity, that is, the correctness of firmware, is checked. • Known vulnerabilities in embedded device firmware are protected against attacks.
2018	[155]	• The framework aimed to provide secure verification of the firmware of the device manufacturer. • The integrity of the distributed firmware to the end device can be preserved. • The firmware update framework consists of four processes: creating a firmware update contract, creating a firmware replication contract, creating a direct firmware update mechanism, and creating an indirect firmware update mechanism.
2019	[148]	• A new firmware management architecture based on blockchains and the InterPlanetary File System (IPFS). • IPFS ensures the integrity of the firmware, whereas blockchain ensures the integrity of the IPFS URL. • By analyzing IoT device update logs, the firmware requestor manager can manage the devices.
2019	[150]	• Combining delta updates and blockchain technology for firmware updates. • The paper identified situations in which delta updates may fail and proposed a private blockchain network-based IoT device firmware integrity verification and update mechanism.
2019	[149]	• A blockchain framework with smart contracts to safeguard a firmware update process's integrity. • Hyperledger Fabric (blockchain), Chain code (smart contracts), and the Wemos D1 Mini board (ESP8266–based IoT device) were used in the proof-of-work framework. • Smart contract terms and conditions were preserved even when the system was under attack, such as denial of service (DoS) and man–in–the–middle (MitM) attacks.
2020	[156]	• A distributed firmware update architecture based on Software Updates for Internet of Things (SUIT) firmware update architecture and blockchain technology. • The firmware image files are stored in a distributed file system, and the hash values of firmware image chunks are stored alongside manifest files on the blockchain. • The architecture allowed for irreversible downloads even if the author was no longer present, and it was tolerant of a single point of failure.
2020	[157]	• The framework's goals were to provide a secure P2P verification mechanism for each new version of firmware released by the corresponding device manufacturer, as well as a reliable method to promptly distribute updated firmware to IoT devices. • The framework supports mutual authentication and defends against major cyber-attacks such as firmware modification, man-in-the-middle attacks, replay attacks, and impersonations.
2020	[158]	A blockchain-based framework for securely updating IoT device firmware using the LoRa communication protocol.
2021	[159]	• A firmware distribution method that provides incentives for distributors to help with distribution to reduce gas costs, using a smart contract and access control based on updated records. • By using access control instead of encryption, the additional computations performed by IoT devices and distributors' key management were reduced when compared to previous studies. • The gas cost per update was successfully lowered.

traditional architectures: XACML, OAuth, and UMA. However, all three architectures fail to provide essential IoT access control characteristics, such as user transparency, scalability, and resilience to wireless intermittent communications [176]. Standard authorization models support centralized access control. Nevertheless, traditional centralized access control methods struggle to support access control in today's large-scale IoT environment because of the unique characteristics of IoT devices, such as mobility, limited performance, and distributed deployment [177]. This may result in a single point of failure and scalability issues. The model also fails when a centralized entity is compromised. Moreover, the trusted entities have the ability to tamper with records without being held accountable. Such flaws in IoT design can be overcome using blockchain technology [174], [175]. Table. 9 introduces some research contributions to IoT access control using blockchain technology.

G. PRIVACY

IoT environments collect and generate massive amounts of sensitive personal data and reveal the behaviors and preferences of users, their activities, and their surroundings, which can reveal sensitive information and threaten their privacy. People's privacy is particularly at risk when such sensitive data are managed by centralized companies, which can illegitimately use these data. Edward Snowden's discoveries revealed that people's data stored by the Internet and telecommunications companies were used in a mass surveillance program known as the PRISM program [96]. As a result, user

TABLE 8. IoT authentication using Blockchain.

Year	Paper	Contribution	Features
2018	[164]	Secure Authentication Management human-centric Scheme (SAMS). SAMS is a blockchain-based authentication scheme for mobile devices.	• When new client nodes are added, the SAMS generates blocks based on the hash value of the master node in mobile resource management (MRM) and the hash value of the resource information in the subordinate client node, and then forms a blockchain by creating and connecting hash values and blocks. • To validate the SAMS for use with MRM, data falsification was tested by a malicious user who gained access to the SAMS, and the results showed that data falsification was impossible.
2018	[151]	A user authentication scheme based on blockchain-enabled fog nodes.	• Fog nodes were used to increase system scalability by relieving IoT devices of heavy computations involving tasks related to authentication and communication with the blockchain.
2018	[165]	A blockchain-based out-of-band two-factor authentication scheme for IoT devices.	• The experimental results showed that the CPU and memory overheads were well tolerated, given that they only occurred during the authentication phase. • The average memory usage for the BeagleBone Black and Raspberry Pi 3 nodes was 29.5M, with a CPU usage of 29.55 percent and 13.35 percent, respectively.
2018	[163]	A decentralized device authentication and data security guarantee.	• A hierarchical blockchain structure (blockchain of blockchains) to address resource issues in IoT. • Allowed the users of powerful cloud servers to mine to overcome the resource limitations of IoT devices and the heterogeneity of IoT networks.
2019	[166]	Two models for integrating blockchain and smart contract technology with the authorization framework of OAuth 2.0.	• Included features such as linking payments to authorization grants, immutably recording authorization information and policies in smart contracts, and providing resilience through smart contract code execution on all blockchain nodes.
2019	[162]	A nodal authentication approach in IoT, that uses a blockchain to ensure the integrity of data passing through IoT nodes.	• The GOST hash function was used to secure and validate the data content of IoT nodes. • The authors were able to perform nodal authentication and verify the transmitted data. This makes it extremely difficult for an attacker to impersonate a node in the communication chain of connected nodes.
2019	[167]	Authentication process carried out using the blockchain structure.	• The use of UDP protocol for communication because IoT devices prefer the UDP protocol instead of the IP protocol. • The message content was encrypted using the Vigenère Cipher encryption method, as unsafe UDP communication was considered.
2020	[168]	A blockchain-based multi-WSN authentication scheme for IoT.	• A blockchain network is built up of various types of nodes to form a hybrid blockchain model that includes both a local chain and a public chain. • According to their capability differences, IoT nodes are divided into base stations, cluster head nodes, and ordinary nodes, which form a hierarchical network. • Ordinary node identity authentication was accomplished using a local blockchain, and cluster head node identity authentication was accomplished using a public blockchain.
2020	[169]	A decentralized authentication and access control mechanism for lightweight IoT devices.	• It is based on fog computing technology and the concept of public blockchain. • The results of the experiments showed that the proposed mechanism outperforms a state-of-the-art blockchain-based authentication technique.
2020	[170]	A novel decentralized authentication of patients in a distributed hospital network using blockchain.	• A healthcare setting in their model included patients and allied health professionals (such as medical doctors, nurses, technicians, etc.) as well as patient health information. • The decentralized authentication of the proposed architecture among a distributed affiliated hospital network eliminates the need for re-authentication. • Significant impact on network throughput, overhead reduction, response time improvement, and energy consumption.
2021	[171]	A multi-server CE-IoT authentication protocol that combines Physical Unclonable Functions (PUFs) and the blockchain technique.	• Privacy-aware authentication protocol • A one-time physical identity and keyed-hash function double-encode the real correlations of challenge-response pairs (CRPs) into mapping correlations (MCs).
2021	[172]	SCAB-IoTA ensures IoT device identification and authentication, while also providing secure communication in an open environment.	• SCAB-IoTA uses a blockchain and a hybrid cryptosystem to improve IoT application security while reducing computational and storage overheads. • The hybrid cryptosystem used in SCAB-IoTA is a combination of Advanced Encryption Standard (AES) and Elliptic Curve Digital Signature Algorithm (ECDSA) cryptographic techniques. • The authors have developed a secure cluster of IoT devices based on angular distance (AD), allowing devices to communicate securely without interruption. • SCAB-IoTA was resistant to a wide range of cyberattacks, including impersonation, botnets, man-in-the-middle, and message replay attacks.
2021	[173]	• A distributed IoT architecture based on a blockchain that employs Hash Chains for secure key management. • Method for generating and managing secure and efficient keys for mutual authentication between communication entities.	• Employing a one-way hash chain technique to provide IoT devices with a set of public and private key pairs that can be verified at any time.

TABLE 9. IoT access control using Blockchain.

Year	Paper	Contribution	Features
2017	[176]	A Blockchain-based architecture for IoT access authorizations.	• The architecture is user-transparent, user-friendly, fully decentralized (no third-party required), scalable, and fault-tolerant. • It is compatible with a wide range of today's IoT access control models that require minor adaptation efforts. • The architecture includes a secure method for establishing relationships between users, devices, and groups of both. • It solved the problems of FairAccess [178] and traditional architectures by being completely decentralized.
2018	[179]	A decentralized data management system in which all data access permissions were enforced via smart contracts, and the audit trail of data access was stored in the blockchain.	Leveraging recent advancements in blockchain technology and trusted computing with Intel SGX, which is a component of a trusted execution environment (TEE) that ensures data security and privacy for sensitive parts of the application (code and data).
2018	[180]	A generic, scalable, and easy-to-manage access control system for IoT.	• Employing a specific design to avoid incorporating blockchain technology into IoT devices, which are largely constrained to support blockchain technology directly, making it easier for current IoT devices to adapt to their system. • The design was implemented in a single smart contract to simplify the entire process and reduce communication overhead between nodes.
2019	[174]	A distributed and trustworthy access control solution based on blockchain mechanisms.	• The use of Acl-smart contract mechanisms.
2019	[181]	A novel attribute-based access control scheme for IoT systems using blockchain.	• The access control process has also been optimized to meet the demands of IoT devices for high-efficiency and lightweight calculations. • The scheme can be implemented easily in IoT and can withstand multiple attacks.
2020	[182]	• An attribute-based access control scheme to address the issue of unauthorized access. • To detect malicious behavior and limit extra authorization for a specific group, a verifiable and controlled collaboration mechanism was used.	• The authors built authority nodes (Ans) for computation tasks and to query or invoke the Chaincode to make the scheme lightweight and suitable for IoT devices. • The access control scheme can efficiently guarantee authorized access by resisting various attacks and providing a revocation and supervision function
2020	[183]	• A data sharing and access control system based on blockchain for IoT device communication. • It was intended to address trust and authentication issues in IoT networks for access control. • The system's goals are to achieve trustworthiness, authorization, and authentication in IoT networks for data sharing.	• To provide efficient access control management, smart contracts such as Access Control Contract (ACC), Register Contract (RC), and Judge Contract (JC) were used. • ACC managed the overall access control of the system, whereas RC was used to authenticate users in the system, and JC implemented a behavior-judging method for detecting a subject's misbehavior.
2020	[177]	• fabric-iot, an IoT access control system based on the Hyperledger Fabric blockchain framework and attributed-based access control (ABAC).	• Fabric-iot can manage IoT access control in a decentralized, fine-grained, and dynamic manner. • There are three types of smart contracts in the system: device contracts (DC), policy contracts (PC), and access contracts (AC). • DC includes a method for storing the URL of device-generated resource data and querying it. The PC can be used by administrators to manage the ABAC policies. AC is the core program used to implement an access control method for normal users.
2021	[184]	• A novel access control framework based on a consortium blockchain for 5G-enabled Industrial IoT (IIoT). • A two-step credit-based Raft consensus mechanism capable of dynamically selecting orderer nodes based on historical behavior records stored in the ledger in order to achieve a fast and reliable consensus.	• The use of three types of Chaincodes: Policy Management Chaincode (PMC), Access Control Chaincode (ACC), and Credit Evaluation Chaincode (CEC). • To implement access control policy management and authorization, the PMC and ACC were deployed on the same data channel. The CEC was deployed on a different channel and was used to add IIoT device behavior records and calculate the credit value of the IIoT domain.
2021	[185]	A multi-agent system to provide lightweight, decentralized IoT access control security mechanisms.	• Blockchain Managers (BCMs) provide access control and secure communication between local IoT devices, fog nodes, core fog nodes, and cloud computing.
2021	[186]	IoT-CCAC, a decentralized capability-based access control architecture designed for IoT consortium networks.	• IoT-CCAC is a secure, scalable, and cost-effective solution that meets the needs of enterprises and businesses, and is adaptable to various IoT interoperability scenarios. • The IoT-CCAC approach produced promising results and was well suited for city and business network applications.
2021	[187]	• SIApps' ledger (SILedger), a decentralized open-trusted access control mechanism based on blockchain and attribute-based encryption (ABE). • The main idea is that SIApps are authorized with ABE-encrypted access tokens, which are then distributed as blockchain currencies.	• Redesign blockchain transaction, token initialization, token encryption, and token update schemes to achieve cross-domain, fine-grained, and flexible permission management for SIApps. • To address the delay and complexity issues associated with blockchain and ABE, the authors developed an access control framework that separates authorization from the call process of SIApps. • The proposed access control mechanism can provide effective access control for SDN-IoT applications (SIApps) with negligible overhead.

data collected and handled by IoT-based applications must be exploited and secured appropriately to protect personal data and user privacy [28].

Privacy determines the rules governing how individuals' data can be accessed. This is a real issue that has the potential to stifle the advancement of IoT. The absence of appropriate mechanisms to ensure the privacy of personal and/or sensitive information limits the adoption of IoT technology. The main reason for requiring privacy in IoT is that IoT is expected to be used in critical applications such as healthcare. Furthermore, the use of wireless channels, which expose the system to attack and eavesdropping due to remote access capabilities, increases the risk of violation. Whereas traditional Internet privacy concerns stem primarily from Internet users (individuals who actively participate), IoT privacy concerns stem from people who do not use IoT services. Therefore, individuals must be able to determine which of their personal data can be collected, by whom, and when. Furthermore, the collected data should only be used to support services authorized by accredited service providers [5]. Furthermore, a citizen must be able to refuse any data-sharing request that he or she finds objectionable. Finally, a user must have the ability to stop a data stream at any time [134]. The contributions of several studies on IoT privacy using blockchain are summarized in Table. 10.

H. TRUST

The true potential of IoT will be realized when billions of devices are connected to the Internet and are able to interact with each other. While more devices are becoming connected, the grand vision of IoT is still far from being realized because these devices do not communicate with one another because of a lack of trust between devices, which is required for secure communication [138]. Trust is a multifaceted concept that is applied in a variety of contexts. It is regarded as a critical IoT concept owing to the dynamic and fully distributed nature of IoT, which makes dealing with trust challenges extremely difficult [5]. An IoT device can act as a service provider and service requester. A service requester wants to find and trust the best service provider. Malicious providers can deliver poor information and services that put the systems at risk [128], [138]. While maintaining service delivery, a mechanism is required to establish trust among IoT devices and distinguish trustworthy devices from malicious ones. A trusted IoT environment ensures that only authenticated and authorized devices can participate in the IoT network's activities [21]. The central component of a trust management framework is trust evaluation. Several methods have been used to assess the level of confidence in distributed networks. They are divided into two types: direct and indirect trust. Direct trust methods rely on direct data observations to generate a trust score, whereas indirect trust methods rely on reputation and recommendations from other nodes [128].

Indeed, the traditional PKI trust model, which is based on a common root of trust, works well for the Internet but it does not fit the scale and heterogeneity of IoT, in which there is no common root of trust and constrained devices belong to separate administrative domains [128], [138], [138]. It is critical to verify the identities and ensure that the transactions are digitally signed by the correct device. Furthermore, in a trusted IoT environment, initial authentication should not be used as a permanent indicator of trust. While current trust models can aid in the detection of abnormal behavior, they fail to validate the integrity of observations and recommendations (past and new) and identity (source of recommendation). A blockchain-based approach is recommended to address these limitations. Trust and reputation models are methods for achieving trust in IoT environments. Typical trust and reputation models employ machine learning or anomaly detection techniques to detect malicious nodes in a network [21].

Blockchain is a promising technology for establishing trust in IoT networks, where network nodes may or may not trust each other. Because of cryptographic hash links and distributed consensus mechanisms, data stored on a blockchain cannot be changed or deleted [13]. Any transaction that takes place between two devices is recorded in the ledger and cannot be changed or forged. Therefore, all transactions are securely stored and have an immutable history, preventing adversaries from influencing trust evaluations of IoT devices by modifying previous transactions. As a result, unauthorized data access or operations on previously saved data can be detected. Transaction data are accessible to authorized devices at all times. Smart contracts are also used to impose specific access control mechanisms on stored data [11], [21]. In an IoT trust model based on blockchain, a transaction can refer to the exchange of information or an update between two network participants [21]. Table. 11 shows the details of the research on IoT trust using blockchain.

I. REPUTATION

Reputation is a measure of how much the community trusts you, which is based on previous interactions and transactions. The greater your reputation, the more trustworthy you are perceived to be in the network. Users choose to behave more honestly on the network when their reputation is at stake. Although successful reputation systems have been implemented, they are all based on a centralized server model, making them unsuitable for use in P2P networks such as IoT. Regardless of how they are deployed or what type of network they are deployed over, all reputation systems face the same fundamental issues. The ability to associate an identity with a single user and prevent the user from obtaining multiple identities is critical in preventing a user from abusing the system by creating multiple identities and transacting between them. Another unresolved limitation shared by all reputation systems is the quantification of reputation. Furthermore, how can we be certain that a user's reputation is correct and based on a real transaction? [196].

Although the number of published papers in this field is limited, it is becoming more common to investigate how blockchain technology can be leveraged for these trust and reputation systems. While P2P reputation systems existed

TABLE 10. IoT privacy using Blockchain.

Year	Paper	Contributions	Features
2018	[134]	A privacy-preserving and efficient data aggregation scheme.	• In this scheme, the users are divided into groups. Each group has its own private blockchain, and each user has multiple accounts (multiple pseudonyms). • A Bloom filter was used for quick authentication.
2019	[188]	Hermes, an open marketplace that allows users to sell their data simply and anonymously.	• It serves as a proxy and a means of resolving disputes between a buyer and seller. • Users reserve the right to stop data broadcasting at any time.
2019	[28]	An end-to-end privacy-preserving framework for IoT data.	• Smart contracts were used to allow the framework to express privacy-preserving policies. • By encrypting the shared data, these files can only be accessed by invoking functions defined on the blockchain's hosted smart contract.
2019	[189]	A novel blockchain-based IoT model was proposed to improve the security and privacy of the current IoT-based remote patient monitoring system.	• The model used the ARX encryption scheme, which is a more advanced and lightweight cryptographic technique. • The authors introduced the concept of Ring Signatures, which offered Signers Anonymity and Signature Correctness privacy properties. • A double-encryption scheme was used. • They applied the Diffie-Hellman key exchange technique to their blockchain-based network to protect their public key from an intruder.
2019	[190]	SecureSVM, a novel privacy-preserving SVM training scheme.	A homomorphic cryptosystem Paillier was used to construct an efficient and accurate privacy-preserving SVM training algorithm.
2020	[191]	Using a secure data transmission mechanism for IoT devices in a distributed architecture.	The proposed solution enabled IoT-based skin surveillance systems to privately and securely store and share medical data over the network without causing disruption.
2021	[192]	A novel privacy-preserving IoT device management framework.	Smart contracts can detect devices that have vulnerabilities, have been hacked, or pose a threat to the IoT network immediately.
2021	[193]	An IoT-aided smart grid system integrated with blockchain to provide an immutable transaction record that is always shared and transparent to all system participants.	To verify and maintain participant privacy, each participant used cryptographic pseudonyms to interact with the smart grid supply chain without revealing personal identities or important private information to malicious entities in the system.
2021	[171]	A privacy-aware authentication protocol for multi-server CE-IoT systems that combines Physical Unclonable Functions (PUFs) and the blockchain technique.	The blockchain was used to securely share physical identities by storing mapping correlations (MCs), efficiently synchronizing them, and incorporating multi-receiver encryption.
2021	[194]	The PPSC-BCAI framework is a privacy-preserving framework that uses blockchain smart contracts and artificial intelligence.	Extreme gradient boosting (XGBoost) was used to analyze data transactions and sharing.
2021	[195]	A Privacy-Preserving and Secure Framework (PPSF) for IoT-driven smart cities.	• A blockchain module was used to securely transmit IoT data, and the Principal Component Analysis (PCA) technique was used to transform raw IoT data into a new shape. • A two-level privacy scheme was trained and evaluated using a Gradient Boosting Anomaly Detector (GBAD).

long before blockchain technology, the first blockchain-based trust and reputation system was created in 2015, six years after the Bitcoin paper was published. Other decentralized reputation systems were proposed to retrieve information on another participant's reputation from online participants. Those solutions required some identities to be assigned to the participants, which were also required to be online for the protocols to work [135]. Table. 12 summarizes studies on IoT reputation using blockchain.

VII. CHALLENGES AND TRENDS

The numerous advantages provided by blockchain technology make it an appealing solution for addressing the aforementioned IoT problems. However, because most existing blockchain schemes are not dedicated to the IoT ecosystem, they are unable to meet the specific requirements of the IoT [98]. IoT environments are resource-constrained with limited capabilities in terms of computation, storage, and energy, which discourages the use of blockchain. Blockchain

has high computational complexity, limited scalability, high bandwidth overhead, and latency, which are unsuitable for IoT [99]. It is worth noting that there are still a large number of research challenges and open issues that must be studied to use these two technologies seamlessly together [4], [10]. Integrating blockchain into the IoT service architecture may result in the following shortcomings.

A. THROUGHPUT

A blockchain's throughput is defined as the number of transactions that can be stored in the blockchain per second. The throughput of traditional blockchain instantiations is low. For example, Bitcoin can handle approximately seven transactions per second (TPS), whereas Ethereum (the PoW version) executes approximately 20 TPS. These are considered extremely low throughputs and longer delays for most business applications, not to mention the requirement to handle billions of transactions as in IoT [12]. Furthermore, Bitcoin takes an average of 10 min to add a new block to the chain, with a maximum of seven TPSs. When compared to the VISA system, this figure is extremely low (dozens of thousands). Because of the low number of transactions per second, the delay can be significant (hours or days for a single payment). If these issues are not resolved, cryptocurrency will become obsolete [4]. However, because of the extensive interactions between various entities, the number of transactions in the IoT ecosystem far exceeds these limits, which exaggerates the problem [12].

B. LATENCY

There is a significant delay in ensuring that a transaction is confirmed by the blockchain nodes. For example, a transaction in Bitcoin can take up to 30 min to be confirmed [12]. Bitcoin-NG [197] proposed a new Byzantine fault-tolerant blockchain protocol that reduces the consensus latency of Bitcoin. Litecoin [198] is technically identical to Bitcoin, but it has faster transaction confirmation times and better storage efficiency owing to a shorter block generation time and a proof of work based on scrypt, which is a memory-intensive password-based key derivation function. Another suggestion is to reduce the propagation delay in the Bitcoin protocol, but this may jeopardize network security [10]. BigchainDB [199], [70] extended a big data distributed database with blockchain features. BigchainDB combines the low latency and high throughput characteristics of big data distributed databases with the decentralized and immutable nature of the blockchain system [10]. Most IoT applications have stricter delay requirements; for example, a service provider in a smart home needs to provide real-time services to the user; thus, it should not wait for several minutes for the data to be processed when requesting data from a smart home sensor [12]. As a result, blockchain technology has a reputation for being so sluggish that it is unsuitable for time-sensitive applications [200].

C. TRANSACTION FEE

Another significant shortcoming is the concept of a transaction fee for all transactions, regardless of the value. Transaction fees are typically calculated based on the amount of gas consumed during a transaction. This makes it inefficient for scenarios involving microtransactions, such as IoT. Transactions involving a small payment can also take several days to be authorized. Some blockchain platforms try to solve this issue; for example, DAG offers a free-less architecture [60].

D. COMPLEX CONSENSUS ALGORITHMS

Most blockchain consensus algorithms require substantial resources from participating nodes, which are far beyond the capabilities of most IoT devices [12]. PoW, the first consensus algorithm used in public blockchain networks, is computationally expensive. Despite the efforts to integrate blockchain full nodes into IoT devices, mining continues to be a significant challenge in IoT owing to its limitations. Recent advances in the development of ''light clients'' for blockchain platforms have enabled nodes to issue transactions in the blockchain network without downloading the entire blockchain. Nonetheless, a single blockchain solution would be insufficient to secure the IoT edge [201]. Furthermore, many blockchains do not yet support lightweight nodes, such as Ethereum, in which lightweight nodes are still in the development stage. Another solution to this issue is to allow for the inclusion of IoT devices, and the consensus protocol could be relaxed; however, this could threaten the security of blockchain implementation [10].

The IoT is primarily made up of resource-constrained devices, but the IoT as a whole has the potential for massive processing power, given that the number of devices is expected to grow over time, as previously stated. To adapt to the consensus in IoT, research efforts should be directed toward this field to leverage the distributed nature and global potential of IoT. These tasks are typically assigned to gateways or other unrestricted devices capable of providing this functionality. Off-chain solutions, which move data outside the blockchain to reduce latency, can also provide functionality [10]. Section III of this paper discussed some research on IoT consensus algorithms.

E. LEGAL ISSUES

The data privacy regulations or laws of a country, such as the data protection directive, have an impact on the IoT domain. The majority of these laws are becoming obsolete and must be revised, particularly as new disruptive technologies such as blockchain emerge. In this regard, laws governing information handling and privacy remain a significant challenge in IoT and will become even more critical when combined with blockchain. The adoption of new laws and standards can make it easier to certify device security features, assisting in the development of the most secure and trusted IoT network. The lack of regulations creates disadvantages because

mechanisms for retrieving or resetting private keys, as well as transaction reversion, are not possible. Some IoT applications envisage a global, unique blockchain for devices, but it is unclear whether this type of network will be managed by manufacturers or open to users. Legal regulations are expected to be necessary. These regulations will have an impact on the future of blockchain and IoT, potentially disrupting the decentralized and free nature of blockchain by introducing a controlling, centralized participant, such as a country [10].

F. REDUNDANCY AND COST

Maintaining a copy of every transaction with every network peer is both costly and redundant. One of the primary benefits of blockchain is the elimination of intermediaries and the introduction of a self-governance model involving only participants. Surprisingly, the elimination of intermediaries resulted in the establishment of a highly redundant network. Furthermore, due to legislative requirements, the role of third parties, whether financial, legal, or regulatory, continues to exist. This redundancy entails additional costs for no comparable benefits. DAG addresses this issue by incorporating the knot concept [60].

G. SECURITY

1) ATTACKS ON THE BLOCKCHAIN

The majority attack, also known as the *51% attack*, is the most common attack on blockchain. This attack is possible if a blockchain participant controls more than 51% of the mining power. The rise and rapid evolution of mining pools (with GHash.io4 briefly holding 51% of Bitcoin mining power in 2014) has increased the likelihood of this attack, which could jeopardize Bitcoin's integrity [202]. A *double-spending attack* entails spending the same coin twice. The confirmation time varies greatly because it is affected by numerous factors. The trader cannot afford to wait in a fast-payment scenario. As a result, a double-spending attack is possible in these scenarios. *Race attacks* can also occur in these scenarios. The *Finney attack* is a more sophisticated double-spend attack because it requires the participation of a miner. The well-known attacks, *Sybil, DoS*, and *Man in the Middle (MitM) attacks*, rely heavily on communication; thus, most P2P protocols and IoT infrastructures are vulnerable to these types of attacks. There is also an *eclipse attack*, in which attackers can monopolize a node's connections, isolating it from the rest of the network, and changing the node's view of the network. Furthermore, owing to the computing power of these computers, *quantum computing* could be viewed as a threat to Bitcoin, compromising the security of digital signatures. Moreover, technology evolves, and new bugs and security flaws are discovered daily. Because blockchain data are immutable, these enhancements and bugs may jeopardize public blockchains with encrypted data [10].

2) ANONYMITY

Blockchain pseudonyms, which are responsible for transaction anonymity, are rendered insufficient because of their ability to de-anonymize participants. Because the blockchain is public, the identities of users in the blockchain network can be revealed through traffic flow analysis or by inspecting the ledger itself. Several de-anonymization techniques are presented, including address changes, multiple inputs, IP associations, and the use of centralized services. All these methods involve disclosing users' identities by revealing the ownership of input addresses, connecting multiple addresses owned by the same participant, associating IP addresses by analyzing traffic patterns, or utilizing a centralized entity for service administration [16]. As a result, pseudonymity was insufficient to ensure complete anonymity. Future research should focus on solutions that reduce the likelihood of IoT devices being linked to their owners [96]. Zerocash [203] and Zerocoin [204] are popular attempts to address the anonymity problem in Bitcoin, proposing that Bitcoin extensions have completely anonymous transactions that conceal the sender, receiver, and information itself. Monero [205] employs ring signatures to make transactions untraceable, so they cannot be easily traced back to a specific person or computer.

3) PRIVACY

The Bitcoin protocol is not intended to protect user privacy. Transparency is a key feature of Bitcoin. Each blockchain transaction can be checked, audited, and traced back to the system's first transaction. This is an unprecedented new level of transparency that will undoubtedly contribute to the development of trust. Despite the fact that there is no direct link between wallets and individuals, user anonymity appears to be jeopardized, despite Bitcoin's mechanisms such as pseudonyms and the use of multiple wallets [10].

Because private blockchains, by definition, must provide authentication and authorization mechanisms, the problem of privacy can be tackled in different ways. Quorum [206], for example, is a private permissioned Ethereum blockchain that uses cryptography to limit sensitive data visibility and segmentation to increase data privacy. Rockchain [207] is also based on Ethereum and it takes a data-centric approach, allowing public calculations to be performed on private data and accumulative results to be obtained while maintaining data privacy. This method offers a distributed file system that enables users to manage data privacy using Ethereum smart contracts. In Multichain [59], user permissions are used to restrict visibility, introduce controls over which transactions are permitted and which users are permitted to mine. To provide privacy control on blockchain networks, Hyperledger Fabric [51] provides access control lists and identity control services via private channels, allowing users to control and limit access to their shared information in the network [10].

Off-chain [208] solution is another method for dealing with data privacy, in which sensitive data are stored

TABLE 11. IoT trust using Blockchain.

Paper	Year	Outcomes	Applied in	Tools	Features	Defense against	Evaluation Metrics	Implementation	Blockchain type
[137]	2017	• Trust Model (BARS). • Reputation Evaluation Algorithm.	Vehicular ad-hoc networks	Python	Three Blockchain • MesBC • CerBC • RevBC	Distribution of forged messages	• Storage overhead. • Time consumption	Yes	Not specified
[15]	2017	• Security model • Block validity check algorithm (in miners) • Formulas for determining the reputation of nodes over time.	Not mentioned	Permissionless Blockchain	Humanlike Knowledge-based Trust (HKT) for trust management	Not mentioned	The change of reputation level for Network Node (NN) with time.	No	Permissionless
[21]	2018	Trust model against sybil attack	Not mentioned	• Hyperledger Fabric. • Docker containers • Apache CouchDB (Chain State)	• The validity of the model ex, easy, medium, strict. • Single-channel	Sybil attack	Packet Delivery Rate (PDR) as an indication of trust score	Yes (Proof of concept)	Permissioned
[94]	2018	Dynamic decentralized IoT trust model	Not mentioned	• Hyperledger fabric • Hyperledger Composer. • Docker containers • Apache CouchDB • Distributed PNNs	• The validity of the model ex, easy, medium, strict. • Single Channel • Distributed Probabilistic Neural Networks (PNNs)	• Sybil attack • Message replay attack • Wormhole attack • Bad-mouthing attack • Good mouthing attack	Packet Delivery Rate (PDR) as an indication of trust score	Yes (Proof of concept)	Permissioned
[138]	2018	• A distributed trust mechanism. • A new tool (blockchain) called the Obligation Chain.	A small coffee shop provides WIFI services for an additional fee	• Obligation Chain • SigningKey, SECP256k1, and VerifyingKey • Python functions from the ecdsa library.	• Obligation Chain. • A built-in reputation mechanism. • Trust between the users and their mobile operators.	• Ballot stuffing attacks. • Sybil attacks. • Reputation attacks, such as rating fraud.	• The time required for service providers (SPs) to compute service consumers (SCs) reputations • Acceptance delay	Yes	Not specified
[93]	2018	Trust List	A practical deployment scenario	• Public and private Ethereum blockchains • Solidity. • Ryu • OpenFlow • Open v Switch	Integrates blockchains and SDN	DDoS attack	• The difficulty of Mining Blocks. • Time Duration for Delivery of Trust List. • Cost of Executing Transaction over Blockchain.	Yes (Proof of concept)	Permissioned and permissionless
[22]	2018	• A distributive trust management scheme for VANET (DTCMV) • Algorithm for Block Validation	Vehicular ad-hoc networks	• Clustering Mechanism • fuzzy logic for making the decision	Scheme for VANET security based on blockchains, Clustering, and fuzzy logic	Attack on message integrity	The credibility of messages based on a reputation value	No	Not specified
[19]	2018	Trust Bit (TB), a reward-based intelligent vehicle communication using Blockchain technology.	Intelligent vehicle (IV)	• Use case on IV communication Intersection scenario	• TB Helps to detect the history of IV. • It also provides fast and secure communication between IVs.	• Message authentication • Message Integrity • Access Control • Message Confidentiality • Privacy • Liability Identification.	• Message transmission time • Receiving time	No	Not specified
[1]	2018	An original decentralized authentication system (Bubble of Trust)	Scenario for: • Smart house • Waste management • Smart factory • Smart road radar	• C++ language. • Ethereum public blockchain. • Solidity language for smart contract. • TestRPC Ethereum.	• An original solution which creates secured virtual zones called bubble of trust	• Sybil attack • Spoofing attack • Message replay attack • Message substitution attack • DoS/DDoS attack	• Average and Standard Deviation of Time Consumption. • Assoc time (ms) • Data msg time (ms) • Average and Standard Deviation of Energy Consumption: • CPU pow assoc (mWatt) • CPU pow data msg (mWatt) • NIC pow assoc (mWatt) • NIC pow data msg (mWatt) • Financial cost	Yes	Permissionless
[11]	2019	• A behavior monitor system. • Using Trusted Execution Technology (Intel SGX) as the root of trust in a local blockchain.	Smart Home	• Deep Autoencoder • A real-time dataset. • tensor flow and Keras libraries in Python language for training and optimization. • Hyperledger Fabric.	• Analyzing and classifying the behavior of IoT devices as normal or malicious using a deep learning strategy (auto-encoders).	• Mirai Attack	• Average Detection time. • accuracy ○ TPR (True Positive Rate) ○ FPR (False Positive Rate)	Yes	Permissioned
[12]	2019	• A Lightweight Scalable blockchain (LSB) • IoT-friendly consensus algorithm (DTC).	Smart home	• NS3	• Change the reward mechanism by generating a valid block gains reputation or the allowance of placing advertisements	• DOS • DDOS • Dropping attack • Blockchain	• Latency • Processing time • Resilience against cyber-	Yes	Not specified

TABLE 11. *(Continued.)* **IoT trust using Blockchain.**

		• Distributed Throughput Management (DTM).				• modification • Compromising time interval • Compromising the waiting time period • Sybil attack • Consensus period attack	attacks.		
[13]	2019	• A trusted layered architecture. • A customized private blockchain architecture.	A smart construction environment	• NS3 network simulator. • Custom private blockchain	• Custom private blockchain • A two-tiered IoT to overcome the constraints of IoT resources	• Malicious sensor nodes • Malicious gateways • Colluding blockchain nodes • Impersonation	• Latencies • Response to attack	Yes	permissioned
[18]	2019	A novel trust management system.	Manufacturing zones in a factory environment.	• NS3 simulation • Multichain	• The use of OpenID Connect (OIDC)	• Bad Mouthing attack • Ballot Stuffing attack • On-off attack	• Average response time • Number of established transactions • Computation power	Yes	Permissioned
[135]	2019	STewARD, SDN and blockchain-based trust evaluation platform for automated risk management of IoT devices.	Smart home	• Multichain	• SDN and blockchain-based trust evaluation. • Automated risk management using the analyzer. • The STewARD can determine whether a new and unknown device can cause harm on a network.	• DDoS attack	• Trust assessment	Yes	Permissioned
[209]	2019	IoT passport Framework	Smart home.	• Use case	• Cross-platform collaboration • Trust-Based Collaboration. • Hierarchical Trust • Synchronization and Collaborative IoT Services	• Not mentioned	-	No	Not specified
[210]	2019	A blockchain trust model (BTM)	WSN	• Truffle to develop and build smart contract • JavaScript using web3.js. • Ganache-cli, a private-chain local simulation tool • NPM	• Malicious node detection in WSNs. • Ensure the traceability of the detection process.	• Malicious node detection	• Security Analysis. • Reliability Analysis • Traceability Analysis	Yes	Not specified
[2]	2020	• A Blockchain Approach for Negotiating Trust in IoT. • Algorithm for establishing trust between IoT devices.	Not mentioned	• Hyperledger Fabric blockchain • Composer Playground	• Algorithm for establishing trust between IoT devices	• Not mentioned	• Querying average speed • Minimum speed for querying the data • Maximum speed for querying the data	Yes	Permissioned
[211]	2020	• A Sybil-resistant scalable blockchain (TrustChain)	Not mentioned	Python	• TrustChain is capable of creating trusted transactions among strangers without central control. • Offers scalability and openness • Replacing proof-of-work with a mechanism to establish the validity and integrity of transactions. • TrustChain includes a novel Sybil-resistant algorithm named NetFlow	• Sybil attack	• Transaction throughput. • Computational time Complexity of NetFlow.	Yes	Permissionless
[92]	2020	• A secure behavior modeling for IoT networks using Blockchain. • Store and monitor IoT devices data and classify its behavior (normal or malicious) to prevent attacks.	Smart home	• TensorFlow and Keras libraries in Python language. • Auto-encoder • Hyperledger Fabric	• A deep learning strategy (auto-encoders) that outperforms on all of the chosen devices in terms of False-positive, True-positive, and detection time. • Incorporating Trusted Execution technology (TEE) as a root-of-trust.	• Mirai attack	• Accuracy • Time required for detection.	Yes (Proof of concept)	Permissioned
[212]	2020	An energy-efficient decentralized trust mechanism for detecting internal attacks in sensor node-powered IoT using a blockchain-based multi-mobile code-driven solution.	WSN	• Ethereum • Ganache and BLOCKBENCH emulator. • Truffle suite and Remix emulators • Atom • JavaScript (Nodejs) and Solidity	• Test-bed experiment • There are five nodes in total, one of which is the fog node, one is the actuator, and the rest are normal SNs. • One additional node is a malicious node.	• Blackhole attack • Grey hole attack	• Message overhead • Malicious node detection time	Yes	Permissionless

outside the chain. However, these off-chain sources must be fault-tolerant and avoid bottlenecks or single points of failure [10]. Furthermore, data privacy laws, such as the EU's data protection directives, need to be updated to reflect the new models enabled by this technology. The use of blockchain as a legal platform should address these regulations to ensure data privacy in accordance with the law [201].

4) INTEGRITY

When the reliability, accuracy, and consistency of network transactions are jeopardized, integrity issues arise in the blockchain. Despite being vulnerable to other attacks on integrity, such as selfish mining attacks, history-revision attacks, and stubborn mining attacks, these are minor attacks. The most notable attack on integrity is the misbehavior of a dishonest miner who may have high processing capacity

TABLE 12. IoT reputation using Blockchain.

Year	Paper	Contributions	Features
2018	[213]	• A blockchain-based anonymous reputation system (BARS). • A trust model was created to improve message trustworthiness by relying on the sender's reputation based on both direct historical interactions and indirect opinions about the sender.	• BARS was used in vehicular networks to establish trust and to break the link between real identities and public keys. • The reputation of each vehicle was gradually built up as transactions generated by the vehicle were verified by other participating nodes. • The participating nodes accept transactions generated by the more reputable nodes. • BARS is capable of establishing distributed trust management while protecting vehicle privacy.
2018	[214]	• A reputation-based data sharing scheme. • This reputation scheme is based on a three-weight subjective logic model that considers event timeliness, interaction frequency, and trajectory similarity.	• This scheme can achieve precise reputation management for high-quality vehicle data sharing. During VECON sharing, vehicles can select the best data providers with high-quality data • According to the security analysis, the proposed system ensured the security of data storage and sharing. • The proposed three-weight subjective logic scheme outperformed traditional reputation schemes in terms of improving the detection rate of abnormal vehicles and ensuring security during data sharing.
2019	[215]	• A blockchain-based decentralized reputation system for fog nodes. • A revised reputation score computation technique that combines client feedback with an assessment of the client's opinion about previous interactions with public fog nodes.	• To enable decentralized trustworthy service provisioning between IoT devices and public fog nodes, the proposed trust model used the public Ethereum blockchain and smart contract technologies. • The implemented solution was broad enough to account for any changes in the evaluated metrics and is applicable to a wide range of domains. • The solution was optimized to ensure the lowest possible cost, and it was tested using solidity on the Remix IDE. • The credibility of the raters was also considered to ensure honest feedback from IoT devices.
2020	[216]	• A reputation model that focuses on increasing an agent's reputation capital in multiagent systems. • An algorithm capable of grouping agents in IoT environments based on reputation capital. • The use of blockchain technology to certify reputation capital in order to disseminate trustworthy and certified information about device/agent reputation in a distributed environment.	• The model can detect almost all misleading agents if their percentage is less than a certain threshold. • Good results were obtained in terms of the group composition. • Malicious devices always paid significantly more for services than honest ones.
2020	[217]	• Reputation Capital model. • An algorithm to form agent groups in each IoT federated domain based on the reputation capital of each agent.	• Adopting blockchain technology to certify the reputation capital of each agent in each federated environment. • The proposed approach can benefit the individual reputation capital of devices and, as a result, the overall reputation capital of the IoT community. • Under certain conditions, almost all deceptive agents can be detected. • Using their reputation model, malicious actors always paid significantly more for services than honest devices.
2020	[218]	• A reputation system for intelligent transportation systems. • The ultimate goal of the proposed system is to provide users with an optimal travel route based on reliable data while maintaining confidentiality.	• Only encrypted communication takes place between the vehicles and the central server, and the consensus process is carried out between all vehicles in the same cluster or geographical area. • The output of the consensus algorithm is the validation or invalidation of road events, as well as the updating of participants' reputations. • After a certain threshold, the system also considered the aging process of the road data.
2021	[219]	• An architecture for managing end-device reputation values in an IoT system based on their location. • To reduce the spatial computation complexity in smart contracts, geographic data are geocoded using one of two spatial indexing techniques known as Geohash or S2. • A compression algorithm for geocoded data was suggested.	• The proposed architecture adhered to the cloud-fog-edge concept by incorporating an intermediate layer known as a fog layer to avoid a heavy workload of the system in the cloud layer. • The location-based component of the system was implemented by storing geographical areas in Ethereum Smart Contracts and subjecting reputation values to different regions based on the geographical location of the device. • IoT devices can function as blockchain nodes. • By querying through the fog layer, they were also able to discover service providers in an area and obtain their reputation values. • Geohash performed better inside the developed smart contracts, whereas S2 encoded the data much faster outside the smart contracts. • The proposed geocoded data compression algorithm reduced the size of the data significantly, but it was computationally more demanding in the developed smart contracts.
2021	[220]	• A distributed reputation system to simulate real-world trust in blockchain-based P2P energy trading. • A fairness indicator that captures the average reputation-based benefits and costs when considering reputation as a contribution to the P2P energy trading market.	• The actions of participants such as consensus nodes, energy buyers, and energy sellers determine the reputation scores. • Helped in the implementation of a blockchain delegated consensus algorithm and a reputation-based [Math Processing Error] k-double auction matchmaking scheme for P2P energy trading. • The numerical results of simulating the entire system showed how distributed reputation improved blockchain efficiency and balanced fairness indicators between sellers and buyers during peer-to-peer energy trading.

ratios in the blockchain network. They may cause blockchain forks, making distributed consensus difficult to achieve, resulting in the loss of some historical data. Furthermore, they have the potential to contaminate blockchain with invalid data or transactions [16], [96]. The integrity of PoW is limited by the number of honest miners; therefore, research on the mitigation of these issues is required [16]. Rather than creating a new blockchain from scratch, it is preferable to build

distributed IoT applications on top of Bitcoin or another secure and stable blockchain, as suggested by [96]. This is possible by employing a layered architecture, such as that proposed by Blockstack. The additional functionalities of the application are defined in another layer on top of the blockchain in this solution. Furthermore, because the blockchain is hidden at the application level, low-power IoT devices are not required to compute the PoW [96].

5) RELIABILITY

The growing number of attacks on IoT networks, as well as the serious consequences of these attacks, highlight the importance of designing an IoT with more sophisticated security. Many experts believe that blockchain technology is critical for improving IoT security. However, the dependability of IoT data is a major challenge in integrating IoT and blockchain [10]. Although blockchain can ensure the immutability of data in the chain and identify transformations, data that arrive corrupted in the blockchain remain corrupted. Corrupted IoT data can result from a variety of causes other than malicious intent. Many factors influence the health of IoT architecture, including vandalism, environment, participants, and device failure. Devices, sensors, and actuators do not always function immediately in a proper manner. This condition cannot be detected until the device in question is tested. Alternatively, it may work properly for a short period of time before changing its behavior for unknown reasons, such as disconnection, short circuit, and programmed obsolescence. In addition to these scenarios, there are numerous threats to the IoT, such as eavesdropping, denial of service, and control. As a result, before being integrated with blockchain, IoT devices should be thoroughly tested, and they should be located and encapsulated in the proper location to avoid physical damage, as well as techniques to detect device failures as soon as they occur [10].

H. A DYNAMIC AND ADAPTABLE SECURITY FRAMEWORK

Heterogeneous devices ranging from low-power devices to high-end servers are deployed in IoT networks. Owing to this disparity in available resources, a single security solution cannot be deployed for all blockchain-based IoT architectures. Hence, the security solution must first adapt to the available resources before deciding which security services to meet the end-users' minimum security requirements. Therefore, one of the future challenges that must be addressed is the design of a flexible and dynamic security framework for blockchain-based IoT architectures [17].

I. STORAGE CAPACITY AND SCALABILITY

One of the major impediments to the business adoption of blockchain technology is its scalability. The block size increases daily. For full transaction and block validation, full nodes must store the entire blockchain (currently more than 150 GB in Bitcoin and 46 GB in Ethereum); therefore, their deployment in IoT devices may be limited [4], [10], [15]. The IoT generates an unprecedented amount of data, and the frequency of data generation events has sharply increased. The storage requirements for each full IoT edge node would explode if all IoT data are encrypted and stored on the blockchain. In addition to storage requirements, algorithmic consensus for validating new blocks adds latency to data transaction events. Thus, the transaction processing speed of publicly deployed blockchains is limited, and a single monolithic blockchain cannot scale up to meet the needs of IoT edge devices [201].

This problem can be solved by using a layered architecture in which the blockchain is separated from the application layer and IoT devices with limited resources store only the portion of the blockchain required for their own transactions (thin clients, which are already present in Bitcoin) [96]. GHOST [221] aims to improve Bitcoin's scalability by changing the chain selection rule. Off-chain solutions [222] are intended to perform transactions outside the chain, thereby increasing the bandwidth while increasing the risk of data loss. Another solution that has been implemented is to separate the data related to the digital signature to reduce the size of each block [4].

However, there is a trade-off between scale and decentralization. The Ethereum blockchain has received considerable attention recently because of its scalability. On December 10, 2017, the Ethereum network was clogged by a new ICO called CryptoKitties, which sold virtual cats that could be bred and collected. Because CryptoKitties overwhelm Ethereum's network, transaction times for all applications running on the decentralized architecture are slowed. DAGs can improve scalability by tying network usage and transaction verification together, which means that a user must handle his/her own transactions to use the network [60]. As previously stated, the scalability and storage capacity of blockchain are still being debated, but in the context of IoT applications, the inherent scalability and capacity limitations significantly exacerbate these challenges. These issues should be addressed through the integration of these technologies [10]. Section IV of this paper discussed additional research contributions to scalability.

VIII. CONCLUSION

This paper conducted an intensive analysis of the current research issues and trends on the usage of blockchain-related approaches and technologies in the IoT security context. This paper first started with a blockchain overview and a discussion of the published articles on the consensus mechanism of blockchain-based IoT and blockchain scalability on IoT. Then, the paper thoroughly explained and chronologically introduced articles on IoT security using blockchain by introducing attacks on IoT and defense mechanisms using blockchain such as intrusion detection systems, firmware updates, and using blockchain to ensure confidentiality, authentication, access control, trust, and reputation.

As a vital conclusion, blockchain faces several critical challenges while providing IoT data security. For a successful blockchain and IoT integration, an analysis of the

main challenges of blockchain and IoT integration should be conducted, considering the challenges identified in this survey. Recently, there has been a significant amount of industry investment and a significant amount of interest from academia to solve major research challenges in blockchain technology. According to the paper scope distribution, we can see that research in the direction of IoT and blockchain is still in its early stages. Very little research has been conducted to address the scalability issue. Moreover, although blockchain can ensure the immutability of data in the chain and identify transformations, data that arrive corrupted in the blockchain remain corrupted. Hence, it is necessary to check the data before entering the blockchain. Some IoT devices may be found in public places. How can blockchain be used to ensure the security and privacy of data stored in an IoT device that is physically under the control of an adversary? Furthermore, there is a requirement for the development of efficient and lightweight blockchain-based IoT security solutions.

As future work, we intend to explore how blockchain, edge computing, and IoT can complement each other in their integration, and how the various security problems and data integrity of edge computing can be addressed by integrating blockchain technologies. Moreover, we are planning to introduce various blockchain applications in IoT because the autonomy enabled by blockchain encourages the development of new IoT marketplaces.

REFERENCES

[1] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018, doi: 10.1016/j.cose.2018.06.004.

[2] S. Knezevic, "A blockchain approach for negotiating trust in IoT," M.S. thesis, Eng. Sci., Florida Inst. Technol., Melbourne, VIC, Australia, 2020. Accessed: Jun. 23, 2020. [Online]. Available: https://repository.lib.fit.edu/handle/11141/3060

[3] R. Boncea, I. Petre, and V. Vevera, "Building trust among things in omniscient internet using blockchain technology," *Romanian Cyber Secur. J.*, vol. 1, no. 1, pp. 1–9, Apr. 2019.

[4] 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, 2018, doi: 10.3390/s18082575.

[5] E. A. Shammar and A. T. Zahary, "The Internet of Things (IoT): A survey of techniques, operating systems, and trends," *Library Hi Tech*, vol. 38, no. 1, pp. 5–66, Oct. 2019, doi: 10.1108/LHT-12-2018-0200.

[6] K. Zhidanov, S. Bezzateev, A. Afanasyeva, M. Sayfullin, S. Vanurin, Y. Bardinova, and A. Ometov, "Blockchain technology for smartphones and constrained IoT devices: A future perspective and implementation," in *Proc. IEEE 21st Conf. Bus. Informat. (CBI)*, Jul. 2019, pp. 20–27, doi: 10.1109/CBI.2019.10092.

[7] S. Dange and M. Chatterjee, "IoT botnet: The largest threat to the IoT network," in *Data Communication and Networks*, vol. 1049, L. C. Jain, Ed. Singapore: Springer, 2020, pp. 137–157, doi: 10.1007/978-981-15-0132-6_10.

[8] C. M. Eliott. (Apr. 26, 2017). *Alexa, Go Ahead and Hand Over Recordings in Murder Case CNN*. Accessed: Jul. 9, 2020. [Online]. Available: https://edition.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html

[9] Facebook and Twitter. *When Amazon Echo, Fitbit & Other Tech Are Witnesses to Murder*. Lifewire. Accessed: Jul. 9, 2020. [Online]. Available: https://www.lifewire.com/when-tech-is-witness-to-murder-4149689

[10] 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, doi: 10.1016/j.future.2018.05.046.

[11] J. Ali, T. Ali, Y. Alsaawy, A. S. Khalid, and S. Musa, "Blockchain-based smart-IoT trust zone measurement architecture," in *Proc. Int. Conf. Omni-Layer Intell. Syst.*, May 2019, pp. 152–157, doi: 10.1145/3312614.3312646.

[12] A. Dorri, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019, doi: 10.1016/j.jpdc.2019.08.005.

[13] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A trust architecture for blockchain in IoT," in *Proc. 16th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, Houston, TX, USA, Jun. 2019, pp. 190–199.

[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," bitcoin.org, Tech. Rep., Aug. 2008, p. 9, doi: 10.2139/ssrn.3440802.

[15] A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," 2017, *arXiv:1706.01730*.

[16] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung, and J. H. Park, "Blockchain-based secure storage management with edge computing for IoT," *Electronics*, vol. 8, no. 8, p. 828, Jul. 2019.

[17] 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.

[18] A. Lahbib, K. Toumi, A. Laouiti, A. Laube, and S. Martin, "Blockchain based trust management mechanism for IoT," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–8.

[19] M. Singh and S. Kim, "Trust bit: Reward-based intelligent vehicle commination using blockchain paper," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 62–67.

[20] G. Kaur and C. Gandhi, "Scalability in blockchain: Challenges and solutions," in *Handbook of Research on Blockchain Technology*. New York, NY, USA: Academic, 2020, pp. 373–406.

[21] S. Asiri and A. Miri, "A sybil resistant IoT trust model using blockchains," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1017–1026.

[22] A. Kchaou, R. Abassi, and S. Guemara, "Toward a distributed trust management scheme for VANET," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–6.

[23] Q. Le-Dang and T. Le-Ngoc, "Scalable blockchain-based architecture for massive IoT reconfiguration," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2019, pp. 1–4.

[24] B. Laurie and R. Clayton, "'Proof-of-work' proves not to work," Comput. Lab., Univ. Cambridge, London, U.K., Tech. Rep., May 2004, p. 9.

[25] Y. Sun, "Research on application of computer big data technology in blockchain computing," *J. Phys., Conf. Ser.*, vol. 1915, no. 3, May 2021, Art. no. 032014, doi: 10.1088/1742-6596/1915/3/032014.

[26] B. Vitalik. (Aug. 26, 2013). *What Proof of Stake is and Why it Matters Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides*. Accessed: Mar. 4, 2021. [Online]. Available: https://bitcoinmagazine.com/culture/what-proof-of-stake-is-and-why-it-matters-1377531463

[27] D. Larimer. (Apr. 2014). *BitShares—Delegated Proof-of-Stake Consensus | BitShares*. Accessed: Mar. 4, 2021. [Online]. Available: https://bitshareshub.io/delegated-proof-of-stake-consensus/

[28] J. Kang, Z. Xiong, D. Ye, D. I. Kim, J. Zhao, and D. Niyato, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.

[29] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," presented at the Italian Conf. Cyber Secur., Milan, Italy, Jan. 2018. Accessed: Jun. 17, 2021. [Online]. Available: https://eprints.soton.ac.uk/415083/

[30] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, New Orleans, LA, USA, Feb. 1999, pp. 173–186.

[31] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Develop. Found.*, vol. 32, p. 97, Feb. 2016.

[32] G. Christofi, "Study of consensus protocols and improvement of the Delegated Byzantine Fault Tolerance (DBFT) algorithm," M.S. thesis, Dept. Telecommun. Eng., Universitat Politècnica de Catalunya, Barcelona, Spain, 2019.

[33] 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.*, vol. 10616, Cham, Switzerland: Springer, Oct. 2017, pp. 282–297.

[34] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST IR 8202, Oct. 2018, doi: 10.6028/NIST.IR.8202.
[35] S. N. Company. (Sep. 2015). *Sudo Null Latest IT News*. SudoNull. Accessed: Mar. 4, 2021. [Online]. Available: https://sudonull.com/post/95149-Overview-of-Proof-of-Work-alternatives-Part-2-Proof-of-Activity-Proof-of-Burn-Proof-of-Capacity-and-
[36] L. Ren and S. Devadas, "Proof of space from stacked expanders," in *Proc. 14th Int. Conf. Theory Cryptogr. (TCC)*, vol. 9985, Berlin, Germany, Oct. 2016, pp. 262–285, doi: 10.1007/978-3-662-53641-4_11.
[37] *Proof of Burn Bitcoin Wiki*. Accessed: Mar. 26, 2021. [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_burn
[38] NEM Technical Reference. (Feb. 2018). *BloodyRookie Gimre Jaguar0625 Makoto*. Accessed: Mar. 26, 2021. [Online]. Available: https://nemplatform.com/wp-content/uploads/2020/05/NEM_techRef.pdf
[39] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Operating Syst. Princ.*, Oct. 2017, pp. 51–68, doi: 10.1145/3132747.3132757.
[40] J. Yu, D. Kozhaya, J. Decouchant, and P. Esteves-Verissimo, "RepuCoin: Your reputation is your power," *IEEE Trans. Comput.*, vol. 68, no. 8, pp. 1225–1237, Aug. 2019, doi: 10.1109/TC.2019.2900648.
[41] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, vol. 5, no. 8, p. 151, 2014.
[42] I. Amores-Sesar, C. Cachin, and J. Micic, "Security analysis of ripple consensus," in *Proc. 24th Int. Conf. Princ. Distrib. Syst. (OPODIS)*. Leibniz Int. Proc. Inform., Nov. 2020, pp. 10:1–10:16, Art. no. 10.
[43] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," 2020, *arXiv:2001.07091*.
[44] N. Chaudhry and M. M. Yousaf, "Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities," in *Proc. 12th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Dec. 2018, pp. 54–63.
[45] M. Bosamia and D. Patel, "Comparisons of blockchain based consensus algorithms for security aspects," *Int. J. Emerg. Technol.*, vol. 11, no. 3, pp. 427–434, Jun. 2020.
[46] A. Amora. (Jul. 2020). *A Complete Guide to Leased Proof-of-Stake (LPOS)*. Accessed: Jun. 17, 2021. [Online]. Available: https://www.mycointainer.com/insight/a-complete-guide-to-leased-proof-of-stake-lpos/
[47] Burstflash. *Burstcoin. PoC (Proof of Capacity) an Ecofriendly Consensus Mechanism. Burstcoin*. Accessed: Jun. 17, 2021. [Online]. Available: https://www.burst-coin.org/features/proof-of-capacity/
[48] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. 41st Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2018, pp. 1545–1550, doi: 10.23919/MIPRO.2018.8400278.
[49] M. Silvio. (Dec. 2020). *Algorand 2021 Performance*. Accessed: Jun. 18, 2021. [Online]. Available: https://www.algorand.com/resources/blog/algorand-2021-performance
[50] G. Wood. (2014). *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. Ethereum Project Yellow Paper. Accessed: Jul. 9, 2020. [Online]. Available: https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf
[51] *Hyperledger Open Source Blockchain Technologies*. Accessed: Jun. 30, 2020. [Online]. Available: https://www.hyperledger.org/
[52] *Full Profile Reimagining Agriculture*. Accessed: Jul. 9, 2020. [Online]. Available: https://www.fullprofile.com.au/
[53] G. Gideon, *MultiChain Private Blockchain White Paper*. London, U.K.: Coin Sciences Ltd, 2015.
[54] S. Popov, "The tangle," Tech. Rep., Apr. 2018, p. 131.
[55] M. I. Mehar, C. L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, and M. Laskowski, "Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack," *J. Cases Inf. Technol.*, vol. 21, no. 1, pp. 19–32, 2019.
[56] *Hyperledger Fabric Hyperledger*. Accessed: Jun. 23, 2020. [Online]. Available: https://www.hyperledger.org/use/fabric
[57] C. Saraf and S. Sabadra, "Blockchain platforms: A compendium," in *Proc. IEEE Int. Conf. Innov. Res. Develop. (ICIRD)*, May 2018, pp. 1–6, doi: 10.1109/ICIRD.2018.8376323.
[58] *Introduction | Hyperledger Composer*. Accessed: Jun. 18, 2021. [Online]. Available: https://hyperledger.github.io/composer/latest/introduction/introduction.html
[59] *MultiChain | Open Source Blockchain Platform*. Accessed: Sep. 26, 2020. [Online]. Available: https://www.multichain.com/
[60] H. Pervez, M. Muneeb, M. U. Irfan, and I. U. Haq, "A comparative analysis of DAG-based blockchain architectures," in *Proc. 12th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Dec. 2018, pp. 27–34.
[61] S. D. Lerner. (Sep. 2015). *DagCoin: A Cryptocurrency Without Blocks*. Accessed: Jun. 19, 2021. [Online]. Available: https://bitcointalk.org/index.php?topic=1177633.msg12395537#msg12395537
[62] L. Zhao and J. Yu, "Evaluating DAG-based blockchains for IoT," in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2019, pp. 507–513.
[63] C. Bai, "State-of-the-art and future trends of blockchain based on DAG structure," in *Proc. Int. Workshop Structured Object-Oriented Formal Language Method*, vol. 11392, Feb. 2019, pp. 183–196, doi: 10.1007/978-3-030-13651-2_11.
[64] *IOTA Next Generation Blockchain*. Accessed: Mar. 4, 2021. [Online]. Available: https://iotatoken.com/
[65] R. G. Brown, "The Corda platform: An introduction white paper," Tech. Rep., May 2018, p. 21.
[66] M. Hearn and R. G. Brown, "Corda: A distributed ledger," *Corda Tech. White Paper*, p. 73, Aug. 2019.
[67] HdacTech. (Feb. 2019). *HDAC: Transaction Innovation IoT Contract & M2M Transaction Platform Based on Blockchain*. Accessed: Mar. 26, 2021. [Online]. Available: https://github.com/Hdactech/doc/wiki/Whitepaper
[68] K. Jae and E. Buchman. (2016). *Cosmos: A Network of Distributed Ledgers*. Cosmos Whitepaper. Accessed: Jun. 19, 2021. [Online]. Available: https://v1.cosmos.network/resources/whitepaper
[69] IoTeX.Team. (2018). *IoTeX—A Decentralized Network for Internet of Things (IoT), Powered by a Auto-Scalable, Extensible, Private-Centric Blockchain. Connecting the Physical World, Block by Block*. White Paper. Accessed: Jun. 30, 2020. [Online]. Available: https://s3.amazonaws.com/web-iotex-static/home/IoTeX_Whitepaper_1.5_EN.pdf
[70] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto, "BigchainDB: A scalable blockchain database," Ascribe GmbH, Berlin, Germany, White Paper version 1.0, Jun. 2016, p. 65.
[71] A. Ellervee, R. Matulevicius, and N. Mayer, "A comprehensive reference model for blockchain-based distributed ledger technology," in *Proc. ER Forum ER Demos Track*, Valencia, Spain, Nov. 2017, pp. 306–319.
[72] R. Creighton. (Mar. 2016). *Domus Tower Blockchain*. Accessed: Mar. 4, 2021. [Online]. Available: https://docplayer.net/31998028-Domus-tower-blockchain-draft-march-22-2016.html
[73] HydraChain. *GitHub*. Accessed: Mar. 4, 2021. [Online]. Available: https://github.com/HydraChain
[74] *Hydra Blockchain*. Accessed: Oct. 10, 2021. [Online]. Available: https://docs.hydrachain.org/
[75] *Openchain Blockchain Technology for the Enterprise*. Accessed: Mar. 4, 2021. [Online]. Available: https://www.openchain.org/
[76] S. Anwar, S. Anayat, S. Butt, S. Butt, and M. Saad, "Generation analysis of blockchain technology: Bitcoin and Ethereum," *Int. J. Inf. Eng. Electron. Bus.*, vol. 12, no. 4, pp. 30–39, Aug. 2020, doi: 10.5815/ijieeb.2020.04.04.
[77] S. Yeasmin and A. Baig, "Permissioned blockchain: Securing industrial IoT environments," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 4, pp. 715–725, 2021, doi: 10.14569/IJACSA.2021.0120488.
[78] *MultiChain*. Chainstack. Accessed: Jul. 16, 2021. [Online]. Available: https://chainstack.com/protocols/multichain/
[79] H. Moudoud, S. Cherkaoui, and L. Khoukhi, "An IoT blockchain architecture using oracles and smart contracts: The use-case of a food supply chain," in *Proc. IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2019, pp. 1–6.
[80] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2343–2355, Mar. 2020.
[81] B. Herudek. (May 1, 2016). *Babelchain Machine Communication Proof of Understanding*. Blockchain News, Opinion, TV and Jobs. Accessed: Jul. 10, 2021. [Online]. Available: https://www.the-blockchain.com/2016/05/01/babelchain-machine-communication-proof-understanding-new-paper/
[82] S. R. Niya, E. Schiller, I. Cepilov, F. Maddaloni, K. Aydinli, T. Surbeck, T. Bocek, and B. Stiller, "Adaptation of proof-of-stake-based blockchains for IoT data streams," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 15–16.

[83] T. Kim, J. Noh, and S. Cho, "SCC: Storage compression consensus for blockchain in lightweight IoT network," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–4.

[84] H. Bai, G. Xia, and S. Fu, "A two-layer-consensus based blockchain architecture for IoT," in *Proc. IEEE 9th Int. Conf. Electron. Inf. Emergency Commun. (ICEIEC)*, Jul. 2019, pp. 1–6.

[85] D. Puthal, S. P. Mohanty, V. P. Yanambaka, and E. Kougianos, "PoAh: A novel consensus algorithm for fast scalable private blockchain for large-scale IoT frameworks," 2020, *arXiv:2001.07297*.

[86] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-authentication for scalable blockchain in resource-constrained distributed systems," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–5.

[87] A. Dorri and R. Jurdak, "Tree-chain: A fast lightweight consensus algorithm for IoT applications," in *Proc. IEEE 45th Conf. Local Comput. Netw. (LCN)*, Nov. 2020, pp. 369–372.

[88] C. Li, J. Zhang, X. Yang, and L. Youlong, "Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices," *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, Art. no. 102602, doi: 10.1016/j.ipm.2021.102602.

[89] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, Jun. 2019.

[90] A. R. Shahid, N. Pissinou, C. Staier, and R. Kwan, "Sensor-chain: A lightweight scalable blockchain framework for Internet of Things," in *Proc. Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2019, pp. 1154–1161.

[91] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020.

[92] J. Ali, A. S. Khalid, E. Yafi, S. Musa, and W. Ahmed, "Towards a secure behavior modeling for IoT networks using blockchain," 2020, *arXiv:2001.01841*.

[93] K. Kataoka, S. Gangwar, and P. Podili, "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 296–301.

[94] S. Asiri, "A blockchain-based IoT trust model," M.S. thesis, Comput. Sci., Ryerson Univ., Toronto, ON, Canada, 2018.

[95] B. Dinesh, B. Kavya, D. Sivakumar, and M. R. Ahmed, "Conforming test of blockchain for 5G enabled IoT," in *Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI)*, Apr. 2019, pp. 1153–1157.

[96] 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.

[97] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-IoT: Hybrid blockchain architecture for Internet of Things–PoW sub-blockchains," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1007–1016.

[98] H. Liu, F. Shen, Z. Liu, Y. Long, Z. Liu, S. Sun, S. Tang, and D. Gu, "A secure and practical blockchain scheme for IoT," in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2019, pp. 538–545.

[99] O. Abdulkader, A. M. Bamhdi, V. Thayananthan, F. Elbouraey, and B. Al-Ghamdi, "A lightweight blockchain based cybersecurity for IoT environments," in *Proc. 6th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)/5th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom)*, Jun. 2019, pp. 139–144.

[100] D. Fakhri and K. Mutijarsa, "Secure IoT communication using blockchain technology," in *Proc. Int. Symp. Electron. Smart Devices (ISESD)*, Oct. 2018, pp. 1–6, doi: 10.1109/ISESD.2018.8605485.

[101] H. Qiu, M. Qiu, G. Memmi, Z. Ming, and M. Liu, "A dynamic scalable blockchain based communication architecture for IoT," in *Proc. Int. Conf. Smart Blockchain*, Tokyo, Japan, Dec. 2018, pp. 159–166.

[102] R. B. Chakraborty, M. Pandey, and S. S. Rautaray, "Managing computation load on a blockchain—Based multi—Layered Internet–of–Things network," *Proc. Comput. Sci.*, vol. 132, pp. 469–476, Jan. 2018.

[103] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "IoTChain: A blockchain security architecture for the Internet of Things," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.

[104] T. Golomb, Y. Mirsky, and Y. Elovici, "CIoTA: Collaborative IoT anomaly detection via blockchain," 2018, *arXiv:1803.03807*.

[105] G. Rathee, A. Sharma, R. Kumar, and R. Iqbal, "A secure communicating things network framework for industrial IoT using blockchain technology," *Ad Hoc Netw.*, vol. 94, Nov. 2019, Art. no. 101933, doi: 10.1016/j.adhoc.2019.101933.

[106] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, and G. Danezis, "Chainspace: A sharded smart contracts platform," 2017, *arXiv:1708.03778*.

[107] J. Huang, L. Kong, G. Chen, L. Cheng, K. Wu, and X. Liu, "B-IoT: Blockchain driven Internet of Things with credit-based consensus mechanism," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2019, pp. 1348–1357.

[108] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "An efficient selective miner consensus protocol in blockchain oriented IoT smart monitoring," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Feb. 2019, pp. 1135–1142.

[109] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, and M. Ylianttila, "Blockchain based proxy re-encryption scheme for secure IoT data sharing," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 99–103, doi: 10.1109/BLOC.2019.8751336.

[110] S. N. Mohanty, K. C. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. K. Lakshmanaprabu, and A. Khanna, "An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy," *Future Gener. Comput. Syst.*, vol. 102, pp. 1027–1037, Jan. 2020.

[111] J. Ali, T. Ali, S. Musa, and A. Zahrani, "Towards secure IoT communication with smart contracts in a blockchain infrastructure," 2020, *arXiv:2001.01837*.

[112] M. Baza, M. Nabil, M. M. E. A. Mahmoud, N. Bewermeier, K. Fidan, W. Alasmary, and M. Abdallah, "Detecting Sybil attacks using proofs of work and location in VANETs," *IEEE Trans. Depend. Sec. Comput.*, early access, May 11, 2020, doi: 10.1109/TDSC.2020.2993769.

[113] H. Abdelatif, S. H. Abdelhakim, and S. Mustapha, "A tractable probabilistic approach to analyze sybil attacks in sharding-based blockchain protocols," 2021, *arXiv:2104.07215*.

[114] A. Bochem and B. Leiding, "Rechained: Sybil-resistant distributed identities for the Internet of Things and mobile ad hoc networks," *Sensors*, vol. 21, no. 9, p. 3257, May 2021, doi: 10.3390/s21093257.

[115] Z. Ahmed, S. M. Danish, H. K. Qureshi, and M. Lestas, "Protecting IoTs from Mirai BotNet attacks using blockchains," in *Proc. IEEE 24th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Sep. 2019, pp. 1–6.

[116] S. Wani, M. Imthiyas, H. Almohamedh, K. M. Alhamed, S. Almotairi, and Y. Gulzar, "Distributed denial of service (DDoS) mitigation using blockchain—A comprehensive insight," *Symmetry*, vol. 13, no. 2, p. 227, Jan. 2021, doi: 10.3390/sym13020227.

[117] Q. Shafi and A. Basit, "DDoS botnet prevention using blockchain in software defined Internet of Things," in *Proc. 16th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Jan. 2019, pp. 624–628, doi: 10.1109/IBCAST.2019.8667147.

[118] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A blockchain-based architecture for collaborative DDoS mitigation with smart contracts," in *Proc. IFIP Int. Conf. Auton. Infrastruct., Manage. Secur.*, vol. 10356, Zürich, Switzerland, Jun. 2017, pp. 16–29.

[119] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating IoT device based DDoS attacks using blockchain," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst.*, Jun. 2018, pp. 71–76, doi: 10.1145/3211933.3211946.

[120] M. Banerjee, J. Lee, Q. Chen, and K.-K.-R. Choo, "Blockchain-based security layer for identification and isolation of malicious things in IoT: A conceptual design," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–6.

[121] M. Chen, X. Tang, J. Cheng, N. Xiong, J. Li, and D. Fan, "A DDoS attack defense method based on blockchain for IoTs devices," in *Artificial Intelligence and Security*, vol. 1253. Singapore: Springer, Sep. 2020, pp. 685–694, doi: 10.1007/978-981-15-8086-4_64.

[122] G. Sagirlar, B. Carminati, and E. Ferrari, "AutoBotCatcher: Blockchain-based P2P botnet detection for the Internet of Things," in *Proc. IEEE 4th Int. Conf. Collaboration Internet Comput. (CIC)*, Oct. 2018, pp. 1–8.

[123] N. Giachoudis, G.-P. Damiris, G. Theodoridis, and G. Spathoulas, "Collaborative agent-based detection of DDoS IoT botnets," in *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2019, pp. 205–211.

[124] G. Spathoulas, N. Giachoudis, G.-P. Damiris, and G. Theodoridis, "Collaborative blockchain-based detection of distributed denial of service attacks based on Internet of Things botnets," *Future Internet*, vol. 11, no. 11, p. 226, Oct. 2019.
[125] P. Cui and U. Guin, "Countering BotNet of things using blockchain-based authenticity framework," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jul. 2019, pp. 598–603.
[126] G. Falco, C. Li, P. Fedorov, C. Caldera, R. Arora, and K. Jackson, "NeuroMesh: IoT security enabled by a blockchain powered botnet vaccine," in *Proc. Int. Conf. Omni-Layer Intell. Syst.*, May 2019, pp. 1–6.
[127] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–6, doi: 10.1109/ICCCN.2018.8487449.
[128] J. Caminha, A. Perkusich, and M. Perkusich, "A smart trust management method to detect on-off attacks in the Internet of Things," *Secur. Commun. Netw.*, vol. 2018, p. 10, Apr. 2018, doi: 10.1155/2018/6063456.
[129] N. Wang, L. Jiao, P. Wang, M. Dabaghchian, and K. Zeng, "Efficient identity spoofing attack detection for IoT in mm-wave and massive MIMO 5G communication," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6, doi: 10.1109/GLOCOM.2018.8647707.
[130] P. Patel and P. Chauhan, "Access control mechanism for IoT using blockchain," *IJRTE*, vol. 8, no. 6, pp. 5473–5481, Mar. 2020.
[131] I.-R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Trans. Services Comput.*, vol. 9, no. 3, pp. 482–495, May 2016.
[132] F. Bao and I.-R. Chen, "Dynamic trust management for Internet of Things applications," in *Proc. Int. Workshop Self-Aware Internet Things Self-IoT*, 2012, pp. 1–6.
[133] M. Devi and A. Majumder, "Side-channel attack in Internet of Things: A survey," in *Applications of Internet of Things*. Singapore: ACM, Aug. 2020, pp. 213–222, doi: 10.1007/978-981-15-6198-6_20.
[134] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.
[135] M. Boussard, S. Papillon, P. Peloso, M. Signorini, and E. Waisbard, "STewARD:SDN and blockchain-based trust evaluation for automated risk management on IoT devices," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2019, pp. 841–846.
[136] G. G. R. Roy and S. B. R. Kumar, "An architecture to enable secure firmware updates on a distributed-trust IoT network using blockchain," in *Proc. Int. Conf. Comput. Netw. Commun. Technol.*, Singapore, Jan. 2019, pp. 671–679, doi: 10.1007/978-981-10-8681-6_61.
[137] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018, doi: 10.1109/ACCESS.2018.2864189.
[138] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the Internet of Things," in *Proc. 23nd ACM Symp. Access Control Models Technol.*, Jun. 2018, pp. 77–83.
[139] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivánkò, and M. Mühlhäuser, "Towards blockchain-based collaborative intrusion detection systems," in *Critical Information Infrastructures Security*. Cham, Switzerland: Springer, Sep. 2018, pp. 107–118, doi: 10.1007/978-3-319-99843-5_10.
[140] D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen, and E. Ilie-Zudor, "Chained anomaly detection models for federated learning: An intrusion detection case study," *Appl. Sci.*, vol. 8, no. 12, p. 2663, 2018.
[141] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," *Future Gener. Comput. Syst.*, vol. 96, pp. 481–489, Jul. 2019, doi: 10.1016/j.future.2019.02.064.
[142] B. Hu, C. Zhou, Y. C. Tian, Y. Qin, and X. Junping, "A collaborative intrusion detection approach using blockchain for multimicrogrid systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1720–1730, Aug. 2019, doi: 10.1109/TSMC.2019.2911548.
[143] H. Liang, J. Wu, S. Mumtaz, J. Li, X. Lin, and M. Wen, "MBID: Micro-blockchain-based geographical dynamic intrusion detection for V2X," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 77–83, Oct. 2019, doi: 10.1109/MCOM.001.1900143.
[144] C. Liang, B. Shanmugam, S. Azam, A. Karim, A. Islam, M. Zamani, S. Kavianpour, and N. B. Idris, "Intrusion detection system for the Internet of Things based on blockchain and multi-agent systems," *Electronics*, vol. 9, no. 7, p. 1120, Jul. 2020, doi: 10.3390/electronics9071120.
[145] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K.-R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9463–9472, Jun. 2021, doi: 10.1109/JIOT.2020.2996590.
[146] W. Li, Y. Wang, J. Li, and M. H. Au, "Toward a blockchain-based framework for challenge-based collaborative intrusion detection," *Int. J. Inf. Secur.*, vol. 20, no. 2, pp. 127–139, Apr. 2021, doi: 10.1007/s10207-020-00488-6.
[147] I. Aliyu, M. C. Feliciano, S. Van Engelenburg, D. O. Kim, and C. G. Lim, "A blockchain-based federated forest for SDN-enabled in-vehicle network intrusion detection system," *IEEE Access*, vol. 9, pp. 102593–102608, 2021, doi: 10.1109/ACCESS.2021.3094365.
[148] M. Son and H. Kim, "Blockchain-based secure firmware management system in IoT environment," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 142–146.
[149] X. He, S. Alqahtani, R. Gamble, and M. Papa, "Securing over-the-air IoT firmware updates using blockchain," in *Proc. Int. Conf. Omni-Layer Intell. Syst.*, May 2019, pp. 164–171.
[150] S. Dhakal, F. Jaafar, and P. Zavarsky, "Private blockchain network for IoT device firmware integrity verification and update," in *Proc. IEEE 19th Int. Symp. High Assurance Syst. Eng. (HASE)*, Jan. 2019, pp. 164–170.
[151] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *Proc. IEEE/ACS 15th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Oct. 2018, pp. 1–8, doi: 10.1109/AICCSA.2018.8612856.
[152] C. Rondanini, B. Carminati, and E. Ferrari, "Confidential discovery of IoT devices through blockchain," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jul. 2019, pp. 1–8.
[153] L. Zhou, L. Wang, T. Ai, and Y. Sun, "BeeKeeper 2.0: Confidential blockchain-enabled IoT system with fully homomorphic computation," *Sensors*, vol. 18, no. 11, p. 3785, Nov. 2018, doi: 10.3390/s18113785.
[154] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, 2017, doi: 10.1007/s11227-016-1870-0.
[155] A. Yohan and N.-W. Lo, "An over-the-blockchain firmware update framework for IoT devices," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Dec. 2018, pp. 1–8, doi: 10.1109/DESEC.2018.8625164.
[156] S. Choi and J.-H. Lee, "Blockchain-based distributed firmware update architecture for IoT devices," *IEEE Access*, vol. 8, pp. 37518–37525, 2020, doi: 10.1109/ACCESS.2020.2975920.
[157] A. Yohan and N.-W. Lo, "FOTB: A secure blockchain-based firmware update framework for IoT environment," *Int. J. Inf. Secur.*, vol. 19, no. 3, pp. 257–278, Jun. 2020, doi: 10.1007/s10207-019-00467-6.
[158] A. Anastasiou, P. Christodoulou, K. Christodoulou, V. Vassiliou, and Z. Zinonos, "IoT device firmware update over LoRa: The blockchain solution," in *Proc. 16th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2020, pp. 404–411, doi: 10.1109/DCOSS49796.2020.00070.
[159] T. Fukuda and K. Omote, "Efficient blockchain-based IoT firmware update considering distribution incentives," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Jan. 2021, pp. 1–8, doi: 10.1109/DSC49826.2021.9346265.
[160] S. P. Gochhayat, E. Bandara, S. Shetty, and P. Foytik, "Yugala: Blockchain based encrypted cloud storage for IoT data," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 483–489, doi: 10.1109/Blockchain.2019.00073.
[161] A. A. A. El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in IoT-based smart cities," *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, Art. no. 102549, doi: 10.1016/j.ipm.2021.102549.
[162] B. T. Asare, K. Quist-Aphetsi, and L. Nana, "Nodal authentication of IoT data using blockchain," in *Proc. Int. Conf. Comput., Comput. Modeling Appl. (ICCMA)*, Mar. 2019, pp. 125–1254, doi: 10.1109/ICCMA.2019.00028.
[163] P. Angin, M. B. Mert, O. Mete, A. Ramazanli, K. Sarica, and B. Gungoren, "A blockchain-based decentralized security architecture for IoT," in *Proc. Int. Conf. Internet Things*, Honolulu, HI, USA, Jun. 2018, pp. 3–18.

[164] H.-W. Kim and Y.-S. Jeong, "Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain," *Hum.-Centric Comput. Inf. Sci.*, vol. 8, no. 1, p. 11, 2018, doi: 10.1186/s13673-018-0136-7.

[165] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for Internet of Things using blockchain technology," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Mar. 2018, pp. 769–773, doi: 10.1109/ICCNC.2018.8390280.

[166] V. A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, and G. C. Polyzos, "OAuth 2.0 meets blockchain for authorization in constrained IoT environments," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 364–367.

[167] R. Yetis and O. K. Sahingoz, "Blockchain based secure communication for IoT devices in smart cities," in *Proc. 7th Int. Istanbul Smart Grids Cities Congr. Fair (ICSG)*, Apr. 2019, pp. 134–138.

[168] Z. Cui, F. XUE, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid BlockChain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Apr. 2020, doi: 10.1109/TSC.2020.2964537.

[169] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Comput.*, vol. 23, no. 3, pp. 2067–2087, Sep. 2020, doi: 10.1007/s10586-020-03058-6.

[170] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K.-R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 8, pp. 2146–2156, Aug. 2020, doi: 10.1109/JBHI.2020.2969648.

[171] Y. Zhang, B. Li, B. Liu, Y. Hu, and H. Zheng, "A privacy-aware PUFs-based multiserver authentication protocol in cloud-edge IoT systems using blockchain," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13958–13974, Sep. 2021, doi: 10.1109/JIOT.2021.3068410.

[172] L. Vishwakarma and D. Das, "SCAB–IoTA: Secure communication and authentication for IoT applications using blockchain," *J. Parallel Distrib. Comput.*, vol. 154, pp. 94–105, Aug. 2021, doi: 10.1016/j.jpdc.2021.04.003.

[173] S. S. Panda, D. Jena, B. K. Mohanta, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Authentication and key management in distributed IoT using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12947–12954, Aug. 2021, doi: 10.1109/JIOT.2021.3063806.

[174] I. Riabi, Y. Dhif, H. K. B. Ayed, and K. Zaatouri, "A blockchain based access control for IoT," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 2086–2091, doi: 10.1109/IWCMC.2019.8766506.

[175] A. Z. Ourad, B. Belgacem, and K. Salah, "Using blockchain for IOT access control and authentication management," in *Proc. Int. Conf. Internet Things*, Seattle, WA, USA, Jun. 2018, pp. 150–164.

[176] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, "ControlChain: Blockchain as a central enabler for access control authorizations in the IoT," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.

[177] H. Liu, D. Han, and D. Li, "Fabric-IoT: A blockchain-based access control system in IoT," *IEEE Access*, vol. 8, pp. 18207–18218, 2020, doi: 10.1109/ACCESS.2020.2968492.

[178] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "FairAccess: A new blockchain-based access control framework for the Internet of Things," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5943–5964, 2016.

[179] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT data management using BlockChain and trusted execution environment," in *Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, Jul. 2018, pp. 15–22.

[180] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[181] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019, doi: 10.1109/ACCESS.2019.2905846.

[182] Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang, and X. Yang, "An attribute-based collaborative access control scheme using blockchain for IoT devices," *Electronics*, vol. 9, no. 2, p. 285, Feb. 2020, doi: 10.3390/electronics9020285.

[183] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices," *Appl. Sci.*, vol. 10, no. 2, p. 488, Jan. 2020, doi: 10.3390/app10020488.

[184] Y. Feng, W. Zhang, X. Luo, and B. Zhang, "A consortium blockchain-based access control framework with dynamic orderer node selection for 5G-enabled industrial IoT," *IEEE Trans. Ind. Informat.*, early access, May 7, 2021, doi: 10.1109/TII.2021.3078183.

[185] S. Algarni, F. Eassa, K. Almarhabi, A. Almalaise, E. Albassam, K. Alsubhi, and M. Yamin, "Blockchain-based secured access control in an IoT system," *Appl. Sci.*, vol. 11, no. 4, p. 1772, Feb. 2021, doi: 10.3390/app11041772.

[186] M. A. Bouras, B. Xia, A. O. Abuassba, H. Ning, and Q. Lu, "IoT-CCAC: A blockchain-based consortium capability access control approach for IoT," *PeerJ Comput. Sci.*, vol. 7, p. e455, Apr. 2021, doi: 10.7717/peerj-cs.455.

[187] W. Ren, Y. Sun, H. Luo, and M. Guizani, "SILedger: A blockchain and ABE-based access control for applications in SDN-IoT networks," *IEEE Trans. Netw. Service Manage.*, early access, Jun. 28, 2021, doi: 10.1109/TNSM.2021.3093002.

[188] P. Tzianos, G. Pipelidis, and N. Tsiamitros, "Hermes: An open and transparent marketplace for IoT sensor data over distributed ledgers," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 167–170.

[189] G. Srivastava, J. Crichigno, and S. Dhar, "A light and secure healthcare blockchain for IoT medical devices," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2019, pp. 1–5.

[190] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[191] S. Juyal, S. Sharma, A. Harbola, and A. S. Shukla, "Privacy and security of IoT based skin monitoring system using blockchain approach," in *Proc. IEEE Int. Conf. Electron., Comput. Commun. Technol. (CONECCT)*, Jul. 2020, pp. 1–5, doi: 10.1109/CONECCT50063.2020.9198409.

[192] F. Loukil, C. Ghedira-Guegan, K. Boukadi, A.-N. Benharkat, and E. Benkhelifa, "Data privacy based on IoT device behavior control using blockchain," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–20, Feb. 2021, doi: 10.1145/3434776.

[193] A. Shahzad, K. Zhang, and A. Gherbi, "Privacy-preserving smart grid traceability using blockchain over IoT connectivity," in *Proc. 36th Annu. ACM Symp. Appl. Comput.*, Mar. 2021, pp. 699–706, doi: 10.1145/3412841.3441949.

[194] B. D. Deebak and F. AL-Turjman, "Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102749, doi: 10.1016/j.jisa.2021.102749.

[195] P. Kumar, R. Kumar, G. Srivastava, G. P. Gupta, R. Tripathi, T. R. Gadekallu, and N. N. Xiong, "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2326–2341, Jul. 2021, doi: 10.1109/TNSE.2021.3089435.

[196] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 131–138.

[197] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. 13th USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, Santa Clara, CA, USA, Mar. 2016, pp. 45–59.

[198] Litecoin. *Litecoin Open Source P2P Digital Currency*. Accessed: Mar. 26, 2021. [Online]. Available: https://litecoin.org/

[199] *BigchainDB o o The Blockchain Database*. BigchainDB. Accessed: Mar. 26, 2021. [Online]. Available: https://www.bigchaindb.com/

[200] A. Mokhtar, N. Murphy, and J. Bruton, "Blockchain-based multi-robot path planning," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Limerick, Ireland, Apr. 2019, pp. 584–589.

[201] M. S. Ali, M. Vecchio, and F. Antonelli, "Enabling a blockchain-based IoT edge," *IEEE Internet Things Mag.*, vol. 1, no. 2, pp. 24–29, Dec. 2018.

[202] J. Bonneau, "Why buy when you can rent," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, Feb. 2016, pp. 19–26, doi: 10.1007/978-3-662-53357-4_2.

[203] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 459–474, doi: 10.1109/SP.2014.36.
[204] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed E-cash from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 397–411, doi: 10.1109/SP.2013.34.
[205] *The Monero Project*. Getmonero.Org. The Monero Project. Accessed: Mar. 26, 2021. [Online]. Available: https://www.getmonero.org//index.html
[206] *Quorum Ledgerium Whitepaper*. Accessed: Mar. 26, 2021. [Online]. Available: https://whitepaper.ledgerium.io/architecture-blockchain/quorum
[207] A. D Alanza and S. Jehan. (Sep. 7, 2017). *Rockchain A Distributed Data Intelligence Platform White Paper Beta 2.3 | Arda D Alanza Academia.edu*. Accessed: Mar. 26, 2021. [Online]. Available: https://www.academia.edu/34666348/Rockchain_A_distributed_data_intelligence_platform_White_Paper_Beta_2_3
[208] A. Lazarovich, "Invisible Ink: Blockchain for data privacy," M.S. thesis, Dept. Sci. Media Arts Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2015. Accessed: Mar. 26, 2021. [Online]. Available: https://dspace.mit.edu/handle/1721.1/98626
[209] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "IoT passport: A blockchain-based trust framework for collaborative Internet-of-Things," in *Proc. 24th ACM Symp. Access Control Models Technol.*, May 2019, pp. 83–92.
[210] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019.
[211] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A sybil-resistant scalable blockchain," *Future Gener. Comput. Syst.*, vol. 107, pp. 770–780, Jun. 2020.
[212] N. Tariq, M. Asim, F. A. Khan, T. Baker, U. Khalid, and A. Derhab, "A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in Internet of Things," *Sensors*, vol. 21, no. 1, p. 23, Dec. 2020.
[213] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 98–103.
[214] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.
[215] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, "IoT public fog nodes reputation system: A decentralized solution using ethereum blockchain," *IEEE Access*, vol. 7, pp. 178082–178093, 2019.
[216] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarne, "Using blockchain in a reputation-based model for grouping agents in the Internet of Things," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1231–1243, Nov. 2020, doi: 10.1109/TEM.2019.2918162.
[217] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarné, "Using blockchain for reputation-based cooperation in federated IoT domains," in *Intelligent Distributed Computing XIII*. Cham, Switzerland: Springer, Jan. 2020, pp. 3–12, doi: 10.1007/978-3-030-32258-8_1.
[218] L.-A. Hîrţan, C. Dobre, and H. González-Vélez, "Blockchain-based reputation for intelligent transportation systems," *Sensors*, vol. 20, no. 3, p. 791, Jan. 2020, doi: 10.3390/s20030791.
[219] P. Weerapanpisit. (Mar. 2021). *Decentralised Location-Based Reputation Management System in IOT Using Blockchain*. Accessed: Jul. 4, 2021. [Online]. Available: https://run.unl.pt/handle/10362/113708
[220] T. Wang, J. Guo, S. Ai, and J. Cao, "RBT: A distributed reputation system for blockchain-based peer-to-peer energy trading with fairness consideration," *Appl. Energy*, vol. 295, Aug. 2021, Art. no. 117056, doi: 10.1016/j.apenergy.2021.117056.
[221] Y. Sompolinsky and A. Zohar, "Accelerating bitcoin's transaction processing," *Fast Money Grows Trees, Not Chains*, vol. 2013, p. 881, Dec. 2013.
[222] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in *Proc. Symp. Self-Stabilizing Syst.*, Edmonton, AB, Canada, Aug. 2015, pp. 3–18.

ELHAM A. SHAMMAR received the bachelor's degree in computer science/software engineering from the Faculty of Science, Sana'a University, Yemen, in 2009. She is currently pursuing the master's degree with the Department of Information Technology, Faculty of Computer and Information Technology (FCIT), Sana'a University. Since 2011, she has been working as a University Instructor at the Faculty of Science, Sana'a University. Her main research interests include the IoT and Blockchain technology.

AMMAR T. ZAHARY (Member, IEEE) was the Vice Chancellor of Azal University for Human Development, Yemen. He is currently an Associate Professor of data communication and networking at the Faculty of Computer and IT, Sana'a University, and an Associate Professor of data communication and networking at the University of Science and Technology, Yemen. He has supervised more than 60 master's theses and about four Ph.D. theses. His research interests include oriented to MANETs, VANETs, the IoT, and ubiquitous computing. He was a member of the Steering Committee of the ACIT conference for many years. He is currently an Editorial Board Member and a Technical Committee Member of many journals, such as the *International Journal of Computational Complexity and Intelligent Algorithms* (Inderscience Publishers), and a reviewer with ISI Q1 journal, such as CMC-*Computers, Materials and Continua* (Tech Science Press) and *Scopus* journal (Library High Tech) (Emarald Publisher). He is also one of the founders of the IEEE Yemen Subsection and the first chair of the subsection, since November 2018.

ASMA A. AL-SHARGABI (Member, IEEE) received the B.Sc. and M.Sc. degrees in computer science from the University of Science and Technology (UST), Yemen, in 1999 and 2006, respectively, and the Ph.D. degree from De Montfort University, U.K., in 2015. From December 2007 to April 2009, she was the Director of the Teaching and Learning Center (TLC), UST. From June 2015 to October 2019, she worked at UST. Since December 2019, she has been a Lecturer at the Department of Information Technology, Qassim University, Saudi Arabia. Her research interests include software engineering, ubiquitous computing, context-aware systems, and data mining.