This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

Blockchain Technologies for the Internet of Things: Research Issues and Challenges

Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, *Member, IEEE,* Abdelouahid Derhab, Leandros Maglaras, *Senior Member, IEEE,* Helge Janicke

***Abstract*—This paper presents a comprehensive survey of the existing blockchain protocols for the Internet of Things (IoT) networks. We start by describing the blockchains and summarizing the existing surveys that deal with blockchain technologies. Then, we provide an overview of the application domains of blockchain technologies in IoT, e.g, Internet of Vehicles, Internet of Energy, Internet of Cloud, Edge computing, etc. Moreover, we provide a classification of threat models, which are considered by blockchain protocols in IoT networks, into five main categories, namely, identity-based attacks, manipulation-based attacks, cryptanalytic attacks, reputation-based attacks, and service-based attacks. In addition, we provide a taxonomy and a side-by-side comparison of the state-of-the-art methods towards secure and privacy-preserving blockchain technologies with respect to the blockchain model, specific security goals, performance, limitations, computation complexity, and communication overhead. Based on the current survey, we highlight open research challenges and discuss possible future research directions in the blockchain technologies for IoT.**

***Index Terms*—Blockchain, Consensus, Security, Threats, IoT**

I. Introduction

In the last few years, we have witnessed the potential of Internet of Things to deliver exciting services across several sectors, from social media, business, intelligent transportation and smart cities to the industries [1], [2], [3]. IoT seamlessly interconnects heterogeneous devices with diverse functionalities in the human-centric and machine-centric networks to meet the evolving requirements of the earlier mentioned sectors. Nevertheless, the significant number of connected devices and massive data traffic become the bottleneck in meeting the required Quality-of-Services (QoS) due to the computational, storage, and bandwidth-constrained IoT devices. Most recently, the blockchain [4], [5], [6], [7], a paradigm shift, is transforming all the major application areas of IoT by enabling a decentralized environment with anonymous and trustful transactions. Combined with the blockchain technology, IoT systems benefit from the lower operational cost, decentralized resource management, robustness against threats and attacks, and so on. Therefore, the convergence of IoT and blockchain technology aims to overcome the significant challenges of realizing the IoT platform in the near future.

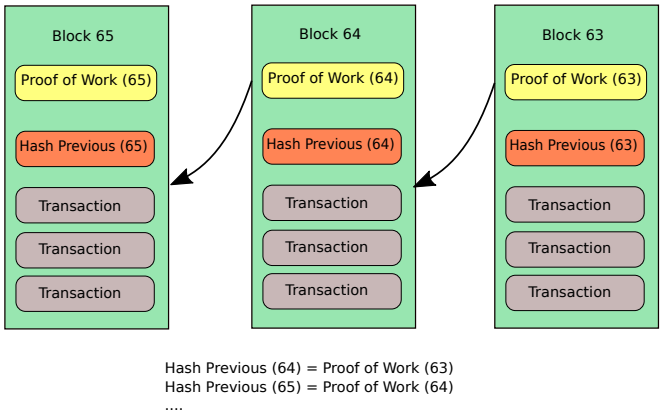

Fig. 1. Blockchain structure. A block in a blockchain architecture is an aggregated set of data, which each block can be identified using a hash function. The formed block will contain a hash of the previous block so that all data can be connected via a linked list structure. Specifically, the block contains a header and relevant transaction data. In the header, several pieces of information are entered: the version of the block, the identifier of the previous block, the date and the difficulty of carrying out the proof of work.

Blockchain, a distributed append-only public ledger technology, was initially intended for the cryptocurrencies, e.g., Bitcoin[1]. In 2008, Satoshi Nakamato [8] introduced the concept of blockchain that has attracted much attention over the past years as an emerging peer-to-peer (P2P) technology for distributed computing and decentralized data sharing. Due to the adoption of cryptography technology and without a centralized control actor or a centralized data storage, the blockchain can avoid the attacks that want to take control over the system. Later, in 2013, Ethereum, a transaction-based state-machine, was presented to program the blockchain technologies. Interestingly, due to its unique and attractive features such as: transactional privacy, security, the immutability of data, auditability, integrity, authorization, system transparency, and fault tolerance, blockchain is being applied in several

(Corresponding author: Mohamed Amine Ferrag)
M. A. Ferrag is with Department of Computer Science, Guelma University, B.P. 401, 24000, Algeria e-mail: mohamed.amine.ferrag@gmail.com, ferrag.mohamedamine@univ-guelma.dz, phone: +213661-873-051
M. Derdour is with Department of Mathematics and Computer Science, University of Larbi Tebessi, Tebessa 12002, Algeria e-mail: m.derdour@yahoo.fr
M. Mukherjee is with the Guangdong Provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis, Guangdong University of Petrochemical Technology, Maoming 525000, China e-mail: m.mukherjee@ieee.org
A. Derhab is with Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia, e-mail: abderhab@ksu.edu.sa
L. Maglaras is with School of Computer Science and Informatics, De Montfort University, Leicester, UK, , and also with General Secretariat of Digital Policy, Athens, Greece, e-mail: leandrosmag@gmail.com
H. Janicke is with School of Computer Science and Informatics, De Montfort University, Leicester, UK, e-mail: heljanic@dmu.ac.uk
Manuscript received 2018.

[1]Apart from Bitcoin, there are several cryptocurrencies such as Litecoin, Peercoin, Swiftcoin, Peercoin, and Ripple.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

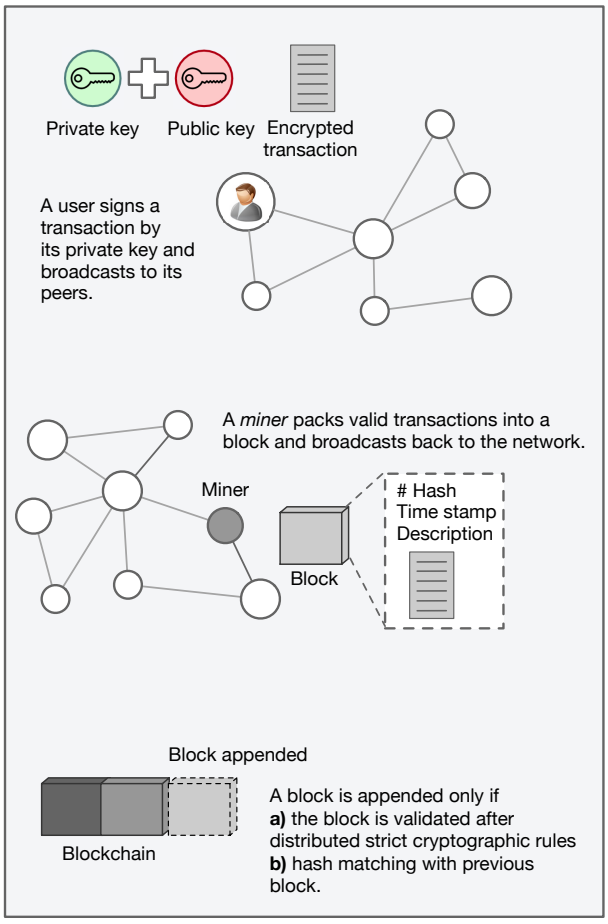

Fig. 2. An illustration of blockchain working methodology. At first, the end-user signs a transaction with the private key and broadcasts the signed transaction to the peers. The peers validate the signed transaction and further disseminate the transaction over the network. After mutually validated by all the involved parties, a consensus agreement is fulfilled. Afterward, the miners includes the valid transaction into a timestamped block that is again broadcasted back into the network. Finally, after validating the broadcast block with the transaction and hash-matching it with the previous block in the blockchain, the broadcast block is appended to the blockchain.

sectors beyond the cryptocurrencies. Some of the areas are identity management [9], intelligent transportation [10], [11], [12], [13], [14], [15], supply-chain management, mobile-crowd sensing [16], agriculture [17], Industry 4.0 [18], [19], Internet of energy [20], [21], [18], [22], and security in mission critical systems [23].

As shown in Fig. 1, the blockchain structure is composed of a sequence of blocks, which are linked together by their hash values. In the blockchain network, a public ledger maintains the digitally signed transactions of the users in a P2P network. In general, a user has two keys: a public key for other users for the encryption and a private key to read an encrypted message, as shown in Fig. 2. From the blockchain perspective, the private key is used for signing the blockchain transaction and the public key represents the unique address. Asymmetric cryptography is used to decrypt the message encrypted by the corresponding public key. At the initial stage, an user signs a transaction using its private key and broadcasts it to its peers. Once the peers receive the signed transaction, they validate the transaction and disseminate it over the network. All the parties who are involved in the transactions mutually validate the transaction to meet a consensus agreement. Once a distributed consensus is reached, the special node, called as miner, includes the valid transaction into a timestamped block. The block, which is included by the miner, is broadcast back into the network. After validating the broadcast block, which contains the transaction, as well as hash-matching it with the previous block in the blockchain, the broadcast block is appended to the blockchain.

Based on the data management and the type of applications, blockchain can classified either as private (permission) or public (permissionless). Both classes are decentralized and provide a certain level of immunity against faulty or malicious users for the ledger. The main differences between private and public blockchains lie in the execution of the consensus protocol, the maintenance of the ledger, and the authorization to join to the P2P network. Detailed examples of these classes are illustrated in [24]. In the context of IoT, blockchains can be classified based on authorization and authentication. As shown in Fig. 3, in a private blockchain, the centralized trusted authority that manages the authentication and authorization process selects the miners. On the other hand, in a public blockchain (in general, permissionless), there is no intervention of any third party for the miner selection and joining for a new user to the blockchain network.

Recently, there is a huge amount of investment from the industries [25], [26] as well as a significant interest from academia to solve major research challenges in blockchain technologies. For example, the consensus protocols are the major building blocks of the blockchain technologies, thus, the threats targeting the consensus protocols become a significant research issue in the blockchain. Furthermore, blockchain forks bring threats to the blockchain consensus protocols. Moreover, it is observed that the vulnerability is about 51% for a new blockchain [27]. At the same time, maintenance of several blockchains requires a significant amount of power consumption [28].

A. Related Surveys and Our Contributions

There are related survey papers [7], [29], [30], [31], [24], [32] that covered different aspects of the blockchain technology. For example, a brief overview of blockchain for bitcoin was discussed in [29], [30]. However, these surveys are very limited regarding detailed discussion on research challenges in the blockchain. Moreover, Sankar et al. [29] briefly presented the feasibility of various consensus protocols in the blockchain. The detailed insights of bitcoin were presented in [7]. Recently, the surveys [24] presented the overview of Blockchain-based IoT (BIoT) applications. The security and privacy aspects are presented in [32], [31] for bitcoin, one of the blockchain applications. Table I summarizes the main focuses and major contributions of the previous comprehensive surveys on blockchain technologies. Although the above-mentioned surveys [7], [31], [24], [32] have laid a solid foundation for blockchain technologies, our survey differs in several aspects. The main contributions of this paper are:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

TABLE I
RELATED SURVEYS ON BLOCKCHAIN TECHNOLOGIES

Year	Author	Main focus/contributions
2016	Tschorsch and Scheuermann [7]	Fundamental structures and insights of the core of the Bitcoin protocol and its applications
2017	Sankar et al. [29]	Feasibility and efficiency of consensus protocols in blockchain.
2017	Kaushik et al. [30]	A brief survey on bitcoin.
2018	Khalilov and Levi [31]	An overview and detailed investigation of anonymity and privacy in Bitcoin-like digital cash systems.
2018	Fernández-Caramés and Fraga-Lamas [24]	A review on developing Blockchain-based IoT (BIoT) applications.
2018	Conti et al. [32]	A systematic survey that covers the security and the privacy aspects of Bitcoin.

- We provide overviews of the different application domains of blockchain technologies in IoT, e.g, Internet of Vehicles, Internet of Energy, Internet of Cloud, Edge computing, etc.
- We classify the threat models, which are considered by the blockchain protocols in IoT networks, into five main categories, namely, identity-based attacks, manipulation-based attacks, cryptanalytic attacks, reputation-based attacks, and service-based attacks.
- We review existing research on anonymity and privacy in Bitcoin systems.
- We provide a taxonomy and a side-by-side comparison, in a tabular form, of the state-of-the-art on the recent advancements towards secure and privacy-preserving blockchain technologies with respect to the blockchain model, specific security goals, performance and limitations, computation complexity and communication overhead.
- We highlight the open research challenges and discuss the possible future research directions in the field of blockchain technologies for IoT.

The remainder of this paper is organized as follows. Section II presents the application domains of blockchain technologies in IoT. In Section III, we present the classification of threat models that are considered by the blockchain protocols in IoT networks. In Section IV, we present a side-by-side comparison, in a tabular form, of the state-of-the-art on the recent advancements towards secure and privacy-preserving blockchain technologies. Then, we discuss open issues and recommendations for further research in Section V. Finally, we draw our conclusions in Section VI.

II. BLOCKCHAIN APPLICATIONS FOR THE IOT

As presented in Fig. 4, the blockchain technology can be effectively applied in almost all domains of IoT. Note that it is not necessary to use blockchain in some cases (e.g., when the IoT entities trust a third party). Fig. 5 presents a procedure that could be applied as an initial check for deciding whether to use a blockchain-based solution in an IoT application.

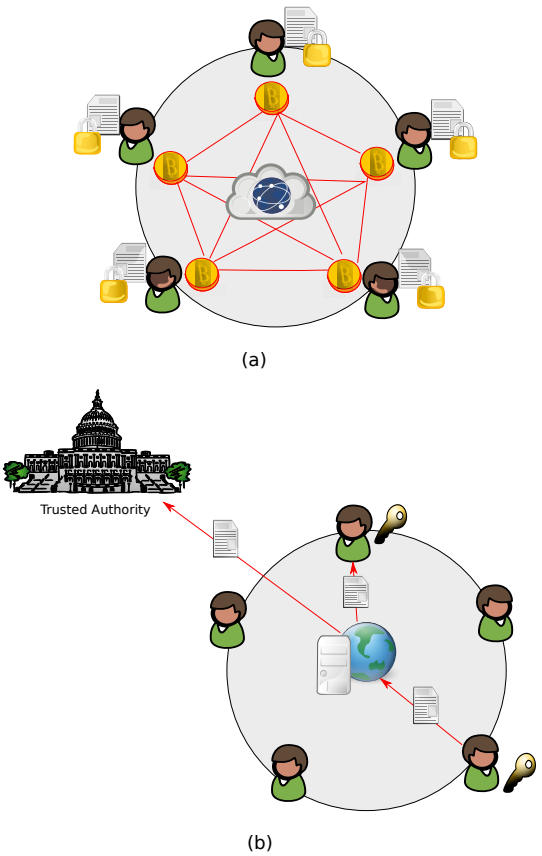

Fig. 3. (a) Public blockchain system, which is completely open and anyone can join and participate in the network (e.g., Bitcoin); (b) Private blockchain system, which the participants need to obtain an invitation or permission from a trusted authority, in order to join and participate in the network (e.g., the Linux Foundation's Hyperledger Fabric)

Scalability issues that may arise due to the increased number of participating nodes and thus the block size, especially for 5G and Internet of Vehicles IoT domains that could affect power usage, network propagation and network congestion should be taken under consideration when blockchain technology is proposed for such systems [33].

A. Internet of healthcare things

The usage of IoT in healthcare has allowed to feed the ehealthcare systems with clinical data related to the patients, their family, their friends, as well as the healthcare providers. The data, called electronic medical records (EMRs), is stored by the responsible healthcare provider. To facilitate patient data portability, there are the electronic health records (EHRs), which have a richer data structure than EMRs. Based on the idea of distributed online database, Esposito et al. [34] proposed the design of a blockchain-based scheme for the IoT in healthcare. In a model of consortium blockchain, a new block is instantiated and distributed when new healthcare data is created. To preserve the privacy of patients and maintain the immutability of EHRs, Guo et al. [35] introduced an attribute-based signature scheme, named MA-ABS, which uses multiple authorities. The MA-ABS scheme uses the blockchain technology and can resist to N-1 corrupted authorities collusion

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

Fig. 4. Blockchain applications for the IoT.

attacks. In addition, the MA-ABS is unforgeable in suffering a selective predicate attack. Therefore, Liang et al. [36] used the blockchain network in mobile healthcare applications for integrity protection, further auditing or investigation.

B. Internet of things in the 5G era

In the IoT era, 5G will enable a fully mobile and connected society for billions of connected objects [53]. To solve the privacy issues in the 5G heterogeneous communication environment, Fan et al. [54] proposed a blockchain-based privacy preserving and data sharing scheme. Based on the idea of adding blocks to the blockchain, each new block is connected to the blockchain by its hash value. Note that the previous hash value can be known from the block header.

C. Internet of vehicles

The Internet of Vehicles (IoV) is an emerging concept, which allows the integration of vehicles into the new era of the IoT in order to establish the smart communication between vehicles and heterogeneous networks such as vehicle-to-vehicle, vehicle-to-road, vehicle-to-human, vehicle-to-sensor, and vehicle-to-everything. However, some recent works try to apply the blockchain technology to IoV. Based on the decentralized security model, Huang et al. [10] proposed a blockchain ecosystem model, named LNSC, for electric vehicle and charging pile management. The LNSC model uses elliptic curve cryptography (ECC) to calculate hash functions electric vehicles and charging piles. To avoid the location tracking in the IoV, Dorri et al. [11] proposed a decentralized privacy-preserving architecture, where overlay nodes manage the blockchain. In addition, the hash of the backup storage is stored in the blockchain.

Without the administration from the central manager, Lei et al. [12] proposed a blockchain-based dynamic key management for vehicular communication systems. Based on a decentralized blockchain structure, the third-party authorities

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

TABLE II
EXISTING RESEARCH ON ANONYMITY AND PRIVACY FOR BITCOIN SYSTEMS

Year	Protocol	Countermeasures	Security models
2013	CoinSwap [37]	- The protocol requires four published transactions	- Anonymity
2013	CoinJoin [38]	- Each user check the mixing transaction before signing on it	- Anonymity
2013	ZeroCoin [39]	- Decentralized e-cash scheme with a tuple of randomized algorithms (Setup, Mint, Spend, Verify) - RSA accumulators and non-interactive zero-knowledge signatures of knowledge	- Anonymity
2014	Mixcoin [40]	- Cryptographic accountability - Randomized mixing fees	- Anonymity
2014	Xim [41]	- Anonymous decentralized pairing	- Anonymity
2014	CoinShuffle [42]	- Requires only standard cryptographic primitives	- Anonymity
2014	Zerocash [43]	- Publicly-verifiable preprocessing zero-knowledge	- Privacy-preserving
2015	Blindcoin [44]	- Blind signature scheme	- Anonymity
2015	CoinParty [45]	- Combination of decryption mixnets with threshold signatures	- Anonymity
2016	Blindly Signed Contract [46]	- Blind signature scheme	- Anonymity
2017	TumbleBit [47]	- Replaces on-blockchain payments with off-blockchain puzzle solving	- Anonymity
2017	Kanemura et al. [48]	- The privacy metric "Deniability"	- Privacy-preserving
2017	Wang et al. [49]	- Elliptic curve cryptography	- Privacy-preserving
2017	Wang et al. [50]	- Homomorphic paillier encryption system	- Privacy-preserving
2018	Liu et al. [51]	- Ring signature - Elliptic curve digital signature algorithm	- Privacy-preserving - Anonymity
2018	Huang et al. [52]	- Commitment-based sampling scheme	- Security requirement of completeness - Security requirement of fairness - Security requirement of accountability

are removed and the key transfer processes are verified and authenticated by the security manager network. Moreover, Kang et al. [13] introduced a P2P electricity trading system, named PETCON, to illustrate detailed operations of localized P2P electricity trading. Using consortium blockchain method, the PETCON system can publicly audit and share transaction records without relying on a trusted third party. To solve the issues of forwarding reliable announcements without revealing users' identities, Li et al. [14] proposed a privacy-preserving scheme, named CreditCoin, for sending announcements anonymously in the IoV. The CreditCoin scheme uses the blockchain via an anonymous vehicular announcement aggregation protocol to build trust in the IoV communications. For data credibility assessment in the IoV, Yang et al. [15] proposed a blockchain-based reputation system, which can judge the received messages as either true or false based on the senders' reputation values.

D. Internet of Energy

The Internet of energy (IoE) provides an innovative concept to increase the visibility of energy consumption in the Smart Grid. Based on the sovereign blockchain technology, Gao et al. [20] introduced a monitoring system on the Smart Grid, named GridMonitoring, for ensuring transparency, provenance, and immutability. The GridMonitoring system is based on four layers, namely, 1) Registration and authentication layer, 2) Smart meter, 3) Processing and consensus nodes, and 4) Data processing on the smart grid network. In modern power systems, Liang et al. [21] proposed a data protection framework based on distributed blockchain, which can resist against data manipulation that is launched by cyber attackers (e.g., false data injection attacks). To guarantee data accuracy, Liang's framework uses the consensus mechanism, which is automatically implemented by every node and has the representative characteristics, namely, 1) Setting of public/private key update frequency, 2) Block generation, 3) Miner selection, and 4) Release of meter's memory periodically. For secure energy trading in Industrial Internet of Things (IIoT), Li et al. [18] introduced the energy blockchain, which is based on the consortium blockchain technology and the Stackelberg game. Aitzhan and Svetinovic [22] implemented a token-based private decentralized energy trading system for in decentralized smart grid energy, which can be applied to the IoE.

E. Internet of Things devices

In the Internet of Things devices, attackers seek to exfiltrate the data of IoT devices by using the malicious codes in malware, especially on the open source Android platform. By utilizing statistical analysis method, Gu et al. [55] introduced a malware detection system based on the consortium Blockchain, named CB-MDEE, which is composed of detecting consortium chain by test members and public chain by users. The CB-MDEE system adopts a fuzzy comparison method and multiple marking functions In order to reduce the false-positive rate and improve the detection ability of malware variants. To protect the embedded devices in the IoT, Lee et al. [56] a firmware update scheme based on the blockchain technology, which the embedded devices have the two different operation cases, namely, 1) response from a verification node to a request node, and 2) response from a response node to a request node.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

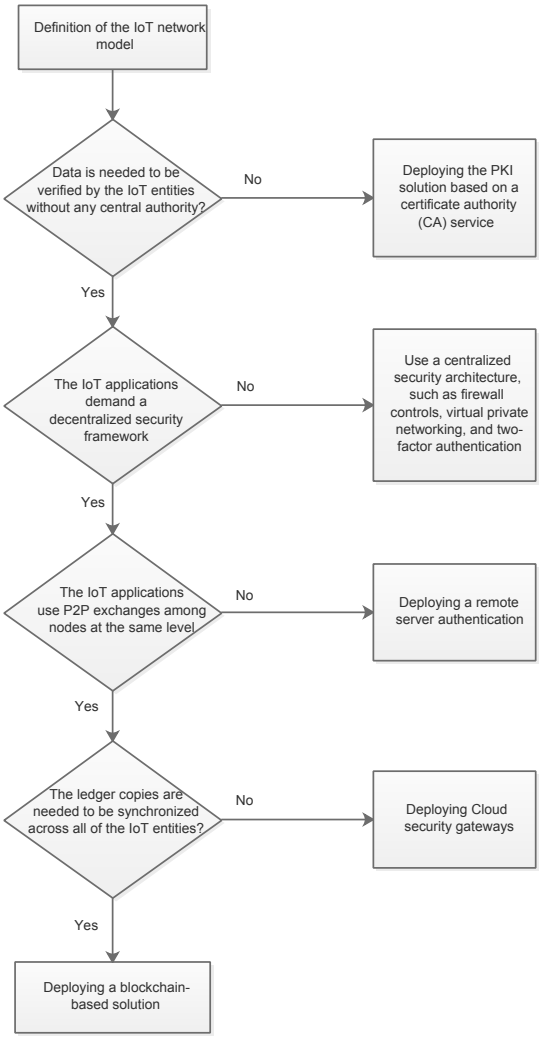

Fig. 5. Flow diagram for deciding when to use a blockchain-based solution in an IoT application.

F. Access Management in IoT

For managing IoT devices, Novo [57] proposed a distributed access control system using the blockchain technology. The architecture of this system is composed of six components, namely, 1) Wireless sensor networks, 2) Managers, 3) Agent node, 4) Smart contract, 5) Blockchain network, and 6) Management hubs. This system brings some advantages for the access control in IoT, such as: 1) mobility, which can be used in isolated administrative systems; 2) accessibility, which ensures that the access control rules are available at any time; 3) concurrency, which allows that the access control policies can be modified simultaneously; 4) lightweight, which means that the IoT devices do not need any modification to adopt this system; 5) scalability, as the IoT devices can be connected through different constrained networks; 6) transparency, where the system can preserve the location privacy.

G. Collaborative video delivery

The diffusion of high-quality content in the IoT nowadays challenges for the internet service providers. However, Herbaut and Negru [58] proposed a decentralized brokering mechanism for collaborative blockchain-based video delivery, which is relying on advanced network services chains. Specifically, this management mechanism is composed of three blockchains, namely, 1) the content brokering blockchain, 2) the delivery monitoring blockchain, and 3) the provisioning blockchain. In addition, this management mechanism is deployed with the open source project Hyperledger-Fabric [2] where the results show that the number of nodes slightly increases the convergence time .

H. Internet of Cloud

In the Internet of Cloud (IoC), billions of IoT devices upload their data to the cloud through the internet connection utilizing virtualization technology. Xu et al. [59] introduced an intelligent resource management for cloud datacenters based on the blockchain technology, in order to save and reduce the total cost of energy consumption. Specifically, the users use their individual private keys to sign a transaction, while the neighboring users verify the broadcast transaction. The block is discarded when it does not pass verification. Therefore, Sharma et al. [60] proposed a distributed cloud architecture that uses three emerging technologies, namely, software-defined networking (SDN), fog computing, and a blockchain technique. The SDN controllers of the fog node are used to provide programming interfaces to network management operators. The blockchain technique is used to provide scalable, reliable, and high-availability services. In addition, Xia et al. [61] proposed a blockchain-based data sharing system, named MeDShare, for cloud service providers. This system uses four layers namely, 1) User layer, 2) Data query layer, 3) Data structuring and provenance layer, and 4) Existing database infrastructure layer.

I. Intrusion Detection

Many techniques for implementing intrusion detection systems (IDSs) in the IoT environment have been proposed, which are based in machine learning. To improve the collaborative intrusion detection systems (CIDSs), Alexopoulos et al. [62] introduced the idea of utilizing blockchain technology in order to secure the exchange of alerts between the collaborating nodes. Meng et al. [63] discussed the applicability of blockchain technology in an intrusion detection systems. Modern intrusion detection systems must be based on collaborative communication among distributed IDSs [64], demanding extensive data sharing among entities and trust computation. In order to deal with the privacy concerns that are raised by the data exchange and to suppress insider attacks, the blockchain technology is applied. In this way, the use of trusted third party, which is also a single point of failure, that is needed in traditional collaborative IDSs can be avoided.

J. Software-defined networking

To increase IoT's bandwidth, researchers have been proposing the Software Defined Networking (SDN) technology,

[2] www.hyperledger.org/projects/fabric

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

which provides intelligent routing and simplifies decision-making processes by the SDN controller [65]. Recently, Sharma et al. [66] proposed a distributed IoT network architecture, named DistBlockNet. Based on the blockchain technology, DistBlockNet architecture can provide scalability and flexibility, without the need for a central controller. The distributed blockchain network uses two type of nodes, namely, 1) the controller/verification node, which maintains the updated flow rules table information and 2) the request/response node, which updates its flow rules table in a blockchain network.

K. Edge Computing

Edge computing is a highly virtualized platform that enables computing and storage between end-users and data center of the traditional cloud computing [5]. Without the third parties, Fog devices can communicate with each other. However, the blockchain technique can be used to facilitate communications between fog nodes and IoT devices. Huang et al. [52] proposed a fair payment scheme for outsourcing computations of Fog devices. Based on the bitcoin, this scheme considers the following security properties, namely, completeness, fairness, and accountability.

L. Distributed P2P Applications

In distributed peer-to-peer (P2P) applications for the IoT, the IoT devices self-organize and cooperate for a new breed of applications such as collaborative movies, forwarding files, delivering messages, electronic commerce, and uploading data using sensor networks. To incentivize users for cooperation, He et al. [67] proposed a truthful incentive mechanism based on the blockchain technique for dynamic and distributed P2P environments. To prevent selfish users and defend against the collusion attacks, this scheme proposed a pricing strategy, which allows intermediate nodes to obtain rewards from blockchain transactions due to their contribution to a successful delivery.

M. Crowdsensing Applications

The emerging mobile crowdsensing paradigm is a novel class of mobile IoT applications (e.g., geographical sensing applications). Wang et al. [16] is an interesting incentive mechanism for privacy-preserving in crowdsensing applications based on the blockchain cryptocurrencies. Specifically, this mechanism can eliminate the security and privacy issues using the miners' verifiable data quality evaluation to deal with the impersonation attacks in the open and transparent blockchain. In addition, to achieve k-anonymity privacy protection, the mechanism uses a node cooperation method for the participating users.

N. Data storage

The data storage can deal with heterogeneous data resources for IoT-based data storage systems. How to share and protect these sensitive data are the main challenges in IoT data storage. Based on the blockchain technology, Jiang et al. [68] proposed a private keyword search, named Searchain, for decentralized storage. The Searchain architecture includes two component, namely, 1) transaction nodes in a peer-to-peer structure and 2) a blockchain of all the ordered blocks. In addition, the Searchain architecture can provide user privacy, indistinguishability, and accountability.

O. Bitcoin

Launched in 2009, Bitcoin is the peer-to-peer (P2P) payment network that does not need any central authorities. Based on the core technique of blockchain, Bitcoin users do not use real names; instead, pseudonyms are used. Therefore, Bitcoin is based on three main technical components: transactions, consensus Protocol, and communication network.

The existing research on anonymity and privacy for Bitcoin system are presented in Tab. II. Khalilov and Levi [73] have published an interesting investigation on anonymity and privacy in Bitcoin-like digital cash systems. Specifically, the study classified the methods of analyzing anonymity and privacy in Bitcoin into four categories, namely, 1) Transacting, 2) Utilizing off-network information, 3) Utilizing network, and 4) Analyzing blockchain data.

As discussed by Wang et al. [49], Bitcoin works in practice, but not in theory,and the main issue is how to protect the potential buyers' privacy in Bitcoin using the public key infrastructure. Wang et al. [49] studied the designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography. Specifically, the authors proposed a privacy-preserving scheme, named DV-PoA, which can satisfy unforgeability. Note that the DV-PoA scheme uses elliptic curve discrete logarithm problem, elliptic curve computational Diffie-Hellman problem, and collision-resistance of cryptographic hash function. In addition, to protect the privacy of simplified payment verification (SPV) clients, Kanemura et al. [48] proposed a privacy-preserving Bloom filter design for an SPV client based on $\gamma-$Deniability.

By removing the trusted third party, Qin et al. [74] proposed a distributively blockchain-based PKI for Bitcoin system, named Cecoin. To ensure the consistency, Cecoin uses an incentive mechanism and a distributed consensus protocol. To provide multi-certificate services and identity assignment, Cecoin converts a triple (address, domain, cert) to a tuple (key, address, cert), and key represents path of cert in the tree. Therefore, to protect the transaction privacy in Bitcoin, Wang et al. [50] proposed a framework by adding the homomorphic Paillier encryption system to cover the plaintext amounts in transactions. To solve the trust problem in Bitcoin, Huang et al. [52] proposed a commitment-based sampling scheme instead of ringer, which can be used for generic computations in the outsourcing computing.

III. Threat models for Blockchain

In this section, we present the vulnerabilities of the blockchain systems, and describe the threat models that are considered by the blockchain protocols in IoT networks. Although blockcahins are one of the promising technologies for securing IoT application, but they suffer from the following vulnerabilities [75], [76]:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

TABLE III
MAJOR ATTACKS ON BLOCKCHAIN-BASED IOT NETWORKS

Attack model	Attack type	Countermeasures	Resistant protocols
Key attack	Application-free	- Different temporary private keys for each session agreement, and elliptic curve encryption is used to calculate the hash functions	LNSC protocol [10]
DDoS/DoS attack	Application-dependent	- Using blockchain to update, validate, and download the flow rules table of a distributed SDN	DistBlockNet protocol [66]
	Application-dependent	- Allowing mixing peers to retain funds of malicious users to protect a decentralized mixing service of the blockchain	CoinParty protocol [69]
	Application-dependent	- Ring signature using ECDSA and banning the misbehaving users to protect the mixing service of the blockchain	Liu et al.'s protocol [51]
	Application-free	-Block size limitation, attribute-based signatures, and multi-receivers encryption	BSeIn protocol [70]
Replay attack	Application-free	- Different temporary private keys for each session agreement, and elliptic curve encryption is used to calculate the hash functions	LNSC protocol [10]
		- The freshness of public/private key pairs	BSeIn protocol [70]
Hiding Blocks	Application-free	- An immutable chain of temporally ordered interactions is created for each agent	TrustChain protocol [71]
False data injection attack	Application-dependent	- Blockchain consensus mechanisms	Liang et al.'s protocol [21]
Tampering attack	Application-free	- Public-key cryptosystem	Wang et al.'s protocol [50]
Impersonation attack	Application-free	- Different temporary private keys for each session agreement, and elliptic curve encryption is used to calculate the hash functions	LNSC protocol [10]
		- Distributed incentive mechanism based blockchain and the node cooperation based privacy protection mechanism	Wang et al.'s protocol [16]
		- Attribute-based signatures	BSeIn protocol [70]
Refusal to Sign	Application-free	- Not interacting with the malicious agent, or splitting the transactions in smaller amounts	TrustChain protocol [71]
Overlay attack	Application-free	- Every transaction is embedded with a Time-Stamp to mark the uniqueness	Wang et al.'s protocol [50]
Double-spending attack	Application-free	- Multi signatures and anonymous encrypted message propagation streams	Aitzhan and Svetinovic's protocol [22]
		- Time-Stamp and the Proof-of-Work mechanism	Wang et al.'s protocol [50]
Modification attack	Application-free	- Different temporary private keys for each session agreement, and elliptic curve encryption is used to calculate the hash functions	LNSC protocol [10]
		- The attribute signature and the MAC	BSeIn protocol [70]
Collusion attack	Application-free	- Blockchain-based incentive mechanism	He et al.'s protocol [67]
Whitewashing attack	Application-free	- Lower priorities are given to the agents of new identities	TrustChain protocol [71]
Quantum attack	Application-free	- Lattice-based signature scheme	Yin et al.'s protocol [72]
Man-in-the-middle attack	Application-free	- Different temporary private keys for each session agreement, and elliptic curve encryption is used to calculate the hash functions	LNSC protocol [10]
		- Secure mutual authentication	BSeIn protocol [70]
Sybil attack	Application-free	- An immutable chain of temporally ordered interactions is created for each agent	TrustChain protocol [71]

- *Private key leakage:* In [77], it has been discovered that Elliptic Curve Digital Signature Algorithm (ECDSA), which is used to generate the private key of the user, is vulnerable. If the private key is generated with limited randomness, it can bre ecovered by an attacker. As a result, many attacks, as shown in Table III can be launched by exploiting this vulnerability such as: key attack, replay attack, tampering attack, impersonnation attack, modification attack,and Man-in-the-middle attack.
- *Double spending:* is the act of using the same bitcoins more than once. This vulnerability is easy to be exploited in the following two cases:
  - An attacker sends the same coin in rapid succession to two different addresses. If the seller accepts the payment without waiting for confirmations, he/she is likely to get the double spending bitcoin, i.e., no receipt of bitcoin.
  - An attacker pre-mines one transaction into a block and spends the same coins before releasing the block to invalidate that transaction.
- *Transaction privacy leakage:* In order to protect the transaction privacy of users, the user needs to assign a private key to each transaction. In this way, the attacker cannot link transaction records to real identities. In Monero [75], users can include some chaff coins, called mixins, when they perform a transaction so that the attacker cannot reveal the linkage between the users and their transactions. However, the privacy protection measures in blockchain are not efficient. Andrews et al. [78] discovered that 66.09% of all transactions do not contain any mixins, which leads to the privacy leakage of the transaction. In addition, it is possible to link the bitcoin accounts with the actual identities through the human activities in daily transactions.
- *51% vulnerability:* The blockchain relies on the distributed consensus mechanism to establish mutual trust among agents. However, this mechanism has 51% vulnerability, i.e., if a single miner has more than 50% of the total computing power of the entire blockchain, then the 51% attack may be launched. An attacker can exploit

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

this vulnerability to perform the following attacks:
  - Tamper with the blockchain information.
  - Reverse transactions, and launch double spending attack.
  - Exclude transactions, and change their ordering.
  - Hinder normal mining operations.
  - Hamper the confirmation of normal transactions.
- *Selfish and repuation-based behaviors:* Due to some specifications of the blockchains, some misbehaviors cannot be avoided such as:
  - *Hiding blocks*: An agent only exposes transactions that have a positive impact on his reputation and hides the ones with negative reputation.
  - *Whitewhashing*: An agent can get rid of its bad reputation by making a new identity.
  - *Refusal to sign*: A malicious agent can decide to not sign a transaction that is not in his favor.

A summary of 16 attacks are given in Table III. The attacks can be classified as: (1) application-dependent and (2) application-free. The first class targets a specific application by exploiting that application vulnerabilities. On the other hand, in the second class, an attack can target any application as it exploits the vulnerabilities of the blockchain. The attacks are also classified into the following five main categories: identity-based attacks, manipulation-based attacks, cryptanalytic attacks, reputation-based attacks, and service-based attacks, as presented in Figure 6.

A. Identity-based attacks

The attacks under this category forge identities to masquerade as authorized users, in order to get access to the system and manipulate it. We classify four attacks, namely: Key attack, Replay attack, Impersonation attack, and Sybil attack.

- *Key attack*: It occurs by exploiting the private key leakage vulnerability. This attack is defined in the context of a system combining electric vehicles and charging piles, as follows: "If the private key of an electric vehicle that has been used for longtime leaks, the attacker can impersonate this electric vehicle to deceive others" [10]. To deal with this attack, LNSC protocol [10] provides a mutual authentication mechanism between the electric vehicles and charging piles. To this end, it uses different temporary private keys of the electric vehicles, charging piles and operators for each session agreement it also employs the elliptic curve encryption to calculate the hash functions, and hence it ensures resiliency against the key leakage attack.
- *Replay attack*: The aim of this attack is to spoof the identities of two parties, intercept their data packets, and relay them to their destinations without modification. If the blockchaim generates a private key with limited randomness during the signature process, the key could be leaked and the replay attack can be launched by exploiting this vulnerability. To resist against this attack, LNSC [10] uses the idea of temporary private keys for each session agreement, and elliptic curve encryption to calculate the hash functions. On the other hand, BSein [70] uses a fresh one-time public/private key pair, which is generated for each request, to encrypt the message and compute the Message Authentication Code (MAC). In this way, the replay attack can be detected.
- *Impersonation attack*: An adversary tries to masquerade as a legitimate user to perform unauthorized operations. If the private key is leaked, this attack might occur. Also, the work of verification in the traceable public blockchain can be checked by everyone. As the miners can obtain transaction contents when verifying the data, they may launch an impersonation attack or collusion attacks to get illegal payment. As presented in Table III, there are three methods that are proposed to protect against this attack. The idea of temporary private keys for each session agreement, and elliptic curve encryption to calculate the hash functions, is proposed by LNSC protocol [10]. Wang et al. [16] propose a distributed incentive-based cooperation mechanism, which protects the user's privacy as well as a transaction verification method of the node cooperation. The mechanism hides the user's private information within a group, and ensures their protection from the impersonation attack. BSeIn [70], on the other hand, replaces the vulnerable ECDSA signature with attribute-based signatures, i.e., only legitimate terminals can generate a valid signature, and hence any impersonation attempt will be detected when its corresponding authentication operation fails.
- *Sybil attack*: Under this attack, an adversary creates many fake identities. By performing many interactions in the network, the adversary can gain a large influence within the community, i.e, increasing/decreasing the reputation of some agents. TrustChain [71] replaces the proof-of-work with a mechanism to establish the validity and integrity of transactions. The blockchain architecture suffers from the following vulnerability: Transacting agents might decide to not append a transaction to their local chain. TrustChain addresses this issue by creating an immutable chain of temporally ordered interactions for each agent. After a transaction between two agents has finished, both parties sign the transaction and append a new block to their local chain. TrustChain computes the trustworthiness of agents in an online community with Sybil-resistance by using prior transactions as input. It ensures that agents who use resources from the community also contribute back.

B. Manipulation-based attacks

They involve an unauthorized access and tamper of data. In this category, four attacks are classified, namely: False data injection attack, Tampering attack, Overlay attack, and Modification attack

- *False data injection attack*: The aim of this attack is to tamper with meter measurements and compromise the data integrity of the control system, in order to make it take wrong control decisions. To resist against this attack, Liang et al. [21] leverage the security characteristics of blockchains. To this end, they consider the meter

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

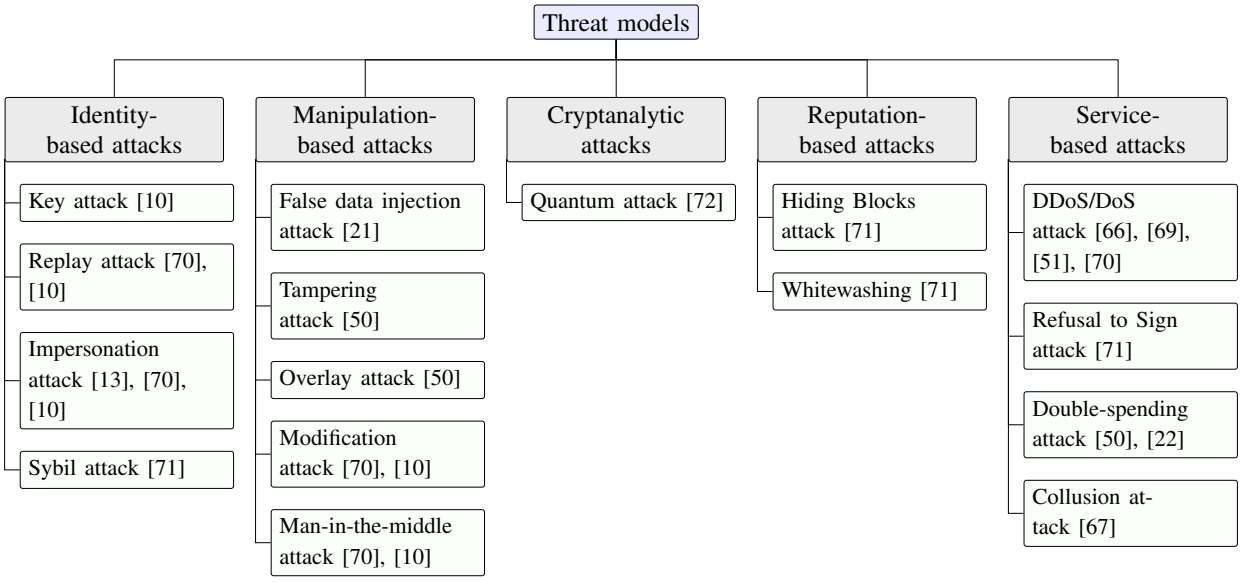

Fig. 6. Classification of threat models for Blockchain.

node as a private blockchain network. In addition, the interactions among the nodes are based on a consensus mechanism, which consists of executing a distributed voting algorithm. Each node can verify the integrity of the received data. The latter is considered correct when a positive agreement is reached.

- *Tampering attack*: In case adversary exploits the private key leakage or 51% vulnerability, he may tamper with the bitcoin transactions of the bitcoin addresses, amounts and other information after signing, . Also, it is possible to link the bitcoin accounts with identities through the human activities in daily transactions. To prevent this attack, Wang et al. [50] use a public-key cryptosystem that is compatible with the existing Bitcoin system. They propose adding the homomorphic Paillier encryption system to hide the plaintext amounts in transactions, and the encrypted amounts will be checked by the Commitment Proof.
- *Overlay attack*: By exploiting the blockchain vulnerabilities, an attacker adds a forgery encrypted amount to the original encrypted amount under the receiver's public key. In [50], this attack is detected as every transaction is embedded with a timestamp to mark its uniqueness. Different inputs under the same trader can be distinguished and linked to the different transactions, and hence resistance against the overlay attack is ensured.
- *Modification attack*: It consists in modifying the broadcast transaction or the response message. To deal with this attack, LNSC [10] uses the idea of temporary private keys for each session agreement, and elliptic curve encryption to calculate the hash functions. BSeIN [70], on the other hand, employs the attribute signature and the MAC.
- *Man-in-the-middle attack*: By exploiting some vulnerabilities like: private key leakage and 51% vulnerability, an attacker by spoofing the identities of two parties can secretly relay and even modify the communication between these parties, which believe they are communicating directly, but in fact the whole conversation is under the control of the attacker. To resist against this attack, BSeIn [70] provides secure mutual authentication. In [10], LNSC provides mutual authentication by using temporary private keys for each session agreement, and elliptic curve encryption to calculate the hash functions.

C. Cryptanalytic attacks

They aim to break the cryptographic algorithm and expose its keys. In [72] the quantum attack is investigated in blockchain. This attack is designed to solve the elliptic curve digital logarithm, i.e., derive the private key from the elliptic curve public key. In this way, an adversary can sign unauthorized transactions and forge the valid signature of users. To deal with this issue, Yin et al. [72] uses the idea of lattice-based signature scheme, which allows deriving many sub-private keys from the seed in the deterministic wallet of blockchain.

D. Reputation-based attacks

An agent manipulates his reputation by changing it to a positive one. In this category, we can find the following attacks, namely: Hiding Blocks attack, and Whitewashing attack.

- *Hiding Blocks attack*: Under this attack, an agent only exposes transactions that have a positive impact on his reputation and hides the ones with negative reputation. In [71], an immutable chain of temporally ordered interactions for each agent. Since each record has a sequence number, any agent in the network can request specific records of others. The requested agents cannot refuse to provide their records. Otherwise, other agents will stop interacting with them.
- *Whitewashing*: When an agent has negative reputation, it can get rid of its identity and make a new one. There is no

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

TABLE IV
SECURITY ANALYSIS TECHNIQUES USED BY BLOCKCHAIN-BASED AUTHENTICATION SCHEMES FOR THE IOT

Year	Scheme	Approach	Main results
2018	Lin et al. [79]	- Using the game between F and a challenger C to describe the unforgeability	- The proposed scheme is unforgeable against an adaptive chosen message forger in the standard model
2018	Lin et al. [70]	- Based on the deployed cryptographic schemes, namely, ABS, MRE, AES, and MAC	- The proposed scheme can satisfy the security requirements (e.g., Mutual authentication, user anonymity, fine-grained access control,...etc)
2018	Li et al. [14]	- Based on Lagrange Interpolation	- The proposed scheme achieves Sybil-resistance
2018	Lin et al. [80]	- Using the game between F and a challenger C to describe the unforgeability	- The ID-based linear homomorphic signature scheme secure against chosen-message and ID attack
2018	Yin et al. [72]	- According to the property of preimage sampleable trapdoor functions	- The proposed scheme is strongly unforgeable under chosen message attack except the probability $e(n)$

way to prevent this behavior. However, it is suggested in [71] to give lower priorities to the agents of new identities when applying the allocation policy.

E. Service-based attacks

They aim either to make the service unavailable or make it behave differently from its specifications. Under this category, we can find the following attacks:

- *DDoS/DoS attack*: It involves sending a large amount of requests to cause the failure of the network. As shown in Table III, there are four methods that are proposed to deal with this attack. The idea of distributed SDN architecture is proposed by DistBlockNet protocol in [66]. In SDN, an attacker might try to inject flow rules that will cause network misbehaviour such as: denying legitimate hosts [81]. To deal with this issue, DistBlockNet uses the blockchain system to update, validate, and download the flow rules table for the IoT forwarding devices. CoinParty [69] proposes a decentralized mixing service that allows users to reestablish their financial privacy in Bitcoin. A DoS attack against a mixing service consists in sending large amounts of request messages and discarding responses. To deal with this issue, CoinParty provides reactive protection by allowing mixing peers to retain funds of malicious users. Liu et al. [51] propose a mixing scheme to conceal the transfer of coins between addresses. To this end, they employ a ring-based signature with Elliptic Curve Digital Signature Algorithm (ECDSA). Protecting the mixing service against the DoS atatck is achieved by banning the misbehaving users. The resilience against DoS in BSeIn [70] is achieved, as in Bitcoin, by limiting the block size, checking the maximum number of attribute signatures for the transaction input, and using multi-receivers encryption to provide confidentiality for authorized participants.
- *Refusal to Sign attack*: A malicious agent can decide to not sign a transaction that is not in his favor. Although preventing this attack is not possible, punishment measures can be taken against the refusal agents. It is proposed in [71] to not interact with the malicious agent, or split the transactions in smaller amounts. If an agent refuses to sign a transaction, the interaction is aborted.
- *Double-spending attack*: It means that the attackers spend the same bitcoin twice to acquire extra amounts. In [50], the Time-Stamp and the Proof-of-Work mechanism is used. In [22], a multi-signature transaction is employed, where a minimum number of keys must sign a transaction before spending tokens.
- *Collusion Attack*: Nodes can collude with each other and behave selfishly to maximize their profit. In [67], an incentive mechanism and pricing strategy are proposed to thwart the selfish behaviors.

IV. EXISTING RESEARCH ON SECURITY AND PRIVACY IN BLOCKCHAIN-BASED IOT

Table V summarizes research for blockchain-based IoT security and privacy.

A. Authentication

In [79], Lin et al. proposed a novel transitively closed undirected graph authentication scheme that can support blockchain-based identity management systems. In comparison to other competing authentication schemes, their proposal provides an additional capability of dynamically adding or deleting nodes and edges. Moreover, this novel scheme that was built on Ethereum solves the authentication problem of non-existent edges, which is a known challenge in transitive signature schemes. Lin et al.in [70] proposed a novel blockchain-based framework that can ensure a secure remote user authentication. The proposed framework combines attribute-based signatures, multi-receivers encryption and Message Authentication Code. In [14], Li et al. proposed a novel privacy-preserving Blockchain-based announcement network for Vanets that is based on a threshold authentication protocol called Echo-Announcement.

Authors in [80] proposed an ID-based linearly homomorphic signature schemes that can be used for realizing authentication in blockchains. The system allows a signer to produce linearly homomorphic signatures, and hence it avoids the shortcomings of public-key certificates. In addition, it is shown to be robust against several attacks. In [82] authors introduced the concept of blockchain as a service.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

TABLE V
EXISTING RESEARCH FOR BLOCKCHAIN-BASED IOT SECURITY AND PRIVACY

Year	Scheme	Blockchain model	Security model	Goal	Performance (+) and limitation (-)	Comp. complexity
2016	Aitzhan and Svetinovic [22]	- Blockchain technology with multi signatures and anonymous encrypted message propagation streams	- Privacy preserving	- Enables peers to anonymously negotiate energy prices and securely perform trading transactions	+ Combat double-spending attacks - A formal proof is not provided on the Sybil-resistance	Medium
2017	Otte et al. [71]	- Every participant grows and maintains their own chain of transactions	- Distributed trust	- Providing strict bounds on the profitability of a Sybil attack	+ A formal proof is provided on the Sybil-resistance - Authentication is not considered	Up to $2n + 1$ max-flow computations
2017	Kanemura el al. [48]	- Blockchain technology with Deniability	- Privacy preserving	- Improving the privacy level of a simplified payment verification client	+ True positive Bitcoin addresses are hidden by the false positives in a Bloom filter - Authentication is not considered	Medium
2017	Wang et al. [50]	- Blockchain technology with the Paillier cryptosystem for encryption and decryption	- Preserving transaction privacy	- Achieving delicate anonymity and prevents active and passive attacks	+ Robust transaction + Prevent the following attacks: Tampering attack, Overlay attack, Double-spending attack - Sybil-resistance	$T_{\text{dec}} = 2T_m + 2iT_E$
2018	Yin et al. [72]	- Quantum attack in the blockchain	- Transaction authentication	- Resisting quantum attack, while maintaining the wallet lightweight	+ Strongly unforgeable under chosen message attack - The Sybil-resistance is not considered	The length of signature is $O(1)$
2018	Jong-Hyouk Lee [82]	- Consortium Blockchain	- Identity and authentication management	- Creating a new ID as a Service	+ It can be implemented as a cloud platform - The threat model is not defined	Medium
2018	Fan et al. [54]	- The blockchain is a public, tamper-resistant ledger	- Privacy preserving - Access control	- Achieve the goal of every data owner's complete control	+ Backward security + Forward security - The Sybil-resistance is not considered	$M + T_m$
2018	Wang et al. [16]	- Blockchain based incentive mechanism	- Privacy preserving	- Achieve k-anonymity privacy protection	+ Resist the impersonation attacks in the open and transparent blockchain - The collusion attacks is not analysed	Medium
2018	Lin et al. [80]	- ID-based linearly homomorphic signature	- Authentication	- Avoiding the shortcomings of the use of public key certificates	+ Secure against existential forgery on adaptively chosen message and ID attack in the random oracle model - Adaptation with the Blockchain is not analyzed	High
2018	Li et al. [14]	- Blockchain-based incentive mechanism	- Privacy preserving - Authentication	- Achieving privacy-preserving in forwarding announcements	+ Maintains the reliability of announcements + Achieve Sybil-resistance - Location privacy is not considered	Medium
2018	Ziegeldorf et al. [69]	- Blockchain technology with Deniability	- Anonymity - Deniability	- Achieving correctness, anonymity, and deniability	+ Resilience against DoS attacks from malicious attackers + Compatible with other crypto-currencies which use the same ECDSA primitive, e.g., Litecoin and Mastercoin - Double-spending attacks is not considered	Medium
2018	Yang et al. [83]	- The blocks maintain the proofs produced by the cloud server	- Accountable traceability	- Achieving public verification without any trusted third party	+ Achieve public verification + Efficient in communication as well as in computation - Tampering attack is not considered	The data owner conducts $(2 + \log_2 m)$ hash computations
2018	Hu et al. [84]	- The Ethereum blockchain	- Distributed trust	- Saving on the overall deployment and operational costs	+ Low-cost, accessible, reliable and secure payment scheme - Accountable traceability is not considered	Low bandwidth
2018	Liu et al. [51]	- The blockchain based on the ring signature with elliptic curve digital signature algorithm (ECDSA)	- Preserving transaction privacy	- Help Bitcoin users protect their account and transaction information	+ Resistant to DoS attacks + Prevent the mixing server from mapping input transactions + Anonymity and scalability - Double-spending attacks is not considered	High
2018	Lin et al. [70]	- The structure of blocks is similar to that in Bitcoin	- Authentication - Access control	- Enforce fine-grained access control polices	+ Resilience to hijacking attacks, user impersonation attacks, DDoS attacks, modification attacks, replay attacks, and man-in-the-middle attacks + Mutual authentication + Session key agreement + Perfect forward secrecy - The Sybil-resistance is not considered	Medium
2018	Lin et al. [79]	- The Ethereum blockchain	- Authentication	- Solving the existing intractability issue in transitive signature	+ Update the certificates without the need to re-sign the nodes + Provide a proof when the edge between two vertices does not exist - Access control is not considered compared to the scheme in [70]	Signature size: 2 points in Z_q^*

Notations :
M: The time for one exponentiation;
T_m: The size of the ciphertext;
T_{dec}: The time for decryption;
T_m: The unit of modular multiplication time;
T_E: The unit of modular exponentiation time

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

Their proposed blockchain based-ID as a Service (BIDaaS) mechanism, is a new type of IDaaS that can be used for identity and authentication management. Authentication can be achieved without the use of any preregistered information of the user. Finally in [72] authors cope with the problem of keeping the wallet in a relatively small size while ensuring the robustness of transaction authentication by introducing a novel anti-quantum transaction authentication scheme.

Tapas et al. [85] proposed an authorization and delegation model for the IoTCloud based on blockchain technology, which is implemented in the form of smart contracts over the Ethereum platform. This model can provide access control and authorization, but privacy is not considered. To provide an authorized access to IoT resources, Alphand et al. [86] proposed a blockchain security architecture, named IoTChain. Specifically, the IoTChain architecture uses a combination of the OSCAR architecture [87] and the ACE authorization framework [88] in order to enable efficient multicasting of IoT resources. In addition, the IoTChain architecture is based on four main phases, including, 1) the creation of a smart contract and his publication into the blockchain, 2) Sending a transaction to the contract address, 3) the client requests the encryption keys to decrypt the resources from the key server, and 4) the client can download the encrypted resources directly from the resource server.

Table IV presents the security analysis techniques used by blockchain-based authentication schemes for the IoT. Note that there are five formal security verification techniques used by authentication schemes for the IoT, namely, BAN-logic, analysis by process (Spi calculus), Game theory, Automated reasoning (ProVerif), and Automated Validation (AVISPA), as discussed in the work [89].

B. Privacy Preservation

In the core of blockchain philosophy lies the private key that can unlock the cryptographic protection of the digital assets. The private key becomes the highest vulnerability of a blockchain system whether it is stored on a piece of paper, screen, disk, in local memory or in the cloud. Users tend to use digital wallets that can be either software or hardware, e.g. Trezor or Keepkey, which are vulnerable to various attacks like fault injections [90].

Another solution that is gaining ground nowadays is the use of hardware security modules (HSMs), a crypto-processor that securely generates, protects and stores keys. The entire cryptographic key lifecycle happens inside the HSM. An HSM can be a standalone device that operates offline or can be embedded in a server, can be hardened against tampering or damage, and is usually located in a physically secure area to prevent unauthorized access. Finally a new generation of ultra-secure PCs that have embedded an HSM and requires two-factor authentication is recently introduced. This PC can be protected against physical attacks with a tamper-proof casing and mechanisms like automatic erasion of the private key in case of any breach of the embedded physical or logical security controls [91]. Using trusted computers both as secure digital wallets and blockchain nodes. Security assurance of users and organizations need in order to trust this new technology can be provided in the near future.

To achieve k-anonymity privacy protection, Wang et al. [16] use a node cooperation verification approach, in which each group contains K nodes to meet the objective of K-anonymity protection. Aitzhan et al. [22] proposed an idea that protects parties from passive eavesdropping by hiding non-content data. For enhancing the transaction privacy in Bitcoin, Wang et al. [50] achieve transaction by using cryptographic methods, i.e., employs the public-key system. Through the standard ring signature and ECDSA unforgeability, Liu et al. [51] proposed an idea that can achieve the anonymity.

One other aspect of privacy in blockchain systems is about anonymity. Although it is possible to design an almost immutable, tamper-resistant transaction, this transaction can be seen throughout all of the nodes on the blockchain network. One promising research on supporting private transactions inside a blockchain is zk-STARKs, which combines zCash and Ethereum. The combination of both technologies makes it possible to keep anonymity when conducting payments, blind auctions, and even voting [74].

To construct a personal data management platform focused on privacy, Zyskind et al. [92] proposed a system that combines blockchain and off-blockchain storage. Specifically, this system protects against the privacy issues, including, data ownership, data transparency and auditability, and fine-grained access control. Similarly to the work [92], Kosba et al. [93] presented a framework, named Hawk, for building privacy-preserving smart contracts. The Hawk framework contains two parts: 1) a private portion which takes in parties' input data as well as currency units, and 2) a public portion which does not touch private data or money. Based on the two aspects, namely, on-chain privacy and contractual security, the Hawk framework can realize the two following specifications: 1) private ledger and currency transfer, and 2) enabling transactional privacy and programmability simultaneously.

Chen et al. [94] proposed a new scheme in order to make some improvements to the InterPlanetary File System (IPFS) [95] based on four layers, including, blockchain layer, virtualchain layer, routing layer, and storage layer. To improve the block storage model, the Chen et al.'s scheme provides a zigzag-based storage model, but authentication and privacy are not considered. Hence, the authentication and privacy-preserving schemes for IPFS system are major challenges and should be investigated in the future. Therefore, the verification of contracts in blockchain networks nowadays challenges for the IoT networks. Recently, Watanabe et al. [96] proposed an idea for recording a trail of consensus onto the blockchain, which the transaction is used as evidence of contractor consent. This idea uses a chain of transactions and the last transaction data is returned to the first contractor, who generated the contract transaction at the beginning. In addition, this idea can confirm the consent of each contractor and protect the privacy of the contract.

C. Trust

A blockchain-based payment scheme that is set up in a remote region setting was introduced in [84]. The proposed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2882794, IEEE Internet of Things Journal

scheme is assumed to have an intermittent connectivity to a bank's central system. Distributed trust is accomplished with the use of a two-layer architecture, where the bank authorizes a set of selected villagers to act as miners who on their turn authorize transactions among villagers with tokens and the bank. In [71] authors present a mechanism where every participant grows and maintains his own chain of transactions. The proposed approach provides distributed trust, without the need of any gatekeeper, while being robust against Sybil attacks.

V. Open questions and research challenges

To complete our overview, we outline both open questions and research challenges that could improve the capabilities and effectiveness of blockchain for the IoT, summarized in the following recommendations:

A. Resiliency against Combined Attacks

As presented in this survey, many security solutions for bloackchain-based IoT have been proposed in the literature, each of which is designed to tackle different security issues and threat models. The attacks that are discussed in the survey are divided into two categories: application-dependent and application-free. The application-dependent attacks are specific for each application, and hence they are easily taken into consideration to secure the application. Besides, in case of application-free attacks, each protocol addressed a subset of attacks, and each application-free attack is tackled using a different security solution. The main question that might arise is how to design a security solution that can be resilient against combined application-free attacks while taking into account the implementation feasibility of the solution, especially in case of low resource-constrained IoT devices.

B. Dynamic and Adaptable Security Framework

Heterogeneous devices are deployed in the IoT network, ranging from low-power devices to high-end servers. Hence, a single security solution cannot be deployed for all the blockchain-based IoT architectures due to the different amount of resources that are provided. Therefore, the security solution should initially adapt itself to the existing resources, and decide which security services to offer, so as to meet the minimum security requirements of the end-users. Thus, one of the challenges that should receive more attention in the future is how to design such a dynamic and adaptable security framework for blockchain-based IoT architectures.

C. Energy-efficient Mining

Mining includes the execution of the blockchain consensus algorithms such as Proof-of-Work (PoW). Besides, the blockchain grows as the users store their transactions. Therefore, more powerful miners are required to handle the consensus protocols in the blockchain. Several energy efficient consensus algorithms such as Proof-of-Space [97], Deligated Proof-of-Space [98] and Proof-of-Stake [99] and mini-blockchain [100], [101] to store only recent blockchain transactions are suggested. However, resource- and power-constrained IoT devices are not always capable of meeting the substantial computational and power consumption in the processing of blockchain consensus and storing of blockchains. Therefore, the design of energy-efficient consensus protocols is one of the significant research challenges in the blockchain technologies for IoT.

D. Social Networks and Trust Management

When we talk about security we have to take in mind that fake news can be a part of a cyber attack. Large-scale rumor spreading could pose severe social and economic damages to an organization or a nation [102] especially with the use of online social networks. Blockchains could be a means for limiting rumor spreading as presented in [103] where a blockchain-enabled social network is presented.

E. Blockchain-specific Infrastructure

The storage-limited IoT devices might not be able to store the large-size blockchain that grows as the blocks are appended in the blockchain. Moreover, it is commonly seen that the IoT devices store the blockchain's data that are not even useful for their own transactions. Therefore, blockchain-specific equipment that supports the decentralized storage of large-size blockchain become a challenging issue. Moreover, the address management and underlying communication protocols play significant roles in blockchain infrastructure. Besides, trustworthiness among the computational resource-enriched devices have to be established in the blockchain infrastructure. Besides, the Application Programming Interface (APIs) should be user-friendly as much as possible.

F. Vehicular Cloud Advertisement Dissemination

As presented in this survey, based on a decentralized blockchain structure, various anonymity schemes are proposed to hide the real identities in IoV. Therefore, since the vehicle's real identity, vehicle's real location, and transaction could possibly be disclosed in vehicular cloud advertisement dissemination [104], critical security issues arise as follows:

- How to design a single-attribute access control protocol based on blockchain technology for preserving transaction privacy in vehicular cloud advertisement dissemination?
- How to devise a privacy-preserving secret sharing scheme based on blockchain technology to acknowledge participation of selected vehicles in transactions? e.g., by using the homomorphic Paillier encryption system.
- How to design a low complexity-based authentication using the blockchain technology between RSUs and participating vehicles during the advertisement dissemination process?

G. Skyline Query Processing

Skyline query has become an important issue in database research, e.g., centralized database, distributed database, and

similarity search. The surveyed schemes have not yet studied the possibility of using the skyline query with blockchain. Recently, Hua et al. [105] proposed a privacy-preserving online medical primary diagnosis framework, named CINEMA, which uses the skyline query. Specifically, CINEMA framework can protect users' medical data privacy and ensure the confidentiality of diagnosis model based on a skyline diagnosis model. Therefore, how to handle the security and privacy issues when a skyline diagnosis model is constructed by a lot of blockchains? Hence, the privacy-preserving schemes based on the blockchain with skyline query are major challenges and should be investigated in the future.

VI. Conclusion

In this paper, we surveyed the state-of-the-art of existing blockchain protocols designed for Internet of Things (IoT) networks. We provided an overview of the application domains of blockchain technologies in IoT, e.g., Internet of Vehicles, Internet of Energy, Internet of Cloud, and Edge computing. Through extensive research and analysis that was conducted, we were able to classify the threat models that are considered by the blockchain protocols in IoT networks, into five main categories, namely, identity-based attacks, manipulation-based attacks, cryptanalytic attacks, reputation-based attacks, and service-based attacks. There still exist several challenging research areas, such as resiliency against combined attacks, dynamic and adaptable security framework, energy-efficient mining, social networks and trust management, blockchain-specific infrastructure, vehicular cloud advertisement dissemination, and Skyline query processing, which should be further investigated in the near future.

References

[1] "IDC, Worldwide Internet of Things Forecast, 2015–2020," IDC #256397.

[2] "IDC, Worldwide Internet of Things Forecast Update 2015–2019," Feb. 2016, Doc #US40983216.

[3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, Sept. 2012.

[4] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Mag.*, vol. 7, no. 4, pp. 6–14, July 2018.

[5] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19 293–19 304, 2017.

[6] M. Swan, *Blockchain: blueprint for a new economy*, 1st ed. ÓReilly Media, Jan. 2015.

[7] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys & Tut.*, vol. 18, no. 3, pp. 2084–2123, Mar. 2016.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[9] D. Wilson and G. Ateniese, "From pretty good to great: Enhancing PGP using bitcoin and the blockchain," in *Network and System Security*. Springer International Publishing, 2015, pp. 368–375.

[10] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13 565–13 574, 2018.

[11] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, dec 2017.

[12] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, dec 2017.

[13] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," *IEEE Trans. Ind. Informatics*, vol. 13, no. 6, pp. 3154–3164, dec 2017.

[14] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–17, 2018.

[15] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun.* IEEE, oct 2017, pp. 1–5.

[16] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications," *IEEE Access*, vol. 6, pp. 17 545–17 556, 2018.

[17] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. IEEE 13th Int. Conf. on Service Systems and Service Management (ICSSSM)*, June 2016.

[18] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Trans. Ind. Informatics*, pp. 1–1, 2017.

[19] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *Proc. IEEE Technology & Engineering Management Conference (TEMSCON)*, June 2017.

[20] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[21] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks," *IEEE Trans. Smart Grid*, pp. 1–1, 2018.

[22] N. Zhumabekuly Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams," *IEEE Trans. Dependable Secur. Comput.*, pp. 1–1, 2016.

[23] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, Nov. 2017.

[24] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, pp. 1–23, May 2018.

[25] "Crypto-currency market capitalizations," accessed on 15 June, 2018. [Online]. Available: https://coinmarketcap.comhttps://coinmarketcap.com

[26] "Blockchain technology report to the US federal advisory committee on insurance," accessed on 15 June, 2018. [Online]. Available: https://www.treasury.gov/initiatives/fio/Documents/McKinsey_FACI_Blockchain_in_Insurance.pdf

[27] L. Bahack, "Theoretical Bitcoin attacks with less than half of the computational power," Dec. 2013, arXiv:1312.7013v1. [Online]. Available: https://arxiv.org/pdf/1312.7013.pdf

[28] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *Proc. Annual Technical Conference (USENIX ATC)*, June 2016, pp. 181–194.

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

[30] A. Kaushik, A. Choudhary, C. Ektare, D. Thomas, and S. Akram, "Blockchain-literature survey," in *Proc. IEEE 2nd Int. Conf. Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, May 2017.

[31] M. C. K. Khalilov and A. Levi, "A survey on anonymity and privacy in Bitcoin-like digital cash systems," *IEEE Commun. Surveys & Tut.*, pp. 1–1, Mar. 2018.

[32] M. Conti, S. K. E, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Commun. Surveys & Tut.*, pp. 1–39, May 2018.

[33] S. Goswami, "Scalability analysis of blockchains through blockchain simulation," Master's thesis, University of Nevada, USA, 2017.

[34] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.

[35] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," *IEEE Access*, vol. 6, pp. 11 676–11 686, 2018.

[36] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun.* IEEE, oct 2017, pp. 1–5.

[37] G. Maxwll, "Coinswap," 2013. [Online]. Available: https://bitcointalk.org/index.php?topic=321228

[38] G. Maxwell, "Coinjoin: Bitcoin privacy for the real world," in *Post on Bitcoin forum*, 2013.

[39] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," in *2013 IEEE Symp. Secur. Priv.* IEEE, may 2013, pp. 397–411.

[40] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for Bitcoin with Accountable Mixes," in *Int. Conf. Financ. Cryptogr. Data Secur.* Springer Berlin Heidelberg, 2014, pp. 486–504.

[41] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-Resistant Mixing for Bitcoin," in *Proc. 13th Work. Priv. Electron. Soc. - WPES '14*. New York, New York, USA: ACM Press, 2014, pp. 149–158.

[42] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin," in *Eur. Symp. Res. Comput. Secur.* Springer, 2014, pp. 345–364.

[43] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in *2014 IEEE Symp. Secur. Priv.* IEEE, may 2014, pp. 459–474.

[44] L. Valenta and B. Rowan, "Blindcoin: Blinded, Accountable Mixes for Bitcoin," in *Int. Conf. Financ. Cryptogr. Data Secur.* Springer Berlin Heidelberg, 2015, pp. 112–126.

[45] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "Coinparty: Secure multi-party mixing of bitcoins," in *Proc. 5th ACM Conf. Data Appl. Secur. Priv. - CODASPY '15*. New York, New York, USA: ACM Press, 2015, pp. 75–86.

[46] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions," in *Int. Conf. Financ. Cryptogr. Data Secur.* Springer Berlin Heidelberg, 2016, pp. 43–60.

[47] E. Heilman, L. AlShenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub," in *Proc. 2017 Netw. Distrib. Syst. Secur. Symp.* Reston, VA: Internet Society, 2017.

[48] K. Kanemura, K. Toyoda, and T. Ohtsuki, "Design of privacy-preserving mobile Bitcoin client based on γ-deniability enabled bloom filter," in *2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun.* IEEE, oct 2017, pp. 1–6.

[49] H. Wang, D. He, and Y. Ji, "Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography," *Futur. Gener. Comput. Syst.*, jul 2017.

[50] Q. Wang, B. Qin, J. Hu, and F. Xiao, "Preserving transaction privacy in bitcoin," *Futur. Gener. Comput. Syst.*, sep 2017.

[51] Y. Liu, X. Liu, C. Tang, J. Wang, and L. Zhang, "Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin," *IEEE Access*, vol. 6, pp. 23 261–23 270, 2018.

[52] H. Huang, X. Chen, Q. Wu, X. Huang, and J. Shen, "Bitcoin-based fair payments for outsourcing computations of fog devices," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 850–858, jan 2018.

[53] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, jan 2018.

[54] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Commun.*, vol. 12, no. 5, pp. 527–532, Mar. 2018.

[55] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium Blockchain-Based Malware Detection in Mobile Devices," *IEEE Access*, vol. 6, pp. 12 118–12 128, 2018.

[56] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, mar 2017.

[57] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[58] N. Herbaut and N. Negru, "A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 70–76, 2017.

[59] C. Xu, K. Wang, and M. Guo, "Intelligent Resource Management in Blockchain-Based Cloud Datacenters," *IEEE Cloud Comput.*, vol. 4, no. 6, pp. 50–59, nov 2017.

[60] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018.

[61] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," *IEEE Access*, vol. 5, pp. 14 757–14 767, 2017.

[62] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivanko, and M. Muhlhauser, "Towards blockchain-based collaborative intrusion detection systems," in *Proc. Int. Conf. Critical Inf. Infrastruct. Secur*, 2017, pp. 1–12.

[63] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," *IEEE Access*, vol. 6, pp. 10 179–10 188, 2018.

[64] T. Cruz, L. Rosa, J. Proença, L. Maglaras, M. Aubigny, L. Lev, J. Jiang, and P. Simões, "A cybersecurity detection framework for supervisory control and data acquisition systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2236–2246, 2016.

[65] K. Kalkan and S. Zeadally, "Securing internet of things (iot) with software defined networking (sdn)," *IEEE Commun. Mag.*, 2017.

[66] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, 2017.

[67] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A Blockchain based Truthful Incentive Mechanism for Distributed P2P Applications," *IEEE Access*, pp. 1–1, 2018.

[68] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, "Searchain: Blockchain-based private keyword search in decentralized storage," *Futur. Gener. Comput. Syst.*, sep 2017.

[69] J. H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, and K. Wehrle, "Secure and anonymous decentralized Bitcoin mixing," *Futur. Gener. Comput. Syst.*, vol. 80, pp. 448–466, mar 2018.

[70] 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, 2018.

[71] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain," *Futur. Gener. Comput. Syst.*, sep 2017.

[72] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An Anti-Quantum Transaction Authentication Approach in Blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.

[73] M. C. K. Khalilov and A. Levi, "A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems," *IEEE Commun. Surv. Tutorials*, pp. 1–1, 2018.

[74] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, "Cecoin: A decentralized PKI mitigating MitM attacks," *Futur. Gener. Comput. Syst.*, oct 2017.

[75] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[76] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[77] H. Mayer, "Ecdsa security in bitcoin and ethereum: a research survey, 2016," *URL http://blog. coinfabrik. com/wp-content/uploads/2016/06/ECDSA-Security-in-Bitcoin-a nd-Ethereum-a-Research-Survey. pdf*.

[78] A. Miller, M. Möser, K. Lee, and A. Narayanan, "An empirical analysis of linkability in the monero blockchain," *arXiv preprint*, vol. 1704, 2017.

[79] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, "A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-based Identity Management Systems," *IEEE Access*, pp. 1–1, 2018.

[80] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, pp. 1–1, 2018.

[81] I. Alsmadi and D. Xu, "Security of software defined networks: A survey," *computers & security*, vol. 53, pp. 79–108, 2015.

[82] J.-H. Lee, "BIDaaS: Blockchain Based ID As a Service," *IEEE Access*, vol. 6, pp. 2274–2278, 2018.

[83] C. Yang, X. Chen, and Y. Xiang, "Blockchain-based publicly verifiable data deletion scheme for cloud storage," *J. Netw. Comput. Appl.*, vol. 103, pp. 185–193, feb 2018.

[84] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, A. Seneviratne, and M. E. Ylianttila, "A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain," jan 2018. [Online]. Available: http://arxiv.org/abs/1801.10295

[85] N. Tapas, G. Merlino, and F. Longo, "Blockchain-based iot-cloud authorization and delegation," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE, 2018, pp. 411–416.

[86] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "Iotchain: A blockchain security architecture for the internet of things," in *Wireless Communications and Networking Conference (WCNC), 2018 IEEE*. IEEE, 2018, pp. 1–6.

[87] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "Oscar: Object security architecture for the internet of things," *Ad Hoc Networks*, vol. 32, pp. 3–16, 2015.

[88] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, "Authentication and authorization for constrained environments (ace)," *Internet Engineering Task Force, Internet-Draft draft-ietf-aceoauth-authz-07*, 2017.

[89] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for internet of things: a comprehensive survey," *Security and Communication Networks*, vol. 2017, 2017.

[90] O. Boireau, "Securing the blockchain against hackers," *Network Security*, vol. 2018, no. 1, pp. 8–11, 2018.

[91] "This ultra-secure pc self destructs if someone messes with it," https://www.wired.com/2017/06/orwl-secure-desktop-computer/, accessed: 2018-06-01.

[92] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 2015, pp. 180–184.

[93] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.

[94] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved p2p file system scheme based on ipfs and blockchain," in *Big Data (Big Data), 2017 IEEE International Conference on*. IEEE, 2017, pp. 2652–2657.

[95] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

[96] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, "Blockchain contract: A complete consensus using blockchain," in *Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on*. IEEE, 2015, pp. 577–578.

[97] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Proc. 35th Annual Cryptology Conference on Advances in Cryptology*, Aug. 2015, pp. 585–605.

[98] "DPOS description on bitshares," accessed on 15 June, 2018. [Online]. Available: http://docs.bitshares.org/bitshares/dpos.html

[99] "Telehash," accessed on 15 June, 2018. [Online]. Available: http://telehash.org

[100] B. F. França, "Homomorphic mini-blockchain scheme," pp. 1–17, Apr. 2015, accessed on 15 June, 2018. [Online]. Available: http://cryptonite.info/files/HMBC.pdf

[101] J. D. Bruce, "The mini-blockchain scheme," 2014, accessed on 15 June, 2018. [Online]. Available: http://www.cryptonite.info/files/mbc-scheme-rev2.pdf

[102] N. Ayres and L. A. Maglaras, "Cyberterrorism targeting the general public through social media," *Security and Communication Networks*, vol. 9, no. 15, pp. 2864–2875, 2016.

[103] Y. Chen, Q. Li, and H. Wang, "Towards trusted social networks with blockchain technology," *arXiv preprint arXiv:1801.02796*, 2018.

[104] Q. Kong, R. Lu, H. Zhu, and M. Ma, "Achieving secure and privacy-preserving incentive in vehicular cloud advertisement dissemination," *IEEE Access*, vol. 6, pp. 25 040–25 050, 2018.

[105] J. Hua, H. Zhu, F. Wang, X. Liu, R. Lu, H. Li, and Y. Zhang, "Cinema: Efficient and privacy-preserving online medical primary diagnosis with skyline query," *IEEE Internet of Things Journal*, pp. 1–1, 2018.

Mohamed Amine Ferrag received the bachelor's, master's, and Ph.D. degrees from Badji Mokhtar - Annaba University, Algeria, in 2008, 2010, and 2014, respectively, all in computer science. Since 2014, he has been an Assistant Professor with the Department of Computer Science, Guelma University, Algeria. His research interests include wireless network security, network coding security, and applied cryptography. He serves on the Editorial Board of several International peer-reviewed journals such as the IET Networks (IET), the International Journal of Information Security and Privacy (IGI Global), the International Journal of Internet Technology and Secured Transactions (Inderscience Publishers), and the EAI Endorsed Transactions on Security and Safety (EAI). He has served as an Organizing Committee Member (the Track Chair, the Co-Chair, the Publicity Chair, the Proceedings Editor, and the Web Chair) in numerous international conferences.

Makhlouf Derdour received his Engineering degree in computer sciences from University of Constantine, Algeria, in 2004, his Magister degree in computer sciences from University of Tebessa, and his Ph.D. degree in computer networks from the University of Pau and Pays de l'Adour (UPPA), France, in 2012. He is currently an assistant professor at Computer Science department of the University of Tebessa, Algeria. His research interests include software architecture, multimedia applications, adaptation and self-adaptation of applications, design and modeling of systems, systems security. He is a general chair of the International Conference on Pattern Recognition and Intelligent Systems (PAIS).

Mithun Mukherjee (S'10, M'16) received his B.E. degree in electronics and communication engineering from the University Institute of Technology, Burdwan University, India, in 2007, his M.E. degree in information and communication engineering from the Indian Institute of Science and Technology, Shibpur, in 2009, and his Ph.D. degree in electrical engineering from the Indian Institute of Technology Patna, in 2015. Currently, he is a specially assigned researcher in the Guangdong Provincial Key Lab of Petrochemical Equipment Fault Diagnosis, Guangdong University of Petrochemical Technology, China. He was a recipient of the 2016 EAI WICON, the 2017 IEEE SigTelCom Best Paper Award, and the 2018 IEEE SYSTEMS JOURNAL Best Paper Award. He is an Associate Editor of the IEEE ACCESS and Guest Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, ACM/Springer Mobile Networks & Applications, and Sensors. His research interests include wireless communications, energy harvesting, and fog computing.

Abdelouahid Derhab received the Engineer, Master, and PhD degrees in computer science from University of Sciences and Technology Houari Boummediene (USTHB), Algiers, in 2001, 2003, and 2007 respectively. He was a full-time researcher at CERIST research center in Algeria from 2002 to 2012. He is currently an assistant professor at the Center of Excellence in Information Assurance (COEIA), King Saud University. His interest research areas are: network security, intrusion detection systems, malware analysis, mobile security, and mobile networks.

Leandros Maglaras (SM'15) received the B.Sc. degree from Aristotle University of Thessaloniki, Greece in 1998, M.Sc. in Industrial Production and Management from University of Thessaly in 2004 and M.Sc. and PhD degrees in Electrical & Computer Engineering from University of Volos, in 2008 and 2014 respectively. He is the head of the National Cyber Security Authority of Greece and a visiting Lecturer in the School of Computer Science and Informatics at the De Montfort University, U.K. He serves on the Editorial Board of several International peer-reviewed journals such as IEEE Access, Wiley Journal on Security & Communication Networks, EAI Transactions on e-Learning and EAI Transactions on Industrial Networks and Intelligent Systems. He is an author of more than 80 papers in scientific magazines and conferences and is a senior member of IEEE. His research interests include wireless sensor networks and vehicular ad hoc networks.

Helge Janicke is the Director of De Montfort University's Cyber Technology Institute. He is the Head of School of Computer Science and Informatics. Prof. Janicke was awarded his PhD in Computer Science in 2007 and worked on Cyber Security with organisations such as Airbus Group, QinetiQ, Ministry of Defence and General Dynamics UK amongst others. His interests are covering formal verification techniques and their application to Cyber Security, SCADA and Industrial Control System Security as well as aspects of Cyber Warfare. He established DMU's Airbus Group Centre of Excellence in SCADA Cyber Security and Forensics Research in 2013. He is a general chair of the International Symposium on SCADA and Industrial Control Systems Cyber Security Research (ICS-CSR).