The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial

Mohamed Amine Ferrag and Lei Shu, *Senior Member, IEEE*

***Abstract*—This article presents research challenges and a tutorial on performance evaluation of blockchain-based security and privacy systems for the Internet of Things (IoT). We start by summarizing the existing surveys that deal with blockchain security for IoT networks. Then, we review the blockchain-based security and privacy systems for seventeen types of IoT applications, e.g., Industry 4.0, software-defined networking, edge computing, Internet of Drones, Internet of Cloud, Internet of Energy, Internet of Vehicles, etc. We also review various consensus algorithms and provide a comparison with respect to the nine properties, such as latency, throughput, computation, storage, and communication costs, scalability, attack model, advantage, disadvantage, etc. Moreover, we present the security analysis techniques and provide a classification into four categories, including Burrows, Abadi, and Needham (BAN) logic, game theory, theory analysis, and AVISPA tool. In addition, we analyze the performance metrics, blockchain testbeds, and cryptography libraries used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks. Based on the current survey, we discuss the major steps to follow for building and evaluating blockchain-based security and privacy systems. Finally, we discuss and highlight open challenges and future research opportunities.**

***Index Terms*—Blockchain, experimentation environments, Internet of Things (IoT), privacy, security, testbeds.**

I. Introduction

TODAY, with the emergence of many low-cost and powerful devices, such as sensors and RFIDs associated with various communication media, the Internet of Things (IoT) has gained tremendous popularity, which offers a high potential for the development of not only different home automation systems but also various industrial applications, such as connected drones, connected health, smart farming, wearables, among other areas. The IoT market is projected to increase from over 15 billion devices in 2015 to more than 75 billion in 2025. This projection indicates that on average, there will be at least 25 personal IoT devices for every person on earth [1]. The large-scale and transverse nature of IoT systems, with the different elements and components associated with the implementation of such systems, has opened new security and privacy challenges [2], [3].

Currently, the "blockchain" is one of the most appropriate candidate technologies that can provide a secure and distributed ecosystem for IoT networks. The security characteristics that blockchain promises are unprecedented and truly inspiring [4], [5]. The concept of a blockchain-based IoT has attracted considerable research interest since decentralizing the IoT using the blockchain technology offers the following five potential advantages: 1) increases fault tolerance and eliminates single points of failure; 2) allows implementing secure software updates on IoT devices; 3) provides accountability and traceability since IoT data stored on the blockchain are immutable; 4) enhances the security by providing authentication, access control, and confidentiality; and 5) allows secure micro-transactions for IoT data [6]. Therefore, there are four primary types of blockchains, namely 1) public blockchain; 2) consortium blockchain; 3) private blockchain; and 4) hybrid blockchain. The public blockchain enables any person to join as miners, developers, users, or other members of the community. Each transaction on a public blockchain is fully transparent, which means that any person can view the details of the transaction. The public blockchain is accompanied with a token, which is usually developed to incentivize and reward network participants [3]. The private blockchain is a network that requires an invitation to join the service. The transactions are private and the network is more centralized than the public blockchain. The private blockchains are especially relevant for companies that want to collaborate and share data. The consortium blockchain is a private blockchain but governed by a group rather than a single entity. The hybrid blockchain combines the characteristics of both public and private blockchains, where members can decide who can participate in the blockchain or which transactions are made public.

In the literature, there are many surveys that covered different aspects of blockchain-based security and privacy systems for the IoT. As shown in Table I, we categorize the blockchain surveys according to the following criteria.

1) *IoT Application:* It states if the survey has provided a taxonomy for blockchain-based IoT applications.

Manuscript received November 2, 2020; revised February 16, 2021; accepted May 4, 2021. Date of publication May 6, 2021; date of current version December 7, 2021. This work was supported in part by the Research Start-Up Fund for Talent Researcher of Nanjing Agricultural University under Grant 77H0603, and in part by the National Natural Science Foundation of China under Grant 62072248. *(Corresponding author: Lei Shu.)*

Mohamed Amine Ferrag is with the Department of Computer Science, Guelma University, Gulema 24000, Algeria, and also with the NAU-Lincoln Joint Research Center of Intelligent Engineering, Nanjing Agricultural University, Nanjing 210031, China (e-mail: ferrag.mohamedamine@univ-guelma.dz).

Lei Shu is with the College of Artificial Intelligence, Nanjing Agricultural University, Nanjing 210031, China, and also with the School of Engineering, University of Lincoln, Lincoln LN6 7TS, U.K. (e-mail: lei.shu@ieee.org).

Digital Object Identifier 10.1109/JIOT.2021.3078072

TABLE I
RELATED SURVEYS ON BLOCKCHAIN FOR IOT NETWORKS

Reference	IoT application	Consensus algorithms	Security analysis techniques	Cryptography libraries	Performance metrics	Testbeds and experimentation environments
Kolb et al. [7]	No	Yes	No	No	Yes	No
Ferrag et al. [8]	Yes	Yes	No	No	No	No
Mehta et al. [9]	Yes	No	No	No	No	No
Belotti et al. [10]	No	Yes	No	No	No	Yes
Dai et al. [11]	Yes	Yes	No	No	No	No
Wu et al. [12]	Yes	Yes	No	No	No	No
Ferrag et al. [13]	Yes	No	No	No	No	No
Taylor et al. [14]	No	No	No	No	No	No
Bao et al. [15]	No	No	No	No	No	No
Mollah et al. [16]	No	Yes	No	No	No	No
Sengupta et al. [3]	Yes	No	No	No	No	No
Li et al. [17]	No	Yes	No	No	No	No
De Aguiar et al. [18]	No	Yes	No	No	No	No
Zhou et al. [19]	No	Yes	No	No	No	No
Our survey	Yes	Yes	Yes	Yes	Yes	Yes

2) *Consensus Algorithms:* It indicates whether the survey presented consensus algorithms and provided a comparative analysis.
3) *Security Analysis Techniques:* It states if the survey has provided the security analysis techniques used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.
4) *Cryptography Libraries:* It indicates whether the survey described cryptography libraries used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.
5) *Performance Metrics:* It indicates whether the survey described performance metrics used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.
6) *Testbeds and Experimentation Environments:* It indicates whether the survey considered testbeds and experimentation environments used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.

Most of the surveys on blockchain-IoT applications outline the countermeasures required for security and privacy without focusing on testbeds and experimentation environments. Some of them have limited their countermeasures covered to 3.0 applications [20], Internet of energy management [21], cyber–physical systems [22], industrial IoT [3], software-defined networks (SDNs) [23], smart contracts formalization or [24]. Ferrag *et al.* [8] focused on security and privacy countermeasures, threats models, blockchain-based solutions for smart agriculture. Kolb *et al.* [7] presented a centralized tutorial that explains the fundamental elements of blockchains using Ethereum as a case study. Therefore, there are recent studies that compare the consensus algorithms for blockchain-based security and privacy systems [4], [25]–[29]. Xiao *et al.* [4] reviewed the consensus algorithms based on the five-component scheme, which consists of an incentive mechanism, block finalization, information propagation, block validation, and block proposal. Ferdous *et al.* [25] studied the consensus algorithms regarding four properties, including performance, security, block and reward, and structural. Bodkhe *et al.* [26] analyzed the consensus algorithms for cyber–physical systems with respect to scalability and attacks, consensus finality, mining and consensus category, energy consumption, communication model and complexity, performance-related parameters, adversary tolerance model, and blockchain type. Lao *et al.* [27] compared the consensus algorithms based on eight properties, including throughput, vulnerability, advantage, blockchain type, disadvantage, tolerated power of adversary, transaction finality, and system scalability.

To the best of our knowledge, our survey is the first that thoroughly covers consensus algorithms, security analysis techniques, cryptography libraries, performance metrics, and testbeds and experimentation environments used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.

Our contributions in this work are as follows.

1) We review the blockchain-based security and privacy systems for IoT applications.
2) We present the security analysis techniques and provide a classification into four categories, including BAN logic, game theory, theory analysis, and AVISPA tool.
3) We present various consensus algorithms and provide a comparison with respect to the following nine properties: a) blockchain model; b) latency; c) throughput; d) computation, storage, and communication costs; e) scalability; f) attack model; g) advantage and disadvantage; h) application; and i) focus of each consensus algorithm.
4) We analyze the performance metrics used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.
5) We provide the blockchain testbeds and cryptography libraries used in the performance evaluation of blockchain-based security and privacy systems.
6) We discuss the major steps to follow for building and evaluating blockchain-based security and privacy systems.
7) We discuss and highlight open challenges and future research opportunities.

This tutorial article is organized into eight main sections, as shown in Fig. 1. Section II presents the blockchain-based security and privacy systems for seventeen types of

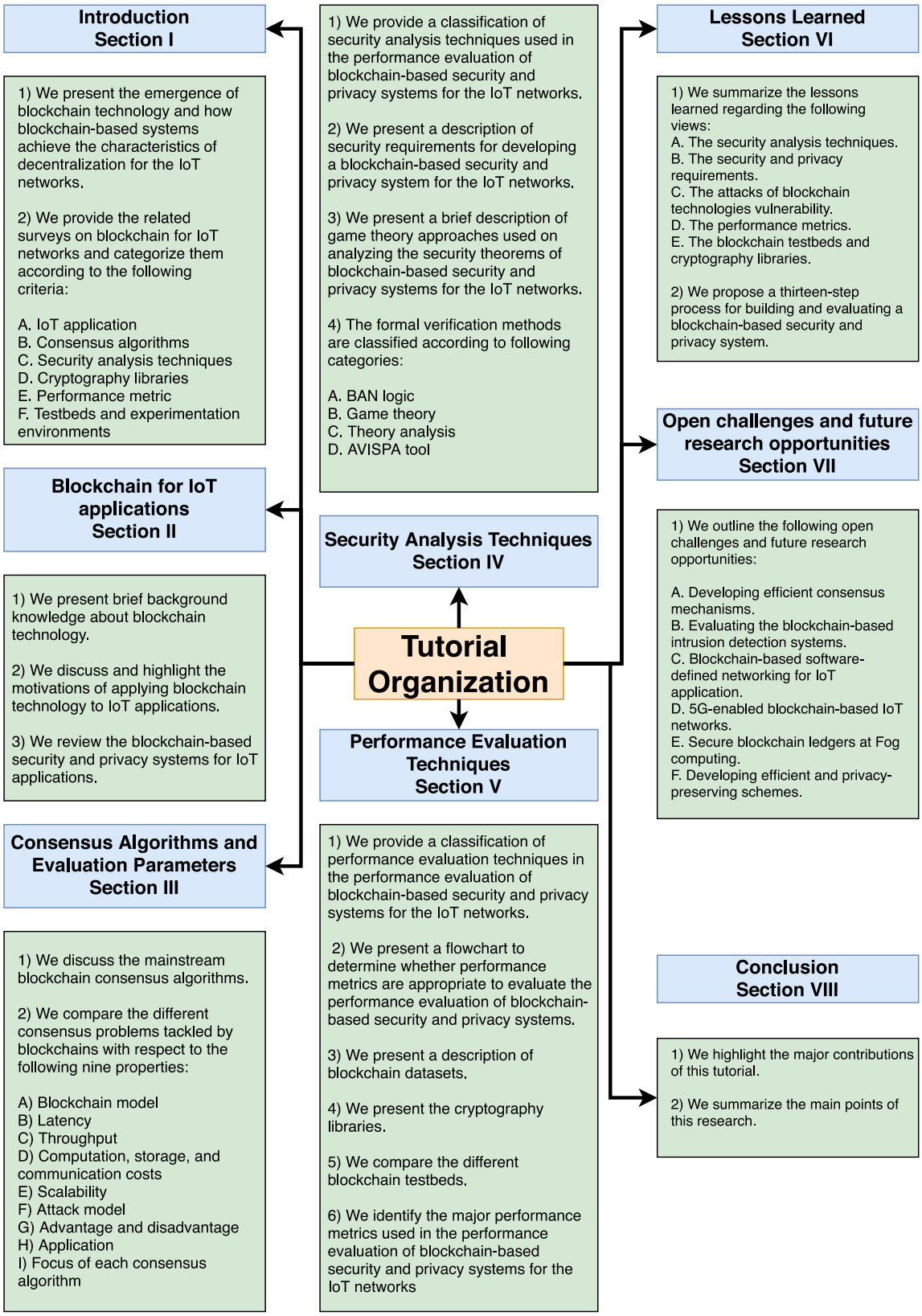

Fig. 1. Organization of the tutorial.

IoT applications. In Section III, we analyze various consensus algorithms and evaluation parameters. In Section IV, we present the security analysis techniques and provide a classification into four categories. In Section V, we provide the performance evaluation techniques used in the performance evaluation of blockchain-based security and privacy systems

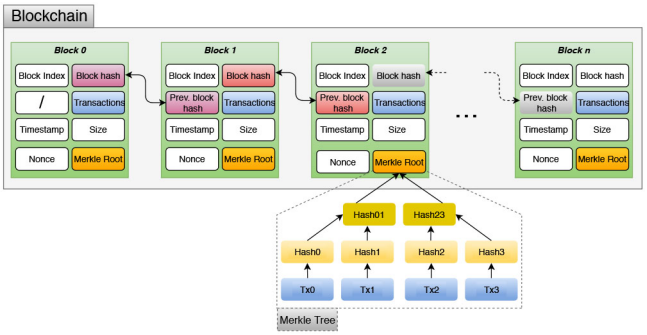

Fig. 2. Blockchain is composed of a list of consecutively connected blocks.

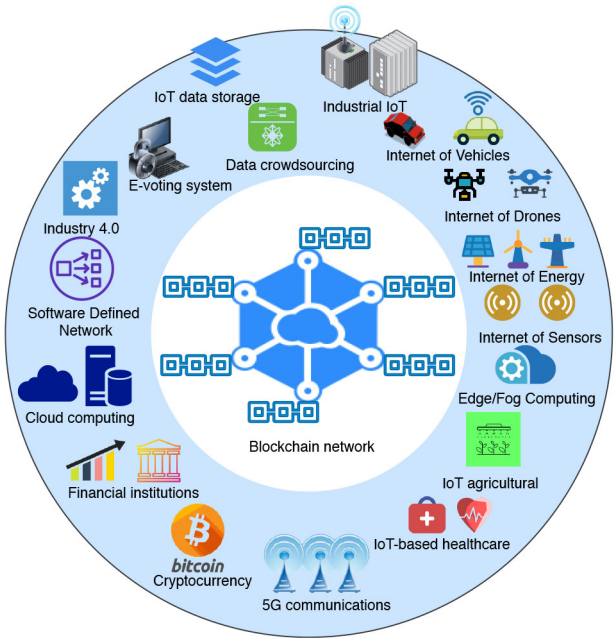

Fig. 3. Blockchain technology applied to seventeen types of IoT applications.

for the IoT networks. Then, we discuss the lessons learned in Section VI and highlight open challenges and future research opportunities in Section VII. Finally, Section VIII presents conclusions.

II. Blockchain for IoT Applications

The blockchain technology is used by the security and privacy systems for the IoT networks as a permanent, public, transparent ledger system for recording all transactions of data. This chain is a linear set of blocks, starting with a first block considered valid by default, which is called a genesis block, as presented in Fig. 2. The blocks are built and chained according to precise rules using a consensus algorithm, which is defined by the network. The validator prepares its block by collecting the new transactions, verifying that they follow the rules, and then including them in the block [13]. The data recorded in the blocks are considered very hard to change and become unforgeable after a period of time. A transaction is considered confirmed when it is included in a validated block. Each block has an identifier, which is a unique cryptographic hash of the data stored in the block [25]. In addition, a block consists of two parts: 1) a block header and 2) the transactions, used to build a Merkle tree. Specifically, a Merkle tree consists of hashing the transactions, then collecting the resulting in pairs and hashing them, and continuing until a single hash called the Merkle Root is obtained. Based on the cryptographic hash chain, this structure is very effective in proving that a complete chain of transactions has remained unchanged [4].

As illustrated in Fig. 3, the blockchain technology can be effectively applied in almost all domains of IoT. In this section, we review the blockchain-based security and privacy systems proposed for seventeen types of IoT applications.

A. Internet of Vehicles

The blockchain technology is used by authentication schemes for the Internet of Vehicles as a distributed peer-to-peer network to manage the ledger that stores vehicle-related information. Noh *et al.* [30] developed a distributed data authentication system using blockchain technology for the Internet of Vehicles, which vehicles are capable of authenticating and validating distributed broadcast data. The proposed system can prevent multiple insider attacks, in which two types of attacks are considered: 1) passive and 2) active. The passive attacks include sniffing, which does not disrupt or damage the target, while active attacks affect the target by falsifying information. Tan and Chung [31] proposed a secure authentication scheme with group key establishment, which is based on the consortium blockchain for vehicular networks. The proposed scheme develops the following three security strategies: 1) certificateless authentication strategy; 2) group key distribution strategy; and 3) dynamic group key updating strategy. The certificateless authentication strategy is used to solve the problem of key escrow in identity-based encryption for cloud-based VANETs with edge computing infrastructure. The group key distribution strategy is used for deploying consortium blockchain in decentralized vehicle-to-vehicle networks, while the dynamic group key updating strategy is used for dynamic updating using the Chinese remainder theorem.

B. Internet of Drones

With the help of the blockchain-based solution, the Internet of Drones overcomes the need for third-party systems to maintain trust as well as ensure high security to the drone communication network. The Internet of Drones has attracted growing attention and is projected to be an important supporting element of the future IoT thanks to its significant benefits in terms of deployment flexibility, high flexibility of mobility and low cost. To broadcast and store the group's key messages in the Internet of Drones, Li *et al.* [32] designed a private blockchain, which is constructed by the ground control station. The drones are able to retrieve lost group keys securely and rapidly using a basic mutual healing protocol. To achieve privacy preservation in drone-delivered services, Ferrag and Maglaras [33] designed an intrusion detection system with a delivery framework, called

DeliveryCoin, which is based on bilinear groups and machine learning approaches. A UAV-aided forwarding mechanism is adopted for achieving a consensus inside, while the machine learning approaches are used for detecting false transactions between self-driving nodes as well as detecting self-driving network attacks. Bera *et al.* [34] considered several drones deployed in different flying zones that communicate with each other, and the information is collected by the ground station server. To enable secure communication between the drones, but also between the drones and the ground station server, the authors introduced a secure blockchain-based access control scheme, in which the blocks are added using the ripple protocol consensus algorithm. Islam and Shin [35] integrated the mobile edge computing and proposed a blockchain-based data acquisition process for the unmanned aerial vehicles-assisted IoT. Specifically, mobile edge computing is used for validates the data and the identity of the sender.

C. Internet of Energy

The adoption of the blockchain framework for the Internet of Energy enables the protection of confidentiality, privacy, and integrity of electricity data. Sheikh *et al.* [36] designed a secured energy trading scheme between electric vehicles and the distribution network. For checking the blocks in the blockchain network, a Byzantine consensus algorithm is used for energy exchange between electric vehicles and the distribution network. The electric vehicles in a parking area can be involved in the process of exchanging energy with a distribution network according to its storage capacity and charging limits. For secure peer-to-peer (P2P) trading and decentralized scheduling within the energy management systems in local energy grids, Yang *et al.* [37] designed an automated demand response scheme, named ADR, which can increase the P2P trading security. To coordinate the consumption behaviors of responsive executors, the ADR scheme adopts a price-sensitive game-theoretic model and a smart contract mechanism. The ADR framework can coordinate actions and balancing supply and demand by taking into account the load transfer of plug-in electric vehicles, vehicle-to-grid support, and energy storage system. For privacy preserving in wide-area (multiarea) smart grids, Kurt *et al.* [38] proposed a distributed dynamic state estimation mechanism. To protect against attacks and data manipulation, the proposed mechanism adopts the blockchain technology. The blockchain operates on the peer-to-peer network of local centers for detecting the measurement anomalies as well as misbehaving. To deal with the exchange of excess energy among neighboring nodes in the Internet of Energy, Ferrag and Maglaras [39] designed a blockchain-based scheme, named DeepCoin, which is based on bilinear pairing, short signatures, and hash functions to achieve privacy preservation. The DeepCoin scheme adopts the practical Byzantine fault tolerance (PBFT) algorithm for build consensus inside blockchain-based energy network. For detecting fraudulent transactions and network attacks, the DeepCoin scheme uses an intrusion detection system based on recurrent neural networks.

D. Cloud Computing

The existing cloud manufacturing concept can be combined with the blockchain technology, which the IoT devices can be trusted without reliance on a trusted third party. Zhu *et al.* [40] proposed to integrate cloud manufacturing with blockchain technology in order to own both centralization and decentralization features. There two types of data stored in the blocks, namely smart contracts and transactions. For global payment, the proposed system created the Cloud manufacturing cryptocurrency, which is based on two methods. One is allocating the Cloud manufacturing cryptocurrency to the initial miners by a genesis file, while the second is creating the Cloud manufacturing cryptocurrency with block rewards for miners. Wei *et al.* [41] proposed a blockchain data-based cloud data integrity protection mechanism, which is based on mobile agent technology. The proposed mechanism adopts a distributed virtual machine agent model that is deployed to the cloud. Specifically, the integrity framework based on the blockchain is built by the virtual machine proxy model, and the unique hash value for the file generated by the Merkel hash tree is used to control the data exchange by the smart contract, and the resulting data is delivered on time.

E. IoT Agricultural

The role of blockchain technology in IoT agriculture focuses on three keys, namely supporting farmers in tracing food origins, enable peer-to-peer agricultural transactions through smart contracts, and guarantee agriculture data integrity [8]. Based on double chain architecture, Leng *et al.* [42] designed a public blockchain of the agricultural supply chain system, which can provide adaptive rent-seeking and matching mechanism for public service platform. Through elliptic curve cryptography, the proposed system ensures the transparency with security and privacy of transaction data. For the traceability and the certification of extra virgin olive oil, Arena *et al.* [43] proposed a blockchain-based application, named BRUSCHETTA, which can trace the production from the plantation to the shops. Therefore, production and sales records are often falsified. Shih *et al.* [44] used the blockchain to guarantee the authenticity of organic vegetables by proposing a marketing environment using Ethereum. The proposed scheme can increase organic vegetable sales and solve the issue of ecological agricultural pollution. To prevent distributed denial-of-service attacks in smart agriculture, Wu and Tsai [45] proposed an intelligent agriculture network security system, which is based on private blockchains. The proposed system applies the bilinear pairings technology to guarantees privacy and integrity in information transmission.

F. IoT-Based Healthcare

Many researchers have tried to apply emerging blockchain technology into the field of healthcare for providing the security and privacy of healthcare data sharing. Wang *et al.* [46] proposed a framework of parallel healthcare systems, named PHSs, which is based on parallel execution approach, the artificial systems, and blockchain technology. The artificial systems are proposed to represent and model the static and dynamic

characteristics of patients and doctors, while blockchain technology is used to facilitate the sharing of electronic health records, records review and auditability of care. For transparent and secure information sharing in structure health monitoring, Jo *et al.* [47] introduced a blockchain-based distributed network, which smart contracts are constructed for autonomous decision making and control. The proposed network adopts the Proof-of-Work (PoW) consensus mechanism in combination with the SHA-256 hash function.

G. IoT-Based NFV/SDN

SDN separates the network hardware from the control mechanism in order to allow easy control and management [48]. The SDN and network function virtualization (NFV) can be coupled with blockchain technology for IoT networks. Therefore, an SDN/NFV architecture for blockchain-based IoT applications is based on four layers, namely perception layer, data plane, virtualization and control plane, and blockchain layer. The perception layer consists of collecting the data from the environment (i.e., things). The data plane enables data transfer to and from the perception layer through IoT gateways. The virtualization and control plane is used to dynamically allocating resources to virtualized controllers. The blockchain layer plays the role of storing data, broadcast the mining and transaction information, and managing a P2P network using a consensus algorithm. To support the efficiency and security of IoT-based NFV/SDN, Rawat [49] combine three technologies, including blockchain technology, software-defined networking, and edge computing. The ultimate goal of this combination is to decrease trade frictions and enhance transparency and trust between participants/stakeholders, as well as to enable a more transparent and dynamic exchange of spectrum and information technology resources in the emerging wireless network. Therefore, Chaudhary *et al.* [50] combined Blockchain with SDN for intelligent transportation systems. Specifically, they proposed a Blockchain-based secure energy trading scheme, named BEST, which the SDN is used for transferring energy trading requests from electrical vehicles to the master controller. The BEST scheme uses blockchain to authenticating and validating participating in electrical vehicles. The SDN architecture adopted by the BEST scheme is composed of three planes, including application, control, and data planes. This blockchain-based SDN architecture provides availability, integrity, confidentiality, and availability to network infrastructure.

H. Edge/Fog Computing

The blockchain technology is applied for Edge/Fog Computing-based IoT networks to achieving the data recoverability property. The edge artificial intelligence-enabled IoT is addressed by Lin *et al.* [51], which they proposed a peer-to-peer knowledge market scheme, which is shown in Fig. 4. The proposed scheme is secure and can provide knowledge management and trading. Therefore, the proposed scheme uses three news mechanisms, namely proof of trading, smart contracts, and cryptographic currency knowledge coin. Based on the primitive of blockchain, Huang *et al.* [52] designed a

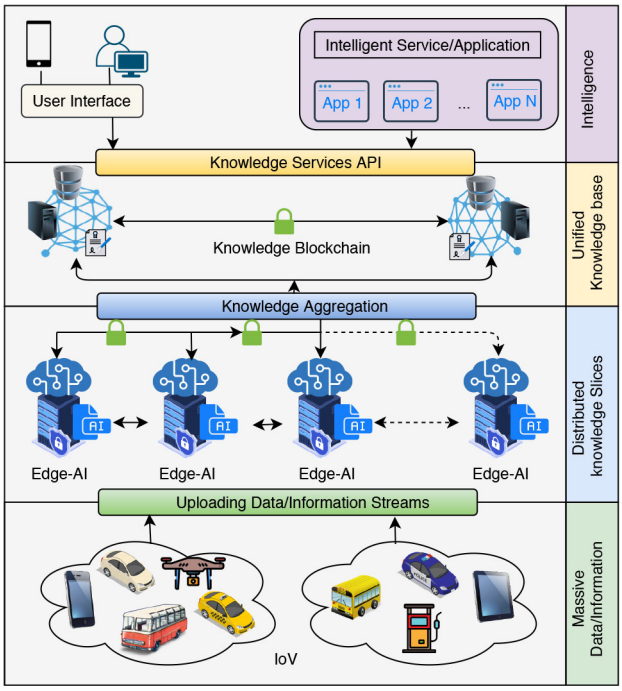

Fig. 4. Edge/fog computing architecture for blockchain-based IoT applications.

fair three-party contract signing protocol for the decentralized fog computing environment. The proposed protocol allows members to contract equitably without the assistance of an arbitrator. Moreover, to protect the privacy of contract content, the proposed protocol adopts the threshold public-key encryption with verifiable encryption. For providing video streaming with mobile edge computing, Liu *et al.* [53] presented a blockchain-based mobile edge computing architecture, where small base stations deploy their computational and communication resources. Based on the transactional information on the blockchain, the components of the proposed architecture (i.e., users, base stations, and video providers) adapt their policies to allow a self-organized video broadcast and transcoding service to run without a centralized controller.

I. Internet of Sensors

To provide decentralized and fine-grained authorization for the Internet of Sensors, Zhang *et al.* [54] designed a collaborative access control scheme, named ABAC, which is based on attributes. The ABAC scheme uses blockchain technology to produce a numeric account for each device to store the access attributes and policy that are used for authorization. When trustworthy collaboration is needed, the ABAC scheme adopts a controlled and verifiable collaboration mechanism, which can prevent unwanted collaboration. However, there are other challenges in the Internet of Sensors, namely data sharing and key-leakage. To solve these challenges, Niu *et al.* [55] designed a blockchain-based key aggregation searchable encryption scheme, named BAI-KASE, for achieving data sharing in the Internet of Sensors. The BAI-KASE is proven secure under the decisional Diffie–Hellman assumption and Goldreich–Leivin Theorem. The BAI-KASE adopts

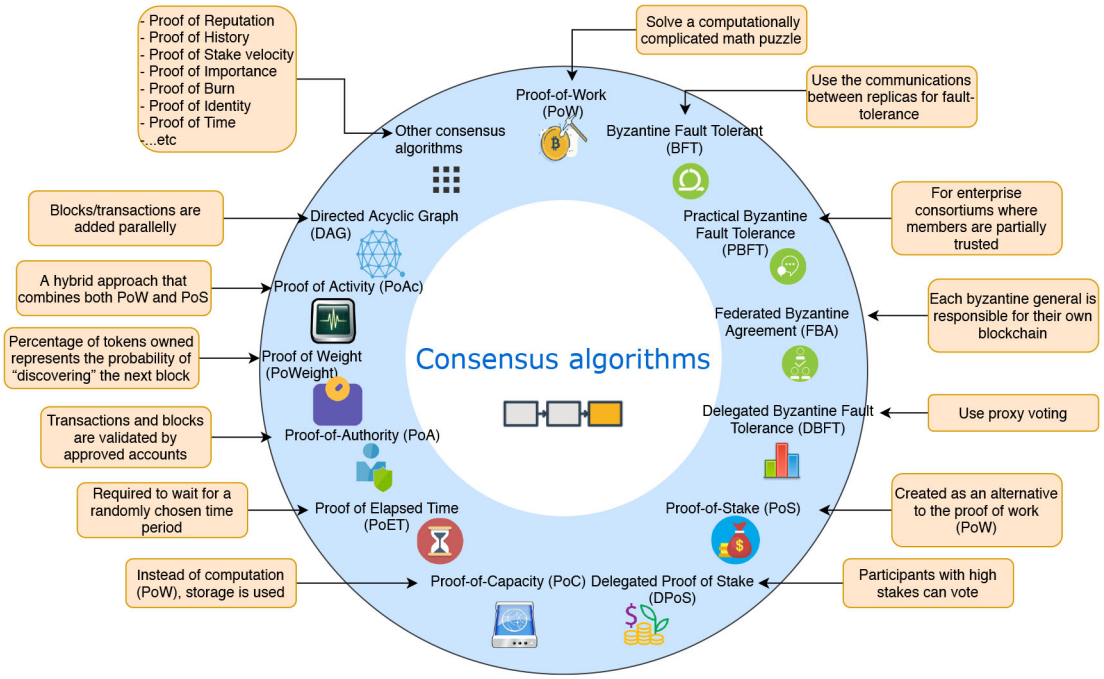

Fig. 5. Several types of consensus algorithms for blockchain-based security and privacy systems.

a data-sharing system, which is based on private and public blockchain with PoW consensus mechanism and PBFT algorithm.

To provide reliable auditing of user's access history in the Internet of Sensors (i.e., Smart Homes), Lin *et al.* [56] designed a blockchain-based secure mutual authentication system, named HomeChain, that can be implemented in intelligent home systems. Based on the elliptic curve integrated encryption scheme (ECIES), the HomeChain system provide confidentiality of the transmitted message, including the response data and the request transaction data. To enable a group member to anonymously request remote access or control, the HomeChain system adopts the group signatures.

III. Consensus Algorithms and Evaluation Parameters

Consensus algorithms are a critical part of each blockchain IoT network since they are responsible for ensuring the integrity and security of these distributed systems. Therefore, the decentralized public IoT blockchains are implemented as distributed systems and since they are not under the control of a central authority, the distributed nodes are required to agree on the validity of the transactions [57]. This is where consensus algorithms are involved. Specifically, a consensus algorithm ensures that protocol rules are followed and that all transactions are reliably processed.

A. Consensus Algorithms

There are several types of consensus algorithms for blockchain-based security and privacy systems [27], [28], as presented in Fig. 5. Each consensus algorithm has advantages and disadvantages when attempting to achieve a successful balance between scalability, security, and functionality.

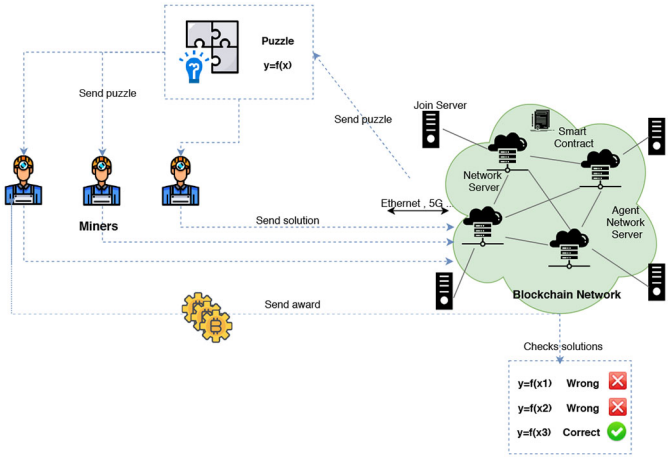

Fig. 6. PoW consensus algorithm, where miners competing to solve a computationally complicated math puzzle in order to perform transactions on the blockchain network and are rewarded afterward.

1) Proof of Work: The PoW algorithm was introduced by Nakamoto [58]. It is designed first to minimize jamming emails and then implemented by Bitcoin. The PoW algorithm is used to confirm transactions and produce new blocks in the blockchain-based security and privacy systems. Specifically, there are IoT nodes, called miners, competing to solve a computationally complicated math puzzle in order to perform transactions on the blockchain network and are rewarded afterward, as presented in Fig. 6. The blockchain-based security and privacy systems that use PoW as a consensus algorithm become resistant to falsification due to the high cost of calculation. Nevertheless, a blockchain system running PoW may also be attacked in the mining operation in which an attacker can gain more profit by launching mining and corruption attacks [27].

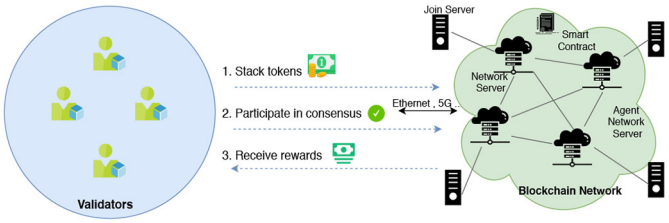

Fig. 7. PoS consensus algorithm, where validators can produce the next block based on their stake.

2) Byzantine Fault Tolerant: This is a well-known issue in distributed computing which is typically solved with Byzantine generals. The issue is that a group of Byzantine generals with different parts of the Byzantine forces have circled a city. They should agree in agreement whether to launch an attack or not. When certain generals launch an attack alone, it will end in tragedy for their siege. The generals are mostly split by distance and are required to transmit some messages in order to communicate. The blockchain-based security and privacy systems that use Byzantine fault tolerant (BFT) as a consensus algorithm become fast and scalable but it used usually for private and permissioned IoT networks [59].

3) Practical Byzantine Fault Tolerance (PBFT): It is one solution to the Byzantine generals problem, proposed by Castro *et al.* [60], which consists of a minimum of $3f+1$ nodes in order to tolerate f defective nodes. The blockchain-based security and privacy systems that use PBFT as a consensus algorithm will have high transaction throughput, but they are centralized and permissioned.

4) Federated Byzantine Agreement: It is another solution to the Byzantine generals problem, where each Byzantine general is responsible for their own blockchain. The federated Byzantine agreement (FBA) consensus is used by Stellar and Ripple [61] which they use quorum slices to reach consensus. The blockchain-based security and privacy systems that use FBA as a consensus algorithm will have low transaction costs, network scalability, and high throughput, but there are trust requirements that should to archives.

5) Delegated Byzantine Fault Tolerance: This consensus was introduced by NEO, which provides a fault tolerance of $f = [(n-1)/3]$ for blockchain-based security and privacy system composed of n nodes. The delegated Byzantine fault tolerance (DBFT) consensus is similar to delegated Proof of Stake (PoS) that allows for large scale collaboration in consensus through proxy voting. The blockchain-based security and privacy systems that use DBFT as a consensus algorithm will have network scalability, high throughput, and high transaction costs.

6) Proof of Stake: To address the issues inherent in PoW, the PoS consensus was developed as an alternative. Specifically, the PoS consensus is based on a completely different approach than PoW and requires no special computing power [62]. Rather than use mining, there should be a certain stake (coins) in the system. More this amount is important, more chances a node will be chosen to update the register of a blockchain, as presented in Fig. 7. The blockchain-based security and privacy systems that use PoS as a consensus algorithm will have the advantage that no large quantities of energy are required to secure a blockchain, but it is vulnerable to the nothing-at-stake problem.

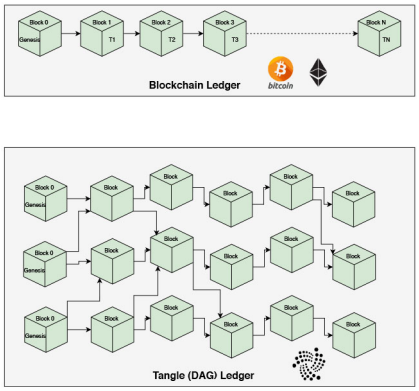

Fig. 8. Difference between blockchain and tangle ledgers.

7) Delegated Proof of Stake: This consensus aims to address the weaknesses of PoS and PoW by proposing a hybrid model. The Delegated PoS (DPoS) consensus operates on the same basic principle as PoS. The IoT nodes in charge of forging blocks must be elected by the community members. The election system ensures that the blockchain is not controlled by a minority of nodes, as can be the case of a miner with a large amount of computing power or a PoS forger with a very large amount of tokens [63]. The blockchain-based security and privacy systems that use DPoS as a consensus algorithm will have the advantage to define a fully participative organization.

8) Directed Acyclic Graph: Unlike the linear structure that is basically adopted by any blockchain system, the directed acyclic graph (DAG) consensus applies an alternative approach to adding the blocks based on parallelism. Specifically, the blocks/transactions are not concatenated in a chained list but in a hierarchy tree [64], as shown in Fig. 8. There are some popular projects which use DAG consensus, including RaiBlocks/Nano, Byteball, HashGraph, and Iota. The blockchain-based security and privacy systems that use Proof of Activity (PoAc) as a consensus algorithm will have high scalability with high communication costs.

9) Other Consensus Algorithms: More consensus algorithms are available which can be adapted by blockchain-based security and privacy systems for IoT networks. The following consensus algorithms are cited: proof of reputation, proof of history, PoS velocity, proof of importance, proof of burn, proof of identity, proof of time, proof of capacity, Proof of Elapsed Time (PoET), Proof of Authority (PoA), Proof of Weight (PoWeight), and PoAc.

B. Evaluation Parameters

In the literature, there are recent studies that compare the consensus algorithms for blockchain-based security and privacy systems [4], [25]–[29]. Therefore, in this tutorial, we compare the consensus algorithms with respect to the following nine properties.

1) *Blockchain Model:* The blockchain-based security and privacy systems for the IoT networks can be divided into two different categories, namely permissioned and

TABLE II
COMPARISON BETWEEN CONSENSUS ALGORITHMS USED IN THE PERFORMANCE EVALUATION OF BLOCKCHAIN-BASED SECURITY AND PRIVACY SYSTEMS FOR THE IOT NETWORKS

Cons.	Model	Latency	Throughput	(C), (S), (Com)	Scalability	Attack model	(+) Pros (-) Cons	Application	Focus of this consensus
PoW	Permissionless	High	Low	(C) High (S) High (Com) Low	Low	Selfish Mining	+ Resistant to falsification - Vulnerable to mining and corruption attacks	- Bitcoin	- Miners are competing to solve a computationally complicated math puzzle. - Each fog node at the fog computing layer are selected as miners.
BFT	Permissioned	Low	High	(C) Low (S) High (Com) High	Low	33% vulnerability	+ Fast and scalable with low transaction cost - High communication cost	- Tendermint	-Improves fault-tolerance using exploitation of communications between IoT devices and fog nodes.
PBFT	Permissioned	Low	High	(C) Low (S) High (Com) High	Low	33% vulnerability	+ High transaction throughput - High communication cost	- Hyperledger Fabric	- The fog nodes create PRE-PREPARE messages to propose to the other replicas the scheduling of the bloc.
FBA	Permissionless	High	High	(C) Low (S) High (Com) High	High	Reputation-based attacks	+ Low transaction costs, network scalability, and high throughput - Trust requirements	- Stellar	- Use quorum slices to reach consensus. The quorum is a set of nodes sufficient to reach agreement. - The IoT node can appear on multiple quorum slices.
DBFT	Permissioned Permissionless	Low	High	(C) Low (S) High (Com) High	High	33% vulnerability	+ Fast and scalable with low computing cost - High communication cost	- Neo	- Allows for large scale collaboration in consensus through proxy voting in the sensors layer.
PoS	Permissionless	Medium	High	(C) Medium (S) High (Com) Low	Low	Service-based attacks	+ Ensure the reliability of the system - Nothing-at-stake problem	- Peercoin - Nxt	- Users holding more currency are more chances to update the register of a blockchain. - All IoT nodes in the sensors layer are selected as the validators.
DPoS	Permissionless	Medium	High	(C) Medium (S) High (Com) Low	High	Manipulation-based attacks	+ More scalable than PoW and PoS-based blockchains - Vulnerable to centralization	- BitShares - EOS	- Uses voting and election process. - Each fog node at the fog computing layer is selected as a delegate.
PoC	Permissionless	High	Low	(C) Low (S) High (Com) Low	Low	- Selfish Mining	+ Can be used for malware detection and denial of service attack prevention - Lost disk space	- SpaceMint - Burstcoin	- Uses the disk idle space of computers in the local area for mining. - Each fog nodes at the fog computing layer are selected as miners.
PoET	Permissioned	Low	High	(C) Low (S) High (Com) Low	High	Reputation-based attacks	+ Prevents high resource utilization - Not appropriate for public blockchains.	- Hyper-Ledger Sawtooth	- Each IoT device at the sensors layer generates a random wait time and sleeps for a fixed period of time.
PoA	Permissionless	Low	Low	(C) Low (S) High (Com) Low	High	Reputation-based attacks	+ Less computational overhead - Trust requirements	- VeChain	- New blocks can only be generated by nodes with authority. - Select all fog nodes in fog computing layer as validators.
PoWe	Permissionless	Medium	Low	(C) Medium (S) High (Com) Low	Low	Service-based attacks	+ Ensure the reliability of the system - Nothing-at-stake problem	- Algorand	- The proportion of coins owned in the sensors layer refers to the probability of finding the next block.
PoAc	Permissionless	High	Low	(C) High (S) High (Com) Low	Low	Selfish and reputation-based behaviors (e.g., Selfish Mining)	+ Resistant to falsification - Vulnerable to mining and corruption attacks	- Decred	- Miners are competing to solve a computationally complicated math puzzle. - A group of fog nodes in the fog computing layer is selected randomly as validators for validating or signing the new block.
DAG	Permissioned	Medium	High	(C) Medium (S) Medium (Com) High	High	Cryptanalytic attacks	+ High scalability with energy efficient - High communication costs	- Byteball - HashGraph - Iota	-A set of the transactions added to the Tangle's DAG are selected as valid by a fog node called Coordinator.

(C) Computation, (S) Storage, (Com) Communication

permissionless. Permissioned blockchains require access to be allowed to be part of the network. There are three types of blockchain permissioned ledger technologies, including public blockchains, federated/consortium blockchains, and private blockchain. However, the permissionless blockchains require no authorization to access and communicate with, which means that anyone can join the network.

2) *Latency:* This metric indicates the time taken to create the next block of transactions in the blockchain network.
3) *Throughput:* This indicates two metrics, namely a) read throughput and b) transaction throughput. The read throughput is a metric of the total number of reading transactions performed within a defined period of time. The transaction throughput is the ratio of valid transactions that are initiated by specific configurations of the blockchain within a defined period of time.
4) *Computation, Storage, and Communication Costs:* The blockchain-based security and privacy systems for the IoT networks can be categorized based on performance

metrics, such as computation cost, storage cost, and communication cost.

5) *Scalability:* This metric indicates two main scalability problems, namely a) the time required to insert a transaction in the block and b) the time required to reach a consensus.
6) *Attack Model:* This metric shows the vulnerability of the blockchain-based security and privacy systems for the IoT networks in case of failures. In this tutorial, we use the threat models presented in the study [13]. Specifically, the threat models against blockchain networks are categorized into five main categories, namely service-based attacks, reputation-based attacks, identity-based attacks, manipulation-based attacks. The service-based attacks include collusion attack, double-spending attack, refusal to sign attack, and DDoS/DoS attack. The reputation-based attacks include whitewashing and hiding blocks attack. The cryptanalytic attacks include quantum attacks. The identity-based attacks include sybil attack, impersonation attack, replay attack, and key attack. The manipulation-based attacks include man-in-the-middle attack, modification attack, overlay attack, tampering attack, and false data injection attack.
7) *(+) Pros (−) Cons:* This metric indicates the important advantage and disadvantages of each consensus algorithm by considering the security level and performance-related parameters.
8) *Application:* This presents the available projects that use each consensus algorithm.
9) *Focus of the Consensus Algorithm:* This indicates the basic idea of each consensus algorithm.

Table II presents the comparison between consensus algorithms used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks. Regarding the scalability and high transaction time cost, the PoS, DAG, FBA, PoET, DPoS, and DBFT provide high performance. The PoW, FBA, PoC, PoAc provide high latency with security levels. Therefore, from the table, we can see that each consensus algorithm has several different levels of advantages and disadvantages, which means that they are suitable for different situations.

IV. Security Analysis Techniques

To evaluate and analyze the security of blockchain-based systems for the IoT networks, security researchers use the following formal security techniques: BAN logic, Game theory, Theory analysis, ProVerif tool, and AVISPA tool, as presented in Table III.

TABLE III
Security Analysis Techniques Used in the Performance Evaluation of Blockchain-Based Security and Privacy Systems for the IoT Networks

Year	Scheme	IoT application	Security analysis technique
2021	Vangala et al. [65]	IoT agricultural	AVISPA tool
2021	Xu et al. [66]	Internet of Vehicles	ProVerif tool
2020	Noh et al. [30]	Internet of Vehicles	BAN logic
2020	Cheng et al. [67]	IoT-based healthcare	BAN logic
2020	Wilczyński et al. [68]	Cloud computing	Game theory
2019	Lai et al. [69]	Internet of Vehicles	Theory analysis
2019	Luo et al. [70]	Internet of Vehicles	Theory analysis
2019	Yao et al. [71]	Internet of Vehicles	Theory analysis
2019	Zhang et al. [72]	IoT-based cryptocurrency	Theory analysis
2019	Bera et al. [34]	Internet of Drones	AVISPA tool
2019	Yang et al. [37]	Internet of Energy	Game theory
2019	Zhang et al. [73]	Edge/Fog computing	Game theory
2019	Lin et al. [56]	Internet of Sensors	Theory analysis
2019	Lin et al. [51]	Edge/Fog computing	Game theory
2019	Wang et al. [74]	Edge/Fog computing	Game theory
2019	Qiu et al. [75]	Internet of Drones	Game theory
2019	Li et al. [76]	Internet of Energy	Game theory
2019	Liu et al. [53]	Edge/Fog computing	Game theory

A. Formal Verification Method

1) Burrows, Abadi, and Needham Logic [98]: It is a widely used analysis model for identity authentication protocols. Noh *et al.* [30] verified the correctness of their proposed system formally, which they use BAN logic based on the following four steps: 1) idealization; 2) assumptions; 3) goals; and 4) verification. The idealization concerns the form of the data. The assumptions concern the relationship between entities and keys. The goals concerns traceability, nonrepudiation, strong privacy preservation, and message integrity. The verification concerns the prove of the hypotheses with the rules of the BAN logic. Cheng *et al.* [67] used BAN Logic to analyze the correctness of the medical data sharing scheme for medical cyber–physical systems.

2) Game Theory: Game theory is a natural approach to addressing competition and decentralized decision-making in the IoT. Tan and Chung [31] used the game theory for analyzing the security theorems of their scheme in terms of the unforgeability against adaptive chosen message attack, resistance to replay attack during authentication phase, preventing unauthorized tracking to specified vehicles, and provide certificateless authentication property. These terms are defined through the games with random oracles by operating the queries from the adversary and the challenger. Therefore, Cheng *et al.* [81] analyzed the incentive mechanism used in their semicentralized scheme with a game theory model. Specifically, they define two-time cost, including travel time as $\omega(\omega > \mu > 0$ and interaction time as $\mu(\mu > 0)$.

1) *Stackelberg game* is a nonsymmetrical game, in which a player named leader has a preferred position and decides first, when the remaining players—the followers—follow his actions. Qiu *et al.* [75] used a game-theoretic approach, called Stackelberg, to perform the spectrum trading and operations among the buyer and seller. Specifically, a Stackelberg game is a strategic game that involves a leader and multiple trackers in competition with each other over some resources. In the proposed scheme, the authors formulate the mobile network operator as the leader and the unmanned aerial vehicle operators as the trackers. Li *et al.* [76] used a Stackelberg game for modeling the energy allocation between microgrids and miners in the Internet of Energy. The microgrid is considered as a game leader that offers a nonuniform pricing strategy for different miners. Wilczyński and Kołodziej [68]

TABLE IV
PERFORMANCE METRICS AND CRYPTOGRAPHY TECHNOLOGIES USED IN THE PERFORMANCE EVALUATION OF BLOCKCHAIN-BASED SECURITY AND PRIVACY SYSTEMS FOR THE IOT NETWORKS

Year	Scheme	IoT applications	Cryptography technology	Consensus algorithm	Performance metric	(+) Pros (-) Cons
2020	Shen et al. [108]	IoT data storage	- Homomorphic cryptosystem and Paillier	PoW consensus mechanism	- Time consumption (s) - Accuracy (%)	+ Confidentiality of the sensitive data - The proposed scheme is not evaluated with cyber attack datasets.
2020	Ma et al. [109]	Data crowdsourcing	- Ciphertext-policy attribute-based encryption - Hash function	N/A	- Cost of smart contracts (USD) - Cost for running data trade (USD)	+ Fine-grained authorization - Data reliability is not considered
2020	Zhang et al. [54]	Internet of Sensors	- Ellipse curve cryptography - Hash function	Solo consensus algorithm	- Computational cost - Storage overhead for IoT devices (bytes) - Time cost (ms)	+ Provide credible credentials - Non-repudiation is not considered
2020	Zhu et al. [40]	Cloud Computing	Public key and SHA256	Open-source consensus standards	- Transaction overhead (USD) - Average number of transaction per second	+ Own both centralization and decentralization features - Whitewashing attack is not analyzed
2020	Liu and Zhang [110]	IoT data storage	- Ellipse curve cryptography asymmetric algorithm - Hash function	Equity-based proof of stake (PoS)	- Speed of encryption (min) - Time complexity (ms) - Encryption accuracy (%)	+ ECC encryption algorithm is efficient compared to RSA and DSA algorithms - Anti-key-leakage attack is not analyzed
2020	Kabra et al. [111]	Financial institutions	- QR based authentication algorithm	Proof-of-Authority (PoA)	- Communication cost - Computation time	+ Provenance and auditability attacks - Non-repudiation is not considered
2020	Noh et al. [30]	Internet of Vehicles	- Message authentication code - Ellipse curve cryptography - Advanced encryption standard	PBFT consensus algorithm	- Consensus delay	+ Authenticate the broadcast data in a distributed manner - Sybil attack is not analyzed
2020	Nkenyereye et al. [79]	Edge/Fog Computing	Signcryption scheme without bilinear pairings - Hash function	Proof of stake consensus algorithm	- Computational cost - Signcryption/Designcryption time (s) - Communication cost	+ Achieves the confidentiality and integrity - Location privacy is not considered
2019	Tan and Chung [31]	Internet of Vehicles	- Ellipse curve cryptography - Hash function - Chinese remainder theorem	N/A	- Communication cost - Computation cost (ms) - Storage overhead (bits)	+ Enables accurate group management in a distributed manner - Trust and access control are not considered
2019	Lai et al. [69]	Internet of Vehicles	- Randomized RSA-based partially blind signature - Pseudonym management mechanism - One-way hash function	N/A	- Computational complexity - The influence of the number of users on the amount of data	+ Ensure completion quality and achieve payment control for vehicle users - Double spending and 51% attacks are not analyzed
2019	Cheng et al. [81]	Internet of Vehicles	- Ciphertext policy attribute-based encryption - Hash function - Digital Signature	Cooperation consensus algorithm	- Time consumption (ms)	+ Manage fine-grained noninteractive access control on traffic data - Bad-mouthing attack is not analyzed
2019	Qiu et al [75]	Internet of Drones	- Elliptic curve digital signature algorithm - Asymmetric cryptography - Hash function	Distributed consensus algorithm	- Impact of spectrum coins and spectrum demands	+ Without reliance on a trusted intermediary - Location privacy and scalability are not considered
2019	Xie et al. [84]	IoT in the 5G era	- SHA-256 hash function	Proof-of-work and proof-of-stake	- Transaction transmission delay - Video encryption time overhead	+ Malicious vehicular nodes are detected - Whitewashing attack is not analyzed
2019	Chaudhary et al. [50]	IoT-based NFV/SDN	- SSL/TLS connection - Hash function	PoW consensus mechanism	- Communication cost - Computation time	+ Low latency and real-time services - The proposed scheme is not implemented via the blockchain platforms
2019	Sheikh et al. [36]	Internet of Energy	- Hash function	Byzantine based blockchain consensus	- Energy demand requirements with and without false data	+ The success probability of an attack reduced using Byzantine-based blockchain consensus - Data reliability and Non-repudiation are not considred
2018	Leng et al. [42]	Green IoT-based Agriculture	- Ellipse curve cryptography - Hash function	Proof of stake consensus algorithm	- Average optimal cost of demand nodes	+ Security and transparency of transaction data - No analysis about resistant to attacks
2018	Jo et al. [47]	IoT-based healthcare	- SHA-256 hash function	PoW consensus mechanism	- Average throughput - Block size against transactions/s	+ Provide the authenticated and immutable records - The effectiveness of the PoW consensus is a major issue
2018	Lin et al. [86]	Industry 4.0	- Attribute-based signatures - Multi-receivers encryption - Hash function	PBFT consensus algorithm	- Time cost (s)	+ Perfect forward secrecy - Sybil attack is not considered

formally modeled schedule confirmation/approval using the Stackelberg game model for blockchain-based cloud computing. In the blockchain-based cloud model, the leader is the node, which initiates a transaction, and the follower is the next node in the sequence of nodes in the blockchain network. Liu *et al.* [53] formulated the video transcoding and delivery problem as a three-stage Stackelberg game for blockchain-based mobile edge computing.

2) *Noncooperative game:* Yang *et al.* [37] modeled a noncooperative game to achieve decentralized scheduling of multiple responsive executors in the energy local networks, which is based on three components, namely a) players; b) strategy space; and c) utility function. The players include all the users of plug-in electric vehicles and battery energy storage. The strategic space includes a collection of achievable patterns of consumption that reduce the utility function of the players, while the utility function includes the measurement of the players' cost in the game. In order to minimize the cost of each mobile equipment for mobile edge computing, Zhang *et al.* [73] modeled the joint coin-loaning and computation-offloading issue as a noncooperative game, in which the mobile equipments can perform distributed decision making. Lin *et al.* [51] proposed an optimal knowledge pricing strategy based on a noncooperative

game to study the quality knowledge related knowledge sellers for edge artificial intelligence-enabled IoT.

3) *Differential game* is a game that involves N players, each one solving an optimal control question, where the other players also solving their optimal control questions. These questions are related since the controls selected by each player affect the evolution of the state variables [99]. Wang *et al.* [74] uses the differential game to model the introduction of blockchain technology in traditional fog computing.

3) Theory Analysis: Lai *et al.* [69] used theory analysis to prove that their scheme can achieve a series of design objectives, namely 1) provide effective and fair incentives; 2) secure and privacy preserving; and 3) ensure the reliability of map update. Luo *et al.* [70] uses theory analysis to prove that their scheme can preserve vehicles' location privacy and resilience to various trust model attacks (such as Sybil attack, on–off attack, whitewashing attack, and badmouthing attack). Yao *et al.* [71] analyzed the security features of the IDaaSoVCC scheme based on two assumptions, namely discrete logarithm assumption and decisional bilinear Diffie–Hellman assumption, which can satisfy identity information privacy, confidentiality, and forward secrecy. In the random oracle model, Zhang *et al.* [72] proved that the linkable group signature can achieve likability, full traceability, and full anonymity for IoT-based cryptocurrency.

4) AVISPA Tool: Reference [100] is used as a formal security verification tool for authentication schemes that used a language called the high-level protocol specification language (HLPSL). Bera *et al.* [34] adopted the AVISPA tool to prove the security of their scheme with the implementation of three basic roles, namely the role for the drone, the role for the ground station server, and the role for the cloud server.

B. Security Requirements

For developing a blockchain-based security and privacy system for the IoTs networks, the following security requirements are fundamental to be achieved.

1) *Privacy:* Consists to prevent the revelation of personally identifiable information based on data containing private and sensitive information (e.g., medical images in medical IoT systems) [30], [87], [92], [101], [102].
2) *Integrity:* The IoT data that is generated and transmitted over the IoT network should not be monitored and altered during communication [69]–[71], [79], [81].
3) *Authentication:* Each IoT device that participates in transmitting the IoT data should be authenticated before it is authorized to join the blockchain-based security and privacy system [69]–[71], [82].
4) *Nonrepudiation:* This constitutes irrefutable proof of the validity and origin of all data transmitted, where an IoT device cannot refuse any participation in the IoT data reporting [30], [79], [81].
5) *Traceability:* The blockchain-based security and privacy system should be able to provide identity privacy preservation conditionally in the IoT network. The tracing authority is able to trace and reveal the real identity of malicious IoT devices through its database [72], [75], [81], [82].
6) *Identity Privacy:* Consists to ensure that the malicious IoT devices cannot learn the identity information from the proof during the data integrity checking process [31], [70], [71], [82].
7) *Location Privacy:* The blockchain-based security and privacy system should be able to preserve devices' location privacy during the anonymous communication process [70].
8) *Scalability:* The blockchain-based security and privacy system should be able to adapt to rapid growth in terms of both the number of participants and the volume of IoT data shared.
9) *Unforgeability:* Guarantees that malicious devices cannot even produce a new signature for an already signed message in the IoT network [103].
10) *Anonymity:* The blockchain-based security and privacy system should be able to guarantee the anonymity of users in the IoT network. In other words, the adversary cannot obtain the real identity of the user by analyzing the transactions [56], [81].
11) *Trust Management:* It depends on the specific use cases where trust management is to be applied. Kochovski *et al.* [104] presented several relevant trust-related attributes in a blockchain-based fog computing platform, such as availability, credibility, and privacy.
12) *Access Control:* This constitutes to regulates the IoT devices that can connect or use resources in an IoT environment. The blockchain-based security and privacy system should be able to perform identification authentication and authorization of users [34], [54], [86], [105], [106].
13) *Data Reliability:* The blockchain-based security and privacy system should be capable of protecting IoT data from suppression or falsification by possible attacks. In addition, the system should be able to store replicated data to ensure reliability in the case of a single-point fault.
14) *Perfect Forward Secrecy:* For the security of the previously transmitted data, the blockchain-based security and privacy system should ensure that session keys cannot be compromised if the server's private key is compromised [56].
15) *Confidentiality:* Only the IoT devices involved in the blockchain-based security and privacy system are allowed to know the content of the smart contract [52], [75], [88].
16) *Data Auditability:* The smart contracts that are saved in the blockchain-based security and privacy system should be securely kept and easily verifiable. Although an IoT device in the blockchain network can be compromised, the malicious IoT device should not be able to modify and upload any smart contract [79], [107].
17) *Unlinkability:* The blockchain-based security and privacy system should be able to ensure that the various operations of the particular user should not be linked together [103].

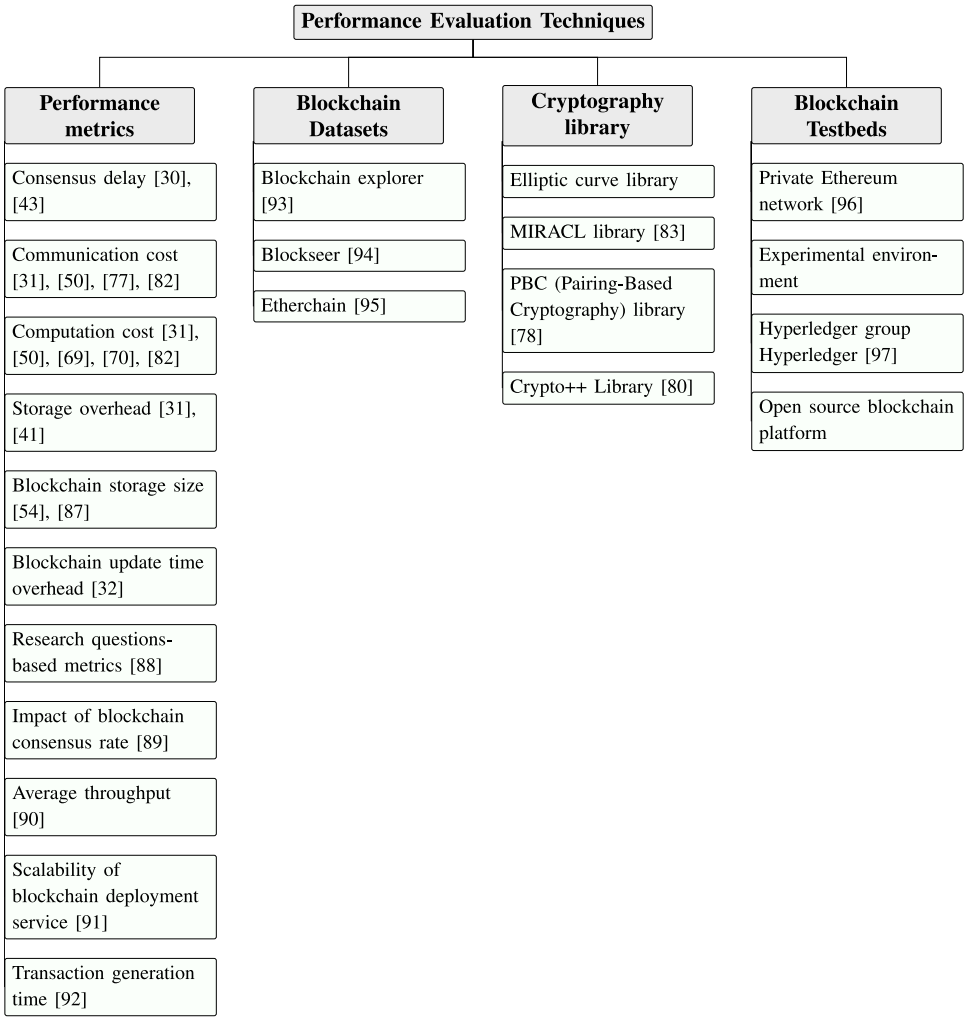

Fig. 9. Classification of performance evaluation techniques in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.

V. Performance Evaluation Techniques

Fig. 9 presents the classification of performance evaluation techniques in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.

A. Performance Metrics

Table IV presents the performance metrics and cryptography technologies used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.

1) Consensus Delay (Latency): Consensus delay (latency) is defined as the time taken for the transaction to be approved and published. Arena *et al.* [43] used this metric for evaluating the performance evaluation of BRUSCHETTA application, which is defined as the delay between generating a transaction and its publication on the blockchain. Noh *et al.* [30] used consensus delay as a performance metric for evaluating the processing time of the consensus algorithm in a blockchain-based system for the Internet of Vehicles. The consensus delay is used also for comparing the overhead analysis with two conventional algorithms, such as hotstuff consensus and loof-fault tolerance. Ferrag and Maglaras [33] analyzed latency of blockchain consensus of the proposed DeliveryCoin and the Prime-based DeliveryCoin under a number of UAVs, probabilities of malicious UAV nodes, and velocities of UAV nodes. Zhou *et al.* [112] used the consensus latency as a performance metric for evaluating the performance of a blockchain-based personal healthcare information system, which is composed of three parts: 1) the time to generate consensus identities; 2) the time for consensus messages to propagate; and 3) the time to count consensus votes.

2) Communication Cost: Tan and Chung [31] analyzed the communication cost of the proposed authentication scheme, which they calculate the required communication rounds for VANET authentication in RSU side. The communication cost includes the system parameter set, authentication request, and acknowledgment message. The communication cost of the proposed authentication scheme demonstrating that fewer communication rounds are required comparing with PATF [113] and EPFA [114]. Ali *et al.* [82] analyzed

TABLE V
CRYPTOGRAPHY LIBRARIES USED IN THE PERFORMANCE EVALUATION OF BLOCKCHAIN-BASED SECURITY AND PRIVACY SYSTEMS FOR THE IOT NETWORKS

Year	Scheme	Cryptography library	Type	Program. language	IoT application	Focus of this work
2020	Eltayieb et al. [77]	PBC library [78]	Pairing-based cryptography library	C	Cloud computing	Evaluate the characteristics of computational complexity
2020	Nkenyereye et al. [79]	Crypto ++ library [80]	Cryptographic schemes		Edge/Fog Computing	Evaluate the characteristics of computation and communication overhead
2019	Cheng et al. [81]	libbswabe-0.9, ibrary bcprov-jdk15on-158, jpbc-plaf-1.2.1, jpbc-api-1.2.1, and commons-codec1.7	Elliptic curve library	Java Runtime Environment 1.8	Internet of Vehicles	Construct bilinear pairs using the elliptic curve
2019	Luo et al. [70]	ECC-secp256k1 and ECDSA-secp256k1	Elliptic curve library	JAVA language	Internet of Vehicles	Evaluate the characteristics of computational overhead and security
2019	Ali et al. [82]	The MIRACL library [83]	Pairing-based cryptography library	C/C++	Internet of Vehicles	Perform mathematical operations underlying Pairing-based cryptography library
2019	Li et al. [32]	ECC-secp256k1 and ECDSA-secp256k1	Elliptic curve library	JAVA language	Internet of Drones	Evaluate the characteristics of computation and communication overhead
2019	Xie et al. [84]	Crypto ++ library [80]	Cryptographic schemes	C++	IoT in the 5G era	Evaluate the transmission delay
2019	Niu et al. [55]	MIRACL library [83]	Pairing-based cryptography library	C/C++	Internet of Sensors	Evaluate the performance of blockchain-based key aggregation searchable encryption
2019	Zhang et al. [72]	MIRACL library [83]	Pairing-based cryptography	C/C++	IoT-based Cryptocurrency	Evaluate the performance of linkable group signature
2019	Li et al. [85]	MIRACL library [83]	Pairing-based cryptography	C/C++	IoT-based Cryptocurrency	Analyze the computational cost of the traceability
2018	Jo et al. [47]	Secp256k1 signature code	Elliptic curve library	N/A	IoT-based healthcare	Evaluate the characteristics of average throughput and Bbock size against transactions/s
2018	Lin et al. [86]	PBC library [78]	Pairing-based cryptography library	C	Industry 4.0	Investigate the time cost of cryptographic algorithms

the communication costs of CL-PKS scheme by considering the size of the parameters, such as certificateless-signature of the vehicle, current time-stamp, public key, and pseudoidentity. Eltayieb *et al.* [77] analyzed the communication cost of the blockchain-based attribute-based signcryption scheme for the cloud environment, which includes the size of the signing key, decryption key, and ciphertext. Therefore, Chaudhary *et al.* [50] analyzed the communication cost of a blockchain-based secure energy trading scheme for IoT-based NFV/SDN, which includes the size of identity key and hash values for an electric vehicle, transaction server, and miner node.

3) Computation Cost (ms): Tan and Chung [31] analyzed the computation cost of the proposed authentication scheme, which they calculate the point multiplication, the pairing operation, and the employed secure hash functions in the RSU and vehicle side. The approximate execution time compared PATF [113] and EPFA [114] shows less computation overhead for resource-limited vehicles. Lai *et al.* [69] calculates the time complexity of running their scheme which is equal to $O(n\log n)$. Luo *et al.* [70] focused on the computational complexity of the vehicle (i.e., requester vehicle, cooperative vehicle without response, and cooperative vehicle providing assistance), in which the construction process involves signature $\mathcal{O}(Sig)$, verification $\mathcal{O}(Sig')$, encryption $\mathcal{O}(Enc)$, and decryption $\mathcal{O}(Enc')$. Ali *et al.* [82] analyzed the computation cost of CL-PKS scheme in the signing of messages and in the verification of the corresponding signature, which the results show approximately 7.6361 ms. Chaudhary *et al.* [50] analyzed the computation time of a blockchain-based secure energy trading scheme for IoT-based NFV/SDN, which is computed on the basis of the operations in the blockchain, such as SHA-1 and the addition operation.

4) Storage Overhead (Bits): Tan and Chung [31] used storage cost as a performance metric for evaluating the storage overhead of RSU and individual vehicles during the authentication phase. The storage cost consists of the length of the identity, the elements in a cyclic additive group, and the delivered session key. Compared to PATF [113] and EPFA [114], Tan and Chung's scheme shows less storage overhead. Wei *et al.* [41] studied the storage cost of a blockchain data-based cloud data integrity protection mechanism, which is the sum of the verification tree storage costs.

5) Blockchain Storage Size: Hîrţan *et al.* [87] analysis the blockchain storage size by assuming an range of 0 to 1 000 000 blocks. The results show that for a quantity of 1 000 000 blocks, a 564-MB storage space is requested. Zhang *et al.* [54] computed the storage overhead for the initial settings file and the session and attributes, which the results show that it takes about 1104 bytes to store session keys where there are 10 requests.

6) Blockchain Update Time Overhead (ms): Li *et al.* [32] analyzed the Blockchain update time overhead in the Internet of Vehicles, in which the results show that the block update time is increased if the sliding window is too small. Note that the UAV nodes utilize a sliding window to store recently updated blocks.

7) Research Questions-Based Metrics: Chen *et al.* [88] studied the performance evaluation of their scheme by defining the following six research questions: 1) Does the proposed scheme scale well for blockchain-based data trading? 2) Does the proposed scheme perform well in different data transmission losses? 3) How much can the proposed scheme follow the law of the market? 4) How can the proposed scheme encourage buyers and sellers to trade data? 5) How much benefit can the brokers gain in the proposed scheme? and 6) How can the proposed social welfare function converge?.

The experimental results under 100 independent trials show that the proposed scheme can perform in different data transmission loss, encourage the buyers and sellers to participate in data trading as well as achieving the maximum social welfare.

8) Impact of Blockchain Consensus Rate: The charge rate of PoW in euro/kWh is evaluated by Dang *et al.* [89], which is an significant and important by-product of blockchain technology. The results show that the cost of PoW is directly related to the amount of electricity purchased from the day-ahead, adjustment and balancing markets.

9) Average Throughput (Requests Per Second): Danish *et al.* [90] used the achieved throughput at the join server connected to the blockchain network as a performance metric in the conducted experiments. This performance metric is featured as a function of the number of join request messages per customer, for a different number of concurrent customers.

10) Scalability of Blockchain Deployment Service: Consist to measure the deployment time of blockchain with various numbers of nodes. Lu *et al.* [91] evaluated the scalability of blockchain deployment service by setting the blockchain type as Ethereum and filling in the nodes' IP addresses for deployment. The good scalability is achieved when the deployment time increases in an approximately linear manner.

11) Transaction Generation Time (ms): Consist to measure the time of generating a transaction in the blockchain-based system. Shen *et al.* [92] used the transaction generation time as a performance metric to evaluate the performance of a blockchain-based system for medical image retrieval. Specifically, the transaction structure consisting of three parts, including time information, retrieval information, and transaction information.

To ease the decision-making process on whether performance metrics are appropriate to evaluate the performance evaluation of blockchain-based security and privacy systems for the IoT networks, we provide a flow chart in Fig. 10.

B. Blockchain Data Sets

The blockchain data sets used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks are based on the search engines of the crypto space, named Blockchain explorers. Specifically, they are similar to an Internet search engine, which can be used to view wallet details, blockchain transactions, blocks, etc.

1) Blockchain Explorer [93]: Blockchain explorer enables users to tag Bitcoin addresses with tags indicating the known Bitcoin address identities. The Blockchain explorer can be used to analyze Ethereum or Bitcoin Cash. Chang and Svetinovic [115] uses Blockchain explorer to identifies 2509 Bitcoin addresses which belong to 515 entities. Wang *et al.* [116] uses Bitcoin blockchain to collect transactions from January 3, 2009 (the genesis block) to June 30, 2017 (block 473, 592), which they observe that about 0.48% of transactions still involve the vulnerability "ECDSA weak randomness" and that 1331 private keys are affected.

2) Blockseer [94]: Blockseer offers the same functionality with Blockchain explorer and displays the connections among addresses and clusters addresses sharing the same label.

3) Etherchain [95]: Etherchain is an Ethereum Blockchain Explorer contains every ether transaction made prior to the present date, which can be extracted for the price prediction experiment. Every element of a record contain a timestamp, beneficiary incentive in Ripple (XRP), sender, and exchange id. Poongodi *et al.* [117] used Etherchain for evaluating the price prediction of the Ethereum blockchain cryptocurrency.

C. Cryptography Library

Table V presents cryptography libraries used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.

1) *Elliptic Curve Library:* Cheng *et al.* [81] used the elliptic curve library to evaluate the performance of semi-centralized traffic signal control mode with attribute-based blockchain. The following libraries are used on Java Runtime Environment 1.8 to construct bilinear pairs : libbswabe-0.9, ibrary bcprov-jdk15on-158, jpbc-plaf-1.2.1, jpbc-api-1.2.1, and commons-codec1.7. To encrypt/decrypt and sign/verify all messages generated, Luo *et al.* [70] uses the following two types of elliptic curves cryptography: a) ECC-secp256k1 and b) ECDSA-secp256k1, which are implemented in JAVA language.
2) *MIRACL library [83]* is multiprecision integer and rational arithmetic cryptographic library, which is used for elliptic curve cryptography. The MIRACL library is used by Ali *et al.* [82] for computing the execution time of the cryptographic operation underlying pairing-based cryptography (PBC). Niu *et al.* [55] used the Miracl library to implement cryptographic operations in order to evaluate the performance of blockchain-based key aggregation searchable encryption. Zhang *et al.* [72] used MIRACL for evaluating the performance of linkable group signature in IoT-based cryptocurrency. Li *et al.* [85] used MIRACL library to analyze the computational cost of the traceability for a privacy and regulation scheme in blockchain-based cryptocurrencies.
3) *Pairing-Based Cryptography Library [78]* is used by Eltayieb *et al.* [77] for evaluating the characteristics of the computational complexity of the concept of attribute-based signcryption with blockchain. The PBC is a free C library which executes the fundamental mathematical processes involved in pairing-based encryption systems.
4) *Crypto++ Library [80]* is a free C++ class library of cryptographic schemes. The library contains many algorithms, such as authenticated encryption schemes (e.g., ChaCha20Poly1305 and XChaCha20Poly1305), high-speed stream ciphers [e.g., Panama, Rabbit (128/256)], message authentication codes (e.g., HMAC), hash functions (e.g., SHA-1 and SHA-2), and elliptic curve cryptography (e.g., ECDSA), etc. Nkenyereye *et al.* [79] uses Crypto++ library to evaluate the characteristics of computation and communication overhead of a secure and blockchain-based scheme.

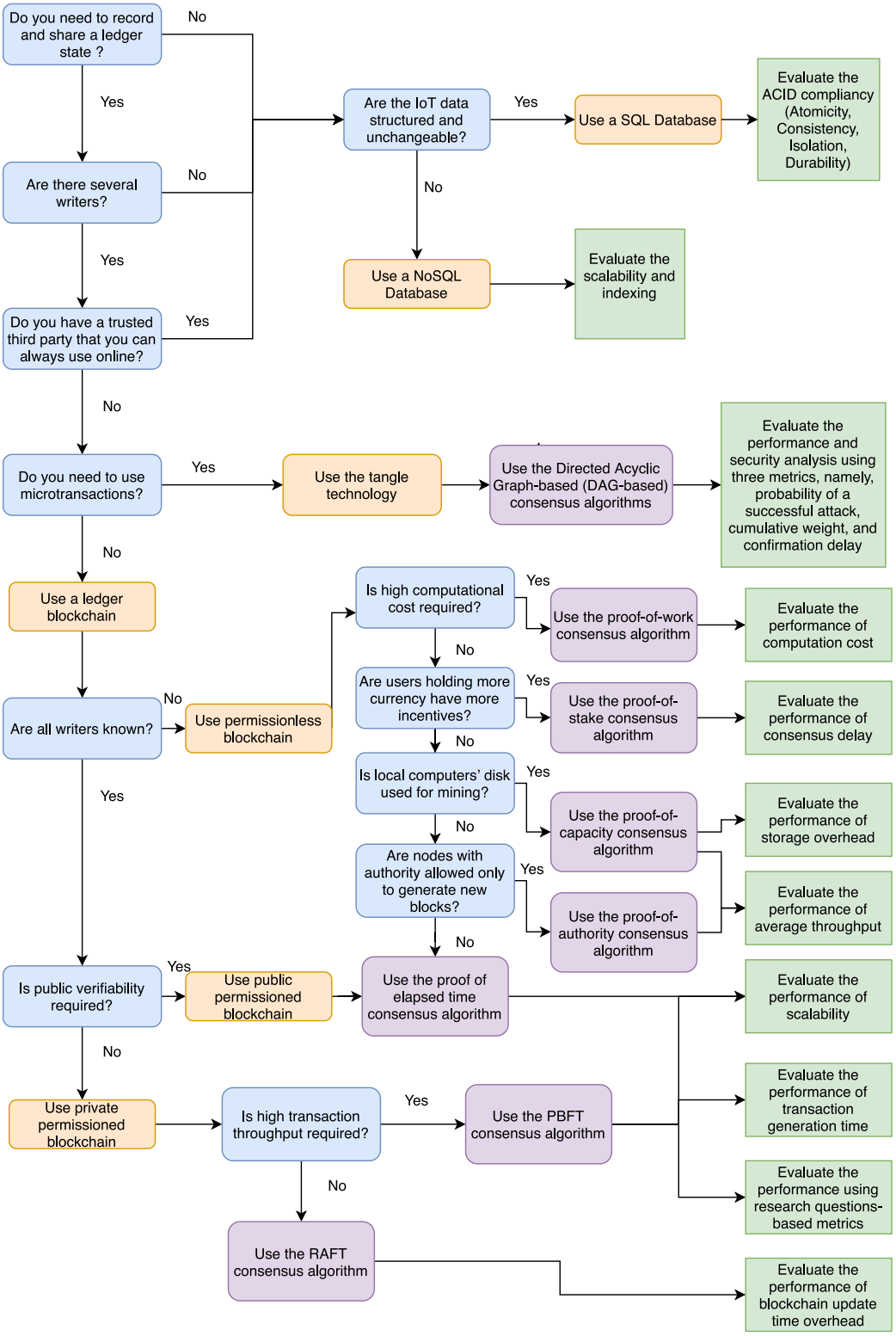

Fig. 10. Flowchart to determine whether performance metrics are appropriate to evaluate the performance evaluation of blockchain-based security and privacy systems.

D. Blockchain Testbeds

Table VI presents the blockchain testbeds used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.

1) Private Ethereum Network: Ethereum is the most used development platform in the performance evaluation of blockchain-based security and privacy systems for the IoT networks.

1) *Ganache [118]* is a private Ethereum blockchain, which can be used to implement smart contracts, develop programs and run scripts and tests. The testbed is available both as a desktop application and as a command-line

TABLE VI
TESTBEDS USED IN THE PERFORMANCE EVALUATION OF BLOCKCHAIN-BASED SECURITY AND PRIVACY SYSTEMS FOR THE IOT NETWORKS

Year	Scheme	Testbeds	Type	IoT applications	Focus of this work in the performance evaluation
2020	Ma et al. [109]	Ganache [118]	Private Ethereum network	Data crowdsourcing	- Evaluate the costs of smart contracts and for running data trade
2020	Liu and Zhang [110]	MATLAB environment [119]	Experimental environment	IoT data storage	- Evaluate the encryption speed of ECC in the blockchain network
2020	Zhang et al. [54]	Hyperledger Caliper [120]	Hyperledger group	Internet of Sensors	- Measuring the performance of blockchain-based collaborative access control scheme
2020	Tanwar et al. [121]	Hyperledger Caliper [120]	Hyperledger group	IoT-based healthcare	- Measuring the performance of blockchain-based access control policy algorithm
2020	Khan et al. [122]	MultiChain [123]	Open source blockchain platform	Electronic voting	- Evaluating the blockchain network in terms of unauthorized and authorized access
2020	Zhu et al. [40]	Ethereum	Private Ethereum network	Cloud Computing	- Building a federated blockchain system
2020	Yazdinejad et al. [124]	FPGA	Experimental environment	IoT-based NFV/SDN	- Implement a blockchain-enabled packet parser architecture
2020	Kadadha et al. [125]	Solidity [126]	Private Ethereum network	Data crowdsourcing	- Develop the smart contracts for a blockchain-based crowdsensing system
2020	Wang et al. [127]	Ethereum environment	Private Ethereum network	Industrial Internet of Things	- Validate the applicability of a reputation module in IIoT
2020	Lin et al. [128]	JUICE platform [129]	Open source blockchain platform	Data crowdsourcing	- To demonstrate the feasibility of the secure and privacy-preserving blockchain-based crowdsourcing system
2019	Maw et al. [130]	Go-ethereum	Private Ethereum network	Industrial Internet of Things	- Implementation of an operational data security scheme
2019	Lai et al. [69]	MATLAB environment [119]	Experimental environment	Internet of Vehicles	- Evaluate the importance of reputational data on the credibility of the data
2019	Islam and Shin [35]	MATLAB environment [119]	Experimental environment	Internet of Drones	- Estimating the effects in mobile edge computing server
2019	Luo et al. [70]	Hyperleader	Hyperledger group	Internet of Vehicles	- Realize the interaction between the consortium blockchain data and the application layer
2019	Li et al. [32]	Hyperledger Fabric 2.0	Hyperledger group	Internet of Drones	- Evaluate the Blockchainupdate time and storage overhead
2019	Kaynak et al. [131]	NEthereum [132]	Private Ethereum network	Cloud Computing	- Integrate Ethereum blockchain into .NET applications with dotnet core framework.
2019	Sharma et al. [133]	MATLAB environment [119]	Experimental environment	Internet of Drones	- Evaluate the reliability through the area spectral efficiency, probability of connectivity, epoch, flyby time, and packet-survivability
2019	Sheikh et al. [36]	IEEE 33 bus system	Experimental environment	Internet of Energy	- Evaluate energy demand requirements
2019	Lu et al. [91]	Ethereum 1.5.9-stable	Private Ethereum network	Cloud Computing	- Evaluate the scalability of blockchain deployment service
2019	Kurt et al. [38]	IEEE-14 bus power system	Experimental environment	Internet of Energy	- Evaluate the false data injection attacks against the sensor measurements
2019	Shen et al. [92]	Ethereum Geth	Private Ethereum network	IoT-based healthcare	- Evaluate the performance of a blockchain-based system for medical image retrieval
2019	Wang et al. [74]	MATLAB environment [119]	Experimental environment	Fog/Edge Computing	- Simulate the optimal resource contribution of the fog node
2019	Ferrag and Maglaras [39]	MultiChain [123]	Open source blockchain platform	Internet of Energy	- Evaluate the performance of blockchain-based energy network
2019	Kochovski et al. [104]	Rinkeby Ethereum testnet [134]	Private Ethereum network	Fog/Edge Computing	- Evaluate the performance of blockchain–based trust management system
2019	Di Silvestre et al. [135]	Tendermint [136]	Open source blockchain platform	Internet of Energy	- Validate the distributed energy system using a blockchain network
2019	Zhou et al. [112]	Golang	Open source programming language	IoT-based healthcare	- Implement a prototype of permissioned blockchain
2019	Zhang et al. [73]	Ethereum environment	Private Ethereum network	Fog/Edge Computing	- Demonstrate the impact of the smart contracts for mobile edge computing
2019	Dang et al. [89]	MATLAB environment [119]	Experimental environment	Internet of Energy	- Study the impact of proof-of-work charge rate on the total cost
2019	Huang et al. [52]	Truffle [137]	Private Ethereum network	Edge/Fog Computing	- Realize the smart contract functionality for the decentralized fog computing environment
2019	Gai et al. [107]	Ethereum Geth	Private Ethereum network	Internet of Energy	- Study the cost of the time required to pack data into the blockchain system
2019	Danish et al. [90]	Ethereum Geth	Private Ethereum network	Internet of Sensors	- Deploy the smart contract and run the private blockchain network
2019	Arena et al. [43]	Hyperledger Fabric [138]	Hyperledger group	Green IoT-based Agriculture	- Implementing the blockchain for the certification and the traceability of extra virgin olive oil
2019	Lin et al. [56]	JUICE platform [129]	Open source blockchain platform	Internet of Sensors	- Evaluate the utility of a blockchain-based secure mutual authentication system
2019	Shih et al. [44]	Remix - Ethereum IDE [139]	Private Ethereum network	Green IoT-based Agriculture	- Testing the smart contract code of Ethereum
2019	Derhab et al. [140]	MultiChain [123]	Open source blockchain platform	Industry 4.0	- Implement a private blockchain for industrial IoT
2019	Dai et al. [141]	Ethereum environment	Private Ethereum network	IoT data storage	- Measure the total time required for a secure data trading ecosystem
2018	Jo et al. [47]	Ethereum Mist Browser	Private Ethereum network	IoT-based healthcare	- Evaluate the feasibility and performance of a blockchain-based distributed network
2018	Lin et al. [86]	JUICE platform [129]	Open source blockchain platform	Industry 4.0	- Investigate the time cost of cryptographic algorithms used in a blockchain-based system

tool. The Ganache testbed is used by Ma *et al.* [109] as a blockchain testing platform to evaluate the costs of smart contracts and for running data trade.

2) *Ethereum Geth [96]* is a decentralized framework that manages smart contracts via the implementation of the Ethereum protocol. Danish *et al.* [90] uses a geth

Ethereum client, which is a Go language implementation of the Ethereum protocol in order to deploy the smart contract and run the private blockchain network. The Ethereum Geth is used by Gai *et al.* [107] for evaluating the time cost for packing up data in the blockchain system. To evaluate the scalability of blockchain deployment service, Lu *et al.* [91] deployed the uBaaS platform on an Alibaba Cloud4 virtual machine with Ethereum 1.5.9-stable and PoW as a consensus algorithm. Zhang *et al.* [73] deployed smart contracts in the Ethereum environment in order to demonstrate the performance of the smart contracts on the blockchain for mobile edge computing, which the results show that the financial cost of the implementation of smart contracts on the Ethereum network is relatively low. Shen *et al.* [92] used Ethereum as a proof-of-concept platform and use Geth as the Ethereum client to evaluate the performance of a blockchain-based system for medical image retrieval.

3) *NEthereum [132]* integrate Ethereum blockchain into .NET applications. Kaynak *et al.* [131] used the NEthereum library in the Ethereum network to execute transactions using the C# language with dotnet core framework.
4) *Rinkeby Ethereum testnet [134]* is test network for developers to develop and to do testing for Ethereum, which is based on a PoA consensus. Kochovski *et al.* [104] used Rinkeby Ethereum testnet to evaluate the performance of the blockchain-based trust management system for fog computing. Note that there are other test networks for Ethereum, namely Kovan, Ropsten, and Görli.
5) *Truffle [137]* is a development and test environment with an asset pipeline for Ethereum, which provides network management for deploying to several public and private networks. Huang *et al.* [52] used Truffle [137] to realize the smart contract functionality for the decentralized fog computing environment.
6) *Remix—Ethereum IDE [139]* is a browser-based compiler and IDE that allows users to debug transactions and build Ethereum contracts using the Solidity language. Shih *et al.* [44] uses Remix—Ethereum IDE to testing the smart contract code of Ethereum for the organic production and trading of vegetables with blockchain.
7) *Ethereum Mist Browser* is a Web application layer that allows visualizing Web-based user interfaces for all types of Ethereum decentralized applications. Jo *et al.* [47] used Mist Browser and Go-Ethereum to simulate and evaluate the feasibility and performance of a blockchain-based distributed network for IoT-based healthcare.
8) *Solidity [126]* is an object oriented, high-level language for implementing smart contracts for Ethereum. Kadadha *et al.* [125] used Solidity with Web3j [142] to create and compile the smart contracts constituting the blockchain-based crowdsensing framework.

2) Experimental Environment:

1) *MATLAB environment [119]* is used by Liu and Zhang [110] for evaluating the encryption speed of ECC in the blockchain network. Specifically, 100 storage nodes are set up with the limited capacity of each node is 3 TB, and the information and storage channel is fixed at 1000 Mbit/s. Lai *et al.* [69] analyzed the impact of reputation values on data credibility for Internet of Vehicles using MATLAB simulation, which the value of services of the vehicle users and the unit cost of vehicle users are chosen uniformly at random. Islam and Shin [35] performed a simulation using MATLAB for estimating the effects of a Blockchain-based secure data acquisition scheme with the use of a mobile edge computing server. Sharma *et al.* [133] analyzed the neural-blockchain-based scheme using the numerically defined system model in MATLAB in order to evaluate the reliability through the area spectral efficiency, probability of connectivity, epoch, flyby time, and packet survivability. Dang *et al.* [89] used the platform of MATLAB with the help of YALMIP toolbox in order to study the impact of PoW charge rate on the total cost. Wang *et al.* [74] used MATLAB R2018b simulation software to simulate the optimal resource contribution of the fog node.
2) *IEEE 33 Bus System:* This system is used by Sheikh *et al.* [36] to evaluate secured energy trading based on Byzantine-based blockchain consensus. The IEEE 33 bus system consists of 33-nodes and 32 branches. The evaluation for highlighting the impact of blockchain is carried out in two parts, namely a) securing different nodes of the system and b) Securing energy and information data exchange.
3) *IEEE-14 Bus Power System:* This system is used by Kurt *et al.* [38] for evaluating the false data injection attacks against the sensor measurements under a distributed dynamic state estimation in the Internet of Energy.
4) *PROMELA [143]* is a specification language for asynchronous systems, which is based on three building blocks, namely process, data object, and message channels. Ali *et al.* [106] evaluated a blockchain-based decentralized architecture in simple PROMELA interpreter (SPIN) model checker. Specifically, the model consists of one "Blockchain" process with "idle," "delegation," "activation" and "on" states.
5) *Field Programmable Gate Array* refers to an integrated circuit consisting of an array of programmable cells, which is renowned for its faster-processing speed, high flexibility, and low resource consumption. Yazdinejad *et al.* [124] used field programmable gate array (FPGA) for the implementation of blockchain-enabled packet parser architecture in order to evaluate in terms of resource utilization and power consumption.

3) Hyperledger Group: Hyperledger [97] is an open-source community, hosted by the Linux Foundation, which focuses on developing a suite of stable frameworks, tools, and libraries for the deployment of blockchains at the enterprise level. Moreover, Hyperledger enables a variety of enterprise blockchain technologies, including intelligent contract engines, client libraries, utility libraries, distributed ledger

frameworks, GUIs, and sample applications. Luo *et al.* [70] employes Hyperledger to realize the interaction between the consortium blockchain data and the application layer. To design smart contract algorithms, Li *et al.* [32] used the Java SDK "fabric-sdk-java" with Hyperleader's ChainCode technology.

1) *Distributed Ledgers:* There are six distributed ledger frameworks, namely Hyperledger Besu [144], Hyperledger Burrow [145], Hyperledger Fabric [146], Hyperledger Indy [147], Hyperledger Iroha [148], and Hyperledger Sawtooth [149]. The Hyperledger Besu is used in both public and private permissioned network, which is designed to be enterprise-friendly with including several consensus algorithms, such as PoW, and PoA. The Hyperledger Burrow can be used for private/consortium networks, which is based on smart contracts and BFT consensus via the Tendermint algorithm. For developing applications with a modular framework, the Hyperledger Fabric can be used, which allows modules, such as membership services and consensus. To choose a distributed ledger framework interoperable with other blockchains for providing digital identities, the Hyperledger Indy can be used, which provides libraries, tools, and reusable modules. The Hyperledger Iroha is designed for IoT projects that require distributed ledger technology with a role-based permission model, while the Hyperledger Sawtooth can be used for IoT projects that require consensus algorithm named PoET. Tanwar *et al.* [121] used Hyperledger Caliper [120] for measuring the performance of blockchain-based access control policy algorithms in IoT-based healthcare.
2) *Libraries:* There are four libraries developed by Hyperledger group for distributed ledger frameworks, namely Hyperledger Aries, Hyperledger Quilt, Hyperledger Transact, and Hyperledger Ursa [150].
3) *Tools:* There are five tools developed by Hyperledger group for distributed ledger frameworks, namely Hyperledger Avalon [151], Hyperledger Caliper [120], Hyperledger Cello [152], Hyperledger Explorer [153], and Hyperledger Grid [154]. Zhang *et al.* [54] used Hyperledger Caliper [120] for measuring the performance of blockchain-based collaborative access control scheme.

4) Open Source Blockchain Platforms:

1) *MultiChain [123]* is a platform for establishing a private blocking chain that can be used by organizations for financial transactions. The MultiChain platform provides a simple API and command-line interface with the property to restrict access to the blockchain via a list of authorized users. In addition, the MultiChain platform is characterized by the scalability of selective stream indexing and the data management of real-time data feeds. Ferrag and Maglaras [39] created a private blockchain using MultiChain to evaluate the performance of blockchain-based energy networks.
2) *Tendermint [136]:* Tendermint Core is BFT middleware that takes a state transition machine and replicates it on many machines. Di Silvestre *et al.* [135] uses Tendermint 0.24 to validate the distributed energy system using a blockchain network.
3) *JUICE platform [129]* is an open permissioned blockchain service platform. This platform can support the design of smart contracts using Solidity and possess a Java and Javascript-based Web/client tools for managing and monitoring. Lin *et al.* [56] used the JUICE platform to evaluate the utility of a blockchain-based secure mutual authentication system. Lin *et al.* [86] used the JUICE platform to investigate the time cost of cryptographic algorithms used in a blockchain-based system with fine-grained access control for industry 4.0 deployments.
4) *Other Blockchain Platforms:* There are other open-source blockchain platforms that can be used as blockchain testbed for the performance evaluation of blockchain-based security and privacy systems. We cite the following ten blockchain platforms: a) Algorand; b) HydraChain; c) Stellar; d) Waves Platform; e) Tezos; f) Smilo; g) Quorum; h) NEM; i) Qtum; and j) Openchain.

VI. Lessons Learned

Blockchain technology becomes the most popular communication platform in the development of the IoT. The blockchain-based security and privacy systems have received a high level of scientific research attention in addressing the challenging issues of security and privacy in IoT networks. For this reason, we have examined the performance evaluation of blockchain-based security and privacy systems for the IoT networks from different perspectives, and we summarize the lessons learned from this review below.

From the security analysis techniques point of view, there are four basic techniques, namely BAN logic, game theory, theory analysis, and AVISPA tool. These techniques can be used for analyzing the security theorems of blockchain-based security and privacy systems in terms of security requirements (e.g., traceability, identity privacy, location privacy, nonrepudiation, authentication, etc.), and resistance to attacks (e.g., replay attacks, quantum attacks, etc.).

Through in-depth analysis and research, we were able to classify the security and privacy requirements for blockchain-based IoT applications into integrity, authentication, nonrepudiation, traceability, identity privacy, location privacy, scalability, unforgeability, anonymity, trust management, access control, data reliability, perfect forward secrecy, confidentiality, and data auditability.

From the attacks of blockchain technologies vulnerability, we found nine-teen attacks discussed by the surveyed blockchain-based security and privacy systems, including replay attack, man-in-the-middle attack, chosen message attack, denial-of-service attack, sybil attack, bad-mouthing attack, on-off attack, whitewashing attack, false data injection attack, impersonation attack, modification attack, physical

capture attack, eavesdropping attack, collusion attack, anti-key-leakage attack, cross-pairing attack, keyword guessing attack, 51% attacks, and double spending.

Based on the performance metrics used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks, we found eleven metrics, including consensus delay, communication cost, computation cost, storage overhead, blockchain storage size, blockchain update time overhead, research questions-based metrics, impact of blockchain consensus rate, average throughput, scalability of blockchain, and transaction generation time.

According to the blockchain testbeds used in the performance evaluation of blockchain-based security and privacy systems, we were able to classify the blockchain testbed into private ethereum network, experimental environment, hyperledger group, and open source blockchain platforms. From the cryptography libraries used in the performance evaluation of blockchain-based security and privacy systems, we found four cryptography libraries, including elliptic curve library, PBC library, crypto++ library, and MIRACL library.

On the basis of the aforementioned studies and analyses that we have performed, we propose a thirteen-step process for building and evaluating a blockchain-based security and privacy system.

1) Configuration of the IoT network (e.g., fog/edge computing, SDN/NFV, cloud computing, etc.).
2) Selection of a consensus algorithm (e.g., PoW, PoS, etc.).
3) Definition of the security and privacy requirements (e.g., integrity, authentication, nonrepudiation, traceability, etc.).
4) Definition of smart contracts to manage transactions under specific conditions.
5) Definition of the threat models (e.g., 51% attacks, denial-of-service attack, sybil attack, bad-mouthing attack, etc.).
6) Identification of vulnerability and possible interdependencies of the blockchain-based security and privacy system.
7) Selection of the cryptographic methods (e.g., SHA-256 hash function, ellipse curve cryptography, ciphertext-policy attribute-based encryption, etc.).
8) Proposition of the principal steps of the blockchain-based security and privacy system (e.g., system initialization, device authentication, etc.) with considering the configuration of the IoT network.
9) Analyzing the robustness of the blockchain-based security and privacy system using different security analysis techniques (e.g., BAN logic, game theory, theory analysis, and AVISPA tool).
10) Selection of a cryptography library (e.g., elliptic curve library, PBC library, crypto++ library, MIRACL library, etc.).
11) Selection of a blockchain explorer (e.g., Blockchain explorer, Blockseer, Etherchain, etc.).
12) Selection of a blockchain testbed (e.g., private Ethereum network, experimental environment, hyperledger group, open source blockchain platform, etc.).
13) Evaluate the blockchain-based security and privacy system using different performance metrics (e.g., consensus delay, communication cost, computation cost, storage overhead, blockchain storage size, etc.).

VII. Open Challenges and Future Research Opportunities

To complete our review, we outline both open challenges and future research opportunities that could improve the capabilities and effectiveness of blockchain-based security and privacy systems for the IoT networks, summarized in the following suggestions.

A. Evaluating the Blockchain-Based Intrusion Detection Systems

There is recent work that combines the intrusion detection systems with blockchain technology for the IoT networks [155]–[157]. The intrusion detection system is proposed to defend against the forged commands and detect network attacks using machine learning (e.g., deep learning), while the blockchain technology is proposed for checking the data integrity as well as enabling transparency of information. Therefore, when evaluating the performance of blockchain-based intrusion detection systems, it is struggling to find comprehensive and valid cyber security data sets [158]. Currently, the most cyber security data sets used in the performance evaluation of intrusion detection systems are not simulated on blockchain-based IoT environments, such as KDD Cup 1999 data set, UNSW-NB15 data set, and NSL-KDD data set. The development of a new data set to build a network intrusion detector under a blockchain-based IoT environment is one of the significant research challenges.

B. Developing Efficient Consensus Mechanisms

The most popular consensus algorithms used in the blockchain are PoW, PoS, and PBFT. These consensus algorithms does not take into consideration the capacity limits for storage and computing of IoT devices. The IOTA project [159] is a cryptocurrency for the IoT industry which enables micropayment transactions between IoT devices and protects the integrity and verifiability of data [160]. The IOTA adopts DAG consensus (i.e., no miners) which can achieve high throughput with low computational overhead [27]. Therefore, there are many characteristics that should be taken into consideration when developing more efficient consensus mechanisms for IoT networks, such as transaction processing rate, security service, quantum computations, and decentralized trust. A possible research direction in this topic could be related to developing a hybrid consensus mechanism that combines the advantages of both DAG and other consensus algorithms. In addition, we believe that performance and security analysis of resistance to quantum computations is needed for the IOTA project.

C. Blockchain-Based Software-Defined Networking for IoT Application

We have seen that the combination of blockchain technology and software-defined networking offers promising opportunities to address the security challenges of the IoT environment and make it more secure. However, several challenges remain for the practical realization of the blockchain-based software-defined networking to replace the existing schemes. The absence of strong cryptographic encryption schemes between the SDN controller and the blockchain database can result in a serious violation of the confidentiality of communications [161]. Hence, autonomous trust mechanisms for establishing the authenticity of communication between the SDN controller and the blockchain database must be designed and implemented. In addition, the issue of man-in-the-middle attacks and denial-of-service attacks against the blockchain-based software-defined networking for IoT application still remains a very challenging one to tackle.

D. 5G-Enabled Blockchain-Based IoT Networks

Since the information on the state and location of an IoT node contained in the broadcast messages could be captured and used for misuse, the privacy leakage risk of blockchain will be more significant in 5G-enabled blockchain-based IoT networks. The technique for hiding the true identity of an IoT device is anonymity, which can be ensured by pseudonyms. Therefore, any person, organization, industry, public sector, or even attacker can access the detailed tracking information of IoT devices (e.g., vehicles) by reviewing the messages broadcasted periodically by IoT devices [162]. Some interesting technologies can be applied to this problem: game theory and reinforcement learning [163], privacy-aware and asynchronous deep learning [164], and privacy-preserving range query [164]. Hence, conducting researches and developing more secure, efficient, and practical privacy-preserving schemes using these technologies for 5G-enabled blockchain-based IoT networks will contribute significantly to the development of blockchain.

E. Secure Blockchain Ledgers at Fog Computing

Caching the blockchain ledgers at the storage spaces on Fog computing is an efficient and cost-effective approach to reducing the latency of IoT-enabled blockchain [165] as well as traffic overhead in large-scale industrial applications [166]. The confidentiality of blockchain ledgers, however, is difficult to preserve, from which attackers can deduce transactions from target IoT devices. To secure blockchain ledgers at fog computing, the following critical challenges need to be solved [167]: 1) how to select trusted nodes at fog computing for caching blockchain ledgers?; 2) when IoT devices request the blockchain ledgers, where cache the requested IoT data?; and 3) when trusted nodes at fog computing are damaged, how to ensure the confidentiality of blockchain ledgers?. Some interesting cache placement strategies can be applied to this problem: privacy-preserving data aggregation [168], enhanced revocable access control [169], fog data dissemination [170], and privacy-preserving range query [171]. Thus, conducting researches on blockchain ledgers replacement approaches and developing more secure, efficient, and practical data retrieval schemes will contribute significantly to the development of secure blockchain ledgers at Fog computing.

F. Developing Efficient and Privacy-Preserving Schemes

The IoT devices in blockchain-based IoT applications have group-based behavior and high/frequent mobility that require new challenges in privacy preserving. However, some emerging cryptographic techniques, e.g., anonymization, mixing, and differential privacy, etc., can be considered to design an efficient and privacy-preserving scheme. The anonymization techniques, such as k-anonymity aim to hide the querying user among k users [172]. The differential privacy techniques aim to protect real-time data by adding random noise based on the mathematical algorithms, e.g., Laplace distribution, Symmetric geometric distribution, etc [173], while mixing technique is used to improve anonymity by mixing tokens [174]. To design efficient and privacy-preserving schemes using these techniques, the following critical challenges need to be solved: 1) how to optimize the computing cost for k-anonymity mechanisms since the IoT devices are characterized by limited resources?; 2) how to add appropriate noises to support differential privacy?; and 3) how to achieve a good tradeoff of efficiency, accuracy, and privacy?. To this end, these cryptographic techniques should be carefully designed to provide efficient and privacy-preserving schemes for blockchain-based IoT applications.

VIII. Conclusion

In this article, we surveyed research challenges and a tutorial on performance evaluation of blockchain-based security and privacy systems for the IoT networks. We reviewed the blockchain-based security and privacy systems for seventeen types of IoT applications, e.g., Industry 4.0, software-defined networking, edge computing, Internet of Drones, Internet of Cloud, Internet of Energy, Internet of Vehicles, etc. We also reviewed various consensus algorithms and provide a comparison with respect to the nine properties, such as latency, throughput, computation, storage, and communication costs, scalability, attack model, advantage, and disadvantage, etc. Through in-depth analysis and research, we were able to classify the security analysis techniques and provide a classification into four categories, including BAN logic, game theory, theory analysis, and AVISPA tool. Furthermore, we analyzed the performance metrics, blockchain testbeds, and cryptography libraries used in the performance evaluation of blockchain-based security and privacy systems for the IoT networks. On the basis of the current survey, we discussed the major steps to follow for building and evaluating blockchain-based security and privacy systems. Finally, we discussed and highlighted open challenges and future research opportunities.

REFERENCES

[1] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.

[2] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[3] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.

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

[5] M. A. Ferrag, L. Maglaras, and H. Janicke, "Blockchain and its role in the Internet of Things," in *Strategic Innovative Marketing and Tourism*. Heidelberg, Germany: Springer, 2019, pp. 1029–1038.

[6] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2018.

[7] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, "Core concepts, challenges, and future directions in blockchain: A centralized tutorial," *ACM Comput. Surveys*, vol. 53, no. 1, pp. 1–39, 2020.

[8] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 32031–32053, 2020.

[9] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," *Comput. Commun.*, vol. 151, pp. 518–538, Feb. 2020.

[10] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3796–3838, 4th Quart., 2019.

[11] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[12] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.

[13] 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.

[14] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, 2020.

[15] J. Bao, D. He, M. Luo, and K.-K. R. Choo, "A survey of blockchain applications in the energy sector," *IEEE Syst. J.*, early access, Jul. 2, 2020, doi: 10.1109/JSYST.2020.2998791.

[16] M. B. Mollah *et al.*, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 18–43, Jan. 2021.

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

[18] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Comput. Surveys*, vol. 53, no. 2, pp. 1–27, 2020.

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

[20] D. D. F. Maesa and P. Mori, "Blockchain 3.0 applications survey," *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, Apr. 2020.

[21] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for Internet of Energy management: Review, solutions, and challenges," *Comput. Commun.*, vol. 151, pp. 395–418, Feb. 2020.

[22] H. Rathore, A. Mohamed, and M. Guizani, "A survey of blockchain enabled cyber-physical systems," *Sensors*, vol. 20, no. 1, p. 282, 2020.

[23] T. Alharbi, "Deployment of blockchain technology in software defined networks: A survey," *IEEE Access*, vol. 8, pp. 9146–9156, 2020.

[24] A. Singh, R. M. Parizi, Q. Zhang, K.-K. R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Comput. Security*, vol. 88, Jan. 2020, Art. no. 101654.

[25] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensuses algorithms: A survey," 2020. [Online]. Available: https://arxiv.org/pdf/2001.07091

[26] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, "A survey on decentralized consensus mechanisms for cyber physical systems," *IEEE Access*, vol. 8, pp. 54371–54401, 2020.

[27] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surveys*, vol. 53, no. 1, pp. 1–32, 2020.

[28] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Exp. Syst. Appl.*, vol. 154, Sep. 2020, Art. no. 113385.

[29] S. Wan, M. Li, G. Liu, and C. Wang, "Recent advances in consensus protocols for blockchain: A survey," *Wireless Netw.*, vol. 26, pp. 5579–5593, Nov. 2020.

[30] J. Noh, S. Jeon, and S. Cho, "Distributed blockchain-based message authentication scheme for connected vehicles," *Electronics*, vol. 9, no. 1, p. 74, 2020.

[31] H. Tan and I. Chung, "Secure authentication and key management with blockchain in VANETs," *IEEE Access*, vol. 8, pp. 2482–2498, 2019.

[32] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11309–11322, Nov. 2019.

[33] M. A. Ferrag and L. Maglaras, "Deliverycoin: An IDs and blockchain-based delivery framework for drone-delivered services," *Computers*, vol. 8, no. 3, p. 58, 2019.

[34] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," *Comput. Commun.*, vol. 153, pp. 229–249, Mar. 2020.

[35] A. Islam and S. Y. Shin, "BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things," *J. Commun. Netw.*, vol. 21, no. 5, pp. 491–502, 2019.

[36] A. Sheikh, V. Kamuni, U. Asfia, S. Wagh, N. Singh, and D. Patel, "Secured energy trading using Byzantine based blockchain consensus," *IEEE Access*, vol. 8, pp. 8554–8571, 2019.

[37] X. Yang, G. Wang, H. He, J. Lu, and Y. Zhang, "Automated demand response framework in ELNS: Decentralized scheduling and smart contract," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 58–72, Jan. 2020.

[38] M. N. Kurt, Y. Yılmaz, and X. Wang, "Secure distributed dynamic state estimation in wide-area smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 800–815, Jul. 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8759957

[39] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2020.

[40] X. Zhu, J. Shi, S. Huang, and B. Zhang, "Consensus-oriented cloud manufacturing based on blockchain technology: An exploratory study," *Pervasive Mobile Comput.*, vol. 62, Feb. 2020, Art. no. 101113.

[41] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Future Gener. Comput. Syst.*, vol. 102, pp. 902–911, Jan. 2020.

[42] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. Van Nieuwenhuyse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology," *Future Gener. Comput. Syst.*, vol. 86, pp. 641–649, Sep. 2018.

[43] A. Arena, A. Bianchini, P. Perazzo, C. Vallati, and G. Dini, "BRUSCHETTA: An IoT blockchain-based framework for certifying extra virgin olive oil supply chain," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, 2019, pp. 173–179.

[44] D.-H. Shih, K.-C. Lu, Y.-T. Shih, and P.-Y. Shih, "A simulated organic vegetable production and marketing environment by using Ethereum," *Electronics*, vol. 8, no. 11, p. 1341, 2019.

[45] H.-T. Wu and C.-W. Tsai, "An intelligent agriculture network security system based on private blockchains," *J. Commun. Netw.*, vol. 21, no. 5, pp. 503–508, 2019.

[46] S. Wang *et al.*, "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 4, pp. 942–950, Dec. 2018.

[47] B. W. Jo, R. M. A. Khan, and Y.-S. Lee, "Hybrid blockchain and Internet-of-Things network for underground structure health monitoring," *Sensors*, vol. 18, no. 12, p. 4268, 2018.

[48] A. Derhab, M. Guerroumi, L. Maglaras, M. A. Ferrag, M. Mukherjee, and F. A. Khan, "BLOSTER: Blockchain-based system for detection of fraudulent rules in software-defined networks," in *Proc. 6th Int. Symp. ICS SCADA Cyber Security Res.*, Jun. 2019, pp. 38–40.

[49] D. B. Rawat, "Fusion of software defined networking, edge computing, and blockchain technology for wireless network virtualization," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 50–55, Oct. 2019.

[50] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K. R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Comput. Security*, vol. 85, pp. 288–299, Aug. 2019.

[51] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6367–6378, Dec. 2019.

[52] H. Huang, K.-C. Li, and X. Chen, "Blockchain-based fair three-party contract signing protocol for fog computing," *Concurrency Comput. Practice Exp.*, vol. 31, no. 22, 2019, Art. no. e4469.

[53] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11169–11185, Nov. 2019.

[54] 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, 2020.

[55] J. Niu, X. Li, J. Gao, and Y. Han, "Blockchain-based anti-key-leakage key aggregation searchable encryption for IoT," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1502–1518, Feb. 2020.

[56] C. Lin, D. He, N. Kumar, X. Huang, P. Vijaykumar, and K.-K. R. Choo, "HomeChain: A blockchain-based secure mutual authentication system for smart homes," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 818–829, Feb. 2020.

[57] V. Gramoli, "From blockchain consensus back to Byzantine consensus," *Future Gener. Comput. Syst.*, vol. 107, pp. 760–769, Jun. 2020.

[58] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[59] K. Driscoll, B. Hall, H. Sivencrona, and P. Zumsteg, "Byzantine fault tolerance, from theory to reality," in *Proc. Int. Conf. Comput. Safety Rel. Security*, 2003, pp. 235–248.

[60] M. Castro *et al.*, "Practical byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

[61] D. Mazieres, *The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus*, Stellar Develop. Found., San Francisco, CA, USA, 2015.

[62] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Cham, Switzerland: Springer, 2017, pp. 297–315.

[63] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019.

[64] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, and S. Mehraeen, "Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7300–7309, Nov./Dec. 2019.

[65] A. Vangala, A. K. Sutrala, A. K. Das, and M. Jo, "Smart contract-based blockchain-envisioned authentication scheme for smart farming," *IEEE Internet Things J.*, early access, Jan. 11, 2020, doi: 10.1109/JIOT.2021.3050676.

[66] Z. Xu, W. Liang, K.-C. Li, J. Xu, and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for Internet of Vehicles," *J. Parallel Distrib. Comput.*, vol. 149, pp. 29–39, Mar. 2021.

[67] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *J. Med. Syst.*, vol. 44, no. 2, p. 52, 2020.

[68] A. Wilczyński and J. Kołodziej, "Modelling and simulation of security-aware task scheduling in cloud computing based on blockchain technology," *Simulat. Model. Practice Theory*, vol. 99, Feb. 2020, Art. no. 102038.

[69] C. Lai, M. Zhang, J. Cao, and D. Zheng, "SPIR: A secure and privacy-preserving incentive scheme for reliable real-time map updates," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 416–428, Jan. 2020.

[70] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2034–2048, Feb. 2020.

[71] Y. Yao, X. Chang, J. Misic, and V. B. Misic, "Lightweight and privacy-preserving ID-as-a-service provisioning in vehicular cloud computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2185–2194, Feb. 2020.

[72] L. Zhang, H. Li, Y. Li, Y. Yu, M. H. Au, and B. Wang, "An efficient linkable group signature for payer tracing in anonymous cryptocurrencies," *Future Gener. Comput. Syst.*, vol. 101, pp. 29–38, Dec. 2019.

[73] Z. Zhang, Z. Hong, W. Chen, Z. Zheng, and X. Chen, "Joint computation offloading and coin loaning for blockchain-empowered mobile-edge computing," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9934–9950, Dec. 2019.

[74] H. Wang, L. Wang, Z. Zhou, X. Tao, G. Pau, and F. Arena, "Blockchain-based resource allocation model in fog computing," *Appl. Sci.*, vol. 9, no. 24, p. 5538, 2019.

[75] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 451–466, Jan. 2020.

[76] J. Li *et al.*, "Decentralized on-demand energy supply for blockchain in Internet of Things: A microgrids approach," *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 6, pp. 1395–1406, Dec. 2019.

[77] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud," *J. Syst. Archit.*, vol. 102, Jan. 2020, Art. no. 101653.

[78] *PBC Library*. Accessed: Mar. 29, 2020. [Online]. Available: http://crypto.stanford.edu/pbc

[79] L. Nkenyereye, B. A. Tama, M. K. Shahzad, and Y.-H. Choi, "Secure and blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing," *Sensors*, vol. 20, no. 1, p. 154, 2020.

[80] *Crypto++ Library*. Accessed: Mar. 29, 2020. [Online]. Available: https://www.cryptopp.com/

[81] L. Cheng *et al.*, "SCTSC: A semicentralized traffic signal control mode with attribute-based blockchain in IoVs," *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 6, pp. 1373–1385, Dec. 2019.

[82] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *J. Syst. Archit.*, vol. 99, Oct. 2019, Art. no. 101636.

[83] *Miracl Library*. Accessed: Mar. 29, 2020. [Online]. Available: https://github.com/miracl/MIRACL

[84] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.

[85] Y. Li *et al.*, "Toward privacy and regulation in blockchain-based cryptocurrencies," *IEEE Netw.*, vol. 33, no. 5, pp. 111–117, Sep./Oct. 2019.

[86] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *J. Netw. Comput. Appl.*, vol. 116, pp. 42–52, Aug. 2018.

[87] L.-A. Hîrţan, C. Dobre, and H. González-Vélez, "Blockchain-based reputation for intelligent transportation systems," *Sensors*, vol. 20, no. 3, p. 791, 2020.

[88] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9110–9121, Sep. 2019.

[89] C. Dang, J. Zhang, C.-P. Kwong, and L. Li, "Demand side load management for big industrial energy users under blockchain-based peer-to-peer electricity market," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6426–6435, Nov. 2019.

[90] S. M. Danish, M. Lestas, H. K. Qureshi, K. Zhang, W. Asif, and M. Rajarajan, "Securing the LoRaWAN join procedure using blockchains," *Clust. Comput.*, vol. 23, pp. 2123–2138, Sep. 2020.

[91] Q. Lu, X. Xu, Y. Liu, I. Weber, L. Zhu, and W. Zhang, "uBaaS: A unified blockchain as a service platform," *Future Gener. Comput. Syst.*, vol. 101, pp. 564–575, Dec. 2019.

[92] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach," *IEEE Netw.*, vol. 33, no. 5, pp. 27–33, Sep./Oct. 2019.

[93] *Blockchain Explorer*. Accessed: Mar. 29, 2020. [Online]. Available: https://www.blockchain.com/explorer

[94] *Blockseer*. Accessed: Mar. 29, 2020. [Online]. Available: https://www.blockseer.com/

[95] *Etherchain*. Accessed: Mar. 29, 2020. [Online]. Available: https://etherchain.org/

[96] *Ethereum Geth*. Accessed: Mar. 29, 2020. [Online]. Available: https://github.com/ethereum/go-ethereum/wiki

[97] *Hyperledger*. Accessed: Mar. 17, 2020. [Online]. Available: https://www.hyperledger.org/ 2020.

[98] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. London A Math. Phys. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.

[99] *Differential Game*. Accessed: Mar. 29, 2020. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/differential-game

[100] *Automated Validation of Internet Security Protocols and Applications*. Accessed: Mar. 29, 2020. [Online]. Available: http://www.avispa-project.org/

[101] M. A. Ferrag, "EPEC: An efficient privacy-preserving energy consumption scheme for smart grid communications," *Telecommun. Syst.*, vol. 66, no. 4, pp. 671–688, 2017.

[102] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 3015–3045, 4th Quart., 2017.

[103] D. Zhang, J. Le, N. Mu, and X. Liao, "An anonymous off-blockchain micropayments scheme for cryptocurrencies in the real world," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 32–42, Jan. 2020.

[104] P. Kochovski, S. Gec, V. Stankovski, M. Bajec, and P. D. Drobintsev, "Trust management in a blockchain based fog computing platform with trustless smart oracles," *Future Gener. Comput. Syst.*, vol. 101, pp. 747–759, Dec. 2019.

[105] Q. Lyu, Y. Qi, X. Zhang, H. Liu, Q. Wang, and N. Zheng, "SBAC: A secure blockchain-based access control framework for information-centric networking," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102444.

[106] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, and Q. E. Ali, "Blockchain based permission delegation and access control in Internet of Things (BACI)," *Comput. Security*, vol. 86, pp. 318–334, Sep. 2019.

[107] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.

[108] Y. Li, Y. Tu, J. Lu, and Y. Wang, "A security transmission and storage solution about sensing image for blockchain in the Internet of Things," *Sensors*, vol. 20, no. 3, p. 916, 2020.

[109] H. Ma, E. X. Huang, and K.-Y. Lam, "Blockchain-based mechanism for fine-grained authorization in data crowdsourcing," *Future Gener. Comput. Syst.*, vol. 106, pp. 121–134, May 2020.

[110] Y. Liu and S. Zhang, "Information security and storage of Internet of Things based on block chains," *Future Gener. Comput. Syst.*, vol. 106, pp. 296–303, May 2020.

[111] N. Kabra, P. Bhattacharya, S. Tanwar, and S. Tyagi, "MudraChain: Blockchain-based framework for automated cheque clearance in financial institutions," *Future Gener. Comput. Syst.*, vol. 102, pp. 574–587, Jan. 2020.

[112] T. Zhou, X. Li, and H. Zhao, "MED-PPPHIS: Blockchain-based personal healthcare information system for national physique monitoring and scientific exercise guiding," *J. Med. Syst.*, vol. 43, no. 9, p. 305, 2019.

[113] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.

[114] N. Gayathri, G. Thumbur, P. V. Reddy, and Z. U. R. Muhammad, "Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 31808–31819, 2018.

[115] T.-H. Chang and D. Svetinovic, "Improving bitcoin ownership identification using transaction patterns analysis," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 9–20, Jan. 2020.

[116] Z. Wang, H. Yu, Z. Zhang, J. Piao, and J. Liu, "ECDSA weak randomness in bitcoin," *Future Gener. Comput. Syst.*, vol. 102, pp. 507–513, Jan. 2020.

[117] M. Poongodi *et al.*, "Prediction of the price of ethereum blockchain cryptocurrency in an industrial finance system," *Comput. Elect. Eng.*, vol. 81, Jan. 2020, Art. no. 106527.

[118] *Ganache*. Accessed: Jan. 28, 2020. [Online]. Available: https://www.trufflesuite.com/ganache

[119] *MATLAB*. Accessed: Jan. 28, 2020. [Online]. Available: https://www.mathworks.com/products/matlab.html

[120] *Hyperledger Caliper*. Accessed: Mar. 27, 2020. [Online]. Available: https://www.hyperledger.org/projects/caliper

[121] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Security Appl.*, vol. 50, Feb. 2020, Art. no. 102407.

[122] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Gener. Comput. Syst.*, vol. 105, pp. 13–26, Apr. 2020.

[123] *Multichain*. Accessed: Mar. 29, 2020. [Online]. Available: https://www.multichain.com/download-install/

[124] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking," *Comput. Security*, vol. 88, Jan. 2020, Art. no. 101629.

[125] M. Kadadha, H. Otrok, R. Mizouni, S. Singh, and A. Ouali, "SenseChain: A blockchain-based crowdsensing framework for multiple requesters and multiple workers," *Future Gener. Comput. Syst.*, vol. 105, pp. 650–664, Apr. 2020.

[126] *Solidity*. Accessed: Mar. 29, 2020. [Online]. Available: https://solidity.readthedocs.io/en/latest/

[127] E. K. Wang, Z. Liang, C.-M. Chen, S. Kumari, and M. K. Khan, "PoRX: A reputation incentive scheme for blockchain consensus of IIoT," *Future Gener. Comput. Syst.*, vol. 102, pp. 140–151, Jan. 2020.

[128] C. Lin, D. He, S. Zeadally, N. Kumar, and K.-K. R. Choo, "SecBCS: A secure and privacy-preserving blockchain-based crowdsourcing system," *Sci. China Inf. Sci.*, vol. 63, no. 3, Feb. 2020, Art. no. 130102. [Online]. Available: https://doi.org/10.1007/s11432-019-9893-2

[129] *Juice Platform*. Accessed: Mar. 29, 2020. [Online]. Available: https://open.juzix.net/

[130] A. Maw, S. Adepu, and A. Mathur, "ICs-blockops: Blockchain for operational data security in industrial control system," *Pervasive Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101048.

[131] B. Kaynak, S. Kaynak, and Ö. Uygun, "Cloud manufacturing architecture based on public blockchain technology," *IEEE Access*, vol. 8, pp. 2163–2177, 2019.

[132] *Nethereum Library*. Accessed: Mar. 29, 2020. [Online]. Available: https://github.com/Nethereum/Nethereum

[133] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K. R. Choo, "Neural-blockchain-based ultrareliable caching for edge-enabled UAV networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5723–5736, Oct. 2019.

[134] *Rinkeby Ethereum Testnet*. Accessed: Mar. 29, 2020. [Online]. Available: https://www.rinkeby.io/

[135] M. L. Di Silvestre *et al.*, "Ancillary services in the energy blockchain for microgrids," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7310–7319, Nov./Dec. 2019.

[136] *Tendermint*. Accessed: Mar. 29, 2020. [Online]. Available: https://tendermint.com/

[137] *Truffle*. Accessed: Mar. 29, 2020. [Online]. Available: https://www.trufflesuite.com/

[138] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.

[139] *Remix—Ethereum IDE*. Accessed: Mar. 29, 2020. [Online]. Available: https://remix.ethereum.org/

[140] A. Derhab *et al.*, "Blockchain and random subspace learning-based IDs for SDN-enabled Industrial IoT security," *Sensors*, vol. 19, no. 14, p. 3119, 2019.

[141] W. Dai, C. Dai, K.-K. R. Choo, C. Cui, D. Zou, and H. Jin, "SDTE: A secure blockchain-based data trading ecosystem," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 725–737, Jul. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8759960

[142] *Web3j*. Accessed: Mar. 29, 2020. [Online]. Available: https://docs.web3j.io/

[143] G. J. Holzmann, "The model checker spin," *IEEE Trans. Softw. Eng.*, vol. 23, no. 5, pp. 279–295, May 1997.

[144] *Hyperledger Besu*. Accessed: Mar. 17, 2020. [Online]. Available: https://www.hyperledger.org/projects/besu

[145] *Hyperledger Burrow*. Accessed: Mar. 17, 2020. [Online]. Available: https://www.hyperledger.org/projects/hyperledger-burrow

[146] *Hyperledger Fabric*. Accessed: Mar. 17, 2020. [Online]. Available: https://www.hyperledger.org/projects/fabric

[147] *Hyperledger Indy*. Accessed: Mar. 17, 2020. [Online]. Available: https://www.hyperledger.org/projects/hyperledger-indy

[148] *Hyperledger Iroha*. Accessed: Mar. 17, 2020. [Online]. Available: https://www.hyperledger.org/projects/iroha

[149] *Hyperledger Sawtooth*. Accessed: Mar. 17, 2020. [Online]. Available: https://www.hyperledger.org/projects/sawtooth

[150] *Hyperledger Ursa*. Accessed: Mar. 27, 2020. [Online]. Available: https://www.hyperledger.org/projects/ursa

[151] *Hyperledger Avalon*. Accessed: Mar. 27, 2020. [Online]. Available: https://www.hyperledger.org/projects/avalon

[152] *Hyperledger Cello*. Accessed: Mar. 27, 2020. [Online]. Available: https://www.hyperledger.org/projects/cello
[153] *Hyperledger Explorer*. Accessed: Mar. 27, 2020. [Online]. Available: https://www.hyperledger.org/projects/explorer
[154] *Hyperledger Grid*. Accessed: Mar. 27, 2020. [Online]. Available: https://www.hyperledger.org/projects/grid
[155] 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.
[156] 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.
[157] 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.*, early access, May 22, 2020, doi: 10.1109/JIOT.2020.2996590.
[158] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020.
[159] *The Tangle*. Accessed: Jan. 28, 2020. [Online]. Available: https://www.iota.org/foundation/research-papers
[160] Y. Li *et al.*, "Direct acyclic graph-based ledger for Internet of Things: Performance and security analysis," *IEEE/ACM Trans. Netw.*, vol. 28, no. 4, pp. 1643–1656, Aug. 2020.
[161] P. Mishra, A. Biswal, S. Garg, R. Lu, M. Tiwary, and D. Puthal, "Software defined Internet of Things security: Properties, state of the art, and future research," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 10–16, Jun. 2020.
[162] C. Lai, R. Lu, D. Zheng, and X. S. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar./Apr. 2020.
[163] Q. Xu, Z. Su, and R. Lu, "Game theory and reinforcement learning based secure edge caching in mobile social networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3415–3429, Mar. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9036917
[164] X. Liu, H. Li, G. Xu, S. Liu, Z. Liu, and R. Lu, "PADL: Privacy-aware and asynchronous deep learning for IoT applications," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6955–6969, Aug. 2020.
[165] M. Mukherjee *et al.*, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.
[166] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1826–1857, 3rd Quart., 2018.
[167] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G vehicle-to-everything services: Gearing up for security and privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, Feb. 2020.
[168] X. Shen, L. Zhu, C. Xu, K. Sharif, and R. Lu, "A privacy-preserving data aggregation scheme for dynamic groups in fog computing," *Inf. Sci.*, vol. 514, pp. 118–130, Apr. 2020.
[169] M. Wen, S. Chen, R. Lu, B. Li, and S. Chen, "Security and efficiency enhanced revocable access control for fog-based smart grid system," *IEEE Access*, vol. 7, pp. 137968–137981, 2019.
[170] Q. Kong, R. Lu, M. Ma, and H. Bao, "A privacy-preserving and verifiable querying scheme in vehicular fog data dissemination," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1877–1887, Feb. 2019.
[171] R. Lu, "A new communication-efficient privacy-preserving range query scheme in fog-enhanced IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2497–2505, Apr. 2019.
[172] J. Wang, Z. Cai, and J. Yu, "Achieving personalized *k*-anonymity-based content privacy for autonomous vehicles in CPS," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4242–4251, Jun. 2020.
[173] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 746–789, 1st Quart., 2019.
[174] U. Sarfraz, M. Alam, S. Zeadally, and A. Khan, "Privacy aware IoTA ledger: Decentralized mixing and unlinkable IoTA transactions," *Comput. Netw.*, vol. 148, pp. 361–372, Jan. 2019.

Mohamed Amine Ferrag received the bachelor's, master's, Ph.D., and HDR degrees in computer science from Badji Mokhtar—Annaba University, Annaba, Algeria, in June, 2008, June, 2010, June, 2014, and April, 2019, respectively.

Since October 2014, he has been a Senior Lecturer with the Department of Computer Science, Guelma University, Guelma, Algeria. Since July 2019, he has been a Visiting Senior Researcher with the NAU-Lincoln Joint Research Center of Intelligent Engineering, Nanjing Agricultural University, Nanjing, China. His research interests include wireless network security, network coding security, and applied cryptography. He has published over 80 papers in international journals and conferences in the above areas. He has been conducting several research projects with international collaborations on these topics. His current H-index is 19, i10-index is 29, and 1847 citations in Google Scholar Citation.

Dr. Ferrag is featured in Stanford University's list of the world's Top 2% scientists for the year 2019. Some of his research findings are published in top-cited journals, such as the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, IEEE ACCESS, *Journal of Information Security and Applications* (Elsevier), *Transactions on Emerging Telecommunications Technologies* (Wiley), *Telecommunication Systems* (Springer), *International Journal of Communication Systems* (Wiley), *Sustainable Cities and Society* (Elsevier), and *Journal of Network and Computer Applications* (Elsevier). He is currently serving on various editorial positions, such as Editorial Board Member in Journals (Indexed SCI and Scopus), such as, *IET Networks*, *International Journal of Internet Technology and Secured Transactions* (Inderscience Publishers), *Security and Communication Networks* (Wiley), and *Journal of Sensor and Actuator Networks* (MDPI).

Lei Shu (Senior Member, IEEE) received the B.S. degree in computer science from South Central University for Nationalities, Wuhan, China, in 2002, the M.S. degree in computer engineering from Kyung Hee University, Seoul, South Korea, in 2005, and the Ph.D. degree from Digital Enterprise Research Institute, National University of Ireland, Galway, Ireland, in 2010.

Until 2012, he was a Specially Assigned Researcher with the Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, Suita, Japan. He is currently a Distinguished Professor with Nanjing Agricultural University, Nanjing, China, and a Lincoln Professor with the University of Lincoln, Lincoln, U.K., where he is also the Director of NAU-Lincoln Joint Research Center of Intelligent Engineering. He has published over 400 papers in related conferences, journals, and books in the areas of sensor networks and Internet of Things. His current H-index is 62 and i10-index is 244 in Google Scholar Citation. His current research interests include wireless sensor networks, and Internet of Things.

Dr. Shu was a recipient of the 2014 Top Level Talents in Sailing Plan of Guangdong Province, China, the 2015 Outstanding Young Professor of Guangdong Province, and the GLOBECOM 2010, ICC 2013, ComManTel 2014, WICON 2016, SigTelCom 2017 Best Paper Awards, the 2017 and 2018 IEEE Systems Journal Best Paper Awards, the 2017 Journal of Network and Computer Applications Best Research Paper Award, and the Outstanding Associate Editor Award of 2017, and the 2018 IEEE ACCESS. He has served as a TPC member for more than 160 conferences, such as ICDCS, DCOSS, MASS, ICC, GLOBECOM, ICCCN, WCNC, and ISCC. He has also served over the 60 various Co-Chair for international conferences/workshops, such as IWCMC, ICC, ISCC, ICNC, Chinacom, especially the Symposium Co-Chair for IWCMC 2012, ICC 2012, the General Co-Chair for Chinacom 2014, Qshine 2015, Collaboratecom 2017, DependSys 2018, and SCI 2019, the TPC Chair for InisCom 2015, NCCA 2015, WICON 2016, NCCA 2016, Chinacom 2017, InisCom 2017, WMNC 2017, and NCCA 2018.