Applications of Blockchains in the Internet of Things: A Comprehensive Survey

Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani, *Senior Member, IEEE*

***Abstract*—The blockchain technology has revolutionized the digital currency space with the pioneering cryptocurrency platform named Bitcoin. From an abstract perspective, a blockchain is a distributed ledger capable of maintaining an immutable log of transactions happening in a network. In recent years, this technology has attracted significant scientific interest in research areas beyond the financial sector, one of them being the Internet of Things (IoT). In this context, the blockchain is seen as the missing link toward building a truly decentralized, trustless, and secure environment for the IoT and, in this survey, we aim to shape a coherent and comprehensive picture of the current state-of-the-art efforts in this direction. We start with fundamental working principles of blockchains and how blockchain-based systems achieve the characteristics of decentralization, security, and auditability. From there, we build our narrative on the challenges posed by the current centralized IoT models, followed by recent advances made both in industry and research to solve these challenges and effectively use blockchains to provide a decentralized, secure medium for the IoT.**

***Index Terms*—Blockchain, IoT, digital technology, trustless, cybersecurity, auditability, privacy, decentralization, consensus.**

I. Introduction

THE TERM "Internet of Things" (IoT) was first used in 1999 by Ashton [1]. In 2015, i.e., about 20 years after the term was coined, the IEEE IoT Initiative released a document whose main goal was to establish a baseline definition of the IoT, in the context of applications ranging from small, localized systems constrained to a specific location, to large global systems composed of complex sub-systems that are geographically distributed [2]. In this document, we can find an overview of the IoT's architectural requirements, its enabling technologies, as well as a succinct definition of the IoT as an *"application domain that integrates different technological and social fields"*. At the core of it, the IoT consists of networked objects that sense and gather data from their surroundings, which is then used to perform automated functions to aid human users. The IoT is still steadily growing worldwide, thanks to expanding Internet and wireless access, the introduction of wearable devices, the falling prices of embedded computers, the progress of storage technology and cloud computing [3]. Today, the IoT attracts a multitude of research and industrial interests. With each passing day, smaller and smarter devices are being implemented in multiple IoT domains, including housing, precision agriculture, infrastructure monitoring, personal healthcare, and autonomous vehicles just to name a few.

However, data gathered by IoT devices may contain confidential and private information, and many security threats have emerged that aim to exploit the weaknesses of current IoT infrastructures [4]. Indeed, most state-of-the-art IoT infrastructures are heavily centralized with single points of failure, which hinder scalability and wide adoption of the IoT, while raising severe privacy and security concerns. Other than that, completely centralized network infrastructure leads to higher latency for end-to-end communications, which can hinder application verticals such as smart grids and smart cities. The IoT edge is steadily being empowered in order to alleviate issues with latency inherent to a centralized IoT [5]. To improve privacy and security within the edge-centric fog and mist architectures, as well as centralized network architectures, a more decentralized approach is seen as the solution to allow the long-term growth of the IoT, and to prevent single points of failure.

Existing centralized methods for providing privacy, security and data handling necessitate high-end servers which are under the control of third-party entities. Users are required to trust such entities for handling their IoT data, which can misuse it or in worst case scenarios, share it with mass-surveillance programs. Centralized network architecture for the IoT is faced with the following challenges:

- The entire network infrastructure risks being paralyzed in the event of a failure in the centralized servers [6]. A successful denial of service (DOS) attack on the centralized servers could result in a single point of failure.
- Data stored in centralized servers can be analyzed to reveal specific personal information pertinent to health, purchasing preferences and behaviours. Users have limited control over how their data is used and by whom.
- Data stored in centralized cloud lacks guaranteed accountability and traceability. Centralized IoT infrastructure mandates trusting a third party for data handling, and data stored on centralized servers has the risk of being deleted or tampered with.

Manuscript received April 3, 2018; revised September 17, 2018 and October 31, 2018; accepted December 8, 2018. Date of publication December 18, 2018; date of current version May 31, 2019. *(Corresponding author: Massimo Vecchio.)*

M. S. Ali, M. Vecchio, M. Pincheira, and F. Antonelli are with the OpenIoT Research Unit, FBK CREATE-NET, 38100 Trento, Italy (e-mail: mvecchio@fbk.eu).

K. Dolui is with imec-DistriNet, KU Leuven, 3001 Leuven, Belgium.

M. H. Rehmani is with the Department of Computing and Mathematics, Waterford Institute of Technology, X91 P20H Waterford, Ireland.

Digital Object Identifier 10.1109/COMST.2018.2886932

- With the exponential growth of the IoT, centralized servers will not be efficient enough in handling the sheer amount of end-to-end communications that facilitate IoT automation functions. Therefore, a centralized approach can hamper the growth of the IoT.

These challenges necessitate fundamentally rethinking how the Internet of Things is structured. Currently, "blockchain" represents one of the most suitable candidate technologies able to support a secure and distributed ecosystem for the IoT [7]. When compared to the IoT, the blockchain technology has a shorter, though occasionally mysterious history. The term first appeared in an article by S. Haber and W.S. Stornetta of 1991, as the abstract description of *"a cryptographically secured chain of blocks" [8]*. However, the universally recognized father of the blockchain technology is S. Nakamoto, an anonymous person (or group of persons) that formally theorized [9][1] and implemented it (in 2008 and 2009, respectively) as a core component of the cryptocurrency Bitcoin, where it still serves as the public ledger for all transactions on the network [10]. Since then, blockchain technology has gone mainstream with uses in an array of industries, e.g., finance, insurance, logistics, and agriculture. With its ability to digitize transactions smoothly and efficiently, this technology is promising a major paradigm shift in making several processes leaner, faster, and more transparent. From a high-level perspective, blockchains employ a heavy use of cryptography to provide *"trustless"* networks without centralized authorities, so data transacting nodes can reach faster reconciliation. Since the inherent features of blockchains lay down the foundations of serverless record-keeping, several researchers are making efforts to leverage blockchains to decentralize IoT communications and to eliminate the need for centralized trusted authorities. The idea of a blockchain-based IoT has garnered substantial research interest, since decentralizing the IoT through blockchains has the following potential benefits:

- The shift from centralized to blockchain-based IoT enhances fault tolerance and removes singular points of failures. It also prevents the bottleneck that was inherent in a growing IoT reliant on centralized servers [11]. A decentralized fabric for handling IoT data also prevents third-party entities to control the personal data of IoT users.
- A decentralized peer-to-peer network architecture enables IoT device autonomy, and end-to-end communications do not have to go through a centralized server for performing automation services. Participants in blockchain networks can verify the integrity of the data they are sent, as well as the identity of the sending participant. The secure, tamper-proof storage in blockchains also enable deploying secure software updates to IoT devices.
- Since no single entity controls the contents of a blockchain, IoT data and event logs stored on the blockchain are immutable, therefore there is guaranteed accountability and traceability. Reliability and trustless IoT interactions are a major contribution of blockchains to the IoT.
- Blockchains offer the functionality of programmable logic through smart contracts [12], and can treat IoT interactions as transactions. They can help perform security functions like access control, confidentiality, and authentication to enhance the security in a blockchain-based IoT.
- Blockchains open up opportunities for an IoT ecosystem where services can be monetized in a truly democratic fashion. The trustless network environment of blockchains allow secure micro-transactions for IoT services and data.

[1]Notice that in [9], the words "block" and "chain" were used separately, but were eventually popularized as a single word, *"blockchain"*, by 2015.

A. Contributions of This Survey Article and Comparison With Related Survey Articles

In recent research, many proposed solutions have appeared that integrate blockchains with the IoT in different application scenarios. Survey articles have attempted to review these proposed solutions in varied degrees of depth and scopes. Conoscenti *et al.* [13] present a generalized survey of the different applications of the blockchain, whereas we provide a comprehensive survey of the applications of blockchains specifically in the IoT. Atzori *et al.* [14] and Christidis and Devetsikiotis [15] examined the pros and cons of integrating blockchains with the IoT. Many more solutions have been proposed in the years since then, and we present an updated view of the lessons learned from them. These lessons include solutions for different areas of the IoT ecosystem, and recently identified challenges for decentralizing the IoT.

Reyna *et al.* [16] discussed the research challenges and opportunities, as well as different architectures for a blockchain-based IoT. In addition to these, we present a comprehensive review of the recent research efforts in different areas of the IoT where blockchains can prove to have a substantial impact. Yeow *et al.* [18] specifically discuss solutions for an edge-centric blockchain-based IoT and the challenges involved, however we present a review of the recent research in a holistic decentralization of the IoT via blockchains.

The areas of blockchain-based IoT privacy and security are reviewed in [17]. The survey by Panarello *et al.* [19] presents recent research efforts by sorting them in different application areas (smart cities, smart grids, etc.). In comparison to these, we present a thorough and updated survey of areas we classify as blockchain-based privacy, trust, security, identity management, data management, and monetization in the IoT. This survey also discusses the various integration architectures for blockchains in the IoT.

Most recently, Neudecker and Hartenstein [20] provided a survey of the networking principles involved in publicly deployed blockchains, including potential attacks and design trade-offs. They also highlight the lack of formal models for analyzing the design trade-offs in implementing public blockchains. In comparison, this article does not present an in-depth survey of the network layer techniques involved in public blockchains, however, this survey article reviews contributions that propose integrating blockchains to the IoT to reap the benefits of decentralization.

TABLE I
COMPARISON OF RECENT SURVEY ARTICLES

Blockchain-Based IoT Survey Contributions	Recent Survey Articles	Addressed in this Survey
Blockchain taxonomy and decentralized consensus	[16], [17], [13], [18], [19], [15], [20]	✓
Blockchain-based IoT architectures	[16]	✓
Blockchains for IoT privacy and trust	[17]	✓
Blockchain-based security for the IoT	[17], [13], [19]	✓
Blockchains for IoT ID and data management		✓
Blockchains for monetization in the IoT	[19]	✓
Challenges and research directions for blockchains in the IoT	[16], [17], [19], [18], [14]	✓

The contribution of this work is a comprehensive discussion on the recent advances in the IoT, blockchain technology and decentralizing the IoT through blockchains. Contributions of this survey include highlighting the roles of the entities involved in the IoT infrastructure when integrated with blockchains. Tradeoffs in selecting appropriate blockchain consensus algorithms for different application scenarios are also discussed. This survey discusses recent research efforts made towards solving key challenges in various areas of research in the IoT, as well as open research directions for future work. A summary of the contributions of this survey is enlisted as follows:

- A discussion on blockchain working principles.
- A discussion on blockchain consensus algorithms and the associated design trade-offs for the IoT.
- Motivations for integrating blockchains and IoT, and blockchain-IoT integration schemes.
- Review of the recently proposed blockchain-based solutions in the ares of:
  - Privacy in the IoT
  - Trustless Architectures for the IoT
  - Security in the IoT
  - Identity Management for the IoT
  - Data Management for the IoT
  - Monetization in the IoT
- A review of alternative IoT decentralization approaches.
- A discussion of the research challenges in decentralizing the IoT through blockchains.

This layout is aimed to enable readers to focus on any specific challenging area of their choice. Ultimately, the goal of this survey is to acquaint readers with the working principles of the blockchain, to allow readers to make educated decisions for integrating blockchains in their IoT projects, and to understand the key open research challenges highlighted in the survey. Table I highlights similarities and differences of the research areas covered in comparison to previous survey articles.

B. Organization of the Survey

The organization of the survey is as follows: Section II outlines the core features and working principles of blockchains, to help us better understand their applications in the IoT. Section III discusses blockchain-consensus algorithms and their place in the IoT. Section IV is a discussion on the current challenges in the IoT and the rationale for decentralizing the IoT using blockchains; followed by a discussion on the various blockchain-IoT integration schemes. Following up from that, Sections V–X discuss recent research efforts towards leveraging blockchains in the IoT for providing privacy, trust, security, identity management, data management, and data monetization respectively. Section XI is an overview of alternate approaches to decentralizing the IoT. Section XII carries the narrative into the issues and open research challenges in this area. Section XIII summarizes the lessons learned from the reviewed literature, and finally, Section XIV concludes the survey.

For readability and better insight into each of the areas discussed in Sections V–X, we begin each section by discussing the associated centralized implementations along with their pertinent challenges, followed by recent decentralization efforts using blockchains.

II. BLOCKCHAIN: FEATURES AND WORKING PRINCIPLES

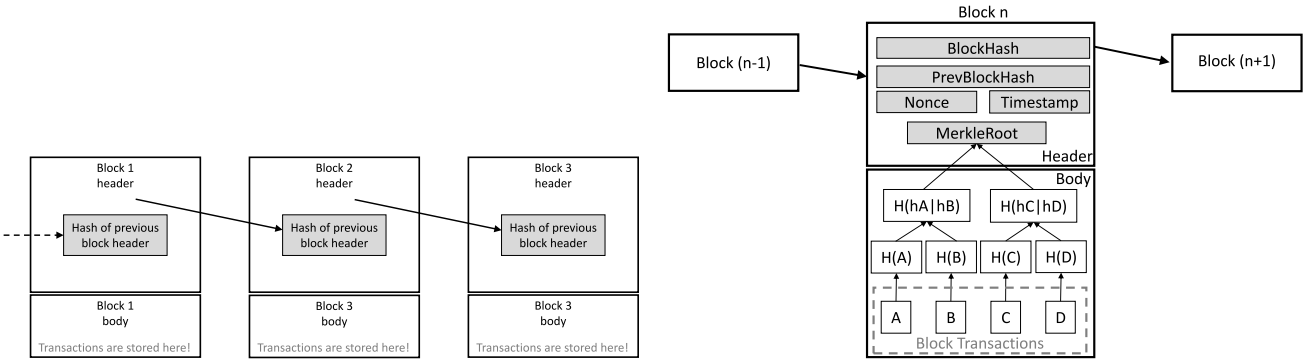
Blockchain-based systems are an amalgamation of cryptography, public key infrastructure, and economic modeling, applied to peer-to-peer networking and decentralized consensus to achieve distributed database synchronization [21], [22]. Essentially, the blockchain is a distributed data structure, and is dubbed a *"distributed ledger"* in its utility of recording transactions occurring within a network [10]. With cryptocurrencies being one application of the record-keeping feature of blockchains, the distributed ledger has the potential to be applied in networks where any form of data exchange takes place. In a peer-to-peer blockchain-based network, all participating peers maintain identical copies of the ledger. New entries, containing information pertaining to transactions, are added to the blockchain by means of decentralized consensus among the peers.

In order to understand the potential applications of blockchains in the Internet of Things, it is important to gain an understanding of the working principles of blockchains, and how blockchains achieve decentralization. In this section, we introduce the main features and working principles involved in achieving immutability, security, and integrity for the stored contents of each block. Finally, we discuss different types of blockchain implementations, as well as the programmability of blockchains through smart contracts.

A. Salient Features of Blockchains

The most important features that turn the blockchain technology into something with the potential of radically reshaping several industries are:

1) *Decentralization:* In centralized network infrastructures, data exchanges (i.e., the *transactions*) are validated and authorized by trusted central third-party entities. This incurs costs in terms of centralized server maintenance, as well as performance cost bottlenecks. In blockchain-based infrastructures, two nodes can engage in transactions with each other without the need to place



(a) Logical representation of a blockchain. (b) Block header fields and Merkle tree for storing transactions in a block.

Fig. 1. Graphical representation of the blockchain: each block of the chain is composed by a header and a body. The header of each block contains (among the other fields) the identifier of the previous block, thus forming a chain of blocks (i.e., a *blockchain*). Transactions are stored within the body of each block, in a data structure called Merkle tree.

trust upon a central entity to maintain records or perform authorization.

2) *Immutability:* Since all new entries made in the blockchain are agreed upon by peers via decentralized consensus, the blockchain is censorship-resistant and is nearly impossible to tamper. Similarly, all previously held records in the blockchain are also immutable and, in order to alter any previous records, an attacker would need to compromise a majority of the nodes involved in the blockchain network. Otherwise, any changes in the blockchain contents are easily detected.
3) *Auditability:* All peers hold a copy of the blockchain, and can thus access all timestamped transaction records. This transparency allows peers to look up and verify transactions involving specific blockchain addresses. Blockchain addresses are not associated with identities in real life, so the blockchain provides a manner of pseudo-anonymity. While records of a blockchain address cannot be traced back to the owner, specific blockchain addresses can indeed be held accountable, and inferences can be made on the transactions a specific blockchain address engages in.
4) *Fault tolerance:* All blockchain peers contain identical replicas of the ledger records. Any faults or data leakages that occur in the blockchain network can be identified through decentralized consensus, and data leakages can be mitigated using the replicas stored in blockchain peers.

B. Blockchain Structure

A blockchain is made up of blocks containing details of transactions that have occurred within the network. The transaction information can be regarded as token transfers occurring in a network, or any manner of data exchange. Each block is logically divided into two parts, namely, the header and the body. Transactions are stored within the body of the block, while the header of each block contains, among other fields, the identifier of the previous block. Therefore, the blocks are connected in a chain similar to a linked list, as shown in Fig. 1(a). The first block in the chain is called "genesis" block [23].

The identifier of each block is obtained by taking its cryptographic hash, which is why having each block linked to the previous block helps the blockchain achieve immutability of its contents. If a hacker were to alter the contents of a past block, its identifier would no longer be valid, and a domino effect would render the parent block hashes in the subsequent blocks invalid as well. Therefore, to successfully alter the contents of a single block, an attacker would have to alter the headers in all successive blocks and have this alteration take place in the majority of the nodes in the network, so as to have the peers reach consensus on this altered blockchain.

Other than the block's own identifier and the identifier of the previous block, the header also contains a timestamp of when the block was published and the Merkle tree root for all the transactions stored within the body of the block [24]. The Merkle tree root significantly reduces the effort required to verify transactions within a block. More in detail, the blockchain is a linearly growing data structure with higher transaction activity inflating the sizes of newer blocks. As part of all consensus algorithms, peers verify transactions recorded in a newly published block. The transactions within a block all have a transaction ID, whereby each transaction ID is the cryptographic hash of the corresponding transaction's information stored in the block. The transaction IDs are hashed together in pairs and a hash tree is built within the block, as shown in Fig. 1(b). As said, the root of this tree is stored in the block header. Hence, to verify a transaction, a local copy of all the transactions is not required, and verification can be carried out by simply using the Merkle tree branch containing the transaction in question. A tampered transaction would produce altered hashes within its branch and would be detected without much computational effort.

In the event of multiple nodes in the blockchain network producing valid blocks at the same time, the blockchain can fork, and maintaining a single canonical version of the blockchain becomes an issue. Mainstream blockchain networks resolve this issue by only considering the longest fork as canon, while all blocks published in the other forks are discarded, or orphaned [9], [25]. Other fields included in

the block header contain information specific to the consensus algorithm used within the blockchain network.

C. Transactions and Digital Signatures

To make transactions, either in cryptocurrency, or simple data exchange, the peers of a blockchain network require a public-private key pair. Peers use their private keys to sign transactions and use the recipient peer's blockchain address to deliver it to them. These addresses are obtained by calculating a cryptographic hash of a user's public key. For example, in Bitcoin, SHA-256 encryption is used to derive user addresses [9]. Essentially, encryption and encoding obfuscate blockchain peers' public keys. In cryptocurrency implementations, serialized tokens do not exist, instead, an initial amount of tokens is associated with the addresses involved in the initial stages of the blockchain. Following the genesis block, the transactions maintain ownership tracking of tokens, by adding or subtracting the tokens associated with each participating address. In implementations outside cryptocurrency, transactions do not assign ownership of tokens, and only involve the exchange of data secured with digital signatures.

To understand how blockchain transactions play out in implementations outside cryptocurrency, assume Alice addresses some transaction data to Bob. After encrypting the transaction data using Bob's public key, Alice creates a digital signature by taking a hash of the data she is sending, and encrypting it using her private key. The entire transaction is made up of the encrypted data itself, and the digital signature included in the transaction header. The transaction is broadcast over the blockchain network, and since it is addressed to Bob, Bob begins verifying the transaction contents. Bob decrypts the digital signature using Alice's public key and decrypts the transaction data using his private key. The transaction data is easily verified when Bob compares a hash of the data to the hash in the digital signature [26]. In cryptocurrency implementations, transactions are verifiable, however, they primarily account for a change in token ownership.

Transactions can also take place in between two separate blockchains via sidechaining [27]. Sidechains are blockchains synchronized with and running in parallel to an existing blockchain, referred to as the "main chain". Tokens can be transferred from the main chain to the sidechain and back, whereby the sidechain uses the tokens it has in an isolated use-case scenario. Therefore, sidechains enhance the functionality of the main chain and provide a testing ground for blockchain application development.

D. Types of Blockchains

Based on how blockchains are used in different application scenarios, they can be classified into multiple types with some distinct attributes. Table II shows a detailed comparison between these implementation types.

1) *Public Blockchains:* Public blockchains are truly decentralized, where all members can participate in publishing new blocks and accessing blockchain contents. Public blockchains are termed *permissionless* in that it allows anyone to maintain a copy of the blockchain and engage in validating new blocks. Examples of public blockchain implementation are cryptocurrency networks, such as Bitcoin, Ethereum, and so on. Devices in public blockchain networks can choose to actively validate new blocks or simply issue transactions within it. Public blockchains are designed to accommodate a large number of anonymous nodes, so it is necessary to mitigate potential malicious behaviour. Publishing new blocks in a public blockchain involves either computationally expensive puzzle solving, or staking one's own cryptocurrency. Each transaction has a processing fee attached to it, which serves as an incentive to the peers attempting to publish new blocks onto the blockchain. This prevents the public blockchain from being hacked since it would be too costly to tamper its contents. Since thousands of other peers are involved in the decentralized consensus, every transaction includes a transaction fee, as an incentive to the peer that validates the transaction into a new block.
2) *Private Blockchains:* In contrast to public blockchains, private blockchains are *permissioned*, and every node joining the network is a known member of a single organization. Private blockchains are suited for single enterprise solutions and are utilized as a synchronized distributed database meant to keep track of data exchanges occurring between different departments or individuals. Private blockchains do not require currency or tokens to function, and there are no processing fees included in its transactions. Since blocks are published by delegated nodes within the network, a private blockchain is not as tamper-resistant as a public blockchain, and the organization may choose to roll back their blockchain to any point in the past.
3) *Consortium Blockchains:* Consortium blockchains, or federated blockchains, are similar to private blockchains in the sense that it is a permissioned network. Consortium networks span multiple organizations and help maintain transparency among the involved parties. A consortium blockchain is used as an auditable and reliably synchronized distributed database, that keeps track of data exchanges taking place between the participating consortium members. Similar to private blockchains, a consortium blockchain does not involve processing fees, and it is not computationally expensive to publish new blocks. While it does provide auditability and lower latency in transaction processing, it is not entirely decentralized or censorship-resistant [26].

E. Smart Contracts

Smart contracts are programmable applications stored in the blockchain, that manage transactions under specific terms and conditions. Therefore, smart contracts are the digital equivalent of traditional economic contracts between various engaging entities. Unlike traditional contracts that are enforced by centralized authorizing entities, a blockchain network does not require authorizing intermediaries to ensure that the conditions in a smart contract are met.

TABLE II
COMPARISON OF PUBLIC, PRIVATE AND CONSORTIUM BLOCKCHAINS

	Public Blockchain	**Private Blockchain**	**Consortium Blockchain**
Participation in Consensus	All nodes	Single organization	Selected nodes in multiple organizations
Access	Public read/write	Can be restricted	Can be restricted
Identity	Pseudo-anonymous	Approved participants	Approved participants
Immutability	Yes	Partial	Partial
Transaction Processing Speed	Slow	Fast	Fast
Permissionless	Yes	No	No

The term "smart contract" was coined by N. Szabo with the objective of *"securing relationships on public networks"* [12]. In blockchain networks, smart contracts perform the function of carrying out transactions in a predetermined fashion, agreed upon by parties participating in the contract. While Bitcoin, the first cryptocurrency implementation of the blockchain, does not deploy and execute smart contracts, it does offer limited programmability via a scripting language, which was not user-friendly or Turing-complete [10]. Newer platforms like Ethereum [25] and Hyperledger [28] have smart contract programmability built into them. When deployed, smart contract code is stored in the blockchain, and the functions written in the smart contract can be invoked by any participant at any time. A smart contract is sometimes termed an "autonomous agent", owing to the fact that smart contracts have their own accounts on the blockchain, with their own blockchain addresses [29]. Therefore, the contract can hold custody or ownership of tokenized assets while the engaging parties work to meet the agreed-upon conditions. Invoking functions in smart contracts incurs an execution fee since an invocation itself is considered a transaction that is logged in the blockchain. Execution fees incentivize peers publishing new blocks and mitigate flooding attacks on the network.

Smart contracts can be utilized to perform a variety of functions within a blockchain network, such as:

1) Allowing 'multi-signature' transactions, whereby a transaction is only carried out when a majority or a required percentage of participants agree to sign it [30].
2) Enabling automated transactions triggered by specific events. This functionality can manifest itself in multiple ways, for example, transactions automatically sent over fixed time intervals or transactions sent in response to other transactions. This facilitates request-response type transactions, for decentralized data access within a blockchain-based system. A smart contract can also be triggered when a message is sent to the smart contract's address [31].
3) Providing utility to other smart contracts. For example, in Ethereum, inheritance can be written into smart contracts, where one contract can invoke functions written in another contract.
4) Allowing storage space for application-specific information, such as membership records, lists or boolean states.

While Bitcoin had very limited scripting capabilities [10], newer blockchain platforms like Ethereum [25] and Hyperledger Fabric [28] use more flexible and Turing-complete smart contract scripting languages. The smart scripting languages Serpent and Solidity are used in writing smart contracts for Ethereum, however Solidity has seen a much more widespread use [31]. The publicly available Remix IDE[2] for scripting Ethereum smart contracts provides a simulated environment for testing the functions written in Solidity smart contracts. Hyperledger Fabric uses smart contract written in Go [28] for permissioned blockchains.

Deployed smart contracts are stored within the blockchain, so they are visible to all participants in the network. Security lapses can occur if a participant exploits any bugs or loopholes in a deployed contract, therefore it becomes critical to practice stringency in the design process. Most notably, in June 2016, the DAO attack in the Ethereum network resulted in the attacker unlawfully siphoning off Ether worth 60 Million USD, with transactions that were valid according to the exploited smart contract [32].

With secure and well-written smart contracts, many applications provide various functionalities, utilities, and algorithmic processing in blockchain networks. For example, Hawk is a smart contract-based platform designed to anonymize transactions [33], while RootStock (RSK) uses smart contracts within sidechains connected to the main Bitcoin blockchain [34].

F. Consensus Algorithms

Consensus algorithms have been an active topic of research for the last three decades, much longer since the advent of the blockchain itself. Turek and Shasha [35] provide an overview of some of the earlier work done in consensus for distributed systems. Consensus algorithms aim to securely update replicated shared states and are the essential piece of the puzzle in the working principles of the blockchain. In the blockchain, a system based on "state machine replication", consensus protocols ensure all replicas of the shared state are synchronized and in agreement at any given point in time.

According to [36] and [37], deterministic consensus in fully asynchronous communication models cannot tolerate any faults, thus assumptions for partial synchrony are required, with maximum thresholds for the latency of propagating transactions. Earlier works on consensus protocols [38]

[2]http://remix.ethereum.org/

involved cryptography and partial synchrony [39], and precursor designs and proposals of digital currency [40], [41] were the building blocks that went into developing "decentralized" consensus algorithms used in blockchain networks. The following section is a discussion about the different types of decentralized blockchain consensus algorithms in existence, and their suitability in IoT networks.

III. Decentralized Consensus Algorithms

Core principles applied in designing consensus algorithms are safety, liveness, and fault tolerance. Safety is the extent to which a system can tolerate failures, say in an (n, f) fault tolerant system, where n represents the total number of processes, the system should be able to tolerate at most f faults. Safety is the ability to mitigate corrupted or out-of-order messages so that all non-faulty nodes reach consensus on results that are valid to the rules of the state machine. Liveness of a fault tolerant system means that in despite the presence of f faults, all correctly participating nodes should be able to move forward with their distributed processes.

Maintaining fault tolerance in a consensus protocol becomes difficult in scenarios where it is possible for nodes to stop participating at any moment, or by nodes acting maliciously. This fault is termed the "Byzantine Generals Problem" [42], using the example of generals taking command of different parts of the Byzantine army. The generals rely on messengers to maintain a synchronized battle plan. The messengers can be caught by the enemy, causing the messages to be lost. More importantly, the messengers or even some of the generals may be corrupted and may cause to maliciously sabotage the battle plan. Therefore, the problem is, how do the generals maintain a synchronized battle plan without traitorous participants getting the upper hand? Similarly, in a distributed system running a consensus protocol, a node can fall under a Byzantine fault as a result of software bugs, or by being compromised. Byzantine faults occur when a node sends false messages and misleads the other nodes participating in the consensus protocol. A number of algorithms are proposed in [43], and in use today, that address Byzantine faults, by making varying assumptions on specific use-cases, network performance and maliciousness of compromised nodes.

Within the context of this survey, we will discuss decentralized consensus algorithms as they are applied in permissioned and permissionless blockchains. Our goal with this discussion is to understand the suitability of private or public blockchain consensus when applied to various IoT scenarios. References [26] and [44] contain exhaustive details on all variations of private and public blockchain consensus algorithms.

A. Permissionless Blockchains

Publicly deployed blockchains that accommodate anonymous participants are termed "permissionless", and reaching consensus using votes in a permissionless blockchain is problematic. If a permissionless blockchain were to use voting to achieve consensus, participants can use multiple accounts on the blockchain to launch a Sybil attack [45], and can drive decisions in their favour. Therefore, in permissionless blockchain implementations, the consensus algorithms are based on a lottery-based selection of a single node that publishes a new block onto the blockchain. To ensure security in public blockchains where anonymous participants are required to transact in a trustless manner, block creation needs to be "expensive" so that the resources of one entity are insufficient to bias the consensus decisions in its favour.

1) Proof of Work: The first public blockchain consensus protocol was the Proof-of-Work (PoW) consensus, as seen in Bitcoin [9]. In the Bitcoin network, any node can participate in publishing new blocks to the blockchain, by showing that it has performed a computationally expensive amount of work, the proof of which forms the basis of the PoW consensus algorithm. Publishing new blocks under the proof of work algorithm is called "mining", and miners engage in a race to find a nonce that, when hashed with the hash of a block, produces a resultant smaller than a predefined threshold. The proportional inverse of this threshold is called the *"difficulty level"*, which is stored in the block header, and gets adjusted with increasing number of participants, to maintain an average block processing time [10], [46]. Here, the calculated nonce is the proof of work a miner does, which the miner adds to the block header, and broadcasts their block to the network. This enables all participating nodes to verify the block published by the miner. Subsequently, the miner claims the processing fees associated with the transactions stored within the block as a reward for mining. In PoW consensus, the computationally expensive block creation and transaction fees secure the network against DDoS attacks and false block creation.

In a fully synchronized system, it would be easier to maintain the correct block sequence in the case of two nodes publishing a block almost concurrently [41]. Such a system is not feasible in geographically spread-out networks since total synchrony cannot be assumed or guaranteed. Consider the case where after a block n, a node in Australia mines a valid block $n + 1$, and at the same time, a node in Sweden mines another valid block $n + 1'$. This creates a temporary fork, where one fork has $n + 1$ after n, and the other has $(n + 1)'$ after n. Beyond this point, more blocks are added to these forks, and the fork with the most work committed to it is hence considered canon, and the other fork is orphaned.

Proof of work based consensus is, however, vulnerable in scenarios where a user takes control of 51% of processing power in the network [47], [48]. Therefore, proof of work consensus provides fault tolerance as long as the total computational power is $n \geq 2f + 1$ where f is the computational power occupied by a single malicious user.

PoW blockchains like Bitcoin and Ethereum delay the 'finality' of a block decision, so the blockchain can be rolled back to a past block height in the event of a 51% attack. After a block is 'finalized' it is considered irreversible. In both Ethereum and Bitcoin blockchains, a transaction is finalized after 6 confirmations. 6 confirmations take 60 minutes in Bitcoin [10], and 2 minutes in Ethereum [46].

2) Proof of Stake: The Proof-of-Stake (PoS) algorithm aims to cut back on the ever-increasing electricity consumption of

PoW blockchain networks [49]. As an alternative to computationally expensive puzzle solving, proof of stake aims to stake peers' economic share in the network [50]. Here, the term "miners" is replaced with "validators," and similar to the proof of work algorithm, one of the validators is chosen to publish a block onto the blockchain. The difference lies in how the validator is chosen. In proof of stake, a validator is selected in a pseudorandom fashion, with the probability of being selected proportional to the validator's share in the network [51], [52]. Naive Proof of Stake consensus mechanisms are prone to attacks like the "nothing at stake" attack, and require further considerations for it to be consensus-safe [53]. Block finality in PoS blockchains is faster compared to PoW blockchains, since there is no computational puzzle solving involved in choosing the validator.

3) Proof of X: Further alternative consensus algorithms for public blockchain deployments came about, and are classified as "Proof of X". Cachin and Vukolić [54] present an exhaustive study of these algorithms.

Proof of activity [55] was proposed as an alternative to Bitcoin mining, designed to deliver consensus by combining aspects of the proof of work and proof of stake. The objective is to reward stakeholders that actively participate in the network. Peers start off with mining potential blocks, similar to proof of work. Decred [56] uses proof of activity to achieve distributed consensus. Computational puzzle solving in proof of activity only involves finding a proof of work against the block header, without the transactions in the block. Beyond this point, a random group of validators are chosen to vote on the validity of the mined block header. Similar to proof of stake, the probability of the validators of being chosen is proportional to their share in the network. The block is considered valid if all the validators vouch for its validity. If some of the validators are offline, the next mined block is chosen, along with a new set of validators, till a block is voted as valid. Transaction fees in this case are split between the miner and validators. Criticism of proof of activity includes concerns pertinent to both proof of work and proof of stake. It requires higher computational power, and a naive implementation can be prone to nothing at stake attacks.

Hyperledger Sawtooth [57] is an open-source project with its own consensus algorithm called ***proof of elapsed time***. Proof of elapsed time runs in a Trusted Execution Environment (TEE), like Intel's Software Guard Extensions (SGX) [58]. A trusted voting model built on the SGX helps elect a validator for publishing a new block. Proof of elapsed time is another lottery based consensus algorithm, however it foregoes the need for expensive computational puzzle solving. Nodes in the Sawtooth blockchain network request for a wait time from a trusted function within the SGX. The validator with the shortest wait time is selected the leader as soon as its waiting time runs out. Another trusted function attests to the fact that the validator did indeed wait an allotted amount of time before publishing a new block. This second function thus provides a proof of the validator being chosen after its allotted time had elapsed. The probability of being elected here is proportional to the resources (general-purpose processors running TEE) contributed to the network. The algorithm meets the prerequisites of a viable lottery based consensus algorithm, however, its limitation is in its use of specialized hardware.

B. Permissioned Blockchains

In "permissioned" blockchain deployments such as private and consortium blockchains, only a limited number of known participants carry a copy of the entire blockchain [59]. Maintaining consensus therefore is much straightforward and doesn't require costly proofs for publishing a new block. Since participants are known, there is no risk of a Sybil attack, therefore voting mechanisms are used to achieve consensus. By this virtue, permissioned blockchains have a much higher performance than permissionless blockchains.

1) Practical Byzantine Fault Tolerance: The Practical Byzantine Fault Tolerance (PBFT) algorithm, as described in [60] involves multiple rounds of voting by all nodes of the network, in order to commit state changes. The PBFT algorithm includes an optimized, encrypted message exchange for making global voting more practical. To solve the Byzantine Generals problem via multiple rounds of voting, this algorithm requires $n \geq 3f + 1$ nodes to tolerate f failing nodes. Hyperledger Fabric [61] is a permissioned blockchain application platform being developed under the Linux Foundation's Hyperledger project. Hyperledger Fabric is designed for private or consortium blockchains, and supports smart contracts written in multiple programming languages, called chaincode. In PBFT consensus, one node is chosen to be the "leader," who assembles a set of ordered transactions into a block and broadcasts it to the network. The validating peers in the network calculate a hash of the block and broadcast it. Validating peers observe the hashes they receive from the rest of the network, which can be seen as "votes," over multiple rounds. If 2/3 votes are in favour of the candidate block, the peers add it to their copy of the blockchain. PBFT consensus provides high throughput and low latency in validating transactions, however, the overhead incurred by broadcasting blocks and votes in PBFT consensus makes it unable to scale beyond a network with tens of validators. Hyperledger Fabric also uses a variation of PBFT called Sieve [62], which is designed to perform consensus while executing non-deterministic chaincode. In scenarios involving non-deterministic chaincode, Sieve runs the chaincode first and speculates the outputs. Sieve then gets rid of minor divergences in the chaincode's output, or gets rid of entire processes resulting in greatly diverging outputs. Subsequently, Sieve maintains consensus in state-changes to the blockchain as was the case in PBFT.

2) Tendermint: Tendermint [63] is a Byzantine Fault Tolerant consensus algorithm, which, similar to PBFT, provides an $n \geq 3f + 1$ fault tolerance. Tendermint uses proof of stake in combination with principles of PBFT to provide security, high throughput, and low block processing times of 1-3 seconds. While in PBFT, a leader node used to get chosen pseudorandomly, Tendermint uses the lottery based properties of proof of stake, and chooses the leader node with probability proportional to the stakeholders' share in the network. After leader selection, Tendermint performs multiple rounds of voting to reach consensus on a new block. Tendermint

requires a supermajority, or 2/3 of its validators to maintain 100% uptime, and if more than 1/3 go offline, the network may stop progressing and lose liveness. Transactions are ordered, and assuming if less than a third of all validators are faulty, Tendermint provides a safety guarantee that no conflicting blocks are created and no forks appear in the blockchain. Tendermint is compatible for public or private chains, however, it does not enjoy the same level of scalability as proof of work or proof of stake blockchains. Transaction finality in Tendermint is approximately 1 second [63].

3) Federated BFT: Blockchain implementations in Ripple [64] and Stellar [65] extended the traditional Byzantine Fault Tolerance and made it open-ended for participation in scenarios involving a consortium or federation of nodes.

Ripple consensus begins with a unique node list (UNL), which is a list of active validator nodes in the network. Each node has a UNL with 100+ nodes in it, and each UNL has to overlap by at least 40% with the UNLs stored by other nodes. Ripple carries out multiple rounds of voting, where nodes assemble transactions into candidate blocks and broadcast them to the nodes in their UNL. Nodes then broadcast votes on each candidate block. Each round of voting helps nodes refine their candidate block, and a new block is added to the ledger once it receives a supermajority vote of 80%. Thus, even though Ripple carries out multiple rounds of votes, it provides a fault tolerance of $n \geq 5f + 1$. Consensus in the entire network is based on consensus within subnetworks, so Ripple allows open-ended participation of users, market entities, and gateways to other subnetworks.

Stellar introduces the idea of quorums in blockchain networks, where a quorum is a set of nodes used to reach consensus. A node in such a network can be part of multiple quorum slices, where each quorum slice securely reaches consensus through voting. Since the quorums and quorum slices are allowed to intersect, stellar allows open participation of nodes in different subnetworks within the main Stellar network. Stellar opts for a safety over liveness property, in the event of malicious behaviour in the network, the blockchain does not progress till the malicious behaviour is resolved. Stellar provides flexible trust, and low latency, since it is computationally inexpensive, and quorums contain limited number of nodes that share vote messages.

C. Performance and Scalability in Consensus Algorithms

Permissionless blockchains are forced to have slower block creation speeds, in order to take into account the propagation speeds of nodes within the network. On the other hand, permissioned blockchains have much lower latency, but suffer from a severe scalability issue. The networking overhead incurred from voting mechanisms limits permissioned blockchains to scale to only hundreds of nodes. The worst case complexity for permissioned blockchains is $O(N^2)$ compared to the $O(N)$ worst case complexity of permissionless blockchains. This limits the usability of permissioned blockchains for the IoT. Therefore, there is a steep trade-off between performance and scalability from PoW consensus to PBFT consensus [66].

Through the virtues of publicly anonymous accessibility and decentralization, permissionless blockchains are better suited to industry-wide IoT applications. Permissioned blockchains are more suited to enterprise solutions due to their higher degree of control and permission granting capabilities. Sharding mechanisms in Ethereum and Tendermint can lead to leveraging the benefits of higher performance, and scalability for IoT applications [67].

IV. Integration of Blockchains and the IoT

The term "Internet of Things" was coined in 1999 by K. Ashton as a bridge to link supply chain RFID's to the Internet. However, according to another authoritative source, the first proof-of-concept for the IoT came to life in 1982, when a group of students turned a Coke machine installed at the Carnegie Mellon University into what may be considered the first smart, connected appliance [68].

Today, the term is used as an umbrella keyword for covering various aspects related to the extension of the Internet and the Web into the physical realm, by means of the widespread deployment of spatially distributed devices with embedded identification, sensing and/or actuation capabilities [69]. However, the IoT is far more than a marketable label, rather it can be seen as a technology that is, sometimes drastically, transforming all industries and markets, enhancing and extending the digitalization enabled by information and communication technology (ICT) towards the broader impact offered by the capability to sense, communicate, and actuate on the whole physical environment where such IoT devices and applications are deployed.

A. Issues and Challenges in the IoT

During the last two years, IoT platforms themselves are proliferating: a recent analysis by Research and Markets[3] enumerated more than 450 of such platforms [70]. These span from horizontal platforms able to accommodate quite generic use cases within different domains to vertical approaches able to address very specific market needs (e.g., cities, spaces, manufacturing, etc.). Clearly, the combinations of functional specializations offered by such platforms are also variegated: device management, enabling applications, data analytics, cloud storage, connectivity, only to mention a few examples. Last but not least, they come with different licensing models, either proprietary or open source. The result of this Babylon is an over-crowded and fragmented market. Moreover, while there is a common understanding on the fact that the IoT technology could play the role of enabler for several business opportunities, there exists a set of technical challenges that, despite being already identified, are slowing down a truly global IoT adoption. The following are brief introductions to these challenges:

1) Cybersecurity: It is considered the most critical and challenging barrier for the IoT. With respect to typical Web security, IoT security is subject to several new factors and conditions that amplify potential threats. First of all, IoT devices

[3]https://www.researchandmarkets.com/

are commonly isolated hardware solutions that, depending on their deployment conditions, are subject to tampering in ways that may be unpredictable by manufacturers. IoT devices are then typically interconnected with other devices making it complex to manage device-to-device interactions and to protect them from malicious data manipulation. Moreover, IoT devices have typically limited computational power: this limitation hinders the adoption of highly sophisticated security frameworks. Once IoT devices are connected with each other and with the Internet, they become an interconnected and complex system which is difficult to immunize against modern security threats. For this reason, such systems become exponentially exposed to several Web attacks (password security attacks, message spoofing/alteration, traffic analysis, Distributed Denial of Service, Sybil attack, eavesdropping, etc.). On the other hand, a generic "one-size-fits-all" security model is difficult to implement. To properly address security in IoT there is a need for novel security models foreseeing the development of specific policies and best practices capable of combining security-by-design approaches with specific technical countermeasures designed at different technological stacks, as well as novel organizational processes capable of addressing information security for IoT in a more holistic way [71].

2) Privacy: The huge amount of data generated by IoT devices may offer detailed information about the context where device owners/users live, and about their habits. This data may be collected without any explicit user consent and exposed to third parties when shared by supporting IoT platforms, depriving users about control on which data and to whom his personal data is given access [72]. While administrative policies exist for providing privacy to IoT users, the challenge is to develop solutions that ensure privacy by design.

3) Massive Data Management: The volume of data generated by IoT devices can be enormous and difficult to manage in terms of elaboration, communication/transmission, and storage. Scalable infrastructures are necessary to efficiently handle this massive growing volume of data [73].

4) Lack of Standardization and Interoperability: The landscape of standards for the IoT is full of open solutions, supported by independent and multinational governance bodies, alliances or organizations (e.g., IEEE, ETSI, IETF, W3C, OMG, OneM2M, ITU-T, OASIS IEC, etc.). These standards cover different aspects of IoT products, services, systems, from communication technologies to architectures. Some of them follow a neutral, cross-domain approach, while others are applicable only to specific vertical domains. Unfortunately, the uncontrolled proliferation of standards, further exacerbated by the lack of commonly accepted standards, only leads to fragmentation and can even become a real barrier for the IoT adoption and for the possibility of performing real integration in multiple application domains [74].

5) Lack of Skills: The complexity and the heterogeneity of the technologies involved in an IoT domain require specific skills for the design, implementation, but also for the operations of the deployed solutions. Such skills are typically difficult to build or acquire by organizations. In this case, the *IoT ecosystem* plays a critical role, as it could guarantee that the right skills are offered and acquired in a proper and effective way [75].

B. Decentralizing the IoT Through Blockchains

Simplifying the concept as much as possible, the aim of the IoT is to have smart objects communicate over the Internet to collect comprehensive data and provide personalized automation services, with little deliberate human interaction [75]. Towards this aim, current IoT platforms are built on a centralized model where a central server or broker provides services like data handling, device coordination, and authorization. This approach necessitates high-end servers and proves to be unsuitable for scenarios where objects are required to autonomously exchange data. In a centralized model, centralized servers authorize objects to communicate with each other, so the increasing number of devices communicating with each other over the Internet steadily increase set requirements for the servers. Other issues associated with a centralized model are of security [76], [77], data privacy [78] and the trust inherently required in using centralized servers [79].

Following the recognition of the opportunities blockchains offer and their potential impact, researchers and developers have taken to create decentralized applications for the IoT. The inherent features of blockchains as discussed previously, make them a natural fit to developing a secure distributed fabric for the Internet of Things and distributed cloud computing in general. Based on these features, the following are the potential benefits and motivations for developing a blockchain-based decentralized IoT framework:

- *Resilience:* IoT applications require integrity in the data being transferred and analyzed, therefore IoT frameworks need to be resilient to data leaks and breakage. Blockchain networks store redundant replicas of records over blockchain peers, which help maintain data integrity and can provide resilience to IoT frameworks.
- *Adaptability:* Currently, the heterogeneity of IoT devices and protocols limit their interoperability, and since blockchains are semantics-independent distributed databases, using blockchains as the network control mechanism for the IoT will add a greater degree of adaptability to it. Blockchains are proven to work over heterogeneous hardware platforms, and a blockchain-based IoT framework holds the promise to adapt to varying environments and use cases to meet the growing needs and demands of IoT users.
- *Fault tolerance:* The Internet of Things represents a proliferation of always-available smart devices that collect data and provide automated functionality. Network control mechanisms for the IoT require high availability, which may not always be the case in architectures involving centralized servers. Blockchains are Byzantine fault tolerant record-keeping mechanisms that can identify failures through distributed consensus protocols.
- *Security and privacy:* One of the most important challenges faced by the IoT, as discussed before is network security. To ensure confidentiality and data protection,

blockchains have pseudonymity in its addressing and distributed consensus for record immutability. Data modification attacks cannot be mounted in public blockchains since the blockchain does not exist in a singular location. Furthermore, the cost added to making new transactions (either monetary or computational) protect the network against flooding attacks and DDoS attacks.

- *Trust:* Blockchains enable trust between transacting parties. The "trustless" features of blockchains remove the need for users to trust centralized entities to handle their IoT data, thus preventing malicious third party entities from accumulating users' private data. Blockchains allow faster settlements for automated contracts without the need for trusted intermediaries.
- *Reduced maintenance costs:* An important step towards the global pervasion of the IoT is to find efficient and economical methods to handle the massive volume of data generated by sensors throughout the IoT. A cloud based IoT framework faces a significant disadvantage in its high server maintenance costs, which not only add monetary cost, but also adds to the communication costs in device-to-device communications. Centralized cloud storage services use geographically spaced data centers which are large central points of failure. Centralized cloud services introduced much lower prices for storage and computing, which led to their widespread adoption. However, blockchains have the potential to significantly reduce costs incurred by maintaining dedicated servers. Public blockchains applications do not require dedicated servers, and utilize the computational and storage capabilities of its participants. Since the participants receive incentives for their contributions, blockchains stand to be the next step in democratizing the IoT. Blockchain-based data storage platforms like Sia[4] demonstrate the reduced costs in storing data using blockchains. In Sia, instead of using dedicated servers, users rent out any available storage space they have, which others utilize to store data. While the cost for storing 1 Terabyte per month on Amazon S3[5] is $25, the cost of blockchain-based data storage in Sia is $2 per Terabyte per month.
- *IoT e-business models:* In current IoT service provision, users surrender their data to centralized service providers in exchange for IoT services, however, data being exchanged over public blockchains can have the added benefit of enabling users to engage in a new data marketplace and monetize their IoT data. Blockchain-based solutions also incentivize users to make IoT resources available for others to use on demand, in exchange for cryptocurrency.

Blockchains show promise in several industry verticals, and startups are locked in a race to develop blockchain-based distributed applications for different use case scenarios. As discussed before, a significant part of these applications have direct link to the IoT. An example of these applications can be seen in the insurance industry.

An example of the numerous industry verticals for a blockchain-based IoT are smart grids. Blockchains have the potential to facilitate trade of energy between producers and consumers. In a blockchain-based smart-grid system, each participant has a unique identifier which can be authenticated without relying on a third-party service provider, thus bridging transacting entities in a democratic fashion. Blockchain-based records and cryptocurrency can be used for negotiating, effectuating trade and maintaining records, as proposed in [80]–[84]. Further details on these proposed solutions are discussed in Section X-B.

Another use case for integrating blockchains with IoT is in smart-insurance. In the insurance sector, many companies have taken up IoT applications to collect data for aiding them in calculating insurance premiums and processing insurance claims. Several management processes within insurance can be automated using smart contracts, while maintaining compliance to legal requirements. Considering the benefits of the combination of the IoT and blockchains, eventually insurance use cases will migrate from telematics to real-time IoT cryptocurrency applications.[6]

Other industry verticals where blockchains and IoT can bring potential benefits include healthcare, supply chains, energy trading smart-grids, smart home applications, connected vehicle fleet management and robot swarm coordination. Peer-to-peer decentralized applications in these areas can bring about a revolution in ubiquitous service provision and distributed oversight of all IoT data transactions.

C. Integration Schemes for Blockchains and IoT

Centralized cloud services have made major contributions in the growth of IoT, but in data transparency, there is an inherent need of trust and a lack of absolute confidence. Centralized cloud services act much like a black box for IoT services, and IoT users do not have control and total confidence in how the data they share will be used. Furthermore, centralized cloud services are vulnerable to faults and lethal security attacks. In the evolution of IoT, the network edge is getting more functionality as compared to the cloud, as seen in fog and mist architectures [85]. The IoT can benefit from the decentralized network paradigms offered by blockchains, so further developments to the IoT can continue while eliminating the need for trust in centralized services. However, blockchains are still in their early stages of research and development, and there are still multiple research challenges towards integrating IoT and blockchains in a seamless manner.

Achieving absolute decentralisation in the IoT using blockchains is problematic, considering the vastly varying devices involved in the IoT. Most devices on the IoT edge have resource constraints, and cannot host a copy of the blockchain or engage in validating new blocks for the blockchain. Therefore, it is important to decide upon what roles the different entities in the IoT edge (devices, gateways, etc) will take.

[4]https://sia.tech/technology

[5]https://aws.amazon.com/s3/

[6]https://www.ibm.com/blockchain/industries/insurance

TABLE III
NODE TYPES IN BLOCKCHAIN NETWORKS

Node Type	Storage	Validator
Full Node	Full Blockchain	Yes
Light Node	Block headers	No
Transaction Issuer	None	No

Table III indicates the possible roles the participants of a blockchain network can assume. Full nodes are participants in the blockchain network that host the entire copy of the blockchain. Full nodes can issue transactions to the blockchain, and can choose to act as a validator for adding new blocks onto the blockchain. Light nodes running a "light-client" application can issue transactions to the blockchain, and can host a copy of the block headers from the blockchain. Light nodes can verify the validity of transactions through the block headers, however they do not publish new blocks to the blockchain. Light nodes are used as an easier entry point to the blockchain, using limited computational resources. A transaction-issuer running a "light wallet" application is a participant that does not maintain a copy of the blockchain or engage in block validation, however it simply issues transactions to the blockchain. In some blockchain platforms, the potential downside of having a light wallet transaction-issuer is that it performs transactions through a light or full node. This can be a node in the same local network as the transaction-issuer, or in the case of the Ethereum platform, a third party service like Infura[7] and Metamask.[8] The former is a more suitable choice since using third party services nullifies the point of decentralization.

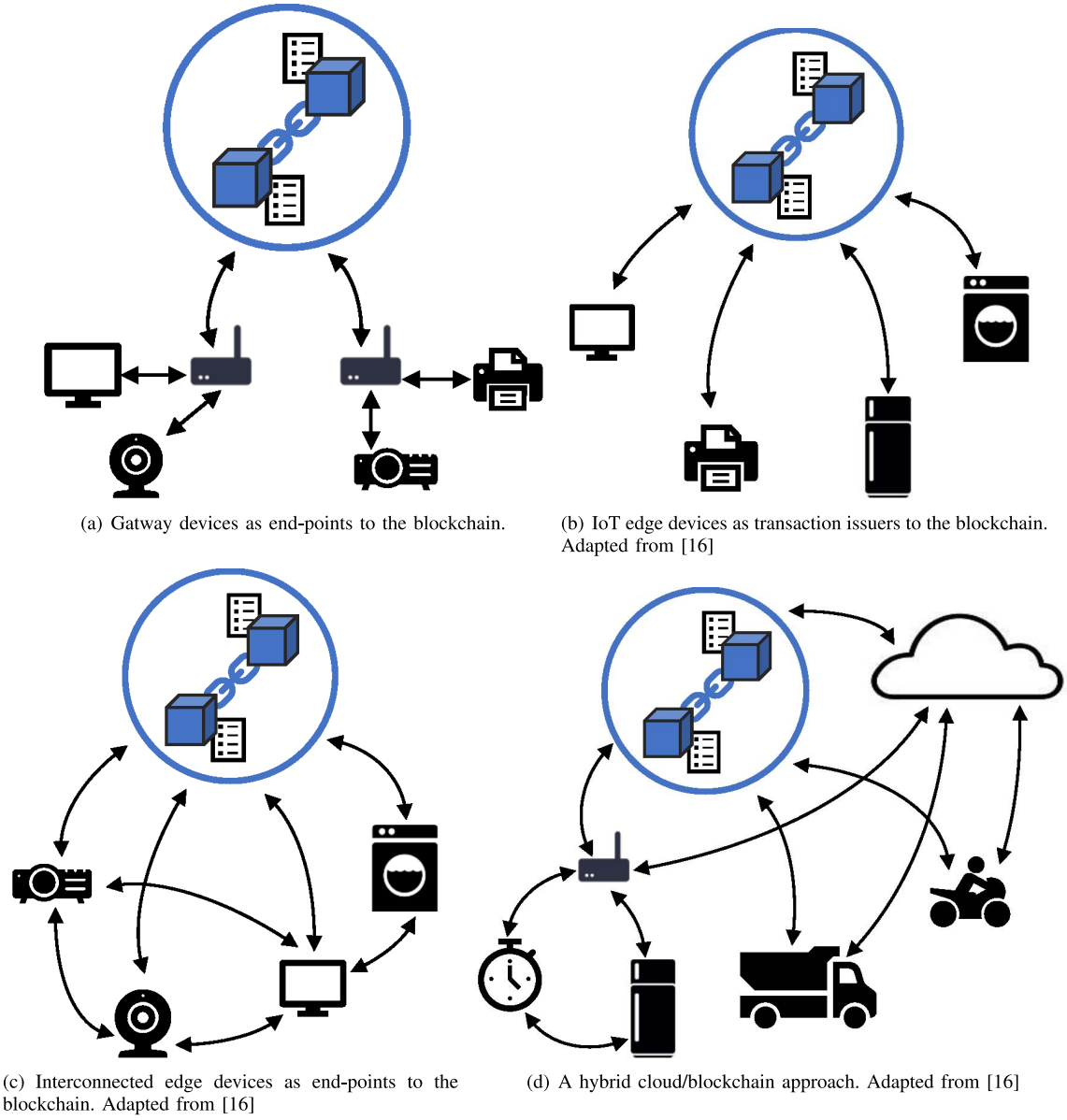
Choosing the right consensus algorithm can prove to be detrimental in integrating blockchains with the IoT. Proof-of-Work based mining remains unfeasible in context of the IoT due to its high computational requirements and high block processing time. In some cases, researchers have attempted to relax the validation requirements of PoW based consensus [86], however, this can lead to compromises in the security afforded to IoT networks by blockchains. PoW consensus with relaxed requirements can be securely implemented in consortium blockchain deployments, since all members of the blockchain are known. In single-enterprise solutions, or use-cases where the blockchain-connected nodes or gateways are known and in the order of hundreds, voting-based consensus like PBFT can be used, to maintain security and low block processing times. For public blockchain deployments, alternate consensus algorithms including Proof-of-Stake and other Proof-of-X algorithms are seen as more suitable for blockchain deployments within the context of the IoT.

Keeping in mind the resource constraints faced by IoT devices, it becomes necessary to employ some design considerations about the extent of their involvement in a blockchain network. Most IoT devices do not have cryptographic capabilities, and do not meet the computational and storage requirements for engaging in blockchain consensus algorithms. To account for these limitations, IoT edge devices only take on the role of simple transaction issuers. Even in the case of light-nodes, most IoT edge devices do not carry sufficient storage capabilities to host the "headers only" version of the blockchain. IoT edge devices or gateways running as simple transaction-issuers have verifiable blockchain-identities without the need to host an entire copy of the blockchain. Therefore, such edge devices are more manageable within blockchain networks and can continue making contributions to the blockchain, while other full nodes in the blockchain network can carry out decentralized consensus and block validation.

In recent literature, we have surveyed a variety of integration schemes that aim to account for IoT edge device constraints in a blockchain-based IoT, with varying requirements of cryptographic capabilities for the IoT edge devices. The following is a discussion of the alternate paradigms as seen in recent literature for integrating blockchains and IoT:

- *Gateway devices as end-points to the blockchain:* In this integration scheme, all communications go through the blockchain, while the IoT gateways act as end-points to the blockchain network. In this case, the IoT devices will be registered to the gateway device, and the gateway issues transactions to the blockchain. This approach enables traceability of all communications involving a specific IoT gateway and IoT service. This integration scheme can also be used to authenticate communications between devices connected to separate blockchain-enabled gateways [87]. In this approach, not all of the data transferred needs to be stored on the blockchain. The blockchain itself can be used as a control mechanism, with smart contracts acting as programmable logic, while data transfer can occur over peer-to-peer technologies like BitTorrent and IPFS.[9] However, recording all IoT interaction events on the blockchain will increase bandwidth and storage requirements, and currently scalability is a well known research challenge towards the integration of blockchains and IoT. Fig. 2(a) is an illustration of this approach. The degree of decentralization achieved through this approach is not as fine-grained as in the case where devices issue transactions directly to the blockchain.
- *Devices as transaction-issuers to the blockchain:* This integration scheme is seen in [16], however, in our discussion we are assuming that the IoT devices are not in fact carrying a copy of the blockchain, but are simply issuing transactions to the blockchain, as shown in Fig. 2(b). Similar to the previous approach, all IoT interaction events are logged onto the blockchain for secure accountability. In this approach, IoT devices can be provided with cryptographic functionality. The trade-off here is higher degree of autonomy of IoT devices and applications, versus increased computational complexity of IoT hardware.
- *Interconnected edge devices as end-points to the blockchain:* In this approach [16], IoT gateways and

[7]www.infura.io
[8]www.metamask.io
[9]www.ipfs.io



(a) Gatway devices as end-points to the blockchain.

(b) IoT edge devices as transaction issuers to the blockchain. Adapted from [16]

(c) Interconnected edge devices as end-points to the blockchain. Adapted from [16]

(d) A hybrid cloud/blockchain approach. Adapted from [16]

Fig. 2. Blockchain integration schemes for the IoT. All arrows indicate interactions.

devices issue transactions to the blockchain and can communicate with eachother off-chain, as seen in Fig. 2(c). While introducing the need for routing and discovery protocols, this approach ensures low latency between the IoT devices and the choice to log specific interactions on the blockchain. This integration scheme would be more suited to scenarios where interactions are much more frequent and high throughput, low latency, reliable IoT data is required.

- *Cloud-blockchain hybrid with the IoT edge:* This approach is an extension to the previous integration scheme, whereby IoT users have a choice to use the blockchain for certain IoT interaction events, and the remaining events occur directly between IoT devices [16]. This approach leverages the benefits of decentralized record-keeping through blockchains as well as real time IoT communication. Fig. 2(d) is an illustration of this hybrid integration scheme.The challenge posed by this approach is to optimize the split between the interactions that occur in real-time and the ones that go through the blockchain. Hybrid approaches can utilize fog computing to overcome the limitations of blockchain-based IoT networks.

Which integration scheme to implement depends upon the requirements of the IoT application. For instance, when there is a need for immutable record-keeping and relatively lower number of interactions are taking place, the first two interaction schemes make more sense. In applications that require higher performance, using a blockchain alone may not be adequate, and it would make sense to use a hybrid integration scheme. In IoT use-cases neither IoT devices or gateways should ever be used as full-nodes, since the storage and computational overheads will not be able to justify the potential benefits. Furthermore, in the case of some applications, an

integration with blockchains may not be necessary. In order to ascertain which application scenarios justify a blockchain integration, the methodology presented in [88] can be used.

Current centralized IoT models are linked to specific drawbacks and limitations that can be canceled or mitigated by the decentralization properties of the blockchains [15]. Blockchains lay the groundwork for developing decentralized IoT platforms that enable secure data exchanges, and trustless record keeping of the messages exchanged between devices without the need for maintaining high-end servers. In the following sections, we will see how the blockchain technology can play a relevant role in addressing and overcoming some of the aforementioned challenges in different areas of the IoT.

V. IoT Privacy Through Blockchains

A. Privacy Concerns in Centralized IoT Models

The IoT provides new capabilities and convenience at the consumer level. In an example consumer IoT smart home, children watch programs on a smart television. A thermostat maintains 22 Celsius degrees and diverts energy from rooms that are empty. Their parents issue voice commands to the home computer, to turn off the lights. In the background, a smart fridge sends out an order for the next day's groceries. All these convenient services come from a centralized service provider that processes and handles sensor data collected in the smart home. Within this centralized and hyperconnected nature of homes and cities, we see concerns related to user data privacy. The privacy issues in IoT are immense, considering the sheer amount of data being collected, transferred, stored, and undoubtedly sold.

Data collection in IoT has diverse purposes, for example, an organization may lease equipment and collect usage data for billing purposes. The organization can draw inferences about user's preferences and habits from the data itself as well as the associated metadata [89]. Customers in this position place their trust in the organizations providing the Internet-based applications and have little knowledge of what data is being transmitted, or if their data is being shared or sold to third-party entities [90]. The worst-case scenario here would be mass-surveillance programs [91], whereby entities collecting user data can collaborate with 'Big Brother' entities and collect data not relevant to the provided service. Apart from having to place trust on the centralized service providers to not breach their privacy, users also have to trust that data is being transferred with confidentiality and integrity. Any unsecured data transfers can allow malicious parties to eavesdrop and collect data without authorization [92].

Apart from authentication and secure cloud computing, in order to prevent violations of privacy, the challenges involved are implementing policies that ensure data confidentiality, integrity, ownership and governance [93]. Reference [94] advocates for "privacy-by-design," and emphasizes the need for empowering users, and giving them the ability to control the data that is collected and shared. Such a design aims to implement access control policies to evaluate requests and decide whether to allow access to data or not. To combat the privacy violation by a rogue sensor network, current solutions in privacy involve users going through a privacy broker [95], which itself if an intermediary entity between the user and the sensor network that can be subject to threats. Similarly, other techniques to provide privacy to traditionally centralized IoT infrastructures, namely group signatures [96] and ring signatures [97] also use heavily centralized intermeiaries that are vulnerable to security threats. The concept in both group and ring signatures is the same: the user transfers data through a broker as part of a group, so as to mask the user's identity. Another proposed solution for privacy and anonymity in IoT is k-anonymity [98], which is an approach meant to prevent identity disclosure by anonymizing data transmitted. The basic working principle of k-anonymity is to suppress attributes of transmitted database entries such that they are similar to $k-1$ other entries. However, k-anonymity and its variations have been met with critique and are not adequate in guaranteeing privacy for IoT data [99]. The main criticism is that common attributes within a k-anonymized data set can be used to infer personal information within a single entry. For example, in k-anonymized hospital records, common attributes of the patients of a specific disease can be used to disclose the medical information of a specific person with matching common attributes. Considering the significant paradigm shift decentralized ledger technology promises for the IoT, research efforts are underway to determine if private-by-design systems can be developed using blockchain techniques.

B. Blockchain-Based Decentralization for IoT Privacy

In the last few years, decentralization is being explored for issues related to privacy. Alcaide *et al.* [119] presented one of the earlier pre-blockchain solutions for decentralized anonymous authentication, based on cryptographic Zero-Knowledge Proof of Knowledge (ZKPK). However, this solution has received criticism: the protocol is susceptible to attack when an adversary impersonates an actual user in the data collection aspect of the protocol [120]. More recently, blockchains have become the primary candidate technology to decentralize the IoT. Blockchains lay down the foundations of decentralizing networks, and carrying out data transfers securely, without the need of any authorizing and authenticating intermediaries. The immutable record-keeping attributes of blockchains provide a viable solution for governing IoT micropayments and data sharing, so privacy-preserving network design for IoT using blockchain and smart contracts is a fertile and active area of research.

All interactions that take place over the blockchain are publicly available and verifiable, therefore, IoT data stored on-chain as well as off-chain is typically kept encrypted, and policies for authorized access are enforced on the blockchain. The first step to developing private-by-design solutions is to ensure data ownership for IoT users, so that they can exercise control over how their data is accessed and when. Users can also choose to keep their data private and encrypted over a decentralized data storage medium. Towards IoT data ownership, Zhang and Wen [100] propose a tokenized access model where people can issue transactions to IoT data owners for access privileges to their encrypted data. IoT users in this case can exercise complete control over what data they want

to share in exchange for services or monetary incentives, and can perform selective expression of their IoT data. Another proposed solution for allowing private ownership of IoT data, FairAccess [101], [102] provides another solution whereby IoT owners have full control over whom they choose to grant access to their IoT data. FairAccess uses smart contracts which IoT users can use to selectively associate role-based privileges to people requesting access to their data, in exchange for monetary or service incentives. Additionally, [103] and [104] have similar tokenized approaches for granting access to requesters upon the IoT data owner's discretion, while the IoT data in these approaches is store off-chain on Decentralized Hash Tables (DHT).

The PISCES framework [105] aims to provide privacy-by-design through enforcing data ownership and data governance. They define roles of data providers and data controllers, and use a Privacy Validation Chain (PVC) to maintain auditable track of data usage events. The added PVC blockchain ensures that the rights IoT users have over their data are respected.

PlaTIBART [106], is a proposed blockchain-based platform for IoT applications that involve data interactions. It provides the tooling and techniques for deploying and managing IoT blockchain applications in private blockchains. They use private blockchains for its privacy features and fast transaction finality times, as well as implement off-chain communications for private data transfer events. Another off-chain data storage and sharing solution is proposed in [107]. In this case, the authors use a private blockchain to log hashes of data chunks stored in a storage platform based on a trusted execution environment (TEE). Additionally, they consider Intel SGX as part of the TEE to ensure privacy of the IoT data as well as the blockchain application code.

Cha *et al.* [87] propose using blockchain-connected gateways to manage legacy IoT devices and issue data transactions over the blockchain. The blockchain gateway maintains privacy-awareness, while the blockchain stores immutable encrypted records of user preferences. The gateway therefore enhances privacy on the IoT edge with BLE devices.

For cloud computing, the proposed solution outlined in [109] introduce software-defined cloud computing with blockchain based access control for a distributed solution for privacy. Another privacy-preserving access model is described in [110] where blockchains and fine-grained access-control policies allow users to govern their own data. Rahulamathavan *et al.* [111] use attribite-based encryption for sensor data to enable privacy in IoT-cloud ecosystems.

Chen *et al.* [112] propose JointCloud, a cloud-blockchain hybrid approach to ensuring privacy for the IoT. More specifically, they use a private cloud for IoT data storage, and an overlay blockchain for recording all data transfer and IoT interaction events. The JointCloud Collaboration Environment (JCCE) serves as a collaborative medium between private clouds, and consists of the JointCloud Blockchain (JCB) which manages transactions, community and supervision functions through smart contracts. The use of a private blockchain to form a collaborative medium over private cloud storages does add private server maintenance costs, but it does maintain an immutable record of IoT transactions while preserving IoT data privacy.

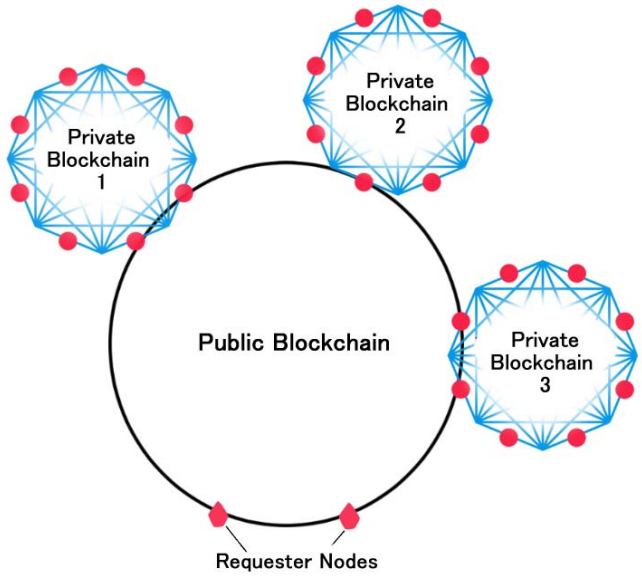


Fig. 3. A tiered architecture with private blockchains connected to a public blockchain. Private blockchain owners can choose to selectively communicate with requester nodes or other private blockchains.

Hardjono and Smith [113] propose privacy preservation in commissioning IoT devices over the cloud, using permissioned blockchains. The authors grant provenance of a resource-constrained IoT device without revealing its identity. This solution is based on the ChainAnchor [121] system that aims to provide pseudonymity within permissioned blockchains using zero-knowledge proof scheme and Enhanced Privacy ID (EPID) [122].

The most promising solution for private-by-design IoT data transfer is using a tiered architecture for blockchains, whereby either multiple private blockchains connect to a public blockchains, or interoperable blockchains are connected together to form a network of blockchains, as shown in Fig. 3. Here, users in separate blockchains can choose to selectively express data to other blockchains. Dorri *et al.* [86] introduce a privacy-preserving architecture where smart home owners can log IoT events in a private sidechain and use cloud storage for IoT data. Users can then choose to share any amount of their encrypted data with others over a public overlay blockchain, according to access-control policies written into the block headers. Smart contracts for access-control was an idea introduced in Hawk [33], which implements programmatic access-control mechanisms via smart contracts. Hawk accounts for sensitive private information and non-sensitive information separately, thus providing varying degrees of privacy-preservation. Conoscenti *et al.* [108] uses peer-to-peer storage to alleviate storage inflation issues within the blockchain. Using a peer-to-peer storage for off-chain data enhances privacy for the IoT user's data. The blockchain stores encrypted hash of the data, and transactional information. Ali *et al.* [114] proposed a multi-layered blockchain architecure, which uses the concepts of smart contract based access

control, as well as peer-to-peer storage. This solution uses IPFS as a distributed storage medium for IoT data.

While power grids are experiencing changes due to a boom in renewable energy solutions, decentralized IoT applications that help to manage transactive microgrids are emerging. Here, blockchains are being researched for use in smart grid applications, where energy sharing applications require privacy, decentralized control, and monetization mechanisms. Aitzhan and Svetinovic [80] use group signatures and off-chain encrypted anonymous message streams to provide privacy in energy trading applications. More recently, Laszka *et al.* [81] proposed a solution towards enabling energy producers to tokenize and trade units of energy with consumers while protecting the energy producers' personal information. The energy producers achieve total anonymity by using new public-private key pairs for every transaction generated and maintained by an autonomous broker. References [82] and [115] use smart contracts to enable privacy and decide tariffs for energy sharing within smart grids in a cost-effective way.

Wang *et al.* [116] propose a privacy-preserving incentive mechanism for crowd sensing applications. The technique used to make crowd sensing streams private is k-anonymity. The authors achieve k-anonymity through node cooperation verification, where k nodes form a group that cooperates to meet the k-anonymity requirements. Despite the inherent shortcomings of k-anonymity techniques, the proposed solution is demonstrated to resist impersonation attacks, however there is no analysis for its protection against collusion attacks.

Recently, a trend to enable privacy in blockchain-based IoT applications is to use pseudonym management solutions. Using fixed singular pseudonymous addressing does not offer adequate privacy, even if the transactions occurring in a network involve transferring off-chain data. Singular blockchain addresses can be traced back publicly and can reveal user identities [123]. Previously, multiple algorithms for updating and changing pseudonymous addresses have been presented, especially for vehicular networks [124]. Recent research efforts have involved developing pseudonymous address management for connected-vehicle privacy using fog-computing [125]. Using a vast number of pseudonyms to mask the identity of a singular vehicle within the Internet of Vehicles (IoV) is proven to boost privacy by a significant margin [126]. Pseudonymous address management in blockchains is being researched to ensure privacy on a transactional level without the need for third party intermediaries. Kang *et al.* [117] propose a privacy preserving solution for secure data sharing in vehicular networks, with privacy preserving features. They use a pseudonymous address updating mechanism which prevents a single vehicle being tied to a singular blockchain address. Further work by Kang *et al.* [83] and Li *et al.* [84] outlines a solution for peer-to-peer energy trading in IIoT and between connected hybrid vehicles, using pseudonymous address updating in a consortium blockchain. They implement a modified version of the proof-of-work consensus mechanism with relaxed constraints, where local aggregators perform block validation and can be held accountable in case of false block creation. Block validation times take up to one minute, and the consortium blockchain acts as a secure medium for conducting energy transactions. Lu *et al.* [127] propose using pseudonymous address updating for privacy in VANETs, while maintaining authorization and messaging records in separate blockchains for added auditability. Gao *et al.* [118] use Hyperledger blockchain to implement a payment mechanism in Vehicle-to-Grid networks, with a registration mechanism and pseudonymous address updating. Their use of Hyperledger PBFT consensus does limit the scalability of the network, but affords higher efficiency and transaction speeds. Separate registration records are maintained, which are only visible to authorized entities for auditability.

C. Blockchain-Based IoT Privacy Solutions in Industry

In industry, an interesting approach to tackle one of the many privacy issues faced by the Internet of Things, is done by the company Lola Cloud,[10] a home intelligence system where users accounts and storage are protected by blockchain smart contracts. COSMOS[11] is a blockchain project in the industry that aims to horizontally interconnect blockchains, so that the contents of one blockchain remain private from the other blockchains it interacts with. Supply chain solutions based on private blockchains aim to maintain immutable private records within the supply chain, inaccessible to external entities. For example, Provenance[12] relies on the auditability of blockchain records to guarantee traceability and transparency of the products in food markets. The supply chain sector is taking advantage of smart embedded devices able to autonomously push data into a blockchain software infrastructure, therefore creating tamper-proof, decentralized records, as is the case of Skuchain[13] and BriefTrace.[14]

D. Summary and Insights

In this section, we learned that since blockchains provide auditability by making all of its contents publicly accessible, achieving privacy becomes a challenge. We discussed recent research contributions towards enabling privacy in blockchain-based IoT frameworks, ranging from proposed solutions that leverage smart contracts in enforcing access policies, to more advanced techniques like tiered blockchain architectures and privacy mechanisms for energy transacting networks. Additionally, pseudonymous address updating is also being researched to boost privacy in blockchain-based IoT on a transactional level. Table IV organizes these contributions in general subcategories of research for privacy in blockchain-based IoT frameworks. From this discussion, we can see that in order to maintain privacy, a public blockchain in itself is not sufficient, since all contents of the public blockchain are visible to the blockchain network participants for the sake of auditability. Therefore, we can infer open challenges like finding an effective balance between auditability and privacy in public blockchains (discussed further in Section XII-A), as

[10] https://lola.cloud/
[11] https://cosmos.network/
[12] https://www.provenance.org
[13] https://www.skuchain.com
[14] https://www.brieftrace.com/

TABLE IV
BLOCKCHAIN-BASED PRIVACY MECHANISMS FOR THE IOT IN RECENT RESEARCH

General Subcategories in Blockchain-Based IoT Privacy	Proposed Solutions	Privacy-Preservation Implemented By
Tokenized Approach for IoT Data Access	Zhang et al. [100]	Tokens for access privileges to IoT data
	FairAccess [101][102]	Smart contract transactions for role-based access privileges
	Enigma [103], Shafagh et al. [104]	Tokens for access privileges to data stored in DHT
Privacy-Preserving Frameworks	PISCES framework [105]	Privacy validation chain (PVC) for verifying data ownership
	PlaTIBART [106]	Private blockchains for logging off-chain communications
	Ayoade et al. [107]	Private blockchain and Trusted Execution Environment (TEE) for data storage
	Cha et al. [87]	Blockchain-connected gateways for managing devices and issuing transactions
	Hawk [33]	Programmable access control policies in smart contracts
	Conoscenti et al. [108]	Permissioned blockchains for validating data store in peer-to-peer storage medium
IoT-Cloud Ecosystem	Sharma et al. [109]	Software-defined cloud computing and blockchains for managing virtual resources
	Zyskind et al. [110]	Governing IoT data on the cloud using fine-grained access policies in blockchain
	Rahulamathavan et al. [111]	Attribute-based encryption for sensor data on the blockchain
	JointCloud [112]	Blockchain-based collaborative environment for private clouds
	Hardjono et al. [113]	Commissioning IoT devices over the cloud through permissioned blockchains
Tiered Blockchain Architecture	Dorri et al. [86]	Private blockchains and an overlay blockchain for managing cloud-data
	Ali et al. [114]	Private blockchains and a public blockchain for transferring IPFS file hashes
Smart Grid and Smart City Applications	Aitzhan et al. [80]	Group signatures and off-chain messaging for energy transacting systems
	Laszka et al. [81]	Autonomous broker for maintaining anonymity of energy producers.
	Knirsch et al. [82], Lombardi et al. [115]	Smart contracts for privately negotiating tariffs for energy transactions.
	Wang et al. [116]	K-anonymous incentive mechanism for crowdsensing applications
Pseudonymous Address Updating and Management	Kang et al. [117]	Pseudonymous address updating for vehicular data exchange
	Kang et al. [84], [83]	Pseudonymous address updating for energy trading in IIoT and connected-vehicles.
	Gao et al. [118]	Registration with multiple addresses for vehicle-to-grid energy trading.

well as maintaining data integrity within private blockchains for tiered blockchain architecture.

VI. TRUSTLESS ARCHITECTURES FOR IOT

A. Issues of Trust in Centralized IoT Architectures

The services offered by the IoT ecosystem are often centered around the cloud computing paradigm where the data from the IoT devices are processed and stored in a cloud infrastructure. However, the IoT ecosystem is affected by the pervasiveness and ubiquity of smart devices, i.e., the devices being closely interactive with the users, collect data which is sensitive and intimate to the user. Even though cloud computing in the IoT ecosystem makes the data widely available and accessible to the users in almost real-time, the data is still mediated and stored by a centralized entity. Given the nature of the data, the assumption of trust the third party requires may lead to breaches of privacy and security in the IoT ecosystem.

Recent research in this area has prompted two research paths: one being strengthening of trustful architecture where more secure algorithms are used to disseminate and store IoT data; and the other being a proposal of "trustless" architectures [139], which relies on a peer-to-peer approach for validation of transactions among participating entities. The first research path aims to add encryption to enhance the trustability of centralized solutions. This can prove to be cumbersome for IoT devices given their resource-constrained nature, which often leads to unencrypted communications or use of simple encryption algorithms. Moreover, the use of more secure algorithms like AES-256 affects the latency of the system and thus dents applications with near real-time requirements. On the other hand, decentralized consensus among a set of peers eliminates the need for trusting any third party services, hence the term "trustless" architecture. A peer-to-peer configuration favors the IoT ecosystem, considering the large number of devices available in a network.

B. Trustless IoT Architectures With Blockchains

The term synchronous with trustless architectures is that of the blockchain. Blockchains maintain an immutable ledger of transactions identically shared among peers in the blockchain as discussed in Section II, thus making them a suitable solution for the centralization problem in cloud computing. Sousa *et al.* [140] study the use of secure multi-party computations (MPC) while leveraging blockchains. The aim of the proposed solution is to create a trustless environment for hyper-localized edge computations in the IoT fog. The

blockchain ensures that the participating entities perform computations on a set of data contributed by the entities without trusting a central authority.

Enigma [103] is a peer-to-peer network which leverages blockchain technology to allow multiple users of the blockchain to store and perform analytics on data while maintaining the privacy of the data. Enigma also leverages the service of a permissionless blockchain to perform public tasks while performing the private computations on its own chain to handle computationally intensive tasks. Liu *et al.* [128] propose a decentralized data integrity verification framework based on the blockchain by the use of smart contracts. The framework allows Data Owner Applications (DOAs) and Data Consumer Applications (DCAs) to verify the integrity of data stored in a cloud infrastructure provider, in a trustless environment. In [129], the proposed solution for improving trust in blockchain transactions is by using javacard secure elements. Instead of using 32 byte secret keys, the authors implement a cryptocurrency smart card designed over the JC3.04 standard platform.

Bahga and Madisetti [130] realize the trustless verification of transactions leveraging blockchains in the Industrial IoT context. Their proposed framework models tasks to be performed on the IoT nodes as decentralized applications on the blockchain. This not only allows logging and storage of the actions performed by the devices (in the form of transactions), but also allows automated maintenance and diagnosis of issues on the nodes themselves. Boudguiga *et al.* [131] propose a decentralized mechanism to push updates on to IoT devices using blockchain. The blockchain is used to record transactions of software updates pushed onto the devices to prevent malicious software updates on the devices. In this case, there is no need for a trusted broker for delivering updates since updates propagated to the devices via the blockchain have guaranteed integrity.

Di Pietro *et al.* [132] aim develop a decentralized trust model for the IoT through a credit-based blockchain they call obligation chain, which has a built-in reputation system. In order to circumvent the transaction delays in traditional blockchains, IoT devices are able to perform transactions on credit, and their ability to pay back their credit adds to their reputation. The obligation chain is a step towards scalable blockchain transactions while enabling end-to-end trust between IoT devices.

IoTChain [133] proposes an trustless IoT architecture where IoT devices register themselves onto a blockchain for securely storing, organizing and sharing streams of data without the need for a trusted intermediary. The authors of IoTChain do not sufficiently address the scalability of blockchains in the use-case where IoT transactions are highly frequent, however they demonstrate trustlessness in end-to-end communication for IoT devices as transaction issuers to a blockchain. In the same vein, Psaras *et al.* [134] propose a edge-centric solution to establish a trustless architecture for the IoT, involving gateways and IoT devices as transaction issuers to the blockchain, while communications between edge devices can take place in a trustless way. In Trustchain [135], Otte *et al.* propose a scalable, Sybil-resistant solution for trustless IoT architecture, while replacing PoW consensus with an alternative mechanism for determining trustworthiness of peers called NetFlow. Trustchain is built on parallel chains that record transactions specific to each participant. Netflow determines whether each peer is actively contributing in maintaining integrity of Trustchain. Trustchain identifies faults when the transactions stored in one chain do not match the corresponding transactions of the other parties involved, and Trustchain refuses further service to the peer responsible for this discrepancy.

Much can be said about how blockchains are used in transparent record-keeping for supply chain IoT use cases. In recent research contributions, [136] outlines a traceable record-keeping architecture for food supply chains. This solution uses BigchainDB [141], a scalable distributed database with blockchain characteristics for publicly available records pertaining to food safety. Reference [137] uses Ethereum smart contracts for trustless and transparent record-keeping for pharmaceutical IoT supply chain use cases. A trustless environment is particularly beneficial in supply chain use-cases, since data related to enterprise solution carries real business value, and a compromised central service provider can lead to business losses.

There have been concerns about the suitability of blockchains to consider IoT devices as nodes participating in the blockchains. This has led to lightweight solutions being proposed for IoT devices and also a move towards edge device based blockchain nodes. Dorri *et al.* [86] propose a lightweight and scalable multi-tier blockchain framework for IoT which allows distributed trust mechanisms among the nodes managing the overlay blockchains as well as distributed throughput management to ensure the allocated throughput for the participating nodes is in coalition with the total available throughput. Samaniego and Deters [138] propose the use of fog layer devices as blockchain nodes instead of the constrained IoT end-devices. Since IoT devices are resource-constrained, the proposed architecture aims to enable trust at the fog layer where more capable nodes are present.

C. Blockchains for Enabling IoT Trust in Industry

Startups are also exploring this issue as a business model, as is the case of Xage Security,[15] with a decentralized approach to provide trust among devices in industrial IoT networks. Their aim is to decentralize industrial control systems to eliminate reliance upon a trusted third party. Ubirch GmbH[16] is currently offering a solution similar to a notary services for the IoT devices and their data, in order to provide trustworthiness on the data, from IoT devices. Multichain[17] is a private blockchain based protocol which offers decentralized access control to devices registered on the blockchain. The protocol runs a decentralized consensus algorithm following a round-robin approval of transactions.

D. Summary and Insights

In this section, we discussed how the "trustless" nature of blockchain record-keeping can be leveraged to create distributed trustless network environments for the IoT. Our

[15] https://xage.com/

[16] https://ubirch.com

[17] https://www.multichain.com/

TABLE V
TRUSTLESS BLOCKCHAIN ARCHITECTURES FOR THE IOT

Proposed Architectures	Main Feature	Trustlessness Ensured By
Enigma [103]	Decentralized data storage and tokenized access control	Permissioned blockchain for local data storage tasks, permissionless blockchain for public tasks
Liu et al. [128]	Verifiable data integrity for application owners and consumers	Permissionless blockchain for recording hash of data
Urien et al. [129]	Cryptocurrency smart cards (CCSC) based on javacard secure elements	Permissioned blockchain and JC3.04 smart cards
Bahga et. al [130]	Automated maintenance and diagnosis for IIoT machines	Permissioned blockchain for recording IIoT interactions
Boudguiga et al. [131]	Secure software update propagation to IoT devices	Immutability of blockchain records
DiPietro et al. [132]	Credit-based blockchain with reputation system	Permissioned blockchains with low latency transactions
IoTChain [133]	Device-to-device communications over blockchains	Blockchain addressing + blockchain immutability
Psaras et al. [134]	Establishing distributed trust through blockchain connected gateways	Blockchain addressing + blockchain immutability
Trustchain [135]	Scalable blockchain-IoT platform using multiple blockchains	Parallel blockchains for every participant
Tian et al. [136]	Traceable record keeping for food supply chains	Private blockchain + BigchainDB immutability
Bocek et al. [137]	Traceable record keeping for pharmaceutical IoT use cases	Blockchain addressing + blockchain immutability
Dorri et. al [86]	Multi-layered blockchain architecture for IoT	Permissioned blockchain for local data storage tasks, permissionless blockchain for public tasks
Samaniego et al. [138]	Blockchain-as-a-Service for the IoT fog	Blockchain addressing + blockchain immutability

discussion covered how blockchains eliminate the need for trusting singular centralized entities in IoT services, including IoT supply chain use cases. Table V lists various proposed mechanisms in recent research for developing trustless architectures for the IoT. This discussion illustrates the potential benefits of decentralizing IoT frameworks using blockchains for improving fault tolerance and guaranteeing trust in IoT interactions.

VII. BLOCKCHAIN-BASED IOT SECURITY

The IoT as it exists today consists of 5 billion devices, and it is projected to grow up to 29 billion by 2022 [142]. As the physical world joins the Internet, the attack surface from known and new threats expands exponentially, resulting in complex security implications [143]. The goal of the IoT is to automate functions while maintaining protection against the threat of a varying range of security attacks. In this section, we will discuss the security threats faced by centralized IoT infrastructures, and how recent research towards decentralizing the IoT has shown potential security benefits of a blockchain-based IoT.

A. Security Issues in Centralized IoT Models

An essential security challenge of the IoT comes from its ever expanding edge. In an IoT network, nodes at the edge are potential points of failure where attacks such as Distributed Denial-of-Service (DDoS) can be launched [144]. Within the IoT edge, a set of corrupted nodes and devices can act together to collapse the IoT service provision, as seen recently in botnet attacks [145]. Identified in August 2016, the Mirai botnet mounted the most potent attack against IoT security, by compromising IoT devices and generating malicious traffic in the degree of Tbps [146]. After the source code of the Mirai botnet was publicly released, more attacks followed, most notably the attack in October 2016, which took many mainstream websites for several hours [145].

Another threat to the availability of IoT service provisioning comes from its heavily centralized configuration [147]. A central point of failure not only is a threat to availability, but also to confidentiality and authorization [148]. A centralized IoT does not provide built-in guarantees that the service provider will not misuse or tamper with users' IoT data. Furthermore, confidentiality attacks arise from identity spoofing and analyzing routing and traffic information. In a data-driven economy, guarantees are necessary to prevent misappropriation of IoT data.

IoT faces confidentiality attacks that arise from identity spoofing and analyzing routing and traffic information, as well as integrity attacks such as modification attacks and Byzantine routing information attacks [149]. Data integrity in the centralized IoT configuration is challenged by injection attacks in applications where decision making is based on incoming data streams. IoT data alteration, data theft and downtime can result in varying degrees of loss. Ensuring security is paramount in a system where smart devices are expected to interact autonomously and engage in monetary transactions. Current security solutions in the IoT are centralized, involving third party security services, as seen in Fig. 4. Using blockchains for security policy enforcement and maintaining publicly auditable record of IoT interactions, without depending on a third party, can prove to be highly benefitial to the IoT.

B. Blockchains for Providing IoT Security

With virtues of decentralized public-key infrastructure, fault-tolerant design, auditability and inbuilt protection against

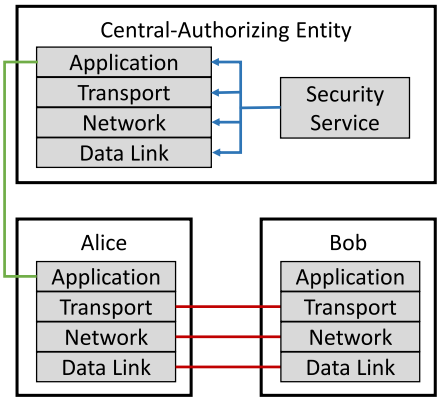


Fig. 4. Security Mechanism Architecture in IoT.

DDoS attacks, blockchains have demonstrated their capabilities in delivering security to transactive networks like Bitcoin.

A blockchain-based IoT solution is resistant to false authentication since all devices issuing transactions have dedicated blockchain addresses. The consensus protocols used in public blockchains prevent malicious actors from launching denial of service attacks since making multiple empty transactions incurs transaction fees [150]. Thus blockchains have the potential to disrupt IoT security mechanisms and provide improved security solutions to the IoT stack.

1) Providing Access Control Through Blockchains: Recent research has seen several proposed solutions for enforcing access control policies in the IoT without relying on a third party service. Blockchains have the potential to improve the availability of security infrastructure for the IoT. Solutions like [151] provide a secure public key infrastructure that is more fault tolerant than centralized solutions. Hashemi *et al.* [152] propose a multi-layer blockchain framework, where data storage and access control are performed in separate layers. The three layers in this framework are: (i) a blockchain-based decentralized data storage where users with specific blockchain address can store their IoT data; (ii) a messaging stream to enable access negotiations between two parties; (iii) access control mechanism for participants of varying roles. Data stored on the blockchain is encrypted which only the participants with access privileges can decrypt.

Zhang and Wen [100] introduce a tokenized approach to performing access control in the IoT through blockchains and smart contracts. The main idea in the paper is to develop a blockchain-based e-business model where users can use custom cryptocurrency to buy temporary access privileges for physical or digital assets. In the case of accessing Alice's IoT data, Bob can buy the custom IoTCoin cryptocurrency, pay Alice with an agreed upon amount, and receive the key to decrypt and access Alice's data for a limited period of time. Another tokenized approach to access control is outlined in [102], where users are assigned different roles, and access control policies written into smart contracts can be used to grant or revoke access privileges for an IoT user's data. Similarly, [153] and Enigma [103] store chunks of encrypted data in the blockchain and uses a tokenized approach and smart contract policies for allowing and revoking access to stored IoT data. Another similar access control model is propose in [154], whereby IoT users can grant and revoke access to stored chunks of IoT data by means of functions written in smart contracts. Es-Samaali *et al.* [155] use an overlay blockchain to provide an access control mechanism for big data. They use programmable smart contracts to inform authorization decisions for big data access requests.

In approaches that aim to reduce transaction fees or design applications without tokenization, access-control policies can be written into the blockchain to manage access privileges and detect malicious activity. This is the solution proposed in [86], where the authors use local blockchains connected to a public overlay blockchain. Access privilege decisions are stored within the blockchain which makes them publicly verifiable, and thus it becomes easy to detect unauthorized access attempts. Ali *et al.* [114] further that idea by dropping any transactions being issued from an anauthorized adversary, or by removing the adversary from the blockchain network altogether. The challenge in developing public blockchains without tokenization is the fact that the network becomes open to Sybil attacks, where users can launch a DOS attack by issuing smaller amounts of empty transactions with multiple blockchain addresses. To avoid Sybil attacks, the authors propose enforcing global policies for participation in the blockchain.

Shafagh *et al.* [104] propose an blockchain-based access control solution for data stored in off-chain Decentralized Hash Tables (DHT). The blockchain in this solution stores access privileges for different users for any stored data in the DHT. DHT nodes lookup the blockchain records to make access control decisions.

2) Maintaining Data Integrity Through Blockchains: To launch a modification attack in a blockchain-enabled IoT architecture, an adversary would attempt to alter the records in the blockchain, or create false blocks in the blockchain, either containing false transactions, or censoring transactions that have occurred. This is near impossible in public implementations of the blockchain, where canonical records of the blockchain are maintained by means of distributed consensus. This further makes the case for decentralizing the IoT using blockchains, since properties inherent to the blockchain prevent attacks that compromise data integrity [162].

Biswas and Muthukkumarasamy [156] propose a blockchain-based smart city solution whereby the integrity of the stored data is guaranteed through the blockchain's inherent immutability features. The solution proposed uses an Ethereum blockchain with smart contracts to define programmability on top of the decentralized blockchain records.

Dorri *et al.* [86] use a multi-tiered blockchain framework to maintain a record of chunks of IoT data stored in the cloud. The public overlay blockchain in this solution uses hashing to maintain an immutable record of the stored data chunks in the cloud. Similarly, [114] use the blockchain to store hashes of IPFS files that contain IoT data. Since files in IPFS are content-addressed with their hash, the contents stored in IPFS are tamper-proof.

Enigma [103] and Shafagh *et al.* [104] propose data storage solutions based on Decentralized Hash Tables (DHT) and immutable blockchain records. Data requests go to DHT nodes while the blockchain ensures integrity of access control policies and the stored data itself.

A blockchain-based data integrity service is outlined in [128], where query-based integrity checks can be performed without third-party verification. Here, the blockchain is used as an added layer for providing security and integrity to data objects stored on the cloud. Issuing queries and verifying the blockchain records are used to detect any loss of data integrity.

Yang *et al.* [157] proposed a blockchain-based credibility assessment mechanism for the Internet of Vehicles. The proposed solution consists of a blockchain-based reputation system which decides the credibility of the messages received based on the reputation of the sender.

Secure software updates for the IoT by applying blockchains in IoT is receiving research attention. In [158], embedded IoT devices receive secure firmware updates in a blockchain network. The proposed scheme uses peer-to-peer technology for delivering firmware updates and ensures the integrity of the firmware installed in embedded devices. Steger *et al.* [159] is a proof of concept for secure software update distribution in smart vehicles, using a tiered blockchain architecture for scalability. The authors use the multi-layered architecture from [86] and propagate software updates securely to the vehicles without compromising integrity. Similarly, Boudguiga *et al.* [131] use permissioned blockchains to store software updates within transactions, so IoT devices can receive updates in a secure, peer-to-peer fashion.

3) Ensuring Confidentiality Through Blockchains: The blockchain has inherent addressing involving public/private key pairs, therefore, blockchain-based applications have built in authorization and confidentiality features since each transaction is signed by the issuer's private key. Axon *et al.* [151] leverage a blockchain-based PKI to manage IoT devices. They used smart contracts that issued commands to the IoT devices using their blockchain addresses. These commands range from changing working policies, to recording energy usage information onto the blockchain.

Aitzan and Svetinovic [80] propose a confidentiality solution for energy transacting smart grids. The aim is to not only keep the information shared between two parties confidential, but to also hide the identity of the energy producers. In this regard, the authors suggest a mechanism for generating and altering blockchain addresses for the energy producers, so as to hide the producer's identity altogether. The solution does not aim for absolute decentralization because it uses Distribution System Operators (DSOs) to manage security among the producers and consumers as an automated intermediary.

Alphand *et al.* [160] proposed a solution which is a platform for IoT security management. It is built on a blockchain that enforces authorization policies and maintains interaction records, and the OSCAR (Object Security Architecture for the IoT) [163] security model, using a group key scheme. The authors use OSCAR to set up authorized multi-signature groups, and the blockchain for flexibly setting authorization rules and maintaining an immutable records of all access events.

Cha *et al.* [87] use an Ethereum blockchain to maintain confidentiality between IoT gateways. The gateways are designed to manage BLE devices like wearables and smart factory devices. The gateway manages the connected BLE devices and interacts with them using smart contracts, on behalf of the user. The gateway maintains information pertinent to the devices and all interactions with the IoT remain confidential under blockchain-based signatures.

Multi-tier solutions like [86] maintain access control policies within the blockchain header, while all users with access privileges receive encrypted chunks of data from the off-chain data storage mechanism. Reference [114] is a similar multi-tier solution that uses IPFS as the off-chain storage mechanism. Whenever a data requester is granted access to IoT data stored in an IPFS file, they are given the key to accessing the file. The key is encrypted using the requesters public key, which only the requester can decrypt, thus confidentiality is guaranteed using blockchain-based PKI.

FairAccess [102] uses a tokenized approach where issuing transactions with a custom cryptocurrency allows access privileges to a user's IoT data. These access granting transactions are signed with the requester's private key, therefore granted and revoked access privileges remain confidential. Reference [113] is an approach for commissioning cloud-based IoT resources. It uses a permissioned blockchain, and all data transferred to and from a commissioning party are kept confidential under blockchain-based PKI.

4) Improving IoT Availability With Blockchains: The proposed blockchain-based security solutions discussed above provide improved availability in the IoT by decentralization properties inherent in blockchains. Solutions that provide on-chain data storage have built-in features for availability, since there are no central points of failure. Off-chain storage solutions have improved availability its interaction records, however the availability of the stored data is dependent upon the off-chain storage mechanisms used. Here, we will discuss some of the proposed solutions that have unique design elements that add to the availability of the IoT. Alphand *et al.* [160] demonstrate a blockchain-based authorization mechanism for the IoT with a higher degree of liveness due to the inherent features of the blockchain, paired with the OSCAR (Object Security Architecture for the IoT) [163] security model.

Chakraborty *et al.* [161] proposed a multi-layered blockchain solution to handle security issues with resource-constrained IoT devices. The nodes in the lower layers are resource-constrained IoT devices that are incapable of enforcing security policies, while the higher layer nodes are devices with higher computational and storage capabilities. The lower layer devices communicate with eachother via the higher layer nodes. Since the higher layer nodes are in a blockchain network which has inherent decentralization and fault-tolerance properties that guarantee liveness of the solution. Ali *et al.* [114] also use a multi-layered blockchain approach, as well as smart contracts to provide access control functionality. For IoT data storage, they use IPFS as an

off-chain storage platform. At the upper tier they use a public Ethereum blockchain, which has ensured availability considering the thousands of Ethereum nodes that are live at any given moment of time. At the same time, the off-chain storage IPFS provides further availability since IPFS itself is a decentralized storage medium and has multiple peers live in perpetuity.

Bahga and Madisetti [130] has IoT devices with blockchain addresses in a blockchain network. The aim is to develop a blockchain-based manufacturing and smart factory system. Since each device is on the blockchain, users can issue manufacturing commands directly to the devices as transactions. These transactions can range from on-demand manufacturing, to machine diagnostics, to supply chain tracking. The authors present a machine maintenance and diagnostics use case. The decentralized nature of connected devices help the network stay live in the event of multiple faults in machines, and in the event of a fault, the remaining live devices can report it.

C. Industry Solutions for Blockchain-Based IoT Security

Security in the Internet of Things is already being addressed by startups using blockchain. SmartAxiom,[18] for example, proposes an edge-oriented software based on blockchain technology, for the identification and authentication of devices, as well as data integrity and privacy. In logistics and supply chain use cases, blockchains can be used to provide secure logistics information to clients [164]. For example, BlockVerify[19] is a company focused on providing anti-counterfeit measures for their clients. Filament,[20] a blockchain startup is making strides towards IoT security through blockchains, and has recently developed a "blocklet" chip for Industrial IoT devices that connects them to blockchain networks.

D. Summary and Insights

Immutable records and distributed consensus are inherent virtues of blockchains that secure cryptocurrency networks against an array of security threats such as DDoS attacks, modification attacks and double spending. This section outlines recent research efforts carried out in leveraging the inherent features of blockchains to provide security to the IoT. Table VI categorizes recent blockchain research publications by the areas of IoT security that they address, to illustrate how blockchains prove to be beneficial in IoT security. These areas include access control, data integrity, confidentiality, availability and secure software update propagation.

VIII. IoT Identity Management Through Blockchains

Since the inception of IPv4 in the 1980's, the serious issue of its addressing scalability was not considered and has recently run out of IP addresses to be assigned to IoT devices. The new IPv6 provides a theoretical maximum of 3.4×10^{13} IP addresses. This vast address space enables the IoT's explosive growth, yet from a security perspective, managing the identities of IoT devices and users remains a critical challenge. While IPv6 allows for every IoT device to have a unique identifier, the widespread usage of proxies and DHCP can hinder accountability and interoperability between devices.

In IoT, devices have relationships with real persons as well as with other devices. Devices can have a change of ownership from person to person, and different people can have access to a device at varying amounts of time. Identity management involves processes related to authentication and authorization, that are necessary to prevent usage without access privileges.

A. Traditional Identity Management Mechanisms in IoT

In the traditional Internet, identity management solutions such as SAML [171] and OpenID [172] incorporate authentication methods, to prove identities and to provide secure channels. Open ID and SAML provide a decentralized method for authentication, but do not enable two parties to engage without an authorizing third party. A SAML or OpenID identity provider is required so that users can sign up for online services. While there is no single central authority for OpenID or SAML, third party identity providers perform authentication and therefore, users are mandated to place their trust on third party entities for authentication.

Classical mechanisms for authentication (user ID and password combinations) often do not work in the IoT. In cases where users are not involved, devices authenticate themselves with tokens or security certificates. Furthermore, in many cases, the protocols used in IoT do not necessarily fit the TCP/IP stack. Over the course of the development of IoT, certain protections have been put in place to prevent identity abuse. OAuth 2.0 [173] is an open authorization framework that has been widely used for IoT applications. OAuth uses tokens to grant or revoke access to specific online applications. Despite its merits in managing IoT device identities, the common issue of traditional identity management solutions is the lack of guaranteed trust and reliance upon third party authorizing entities. In the case of OAuth, this is the Authorization Server, that controls the issuance and revocation of tokens.

For current identity management protocols in the IoT, interoperability is an ongoing challenge. Interoperability becomes difficult in the presence of multiple protocol options, cross-platform architectures, and variations in semantics and conformance. Traditional centralized naming systems like DNS do not serve the IoT well, and IoT identity management systems need to cope with the unique and inherent requirements of the IoT while managing the identities of a huge number of heterogeneous devices.

B. Blockchain-Based ID Management for IoT

A blockchain-based IoT ecosystem would provide identification for every device, that can be used as a watermark over all the transactions a device makes. The IoT, and as an extension, the Internet, can benefit greatly by blockchain identity management solutions. The most pronounced benefits are distributed trust and security since blockchains render centralized authenticating servers irrelevant.

While multiple startup companies have identity management applications in varying stages of development,

[18] http://www.smartaxiom.com
[19] http://www.blockverify.io/
[20] http://www.filament.com

TABLE VI
BLOCKCHAIN-BASED MECHANISMS FOR IOT SECURITY IN RECENT RESEARCH

General Areas for IoT Security Through Blockchains	Proposed Solutions	Main Feature Used
Access Control	Axon et al. [151]	Blockchain-based PKI
	Hashemi et al. [152]	Separate blockchains for data storage and access control
	Zhang et al. [100], FairAccess [102]	Tokenized access privilege for off-chain data
	Novo et al. [153], Enigma [103]	Tokenized access privileges for on-chain data
	Capchain [154]	Smart contract functions for access control
	Hamza et al. [155]	Overlay blockchain for access control in big data
	Dorri et al. [86]	Access control policies written in block headers
	Ali et al. [114]	Access control policies for IPFS files written in smart contracts
	Shafagh et al. [104]	Smart contracts for access control for data stored in DHT
Data Integrity	Biswas et al. [156]	Tamper-proof blockchain records
	Dorri et al. [86]	Multi-layered blockchain maintaining records of cloud-based data
	Ali et al. [114]	Sharing keys in blockchain transactions for IPFS content addressing
	Enigma [103], Shafagh et al. [104]	Tamper-proof blockchain records of data stored in DHT
	Liu et al. [128]	Blockchain-based querying for verifying integrity of cloud-based data
	Yang et al. [157]	Blockchain-based reputation system for credibility of incoming messages
	Lee et al. [158]	Blockchain transactions for propagating updates to embedded devices
	Steger et al. [159]	Making software updates available to smart cars using overlay blockchain
	Boudguiga et al. [131]	Storing software updates in the blockchain for IoT devices
Confidentiality	Axon et al. [151]	Blockchain-based PKI
	Aitzan et al. [80]	Distribution System Operators (DSOs) to maintain blockchain addressing
	Alphand et al. [160]	Smart contract security policies, with OSCAR security model
	Cha et al. [87]	Gateways for enabling interactions between blockchain-connected BLE devices
	Dorri et al. [86]	Encrypted data shared with participants over multi-layered blockchain architecture
	Ali et al. [114]	Encrypted IPFS file hash shared with participants over public blockchain
	FairAccess [102]	Access privileges granted with signed cryptocurrency transactions
	Hardjono et al. [113]	Permissioned blockchains for commissioning IoT resources
Availability	Alphand et al. [160]	Blockchain-based fault tolerance for authorization model
	Chakraborty et al. [161]	Connecting IoT devices via nodes of a fault-tolerant blockchain network
	Ali et al. [114]	Transactions for IPFS file access over public Ethernet blockchain
	Bahga et al. [130]	Smart-manufacturing devices connected to a blockchain network

proposed solutions have emerged in recent research publications for managing identities of connected devices in the IoT. Reference [151] highlights the potential benefits of PKI without single points of failure by using blockchains. This study demonstrates varying levels of privacy-awareness that can be achieved with blockchain-based PKI.

Laszka *et al.* [81], Imbault *et al.* [165], and Kikitamara *et al.* [166] propose identity management systems based on blockchains for transacting energy systems. Table VII details the technique these solutions use for identity management. Applications like these contribute to the vision of an open model energy sharing system, and to the goal of developing smart grids with renewable energy.

In [167], the proposed solution for hosting IoT devices on the cloud calls for identity management, and the authors detail their findings on performance analysis in blockchain deployment over IBM Bluemix. They use blockchain-based addressing to host virtual IoT resources, that users can transact with using their specific blockchain address. Kravitz and Cooper [168] use permissioned blockchains to propose a solution for distributed identity management. Since all participants in a permissioned blockchain have to be known, a participant makes their identity known and linked to their blockchain address, which can then be used for IoT interactions. This does not allow for anonymity, but for specific enterprise-level IoT applications, it is a viable decentralized identity management mechanism. Huh *et al.* [169] implemented an identity management system for interconnected devices using Ethereum smart contracts. They implement smart

TABLE VII
BLOCKCHAIN-BASED IDENTITY MANAGEMENT MECHANISMS

Mechanisms/Frameworks	Main Identity Management Technique	Anonymity
A privacy aware blockchain-based PKI [151]	Blockchain-based PKI	Pseudonymity
Blockchain-based multi-signature transacting system [81]	Multi-signatures and anonymous message streams	Anonymity
Blockchains for managing energy systems [165]	Pseudonymous blockchain addressing	Pseudonymity
ID management on blockchain for energy system [166]	Federated identities or user-centric identities	Hybrid
Blockchain for hosting IoT edge devices [167]	Blockchain addressing for software-defined IoT resources	Pseudonymity
Permissioned blockchains for securing identities and transactions [168]	Permissioned blockchain addressing	None
Blockchain-based platform for managing IoT devices [169]	Ethereum smart contracts for maintaining identities	Pseudonymity
Blockchain identities as a service [170]	Blockchain identities for authentication	Pseudonymity
Cryptocurrency smart cards (CCSC) for identity [129]	Smart cards developed on the JC3.04 standard platform	Anonymity

contract programmability for managing keys in a fine-grained fashion.

Lee [170] propose a blockchain-based identity and authentication management system for mobile users as well as IoT devices. Their proposed solution involves generating and maintaining blockchain identities as a service, without any considerations for interactions or communications through the blockchain. The blockchain-based identities in this case are only meant for decentralized authentication purposes. Urien [129] propose a unique identity management solution for a blockchain-based IoT. They developed cryptocurrency smart cards (CCSC) based on javacard secure elements. The smart card, developed on the JC3.04 standard platform provides improved security compared to 32 byte keys typically used in blockchain networks.

C. Blockchains for IoT ID Management in Industry

Identity management is a challenge being actively worked upon in blockchain research and development. Early contributions like Kalodner *et al.* [174] aimed to provide a distributed domain naming system for the Internet using blockchains. Several startups are developing solutions for blockchain-based identity management for online entities, including IoT devices. ShoCard [175] is an identity verification platform built on a public blockchain, where users can verify their blockchain ID simply by passing their card over a sensor. Thus, ShoCard provides an identity solution for humans by leveraging IoT and blockchains. A startup that aims to provide identity management for IoT devices is Uniquid [176], a platform for access and identity management for devices, cloud services, and humans. Furthermore, Chronicled[21] is a company that is using the IoT and blockchain to provide digital identity to physical products, while Riddle and Code[22] offers its own hardware and software stack to provide any physical object with a unique tamper-proof identity. These solutions are independent of tokens, certificates or IP addressing and instead rely on blockchain addressing that has tamper-proof logging for every interaction a specific address is involved with.

Apart from identity management specifically for the IoT, companies are endeavouring to create blockchain-based identity management systems in the healthcare domain. Here, the main use of the blockchains consists in providing decentralized data repositories where all kind of sensitive information (e.g., personal data, Electronic Health Records (EHR), Protected Health Information (PHI) etc.) can be stored in a secure and private way, with total control of the owner, following strict standards, such as the Health Insurance Portability and Accountability Act (HIPAA) [177] o the European Data Protection Directive 95/46/EC [178]. However, since these consolidated, secure and trusted user/patient records represent also a valuable asset, companies are creating virtual marketplaces engaging external stakeholders (e.g., research institutions, pharmaceutical companies). In this way, users can anonymously trade their personal information in exchange for rewards. This is the case, for instance, of DocAi,[23] a platform focused on collecting personal information at large scale, in order to build predictive machine learning-based models for health analytics, with strict access control policies. Also, GemOS[24] is using blockchain to consolidate personal data from several sources, allowing the user/patient to securely store and share their information, meeting HIPAA compliance.

D. Summary and Insights

This section outlines identity management for the IoT using blockchain-based solutions. We discussed different proposed identity management solutions from recent research, with varying degrees of anonymity and multiple key techniques for managing IoT device identities. Table VII enlists the aforementioned research outcomes against the techniques used for addressing and managing IoT identities. These techniques include simple blockchain addressing, as well as multi-signature transactions and identity management through smart contracts.

IX. BLOCKCHAINS FOR IOT DATA MANAGEMENT

Research challenges in IoT remain open for storing and handling data produced by smart objects which surpass the human

[21] https://chronicled.com/
[22] https://www.riddleandcode.com
[23] https://www.doc.ai
[24] https://gem.co

TABLE VIII
DATA MANAGEMENT SOLUTIONS WITH TRADITIONAL IOT INFRASTRUCTURE

Framework/Mechanism	Heterogeneity	Integrity	Architecture	Storage
Service-oriented data management framework [179]	✓	✓	Centralized	Local/Cloud
A data-centric framework for deploying IoT applications [180]	×	×	Partially Decentralized	Cloud
Gem: A large-scale object-based storage platform [181]	×	✓	Partially Decentralized	Cloud
An architecture based on IoT to support mobility [182]	×	✓	Centralized	Local/Cloud
Large data management in IoT applications [183]	×	×	Centralized	Cloud
A storage solution for massive IoT data based on NoSQL [184]	✓	×	Partially Centralized	Cloud
Frequently Updated, Timestamped and Structured (FUTS) framework [185]	✓	×	Centralized	Cloud
Efficient storage of multi-sensor object-tracking data [186]	✓	×	Partially Decentralized	Cloud
A unified storage and query optimization framework for sensor data [187]	×	✓	Partially Decentralized	Local/Cloud
IoT data management methods for publish/subscribe services [188]	✓	✓	Partially Decentralized	Cloud

population. Recent research efforts have attempted to develop frameworks and mechanisms to manage the sheer volume of data generated in the IoT.

Data management in the IoT involves online data aggregation while providing event logs, auditing, and storage, for offline query-processing and data analysis. Thus, data management systems are required to have live dual operations in communication as well as storage. Any data management system for the IoT should be able to abstract complex semantics for high-level IoT applications since unprocessed IoT data faces non-uniformity and weak semantics [193]. In many IoT architectures, semantic processing for data is done via middleware, a layer considered between network and application layer [194]. In addition to this, many IoT application domains are time-critical, therefore processing IoT data in a timely manner is important while considering the constrained capabilities of IoT devices.

A. Data Management Solutions for Traditional IoT

Here, we survey some of the recent data management solutions IoT based on the current IoT infrastructure and highlight the gaps where blockchain can be put to use to provide data management services required of the IoT. Data management solutions based on the current IoT infrastructure generally follow a design trend where IoT data is handled in a centralized fashion. The table highlights whether the data management frameworks have in-built measures for ensuring data integrity and for catering to the heterogeneity of IoT data.

Centralized solutions based on the current IoT infrastructure range from service-oriented [179] to data-oriented [180] approaches, as well as from being able to handle large amounts of data [181], [183] to handling mobility in IoT data [182]. Despite their merits, the problems seen in these centralized approaches is that they do not simultaneously provide guarantees for data integrity and trust in handling heterogenous IoT data, as seen in Table VIII. Data management solutions based on the Frequently Updated, Timestamped and Structured (FUTS) framework [185] handles timestamping for data generation events, but are heavily centralized. The common factor among these data management solutions are that they do not have inherent features that provide a layer of security and trust that is necessary in handling IoT data.

Some data management solutions for the traditional IoT infrastructure suggest a partially decentralized approach by using clusters of distributed database services [184], [186]. Li *et al.* [184] leverage NoSQL databases for storing heterogenous IoT data and for different types of querying for IoT data. As a similar approach in using distributed storage, [186] uses an HDFS cluster, which does increase the scalability of handling IoT data, but does not provide guarantees of tamper-resistance. Another partially decentralized approach with similar shortcomings is to use sub-servers to enable better scalability [187], [188]. These solutions do address the bottleneck of centralized data management systems, but they do not guarantee liveness equivalent to a blockchain network, and they do not provide trustlessness in data management for the IoT.

B. Proposed Blockchain-Based IoT Data Management Solutions in Research

While latency and scalability remain an open challenge for data storage within blockchains, using blockchains to design data management frameworks for IoT has the benefits of globally enforced data integrity and a non-dependence on semantics for logging IoT data creation events. With distributed storage mechanisms like IPFS working alongside blockchains, the bulk of IoT data can be stored off-chain, while maintaining immutable logs and links to the data within the blockchain. Blockchain-based solutions are envisioned to be at least partially distributed, where the IoT data of users is kept private and secure, without third-party handling for service provision.

Multiple works in recent research leverage on the main blockchains features to improve data management for the IoT. Reference [189] leverage the immutability and auditability of blockchain records, while storing collected data from drones using traditional cloud service. While the storage of data itself can be made decentralized using distributed databases, the main benefit the blockchain brings here is guaranteed tamper-proofing and data integrity.

Similarly, [104] leverage auditability of blockchain records to facilitate sharing of stored data without authorizing intermediaries. Their proposed solution is built on three layers, which are: (i) a cloud data storage based on off-chain Decentralized

Hash Tables (DHT); (ii) an access control blockchain-based mechanism for the IoT data stored in the DHT, and (iii) the IoT-edge devices. DHT nodes query the blockchain for access privileges when it receives a data request.

Azaria *et al.* [190] propose a framework for storing medical records, using blockchain solely for maintaining records and querying, while using existing IoT data storage mechanisms for hosting IoT data. Approaches that keep storage responsibilities off-chain greatly reduce the storage requirements for hosts that maintain full copies of the blockchain.

Similar solutions with off-chain storage hold the most promise towards a distributed data management mechanism for the IoT. Reference [86] is a multi-tiered cloud-blockchain hybrid architecture for providing IoT data storage. In this solution, private blockchains connected to an overlay public blockchain use cloud-based solutions for storing and retrieving blocks. The proposed architecture in [114] uses the IPFS distributed storage mechanism to store IoT data, while the hashes of stored IPFS files are recorded in the blockchain. IPFS files are addressed using the hash of the file itself, so data integrity is ensured.

FairAccess is a multi-layered framework that focuses on privacy, reliability and integrity in its design as a blockchain-enabled IoT architecture [101], [102]. Fairaccess has transaction definitions for granting and revoking access to users' IoT data, for decentralized access control. For storage, FairAccess adds a separate storage layer where data is stored in off-chain, decentralized storage systems.

Enigma [103] utilizes a network of nodes running a DHT for storing IoT data in off-chain storage spaces. The data is accessible via the blockchain, with access-control policies written into the blockchain. The difference between Enigma and the solution proposed in [104] is that the latter uses key-value pairs, where the key is the user ID and the value is the encrypted chunk of data.

Xu *et al.* [191] propose a blockchain-based storage system called Sapphire, built on smart contracts for IoT analytics. In Sapphire, data from IoT devices is stored as objects with attributes that can be queried for analyzing specific application data. Sapphire parallelizes smart contract execution over the computational power available to it through varying IoT devices. The benefit of this is more readily available analytics on IoT data without extensive IoT data transfer. Sapphire has multiple roles for different IoT devices (super, regular and light) that classify nodes based on their capabilities and constraints. Light nodes have low computational and storage capabilities and do not host a complete copy of the blockchain, and instead simply issue transactions to the blockchain maintained by the super and regular nodes.

Missier *et al.* [192] propose using the Ethereum blockchain for securely transferring IoT data stored in Oraclize.[25] Retrieving IoT data from Oraclize through broker accounts on the Ethereum blockchain carries with it extra transaction costs.

Researchers at CSIRO Australia propose a data integrity service powered by blockchain [128]. The service provides querying to verify the integrity of IoT data stored in the cloud, without the need for a third party to perform any verification.

C. Blockchains for IoT Data Management in Industry

The startup Datum,[26] offers a platform based on a NoSQL database backed by a blockchain ledger that provides high performance data handling for the IoT. Datum leverages the programmable logic of Ethereum smart contracts, and distributed storage platforms IPFS and BigchainDB. The platform aims to deliver secure and anonymous storage of structured data from social networks and IoT devices such as wearables and smart homes.

D. Summary and Insights

At their core, blockchains are distributed databases with distributed consensus on the new entries added to them. In contrast to traditional data management solutions, blockchains have inherent features for guaranteeing fault tolerance, and for eliminating the need to trust a central or third party entity. However, simply using public blockchains as distributed databases is not a viable solution for the IoT, because IoT applications generate high volumes of traffic and are often time-critical. Therefore, there is room for developing data management solutions for blockchain-based IoT frameworks. Table VIII outlines solutions that were targeted towards centralized cloud based techniques, and Table IX contains blockchain-based frameworks for managing IoT data. For blockchain-based decentralized approaches, recent research contributions propose solutions that include high throughput record-keeping in private blockchains, and off-chain data storage solutions with management functions assigned to the blockchain. From recent research efforts, we also gain insight on how blockchains can be used to ensure data integrity and transparency in applications that require auditable records.

X. Monetization of IoT Devices or IoT Data

The Internet of Things ecosystem has grown leaps and bounds in the technological context with the recent advances in this field. However, the extension of the IoT ecosystem from being valued as a technology platform to being valued as a business model faces quite a few challenges. These challenges include the lack of standardization and interoperability among different vendors, which acts as a barrier to large-scale implementations. The unstructured nature of the architecture also plays a key role, making it cumbersome to define roles and pertinent business policies in the IoT ecosystem.

Few articles in the existing literature have attempted addressed this problem. Reference [208] proposes an ecosystem-based business model instead of a firm-based business model. The ecosystem business model takes into consideration the overall values of the entire IoT ecosystem instead of fragmented individual values of the different roles or actors in the ecosystem. Understanding the relationships between entities in the ecosystem is such a holistic way leads to an evolution in how the business model is designed. On the other

[25]https://docs.oraclize.it/

[26]https://www.datum.org

TABLE IX
PROPOSED BLOCKCHAIN-BASED DATA MANAGEMENT SOLUTIONS FOR THE IOT IN RECENT RESEARCH

Framework/Mechanism	Heterogeneity	Integrity	Architecture	Storage
Framework for drone data management using blockchains [189]	✓	✓	Partially decentralized	Cloud/On-chain
Blockchain-based auditable data storage and sharing framework [104]	✓	✓	Decentralized	Cloud
MedRec [190]	×	✓	Decentralized	Local/On-chain
FairAccess [101]	✓	✓	Decentralized	Off-chain
Lightweight scalable blockchain for IoT [86]	✓	✓	Decentralized	Cloud/off-chain
Enigma [103]	✓	✓	Decentralized	Off-chain
Decentralized personal IoT data protection using blockchains [110]	✓	✓	Decentralized	Off-chain
A blockchain-based big data access model [155]	✓	✓	Decentralized	Cloud/off-chain
Sapphire [191]	✓	✓	Partially decentralized	Cloud/off-chain
IoT data privacy through blockchains and IPFS [114]	✓	✓	Decentralized	Off-chain
Data integrity verification service [128]	✓	✓	Partially decentralized	Cloud/off-chain
Managing Oraclize data with Ethereum [192]	✓	✓	Decentralized	Off-chain

TABLE X
IOT VENDORS AND SERVICE PROVIDERS

Type of vendor/provider	Vendor name
Hardware vendor	Libelium[195], Huawei[196], Qualcomm[197], LG[198], Samsung[199], Cisco[200]
Software vendor	Carriots[201], Cisco[200], Eurotech[202], IBM[203]
End-to-end provider	Blueapp.io[204], Huawei[196], Carriots[201], Eurotech[202], Ericsson[205]
Connectivity provider	Deutsche Telecom[206], Vodafone M2M[207]

hand, [209] defines the IoT business model as a multi-faceted market where the different entities involved in the ecosystem can serve multiple sides of the market and play multiple roles in the business model.

The IoT ecosystem can be perceived as a three-tier architecture, which involves the data producers in the form of the end-devices or the 'Things', connecting to IoT gateways which in turn relay the data to the highest layer, the cloud platforms which act as data consumers processing and analyzing the data for gathering meaningful information. The roles in this architecture can be defined as the following, the device owner and gateway owner deploying the end devices and the gateway respectively followed by the cloud platform owner responsible for offering services on their platform. This model ensures that the device and gateway owner can deploy their hardware while offering their data to the platform owners to compensate for their deployment costs. Similarly, the cloud platform can offer their processing and storage services to consumers without having to worry about the hardware deployment costs of the gateway and the end-devices. This is how we can comprehend the IoT business model as an ecosystem as defined by [208].

A. Monetization in Centralized IoT

The types of vendors in the IoT business models can be classified into four categories namely software vendors, hardware vendors, end-to-end service providers and connectivity providers. The hardware vendors sell devices and gateways as well as add-on modules for different IoT use-case applications like smart grid and smart city among others. On the other hand, software vendors offer services that run on the back-end of the system on the cloud platforms and gateways primarily involving management of data and devices along with processing and analysis of data. End-to-end providers offer all the components in the IoT architecture from the end-devices to the cloud platform thus relieving the consumer of the underlying complexity of device-cloud connectivity. Finally, the connectivity providers offer modules for communication among the different tiers of the IoT architecture leveraging various communication standards including BLE, LoRa, and NarrowBand IoT among others. Thus, an end-to-end provider can serve as both the software vendor and the hardware vendor. Moreover, the hardware vendor for the devices might deliver connectivity as well serving multiple sides of the market along the lines of the service model illustrated by [209]. A list of IoT vendors is depicted in Table X with their corresponding vendor types. The presence of a specific vendor in multiple rows can be comprehended as a multiple-side provider of the market [210].

Other than the business models mentioned above, the monetization of data plays a key role in the IoT ecosystem in the form of data-ownership and sharing. The data generated by the IoT devices is usually context-rich in nature and thus can be valuable to vendors. On the other hand, the data shared along with its context can lead to exposure of personal data especially in use-case applications like smart health and domotics. A survey conducted by Fortinet [211] on data privacy concerns among consumers in the smart home scenario, depicts a majority of the respondents consider data privacy to be a sensitive issue while also expressing a desire to have control

on their own data and the flow of data to different entities. Perera *et al.* [212] has laid out the privacy challenges involved in this context which include user content acquisition over data-sharing as well as control and customization of the content being shared.

Two business models are prominent in this scenario, first, where the owner of the data offers their data in exchange of services offered by a third party provider or the owner pays to keep his data protected while using the same services. These models rely on analytics to sell IoT data for targeted advertisement. These business models do not provide client-side services therefore users willingly surrender their data to third-party service providers. Users are not afforded ownership of their data and do not have the option to monetize and benefit from their IoT resources.

B. Blockchains for Monetizing the IoT

With these aforementioned challenges and business models, blockchains offer a feasible solution to the problem, while eliminating the need to trust third party service providers. Here we will discuss the recently proposed solutions specifically in how they add monetization capabilities to the IoT through blockchains.

1) Monetizing IoT Data and Resources: In existing relevant literature, Shafagh *et al.* [104] propose a blockchain-based decentralized data storage and sharing platform for IoT time-series data with a secure access control management layer on top of the storage layer. This technique uses access control policies to grant and revoke access to certain data, in exchange for cryptocurrency. On the other hand, Xu *et al.* [191] devise a model for the IoT end-devices to expose data analytical operations as a service on the blockchain instead of handing over the raw data acquired. Enabling analytics on IoT data without compromising the users' ownership of their own data will encourage users to contribute to training machine learning models for monetary incentives.

Within the IoT ecosystem, an IoT data owner and a service provider can interact over a blockchain as transacting participants without an intermediary. Firstly, the granularity of the data being shared is in control of the data owner with the use of smart contracts to define precisely the amount and type of data to be shared along with the timespan. Secondly, with the distributed ledger, the data owner can follow the data flow among various entities on the blockchain. Moreover, with the use of cryptocurrencies, the data can be monetized using the blockchain as well. Xu *et al.* [213] enable a shared data economy by leveraging zero-knowledge schemes and privacy-preserving smart contracts. They have an negotiation functions written into their smart contract, which can enable users to exercise control over the extent of the data they are selling. Reference [192] introduces the idea of sharing "data cubes," where IoT data is stored in Oraclize,[27] and users can market their data to potential buyers using broker accounts within the blockchain network. Reference [100] introduces an e-business model for IoT data using blockchains, where Decentralized Autonomous Corporations (DACs) defined within a public blockchain network engage in transactions involving IoT data and cryptocurrency.

Samaniego and Deters [167], [214] use blockchains to host and monetize software-defined IoT management resources, in an effort to empower a decentralized IoT-edge. They demonstrate high throughput of their proposed solution using permissioned blockchains for secure code distribution and immutable data storage.

2) Peer-to-Peer Energy Trading Systems: Blockchains are being researched to develop a secure decentralized medium for energy trading between energy producers and consumers within a smart grid. Kang *et al.* [117] developed an architecture for data sharing in vehicular edge computing, where they use consortium blockchains and smart contracts to enforce access control for data transfer, and a reputation system for data integrity. Furthermore, they use a pseudonymous address management system to mask the identity of singular entities with multiple addresses. Updating pseudonyms boosts privacy within blockchain networks, while maintaining security for data transactions. Their further work [83], [84] involves using the consortium blockchain architecture for not only allowing data transactions, but also monetary transactions for energy trading in the IIoT and hybrid vehicle networks. Their approach to circumvent the waiting time for transaction finality is to introduce a credit-based payment scheme, which enables fast and secure energy transactions. Knirsch *et al.* [82] use smart contracts and group signatures to preserve privacy and define varying tariffs in energy-trading smart grid applications. Every transaction that occurs for energy trading involves a group signature, within which the identity of the producers or consumers are concealed, in a k-anonymous fashion.

Aitzhan and Svetinovic [80] and Laszka *et al.* [81] leverage the decentralization and efficiency of consortium blockchains for energy transactions in smart-grid applications, and provide an off-chain anonymous messaging stream for energy consumers and producers to engage in negotiation. They apply context-aware address updating to boost anonymity in negotiations and on-chain transactions. Nehaï and Guerard [215] suggest a blockchain-based smart grid solution where the blockchain and smart contracts manage peer-to-peer energy transactions between participants of a single smart grid. Any user preferences as well as terms and conditions for the energy transfer is handled by the smart contract. Extended from this solution is the idea that several smart grids will have their own governing blockchains for energy transactions within them.

Moving beyond payment systems for smart grids, Münsing *et al.* [216] propose a blockchain-based solution for energy sharing control and optimization. This solution is built on a blockchain-based decentralized optimal power flow (OPF). The OPF is meant to perform scheduling for energy transfers, power offloading in electricity distribution networks. Here, smart contracts perform coordination tasks for optimum energy sharing scheduling. Optimal schedules are stored on the blockchain, following which payments can take place autonomously without the need for a microgrid operator.

[27] https://docs.oraclize.it/

C. Startups Monetizing IoT Data Using Blockchains

From a business perspective, the use of blockchain is already being exploited within several domains like Social Networks, Artificial Intelligence, Identity, and Healthcare in order to monetize the user data. However, there are a few startups that are focusing their efforts on the monetization of data generated by IoT devices in particular, thus creating a domain not only interesting for research, but also for new business models. One such startup is Slock.it,[28] which is enabling smart-objects, including assets like houses or cars, to be directly rented, thanks to the transparency and auditability provided by the blockchain, and Filament[29] is developing a platform that enables IoT devices to directly transact and interact. In the smart-grid sector, the information provided by IoT devices is also enabling new business models, such as Dajie [217] where IoT devices, backed by the blockchain, are able to monetize energy and data.

D. Summary and Insights

The first use-case of blockchains as a replicated state machine was to maintain decentralized records of monetary transactions. It makes sense that when integrated with the IoT, blockchains can be used to enable innovated electronic business models based on the IoT. The trends and perspectives seen in recent literature show two basic areas for blockchain-based monetization in the IoT: monetizing IoT resources, and enabling energy trading within peer-to-peer smart grid applications. In energy transaction systems, much of the focus of the research is dedicated to providing privacy for energy producers and consumers, either through pseudonymous address updating, or smart contract functions. Blockchains are being seen as a key to empowering IoT users, and allowing them to exercise authority on their data as well as to profit from their IoT resources.

XI. Alternative Approaches Towards Decentralizing IoT

To achieve scalability and higher throughput in application domains such as the IoT, alternative approaches for distributed record keeping are being worked upon. The main idea here is to use directed acyclic graphs (DAG) instead of a singular sequence of blocks, in order to improve the scalability of a decentralized ledger.

A. BlockDAG

BlockDAG, as described in [218], is built on a data structure where blocks are organized in a DAG. Vertices in this DAG represent a block, and the edges represent the multiple previously published blocks each block is linked to. BlockDAG does not aim to eliminate PoW mining or transaction fees, however, it leverages the structural properties of the DAG to meet the challenges related to the high orphan rates in blockchains.

[28]https://www.slock.it

[29]https://www.filament.com

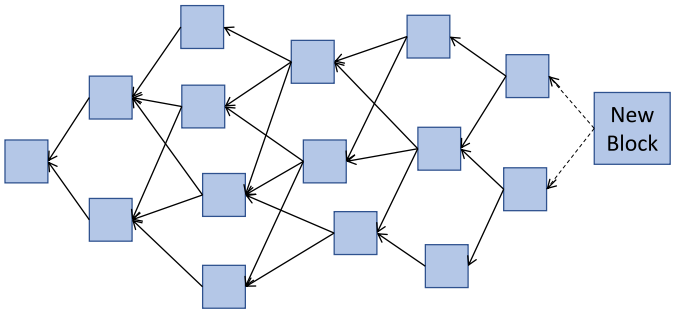


Fig. 5. BlockDAG structure. Each block references the tip of the graph as visible locally to the validator.

As previously discussed in Section II-B, orphan blocks are blocks published outside the longest chain because of propagation delays in the blockchain network. Block creation rates in public blockchains are kept constant to accommodate propagation speeds, and if the block creation rate is increased, it increases the likelihood of orphan blocks being created. A high orphan rate compromises blockchain security, because more honest blocks will end up outside the longest chain, and will be discarded [219]. This artificial latency in block creation hampers scalability, and it is worth considering that a DAG could perform better in dealing with forks.

Forks are accounted for in a DAG-based ledger by having blocks reference all forks in the graph, instead of referencing the top block in the longest chain. This allows for faster block creation rates and improved thoughput. As an added benefit, weaker miners that publish blocks onto a smaller fork are also rewarded. BlockDAG is purely a structural alternative to the blockchain, and does not present a new form of decentralized consensus. In [218], blocks being added on different forks may contain conflicting transactions, therefore it faces a scalability/security trade-off.

Further considerations need to be taken in blockDAG approaches to achieve consensus and avoid contradictions. The blockDAG mechanism in [218], Spectre [220] and Jute[30] allow contradicting transactions, but use sorting to maintain organization. Braidcoin[31] is a blockDAG approach that preserves payment verification functionality by not allowing conflicting transactions.

B. TDAG Distributed Ledgers

Another approach is the TDAG, where the DAG is built on transactions instead of blocks. This solution effectively is not a blockchain, however, the projects working on this approach are worth mentioning.

IoT Chain,[32] IOTA Tangle [221] and Byteball [222] are projects currently using TDAG for linking transactions together instead of blocks. The transactions recorded in these platforms contain within themselves a Merkle-tree of previous transaction IDs. Validation of each transaction relies on confirmations from local peers, thus the waiting time for mining is theoretically cut short. TDAG is seen to be a solution

[30]https://github.com/Taek42/jute

[31]https://github.com/mcelrath/braidcoin

[32]https://iotchain.io/

for scalability in the IoT application domain. The TDAG structure becomes wide with a high incoming rate of transactions and is not limited to linear processing as seen in most non-TDAG blockchains. All new incoming transactions are linked to multiple previous transactions, and each transaction is tasked with validating the previous transactions it is linked with, thus transaction validation is fast and computationally efficient. In blockchains, simply adding new transactions and not bundling them in blocks is not scalable, since there would be a huge rate of orphan chains. This problem can be potentially solved using TDAGs. Transactions in a TDAG simply reference any parent transactions as visible locally to the transaction issuer. Subsquently, TDAGs outperform blockDAG approaches since there is no waiting time for mining new blocks, and transactions can instantly obtain confirmations. Since transactions reference multiple tips of the DAG, any forks in the chain are effectively included in the DAG. High volumes of incoming transactions will cause a TDAG to grow wider than blockDAGs, thus making TDAGs more scalable.

To accommodate smaller IoT devices, IOTA offers a light-client feature whereby IoT devices will not be required to store the entire Tangle. Another feature of the light-client is that IoT devices can simply sign transactions and another participant can validate and add the transaction to the Tangle. Therefore, IOTA is well-suited to edge-centric IoT solutions where micropayments can be made over machine-to-machine communications since transactions do not incur fees. Transaction finality in Byteball is deterministic, while in IOTA it is probabilistic and based on a Markov Chain Monte Carlo (MCMC) approach. IOTA is a token based decentralized ledger specifically aimed at facilitating IoT micro-transactions, however Byteball is open to more use-cases, supports smart contracts and defining assets with attributes. The degree of privacy offered by IOTA remains unclear since all records in the Tangle are kept permissionless and publicly accessible, however in Byteball, assets can be made private [222].

Despite the obvious potential benefits, criticisms of IOTA include heavy centralization at the early stages of deployment. At the beginning, when there is a lower number of participants and incoming transactions, a central coordinator is needed to prevent a 33% attack on the IOTA tangle. Hashing only occurs at the point of creation of each transaction, and a tampering attack can be mounted with 33% of the network hashing power. The coordinator will no longer be required only after a significant growth of the network and the tangle will be decentralized at that point. Essentially, in the IoT, with heterogeneous devices having varying levels of low computational power, sufficiently strong computational resources will render the tangle insecure. This is a problem in traditional proof-of-work blockchains as well, however, they provide a much greater degree of security through higher fault tolerance and transaction fees. Furthermore, criticism of the IOTA Tangle by MIT Media Labs have exposed cryptographic vulnerabilities in IOTA [223], which the IOTA team has resolved by using SHA-3 based cryptography, instead of their proprietary Curl hash function. In its early stages, there is a scalability/trustlessness tradeoff in using either a blockchain or the Tangle.

Hybrid approaches involving blockchains and TDAG ledgers are also being researched for IoT applications. Most notably, the Virtualized Distributed Ledger Technology (vDLT) as proposed by Yu *et al.* [224] is a framework for reaping the benefits of token-based transactions in traditional blockchains, as well as the high thoughput of TDAGs. In the vDLT, different virtualized DLT functions (vDLTFs) can be assigned to multiple ledgers under the same framework, therefore, for functions that require security delivered by enforcing transaction fees, a vDLTF can access a traditional blockchain, and for functions that require low latency transactioning, the same vDLTF can access a TDAG through APIs written in the framework.

XII. Issues and Future Research Directions

All in all, the blockchain is a powerful, though emerging technology. As a result, despite its major advantages, it is facing multiple challenges in its development, as well as in its adoption in the IoT. These challenges can be broken down into three major areas: privacy-preservation, scalability and utilizing blockchains in scenarios involving devices with constrained capabilities. In this section, we will discuss these challenges, administrative trade-offs in public and private blockchain implementations and future research directions towards integrating blockchains in the IoT.

Indeed, blockchains provide extremely efficient auditability, however, having all of the data stored in a publicly accessible blockchain creates privacy-related issues. Furthermore, when dealing with blockchains, scalability is often a serious drawback. For instance, current public implementations of blockchains are capable of processing only 4-20 transactions per second [225], [226]. Therefore, they do not scale well for applications involving heavy amounts of traffic, like an automated micropayment platform for the IoT. In the IoT space, the ideal distributed platform would support the following main functionalities:

- Trustless peer-to-peer M2M communication
- Decentralized access control
- Private-by-design file sharing
- Scalable security provision over multiple IoT use-cases

In this section, we outline the implications of these challenges and open research opportunities for future research. Fig. 6 is a graphical representation of the existing issues and open research directions in the area of a blockchain-based decentralized IoT.

A. Privacy in Permissionless Blockchains

Blockchains in public networks like Bitcoin have stored transactions associated with generated blockchain addresses, and all transaction records are visible to participants of the Bitcoin network. These addresses are not linked to any real-world identities, and users can carry out transactions on multiple addresses, so as to avoid information leakage from all of their transaction information having been stored against one address [227]. The privacy in these records is merely to the extent of *"pseudonymity"*, since account balances and

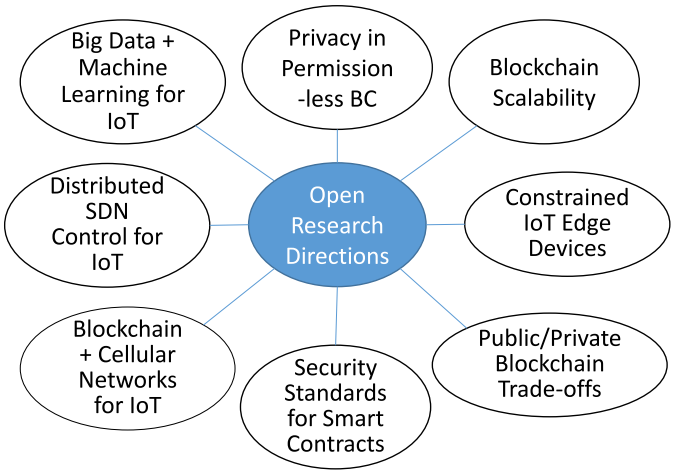


Fig. 6. Open research directions in decentralizing the IoT through blockchains.

transaction records for specific public keys are publicly accessible [33], [228]. However, such open records can lead to inferences revealing user information [229], and can even be used to triangulate and track user's IP addresses [123]. A privacy breach can also occur by drawing inferences based on graph analysis of the network of nodes a user transacts with [230], [231]. In blockchain applications, the ideal solution for privacy would be a form of decentralized record keeping that is completely obfuscated and anonymous by design.

Towards developing privacy-preserving blockchain applications, Zerocoin is a blockchain implementation purposely developed to enable anonymization for peer-to-peer transactions [232]. In Zerocoin, transactions are unlinked from the source of payment, hence preventing inferences via graph analysis. The transaction amount and destination are still on display. Subsequently, Zcash was developed to keep account balances and transaction information private [233]. Zcash is heralded as the most promising solution towards enabling privacy in blockchain applications and offers guaranteed anonymity by leveraging zero-knowledge cryptography [234]. In Zcash, transactions are fully encrypted and validated using proofs called "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge" (zk-SNARKs). While Zcash provides guaranteed anonymity, it comes at a cost: the Zcash blockchain has no auditability. A recently proposed auditability mechanism applicable to Zerocoin and Zerocash is detailed in [235].

For identity applications and transaction anonymization, a promising technique is to use ring signatures [236]. Ring signatures are more complicated and mathematically involved than conventional signatures in blockchain transactions. This technique involves a group of nodes signing a transaction. The generated signature serves as proof that a specific private key belongs to one of the signing nodes while making it cryptographically impossible to determine which node it is. However, to use the same private key in multiple transactions can reveal the user from within the group of nodes signing the ring transaction. Linkable ring signatures is an upgraded version, that does not use signatures with a private key, but requires proof that the user is indeed part of the signing group of nodes [237]. Linkable ring signatures and financial incentives together lay down the basis of file sharing applications that enable more anonymity than the current peer-to-peer file sharing platforms like Bittorent [238].

Address mixing is a service that enables anonymity by sending transactions from multiple addresses to multiple destinations [239], [240]. Mixing is essentially laundering transactions within the blockchain network via intermediaries. While having an intermediary compromises decentralization in the blockchain network, it is a viable technique for transacting with peers anonymously. Consider Alice with address A, wants to transfer tokens to Bob, whose address is B. Alice transfers her tokens to Charlie, who runs a mixing service. Charlie uses varying token values over multiple addresses, and signs transactions addressed to multiple destinations, one of the destinations being B. Charlie transfers the amount Alice intended to Bob, and the mixed addresses launder and anonymize Alice's transaction. An obvious disadvantage of this service is having to place trust on Charlie, the intermediary. The intermediary can choose to be dishonest and reveal Alice and Bob's transaction history. An even more malicious breach of trust would result in Charlie never sending the tokens to Bob in the first place. Mixcoin is a service that attempts to mitigate malicious behavior while performing address mixing [241]. Mixcoin adds accountability to detect if the intermediary has in fact cheated, however, it offers no preventive measures. Another solution is to use multiple pseudonym address management systems instead of singular pseudonymous addressing. Multiple pseudonymous addresses can be used to mask the identity of any singular participant in a blockchain network. So far, this is the most promising solution towards providing privacy, however, the more addresses any entity uses, the more complicated accountability becomes for use-cases where transaction transparency is required to serve legal purposes. Pseudonymous address management systems that change addresses timely, or on a context-aware basis may need further immutable record keeping for the addresses any singular entity has used in the past, in order to provide a trail for legal proceedings.

The challenge in developing a blockchain-based IoT platform that maintains the delicate balance of preserving accountability and privacy has prompted many proposed solutions, yet remains open to further research and development. Proposed solutions involve either implementing access policies within the blockchain itself, or implementing access policies through smart contracts. A promising method to provide privacy in blockchain-based IoT platforms is a tiered architecture, where secluded private blockchains are connected through a public blockchain. In a tiered architecture, an important research challenge is to maintain data integrity within the private blockchains, while providing data seclusion and selective expression for privacy. Providing auditability and preventing double-spending led to sacrificing anonymity in blockchains, therefore, guaranteed privacy remains a fertile area of research [242] for applications that have privacy built into them by design.

B. Scalability in Blockchains

Currently, all blockchains' consensus protocols, both in private and public blockchains, require every fully participating node to hold a copy of all the transactions recorded in the history of the blockchain. While this provides decentralization, security and fault tolerance, it comes at a cost of scalability. Traditionally, databases only require additional storage to cope with a growing number of records, however, in blockchains, every full node requires added storage to host a full copy of the blockchain. This problem is compounded in proof-of-work based consensus, where a growing number of participants in the network would require added computational power for mining nodes, in order to process transactions faster. In other words, as the blockchain grows, the requirement for storage grows; additionally, depending on the consensus algorithm being used, requirements of bandwidth and computational power also grow.

Recent advances with *"light-clients"* developed by blockchain platforms like Ethereum, improve upon the growing storage requirements of a steadily growing blockchain [243]. However, in applications beyond cryptocurrencies, and specifically the Internet of Things, blockchains remain out of the reach of devices with limited storage, computational and networking capabilities.

Scaling the blockchain has been an area of active research [225], starting with Segwit [244] and an increased block size [46]. Both techniques were applied to the Bitcoin network and were aimed to enable vertical scalability in blockchains. Horizontal scalability via sidechains and inter-blockchain communications are also being researched [86], [114]. Similar to multi-tiered blockchain architectures [87] suggests connecting IoT gateways to public blockchain networks. These solutions on their own provide incremental scalability but may not serve to be the silver bullet required for future-proofing scalability in blockchain networks. Challenges in blockchain scalability is an open area of research. Many different approaches are seen in recent research, that aim to improve scalability in blockchains, from SegWit for the Bitcoin blockchain to the more recent sharding [67] techniques being developed by Ethereum. More promising solutions involve either moving processing and storage load off-chain [245], [246], or limiting the scope of consensus over different parts of a blockchain network, or developing inter-blockchain communications [247] for connecting multiple blockchains.

Scaling blockchains remains a huge issue in their implementation in digital finance and beyond, due to their high performance and networking overhead. In digital finance, current public blockchain implementations do not scale well enough to compete with the transaction processing speed of credit card companies. The issue surrounding low throughput is exacerbated in the IoT where a much higher volume of data transactions occur; either data creation or transfer. Vertically scaling blockchain as a distributed database is one potential direction. On the other hand, horizontal scaling shows more promise in solving blockchain scalability issues, therefore semantics independent inter-blockchain communications is another key research direction. Solving scalability in the blockchain will be a huge step forward in creating decentralized infrastructures for the IoT.

C. IoT Edge-Device Constraints

The IoT augments the traditional Internet by connecting smart devices together for performing automated tasks. Most IoT devices have strict computational and networking constraints, which pose an issue when using blockchain-based decentralized architectures. Most IoT devices cannot engage in PoW consensus due to their limited computational power and battery life. Even if devices are added to a blockchain where the device does not mine new blocks, or in blockchains that use alternate consensus algorithms, IoT devices do not come with the required storage space to host a complete copy of the blockchain [156]. While integrating IoT devices to the blockchain using blockchain-connected gateways, the degree of decentralization achieved remains limited. A recent contribution towards this challenge was in [248], which is a memory-optimized blockchain for IoT networks of larger scale.

Apart from computational and networking constraints, IoT edge devices suffer from limited interoperability and a lack of authentication and authorization standards. Blockchains can be implemented to record structured and unstructured data transfer over data transacting networks, therefore they have the potential to enable interoperability over different IoT edge devices. Blockchain platforms like Hyperledger's Burrow [28] and Sawtooth [57] create roles for nodes in blockchain networks, including limited roles well-suited for IoT edge devices, where nodes can simply push transactions to the blockchain without needing to store a full copy. So far, this solution only works in private blockchain implementations, however, for public blockchains, pushing transactions through IoT gateways is seen as one possible solution [86], [114], however it would require computationally capable gateways to participate in a public blockchain.

A key future research direction is to extend blockchains to the IoT edge. The high performance and networking overheads of blockchains limit their use over constrained IoT devices. A significant proposed solutions in research is performing end-to-end communications over the blockchain through computationally capable IoT gateways. The challenge in this research direction would be to enable IoT devices and gateways to push transactions to the blockchain using light clients, without creating centralized block validation pools.

D. Trade-Off in Public-Private Blockchains

In finance applications, blockchains have not reached the technological maturity to compete with the transaction processing times of mainstream financial systems like Visa or Paypal. Paypal averages at 193 transactions per second, while Visa achieves an even faster rate of processing around 1667 transactions per second [249]. At the same time, mainstream cryptocurrencies Bitcoin and Ethereum have transaction processing times of 4 and 15 transactions per second respectively [225], [226].

While private blockchains have a much higher transaction throughput, they do not provide total decentralization, and in fact, blockchains run by organizations are under the centralized control of the organization itself. The consensus protocols used in private blockchains involve rounds of voting to provide Byzantine fault tolerance, which is not suitable for public blockchain implementations. In public blockchain platforms, the philosophy of all users being equal, without a governing entity prevails. The latency in public blockchains is inherent to the lottery-based consensus algorithms they employ, which aim to create a secure and permissionless transaction processing platform. Thus, blockchain consensus protocols make the tradeoff between high-speed transactions and decentralization [250].

For applications beyond cryptocurrencies, the challenge is to provide privacy to the users, along with scalability while providing multiple application services. In applications where the blockchain spreads over multiple geographic locations and multiple use case scenarios, like the Internet of Things, there will be a need for multiple blockchains communicating with each other to provide IoT services, thus being able to scale vertically and horizontally.

E. Security Standards for Scripting Smart Contracts

Despite the inherent security features of the blockchain, the weak link proves to be the exploitable loopholes within smart contracts. An example of adversaries exploiting the shortcomings of a smart contract was seen in the DAO attack [32]. A direction of research for blockchain IoT integration is in developing security standards for scripting smart contracts in such a way that there are no loopholes that compromise the security of the devices in the IoT network.

F. Blockchains and Cellular Networks for the IoT

In the constant evolution of LTE cellular networks, research is underway in finding a balance between centralized and decentralize control mechanisms. Decentralizing cellular networks from a control perspective can bring the inherent application layer security features of the blockchain to the IoT edge, and it can also help leverage the authentication and data protection features offered by cellular networking at lower layers. An example of such a decentralized control plane for cellular networks is seen in Qlink,[33] which aims to build an architecture on public and private blockchains for cellular networks. At the public blockchain level, infrequent transactions between telecom companies take place, while at the private blockchain level, faster transactions can take place to provide services based on smart contracts. The aim is to not only benefit from the security features of blockchain and cellular networking, but to also provide flexible data packages and wifi resource sharing.

Much of the IoT edge relies on cellular networking, and the research for decentralizing cellular networks is still at very nascent stages. For existing blockchain protocols, the demonstrated performance only scales up to thousands of peers, so scalability will be detrimental for research in this direction. Blockchains can assist with existing approaches for cellular networks like application-layer traffic optimization [251], and can help in hosting virtualized resources. Virtualized network resources will further the logical evolution of cellular networks, and blockchains have the potential to perform resource scheduling via distributed applications.

[33]https://qlink.mobi

G. SDN Integration for Blockchain-Based IoT Edge

In the future of development for the Internet, and specifically the IoT, Software-Defined Networking (SDN) and Network Function Virtualization (NFV) aim to provide a virtualized edge platform, where virtual hosts can be dynamically deployed. Thus SDN and NVF are complementary to each other and are key to enabling a shared IoT edge with virtualized IoT assets [167]. Virtualized hosts or IoT assets can be made responsible for specific applications in providing security through firewalling and intrusion detection, and commissioning IoT devices to remote edge users. Since SDN split control plane and data forwarding functionalities, it can be used to easily control virtual IoT assets. This direction in IoT's development has the potential to enhance the IoT edge with easy configuration and management capabilities. However, while SDN and NFV evolve respectively, newer cybersecurity issues arise, which are compounded when integrated with the Internet of Things.

SDNs provide enterprises the capabilities of adding, removing and updating virtualized networking assets with centralized control. All SDN asset configurations are managed and stored in a central control application which leads to a very centralized attack surface. Within the SDN and NFV research space for the IoT, there are existing security issues that can potentially hamper the development of a software-defined IoT. These include Denial of Service (DoS) attacks, confidentiality attacks through spoofing and data modification attacks within virtualized IoT environments [252]. Integrity of SDN configuration is paramount for secure functioning of virtualized networking assets. One of the pioneering papers in this research direction is by Sharma *et al.* [253], which proposes an architecture for decentralizing the network control plane through blockchains. Securing virtualized IoT through blockchains will prove to be a research direction which we anticipate will yield interesting outcomes in the future.

H. Big Data and Machine Learning for Decentralized IoT Frameworks

The recent renaissance of machine learning and artificial intelligence has seen revolutionary developments in only the last few years in areas including autonomously driving vehicles, computer vision and the IoT. To fully realize the vision of the IoT for performing automated tasks for human users, it is essential to incorporate machine learning in the IoT. Machine learning, and specifically deep learning algorithms perform best in an abundance of data available for predictive models and parameter tuning. In the IoT, machine learning can be used to make intelligent decisions to optimize automation tasks like managing IoT assets, scheduling and energy transactions.

TABLE XI
SUMMARY OF OPEN RESEARCH DIRECTIONS FOR INTEGRATING BLOCKCHAINS WITH THE IOT

Research Direction	Description
Privacy in permissionless blockchains	- Contents of all permissionless blockchains are public for auditability; - Blockchain addressing is pseudonymous; there is a need for total anonymity for privacy.
Blockchain scalability	- Decentralized consensus reduces transaction throughput in permissionless blockchain; - Storing network-wide transactions results in increasing storage requirements.
IoT edge device constraints	Resource-constrained IoT devices need computational complexity for directly issuing transactions to the blockchain. Blockchain-connected IoT gateways need substantial computational and storage capabilities to be a peer in a blockchain network.
Public/private blockchain tradeoff	- Public blockchains scale up to thousands of nodes, have guaranteed immutability and auditability, but high latency and reduced throughput; - Private blockchains have high transaction throughput, but do not have guaranteed accountability, and only scale up well enough to tens of nodes.
Security standards for smart contracts	Blockchain-based IoT requires standards for writing secure smart contracts that cannot be exploited for nefarious purposes.
Blockchains + cellular networks for IoT	Decentralizing the cellular networking at the IoT edge will bring complimentary low layer security features of cellular networks and application-layer security features of blockchains.
Distributed SDN control for IoT	SDN typically has heavily centralized control planes that can be subject to security threats. Blockchains have the potential to decentralize and secure SDN control plane.
Big data + machine learning for decentralized IoT	- Room for research in leveraging blockchains for maintaining crowdsensing and big data applications - Incentivizing users to contribute data to open-source big data repositories, that improve machine learning models for automating the IoT

Machine learning and deep learning models have the potential in the IoT to predict and identify cybersecurity threats and vulnerabilities. Intrusion detection systems can detect malicious activity and can help further bolster the blockchain-based IoT's security. The most compelling use cases for machine learning algorithms are at the IoT edge where natural language processing and image recognition can significantly benefit IoT users. Connecting artificial intelligence and the IoT requires systems that can maintain trust while retrieving data from anonymous data sources at the IoT edge, instead of data warehouses that conventionally enrich machine learning models. With the trustless network ecosystem blockchains provide, that vision is within reach. Once a blockchain-based IoT edge comes to fruition, IoT users will be able to monetize their data and can crowdsource data to machine learning models for IoT services. One such example is [254], where blockchains can make big data available for an open collaborative IoT edge. Publicly available big data repositories secured by the blockchain can help improve training for automated functionality. On the other hand, for sensitive big data repositories, for example medical records, blockchains can be used to enforce access control mechanisms as required by the IoT application.

With the added benefit of artificial intelligence, IoT sensors can truly be the augmented eyes and ears of human users, and can extend the limits of the human experience. Using blockchains to maintain integrity for big data analysis in the IoT is a significant direction for future research.

I. Summary of Open Research Directions

From this section, we have seen that blockchain in itself is a nascent technology, with ample of room for further development, specifically in the IoT domain. Table XI shows a summary of the issues present in the area of decentralizing the IoT through blockchains.

XIII. SUMMARY OF LESSONS LEARNED

In this survey, we have covered the recent research contributions made towards decentralizing the IoT with blockchains. While blockchains have great potential in establishing a democratic and secure fabric for the Internet of Things, it is not without its limitations that need to be worked upon. In this section, we will reiterate and summarize the insight we have gained in the different areas of the IoT, as discussed in this survey. To visualize the papers reviewed in this survey, Table XII enlists all the research contributions towards developing a blockchain-based IoT, along with information on which areas of the IoT mentioned in this survey is sufficiently addressed by them. These research contributions utilize the inherent virtues of the blockchain and other distributed ledger technologies in these areas of the IoT, as well as specific techniques as discussed in previous sections.

Public blockchains provide immutability through decentralized consensus, along with accountability, since all transaction contents of the blockchain are visible to the participants of the blockchain network. On the other hand, while private

TABLE XII
SUMMARY OF REVIEWED RESEARCH CONTRIBUTIONS

Research Contributions	Privacy	Trust for IoT	Security				Identity Management	Data Management	IoT Monetization
			Access Control	Data Integrity	Confidentiality	Availability			
FairAccess [101][102]	✓	✓	✓	✓	✓	✓	✓	✓	✓
Zhang et al. [100]	✓	✓	✓	✓	✓	✓	✓	✓	✓
Enigma [103][110]	✓	✓	✓	✓	✓	✓	✓	✓	✓
Shafagh et al. [104]	✓	✓	✓	✓	✓	✓	✓	✓	×
PISCES [105]	✓	✓	✓	✓	✓	✓	✓	✓	×
PlaTIBART [106]	✓	✓	×	×	✓	✓	✓	×	×
Ayoade et al. [107]	✓	✓	×	×	✓	✓	✓	✓	×
Cha et al. [87]	✓	×	×	×	✓	✓	×	×	×
Hawk [33]	✓	✓	✓	✓	✓	✓	✓	✓	✓
Conoscenti et al. [108]	✓	✓	×	✓	✓	✓	✓	✓	×
Sharma et al. [109]	✓	✓	✓	×	✓	✓	✓	✓	×
Rahulamathavan et al. [111]	✓	✓	×	✓	✓	✓	✓	✓	×
JointCloud [112]	✓	×	×	×	✓	✓	✓	✓	×
Hardjono et al. [113]	✓	✓	✓	×	✓	✓	✓	✓	×
Dorri et al. [86]	✓	✓	✓	✓	✓	✓	✓	✓	×
Ali et al. [114]	✓	✓	✓	✓	✓	✓	✓	✓	×
Aitzhan et al. [80]	✓	✓	×	✓	✓	✓	✓	×	✓
Laszka et al. [81]	✓	✓	×	✓	✓	✓	✓	×	✓
Knirsch et al. [82]	✓	✓	×	✓	✓	✓	✓	×	✓
Lombardi et al. [115]	✓	✓	×	✓	✓	✓	✓	×	✓
Gao et al. [118]	✓	×	✓	✓	✓	✓	✓	✓	×
Kang et al. [117]	✓	✓	✓	✓	✓	✓	✓	✓	×
Kang et al. [84], [83]	✓	✓	✓	✓	✓	✓	✓	×	✓
Wang et al. [116]	✓	×	✓	×	✓	✓	✓	×	×
Liu et al. [128]	×	✓	×	✓	✓	✓	✓	×	×
Urien et al. [129]	×	✓	×	×	✓	✓	✓	×	×
Bahga et. al [130]	×	✓	×	✓	✓	✓	✓	×	×
Boudguiga et al. [131]	×	✓	×	✓	✓	✓	✓	×	×
DiPietro et al. [132]	×	✓	×	✓	✓	✓	✓	×	×
IoTChain [133]	×	✓	×	✓	✓	✓	✓	✓	×
Psaras et al. [134]	×	✓	×	✓	✓	✓	✓	×	×
Trustchain [135]	×	✓	×	✓	✓	✓	✓	×	×
Tian et al. [136]	×	✓	×	✓	✓	✓	✓	✓	×
Bocek et al. [137]	×	✓	×	✓	✓	✓	✓	✓	×
Samaniego et al. [138][167]	×	✓	×	×	✓	✓	✓	×	✓
Axon et al. [151]	×	✓	✓	✓	✓	✓	✓	×	×
Hashemi et al. [152]	×	✓	✓	✓	✓	✓	✓	✓	×
Novo et al. [153]	×	✓	✓	✓	✓	✓	✓	✓	×
Capchain [154]	×	✓	✓	✓	✓	✓	✓	✓	×
Hamza et al. [155]	×	✓	✓	✓	✓	✓	✓	✓	×
Biswas et al. [156]	×	✓	✓	✓	✓	✓	✓	✓	×
Yang et al. [157]	×	✓	×	✓	✓	✓	✓	×	×
Lee et al. [158]	×	✓	×	✓	✓	✓	✓	✓	×
Steger et al. [159]	✓	✓	✓	✓	✓	✓	✓	✓	×
Alphand et al. [160]	×	✓	×	✓	✓	✓	✓	✓	×
Chakraborty et al. [161]	×	✓	×	✓	✓	✓	×	✓	×
Imbault et al. [165]	×	✓	×	✓	✓	✓	✓	×	×
Kikitamara et al. [166]	×	✓	×	✓	✓	✓	✓	×	×
Kravitz et al. [168]	×	×	×	×	✓	✓	✓	×	×
Huh et al. [169]	×	✓	×	✓	✓	✓	✓	×	×
Lee et al. [170]	×	✓	×	✓	✓	✓	✓	×	×
Liang et al. [189]	✓	✓	✓	✓	✓	✓	×	✓	×
Azaria et al. [190]	✓	✓	✓	✓	✓	✓	✓	✓	×
Xu et al. [191]	×	✓	×	✓	×	✓	✓	✓	✓
Missier et al. [192]	×	×	×	✓	✓	✓	×	✓	✓
Nehai et al. [215]	×	✓	×	✓	×	✓	✓	×	✓
Münsing et al. [216]	×	✓	×	✓	✓	✓	✓	×	✓
Spectre [220]	×	×	×	✓	×	✓	✓	✓	×
Lewenberg et al. [218]	×	×	×	✓	×	✓	✓	✓	×
IOTA Tangle [221]	×	×	×	✓	×	✓	✓	✓	✓
Byteball [222]	×	×	×	✓	×	✓	✓	✓	×
Yu et al. [224]	×	✓	✓	✓	✓	✓	✓	✓	×

blockchains retain privacy within one organization, they do not guarantee accountability, since it is not sufficiently decentralized. This leads to a trade-off in auditability and privacy in choosing public versus private blockchains. Recent research efforts towards developing a privacy-preserving decentralized IoT involve access policies written into either the

transactional model of the blockchain, the block headers or smart contract conditions [33], [102], [103]. Other solutions involve tiered architectures built on public and private blockchains [86], [114], where the benefits of both private and public blockchains can be reaped. While recent research efforts propose promising solutions, the problem of maintaining privacy in public blockchains remains an open research challenge. We also learned how the "trustless" networking environment provided by blockchains can be leveraged to perform monetary and data transactions without the need for any trusted intermediaries. Recent research has shown the benefits of blockchain-based trustlessness in IoT services, specifically supply chain management [136], [137]. Thus blockchains prove to be a key technology in guaranteeing trust in IoT services.

In providing security for the IoT, we learned how the cryptographic features of blockchain addressing and transactions enable confidentiality in the IoT [80], [151]. Blockchain smart contracts enforce terms and conditions where access control policies can be written for secure data access. The decentralized nature of blockchains prevent IoT services from having centralized points of failure, and transaction fees in public blockchains prevent flooding attacks, thus preserving the availability of the IoT [130], [160]. Decentralized consensus ensures all contents of the blockchain are immutable, which form the basis of solutions that ensure data integrity in data stored on-chain and in off-chain storage mechanisms [128], [156].

We discussed identity management solutions for the IoT based on blockchains, as proposed in recent research. These solutions promise identities for devices and entities participating in end-to-end IoT communications, in varying degrees of anonymity [81], [151]. Blockchain-based solutions provide data management with guaranteed integrity and resilience. Current cloud solutions depend on centralized servers for handling and storing IoT data, whereas blockchains democratize data management, and eliminate the chances of centralized services unfairly exploiting user data. Blockchains also provide a platform for automated micropayments, data monetization and energy transactions. The recent research papers we reviewed in the matter of IoT monetization involve various techniques by which blockchains can help develop a decentralized and democratized IoT marketplace.

XIV. Conclusion

In this paper, we provided an extensive survey of the recent attempts in bringing the blockchain technology to maturity, with a specific focus on the current research efforts in designing and developing blockchain-based platforms, applications, and services suitable for the new era of the Internet of Things. We began our narrative outlining the core features of the Blockchain technology, which is a distributed ledger with immutable and verifiable transaction records. Blockchains achieve immutable and secure records through distributed consensus algorithms. Therefore, blockchains provide a *"trustless"* environment for record keeping, where no trust is required to be placed on any individual centralized entity.

Following the degree of decentralization that blockchains have achieved in cryptocurrency networks, blockchains are hailed as the potential solution to decentralizing the IoT. In current IoT framework, centralized authentication, authorization, and access models require users to trust centralized third-party entities for managing, handling and processing their IoT data. Blockchains can lay down the foundation for a decentralized fabric for the IoT, with no managing or authorizing intermediaries. We highlighted the different scopes within the IoT framework where research efforts are already demonstrating the potential benefits of blockchain-based decentralization. As discussed, these areas include privacy, trustless and secured communications, identity and data management, as well as monetization of IoT data and resources.

To conclude, we have conducted an in-depth survey of blockchains, along with their main features and characteristics, as well as technical working principles. Then, we discussed recent research efforts that are leveraging the benefits of the blockchain within different challenging areas of the IoT. These areas where Research & Development is currently more concentrated, helped us reveal open research directions that have the potential to yield major outcomes in the near future.

References

[1] K. Ashton, "That 'Internet of Things' thing," *RFID J.*, Jun. 2009.

[2] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)," *IEEE Internet Initiative*, vol. 1, pp. 1–86, 2015.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[4] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[5] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet of Everything*. Singapore: Springer, 2018, pp. 103–130.

[6] U. Kumar and S. Sanyal, "Survey of security and privacy issues of Internet of Things," *Int. J. Adv. Netw. Appl.*, vol. 6, no. 4, pp. 2372–2378, 2015.

[7] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of Things, blockchain and shared economy applications," *Procedia Comput. Sci.*, vol. 98, pp. 461–466, 2016.

[8] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptol.*, vol. 3, no. 2, pp. 99–111, Jan. 1991.

[9] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Dec. 12, 2018. [Online]. Available: http://bitcoin.org/bitcoin.pdf

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

[11] P. Brody, V. Pureswaran, S. Panikkar, and S. Nair, "Empowering the edge practical insights on a decentralized Internet of Things," Armonk, NY, USA, IBM Inst. Bus., White Paper, 2015.

[12] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

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

[14] M. Atzori, "Blockchain-based architectures for the Internet of Things: A survey," *SSRN Electron. J.*, 2017. [Online]. Available: https://ssrn.com/abstract=2846810

[15] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

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

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

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

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

[20] T. Neudecker and H. Hartenstein, "Network layer aspects of permissionless blockchains," *IEEE Commun. Surveys Tuts.*, to be published, doi: 10.1109/COMST.2018.2852480.

[21] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*. Cheltenham, U.K.: Edward Elgar Publ. Incorporat., 2015.

[22] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "Blockchain-the gateway to trust-free cryptographic transactions," in *Proc. 24th Eur. Conf. Inf. Syst. (ECIS)*, Istanbul, Turkey, 2016, pp. 1–15.

[23] P. Mueller, A. Rizk, and R. Steinmetz. (2017). *BlockChain a New Foundation for Building Trustworthy and Secure Distributed Applications (DAPP's) of the Future*. Accessed: Dec. 12, 2018 [Online]. Available: http://dspace.icsy.de:12000/dspace/handle/123456789/432

[24] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Proc. Adv. Cryptol. (CRYPTO)*, 2000, pp. 369–378.

[25] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Zug, Switzerland, Ethereum Project, Yellow Paper, 2014.

[26] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 1–23, 2017.

[27] A. Back *et al.* (2014). *Enabling Blockchain Innovations With Pegged Sidechains*. [Online]. Available: https://www.opensciencereview.com

[28] V. Dhillon, D. Metcalf, and M. Hooper, "The hyperledger project," in *Blockchain Enabled Applications*. Berkeley, CA, USA: Apress, 2017, pp. 139–149.

[29] J. A. T. Fairfield, "Smart contracts, bitcoin bots, and consumer protection," *Washington Lee Law Rev. Online*, vol. 71, no. 2, pp. 35–50, 2014.

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

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

[32] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SOK)," in *Proc. 6th Int. Conf. Principles Security Trust*, 2017, pp. 164–186.

[33] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Security Privacy*, 2016, pp. 839–858.

[34] *RSK Website*. Accessed: Dec. 12, 2018. [Online]. Available: https://www.rsk.co/

[35] J. Turek and D. Shasha, "The many faces of consensus in distributed systems," *IEEE Comput.*, vol. 25, no. 6, pp. 8–17, Jun. 1992.

[36] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of distributed consensus with one faulty process," *J. ACM*, vol. 32, no. 2, pp. 374–382, 1985.

[37] D. Dolev, C. Dwork, and L. Stockmeyer, "On the minimal synchronism needed for distributed consensus," *J. ACM*, vol. 34, no. 1, pp. 77–97, 1987.

[38] D. Malkhi and M. Reiter, "Byzantine quorum systems," *Distrib. Comput.*, vol. 11, no. 4, pp. 203–213, 1998.

[39] L. Law, S. Sabett, and J. Solinas, *How to Make a Mint: The Cryptography of Anonymous Electronic Cash*, Nat. Security Agency Office Inf. Security Res. Technol. Cryptol. Division, Fort Meade, MD, USA, 1996.

[40] N. Szabo. *Bit Gold*. Accessed: Dec. 12, 2018. [Online]. Available: http://unenumerated.blogspot.de/2005/12/bit-gold.html

[41] W. Dai. (1998). *B-Money Website*. Accessed: Dec. 12, 2018. [Online]. Available: http://www.weidai.com/bmoney.txt

[42] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

[43] M. Correia, G. S. Veronese, N. F. Neves, and P. Verissimo, "Byzantine consensus in asynchronous message-passing systems: A survey," *Int. J. Crit. Comput. Based Syst.*, vol. 2, no. 2, pp. 141–161, Jul. 2011.

[44] A. Baliga, "Understanding blockchain consensus models," Pune, India, Persistent Syst. Ltd., White Paper, 2017.

[45] J. R. Douceur, "The Sybil attack," in *Proc. Int. Workshop Peer-to-Peer Syst.*, 2002, pp. 251–260.

[46] A. Gervais *et al.*, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 3–16.

[47] A. Miller and J. J. LaViola, Jr. (2014). *Anonymous Byzantine Consensus From Moderately-Hard Puzzles: A Model for Bitcoin*. [Online]. Available: http://nakamotoinstitute.org/research/anonymous-byzantine-consensus

[48] D. Bradbury, "In blocks [security bitcoin]," *Eng. Technol.*, vol. 10, no. 2, pp. 68–71, Mar. 2015.

[49] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *Proc. 25th IET Irish Signals Syst. Conf. China–Ireland Int. Conf. Inf. Commun. Technol. (ISSC/CIICT)*, Jun. 2014, pp. 280–285.

[50] *Peercoin Website*. Accessed: Dec. 12, 2018. [Online]. Available: https://peercoin.net

[51] "NXT Whitepaper," Orlando, FL, USA, NXT Community, White Paper, 2014.

[52] P. Vasin, "Blackcoin's proof-of-stake protocol v2," London, U.K., Blackcoin, White Paper, 2014. [Online]. Available: https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper.pdf

[53] N. Houy. (2014). *It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency*. Accessed: Dec. 27, 2018. [Online]. Available: https://ssrn.com/abstract=2393940

[54] C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild (keynote talk)," in *Proc. LIPIcs-Leibniz Int. Proc. Informat.*, vol. 91, 2017.

[55] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, Dec. 2014.

[56] *Decred Documentation*. Accessed: Dec. 12, 2018. [Online]. Available: https://docs.decred.org/research/overview/

[57] *Sawtooth Documentation*. Accessed: Dec. 12, 2018. [Online]. Available: https://goo.gl/izmMYn/

[58] V. Costan and S. Devadas, "Intel SGX explained," *IACR Cryptol. ePrint Archive*, vol. 2016, p. 86, Jan. 2016.

[59] M. Walport, *Distributed Ledger Technology: Beyond Blockchain*, U.K. Govt. Office Sci., London, U.K., 2016.

[60] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

[61] E. Androulaki, C. Cachin, A. De Caro, A. Kind, and M. Osborne, "Cryptography and protocols in hyperledger fabric," in *Proc. Real World Cryptography Conf.*, 2017, pp. 1–49.

[62] C. Cachin, S. Schubert, and M. Vukolić, "Non-determinism in Byzantine fault-tolerant replication," in *Proc. LIPIcs-Leibniz Int. Proc. Informat.*, vol. 70, 2017.

[63] J. Kwon. (2014). *TenderMint: Consensus Without Mining*. [Online]. Available: http://tendermint.com/docs/tendermint.pdf

[64] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," San Francisco, CA, USA, Ripple Labs Inc., White Paper, 2014.

[65] D. Mazieres. *The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus*. Accessed: Dec. 12, 2018. [Online]. Available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf/

[66] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Prob. Netw. Security*, 2015, pp. 112–125.

[67] (2017). *Ethereum Sharding FAQ*. Accessed: Dec. 12, 2018. [Online]. Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ

[68] B. Greenstein. (2018). *IoT Trends in 2018: AI, Blockchain, and the Edge*. Accessed: Dec. 12, 2018. [Online]. Available: https://iot.ieee.org/newsletter/january-2018/iot-trends-in-2018-ai-blockchain-and-the-edge#_ftn1

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

[70] "List of 450 IoT platform companies research and markets," 2017.

[71] A. Barki, A. Bouabdallah, S. Gharout, and J. Traoré, "M2M security: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1241–1254, 2nd Quart., 2016.

[72] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[73] M. Mohammadi and A. Al-Fuqaha, "Enabling cognitive smart cities using big data and machine learning: Approaches and challenges," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 94–101, Feb. 2018.

[74] V. Gazis, "A survey of standards for machine-to-machine and the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 482–511, 1st Quart., 2017.

[75] D. S. Nunes, P. Zhang, and J. S. Silva, "A survey on human-in-the-loop applications towards an Internet of all," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 944–965, 2nd Quart., 2015.

[76] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Security Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[77] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Security (CIS)*, 2013, pp. 663–667.

[78] J. S. Kumar and D. R. Patel, "A survey on Internet of Things: Security and privacy issues," *Int. J. Comput. Appl.*, vol. 90, no. 11, pp. 20–26, 2014.

[79] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.

[80] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2016.

[81] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers," in *Proc. 7th Int. Conf. Internet Things (IoT)*, 2017, pp. 1–13.

[82] F. Knirsch, A. Unterweger, G. Eibl, and D. Engel, "Privacy-preserving smart grid tariff decisions with blockchain-based smart contracts," in *Sustainable Cloud and Energy Services*. Cham, Switzerland: Springer, 2018, pp. 85–116.

[83] J. Kang *et al.*, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[84] Z. Li *et al.*, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[85] P. G. Lopez *et al.*, "Edge-centric computing: Vision and challenges," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 37–42, Sep. 2015. [Online]. Available: http://doi.acm.org/10.1145/2831347.2831354

[86] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, 2017, pp. 618–623.

[87] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for BLE-based devices in the Internet of Things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.

[88] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 45–54, doi: 10.1109/CVCBT.2018.00011.

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

[90] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[91] G. Greenwald and E. MacAskill, "NSA prism program taps in to user data of Apple, Google and others," *Guardian*, vol. 7, no. 6, pp. 1–43, 2013.

[92] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the Internet of Things," in *Proc. Internet Things*, 2010, pp. 389–395.

[93] O. Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. Gistrup, Denmark: River, 2013.

[94] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[95] G. V. Lioudakis *et al.*, "A proxy for privacy: The discreet box," in *Proc. Int. Conf. Comput. Tool (EUROCON)*, 2007, pp. 966–973.

[96] D. Chaum and E. Van Heyst, "Group signatures," in *Proc. Workshop Theory Appl. Cryptograph. Tech.*, 1991, pp. 257–265.

[97] F. Li, Z. Zheng, and C. Jin, "Secure and efficient data transmission in the Internet of Things," *Telecommun. Syst.*, vol. 62, no. 1, pp. 111–122, 2016.

[98] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty Fuzziness Knowl. Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.

[99] J. Domingo-Ferrer and V. Torra, "A critique of k-anonymity and some of its enhancements," in *Proc. 3rd Int. Conf. Availability Rel. Security*, 2008, pp. 990–993.

[100] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 983–994, 2017.

[101] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Proc. Europe MENA Cooper. Adv. Inf. Commun. Technol.*, 2017, pp. 523–533.

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

[103] G. Zyskind, O. Nathan, and A. Pentland. (2015). *Enigma: Decentralized Computation Platform With Guaranteed Privacy*. Accessed: Dec. 12, 2018. [Online]. Available: https://enigma.co/enigma_full.pdf

[104] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proc. Cloud Comput. Security Workshop*, 2017, pp. 45–50.

[105] N. Foukia, D. Billard, and E. Solana, "PISCES: A framework for privacy by design in IoT," in *Proc. 14th Annu. Conf. Privacy Security Trust (PST)*, 2016, pp. 706–713.

[106] M. A. Walker, A. Dubey, A. Laszka, and D. C. Schmidt, "PlaTIBART: A platform for transactive IoT blockchain applications with repeatable testing," in *Proc. 4th Workshop Middleware Appl. Internet Things*, 2017, pp. 17–22.

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

[108] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Peer to peer for privacy and decentralization in the Internet of Things," in *Proc. IEEE/ACM 39th Int. Conf. Softw. Eng. Companion (ICSE-C)*, 2017, pp. 288–290.

[109] 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.

[110] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops (SPW)*, San Jose, CA, USA, 2015, pp. 180–184.

[111] Y. Rahulamathavan, R. C.-W. Phan, S. Misra, and M. Rajarajan, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, 2017, pp. 1–6.

[112] W. Chen, M. Ma, Y. Ye, Z. Zheng, and Y. Zhou, "IoT service based on jointcloud blockchain: The case study of smart traveling," in *Proc. IEEE Symp. Service Oriented Syst. Eng. (SOSE)*, Mar. 2018, pp. 216–221.

[113] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains," in *Proc. 2nd ACM Int. Workshop IoT Privacy Trust Security*, 2016, pp. 29–36.

[114] M. S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS," in *Proc. 7th Int. Conf. Internet Things*, 2017, Art. no. 14.

[115] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, "A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids," in *Proc. Living Internet Things Cybersecurity (IoT)*, 2018, pp. 1–6.

[116] J. Wang *et al.*, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *IEEE Access*, vol. 6, pp. 17545–17556, 2018.

[117] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2875542.

[118] F. Gao *et al.*, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Netw.*, vol. 32, no. 6, pp. 184–192, Nov./Dec. 2018.

[119] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," *Comput. Security*, vol. 37, pp. 111–123, Sep. 2013.

[120] X.-J. Lin, L. Sun, and H. Qu, "Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications," *Comput. Security*, vol. 48, pp. 142–149, Feb. 2015.

[121] T. Hardjono, N. Smith, and A. S. Pentland, "Anonymous identities for permissioned blockchains," MIT Connection Sci., Rep., 2016.

[122] E. Brickell and J. Li, "Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities," in *Proc. ACM Workshop Privacy Elect. Soc.*, 2007, pp. 21–30.

[123] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin P2P network," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2014, pp. 15–29.

[124] A. Boualouache and S. Moussaoui, "Urban pseudonym changing strategy for location privacy in VANETs," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 24, nos. 1–2, pp. 49–64, Jan. 2016. [Online]. Available: https://doi.org/10.1504/IJAHUC.2017.080914

[125] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2627–2637, Aug. 2018.

[126] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007. [Online]. Available: http://dl.acm.org/citation.cfm?id=1370616.1370618

[127] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[128] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Honolulu, HI, USA, 2017, pp. 468–475.

[129] P. Urien, "Towards secure elements for trusted transactions in blockchain and blochchain IoT (BIoT) Platforms," in *Proc. 4th Int. Conf. Mobile Secure Services (MobiSecServ)*, 2018, pp. 1–5.

[130] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, p. 533, 2016.

[131] A. Boudguiga *et al.*, "Towards better availability and accountability for IoT updates by means of a blockchain," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS&PW)*, 2017, pp. 50–58.

[132] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the Internet of Things," in *Proc. 23rd ACM Symp. Access Control Models Technol. (SACMAT)*, 2018, pp. 77–83. [Online]. Available: http://doi.acm.org/10.1145/3205977.3205993

[133] B. Yu *et al.*, "IoTchain: Establishing trust in the Internet of Things ecosystem using blockchain," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 12–23, Jul./Aug. 2018.

[134] I. Psaras, "Decentralised edge-computing and IoT through distributed trust," in *Proc. 16th Annu. Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, 2018, pp. 505–507. [Online]. Available: http://doi.acm.org/10.1145/3210240.3226062

[135] P. Otte, M. de Vos, and J. Pouwelse, "Trustchain: A Sybil-resistant scalable blockchain," *Future Gener. Comput. Syst.*, Sep. 2017.

[136] F. Tian, "A supply chain traceability system for food safety based on haccp, blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manag. (ICSSSM)*, 2017, pp. 1–6.

[137] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—A use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, 2017, pp. 772–777.

[138] M. Samaniego and R. Deters, "Blockchain as a service for IoT," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber. Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2016, pp. 433–436.

[139] S. Tai, "Continuous, trustless, and fair: Changing priorities in services computing," in *Proc. Eur. Conf. Service Oriented Cloud Comput.*, 2016, pp. 205–210.

[140] P. R. Sousa, L. Antunes, and R. Martins, "The present and future of privacy-preserving computation in fog computing," in *Fog Computing in the Internet of Things*. Cham, Switzerland: Springer, 2018, pp. 51–69.

[141] T. McConaghy *et al.*, "BigchainDB: A scalable blockchain database," Berlin, Germany, BigChainDB, White Paper, 2016.

[142] W. Obile, *Ericsson Mobility Report*, Ericsson, Stockholm, Sweden, Nov. 2016.

[143] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[144] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in *Proc. Int. Conf. Comput. Sci. Electron. Eng. (ICCSEE)*, vol. 3, 2012, pp. 648–651.

[145] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[146] E. Bertino and N. Islam, "Botnets and Internet of Things security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[147] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[148] S. Sicari, A. Rizzardi, C. Cappiello, D. Miorandi, and A. Coen-Porisini, "Toward data governance in the Internet of Things," in *New Advances in the Internet of Things*. Cham, Switzerland: Springer, 2018, pp. 59–74.

[149] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, 2015.

[150] H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS&PW)*, Paris, France, 2017, pp. 1–3.

[151] L. M. Axon and M. Goldsmith, *PB-PKI: A Privacy-Aware Blockchain-Based PKI*, vol. 6, SCITEPRESS, 2016, doi: 10.5220/0006419203110318.

[152] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered IoT users," in *Proc. IEEE 1st Int. Conf. Internet Things Design Implement. (IoTDI)*, Berlin, Germany, 2016, pp. 13–24.

[153] 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.

[154] T. Le and M. W. Mutka, "CapChain: A privacy preserving access control framework based on blockchain for pervasive environments," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2018, pp. 57–64.

[155] H. Es-Samaali, A. Outchakoucht, and J. P. Leroy, "A blockchain-based access control for big data," *Int. J. Comput. Netw. Commun. Security*, vol. 5, no. 7, p. 137, 2017.

[156] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun. IEEE 14th Int. Conf. Smart City IEEE 2nd Int. Conf. Data Sci. Syst.*, Sydney, NSW, Australia, 2016, pp. 1392–1393.

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

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

[159] M. Steger *et al.*, "Secure wireless automotive software updates using blockchains: A proof of concept," in *Advanced Microsystems for Automotive Applications 2017*. Cham, Switzerland: Springer, 2018, pp. 137–149.

[160] O. Alphand *et al.*, "IoTchain: A blockchain security architecture for the Internet of Things," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Barcelona, Spain, 2018, pp. 1–6.

[161] R. B. Chakraborty, M. Pandey, and S. S. Rautaray, "Managing computation load on a blockchain-based multi-layered Internet-of-Things network," *Procedia Comput. Sci.*, vol. 132, pp. 469–476, Apr. 2018.

[162] J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry*, vol. 9, no. 8, p. 164, 2017.

[163] M. Vučinić *et al.*, "OSCAR: Object security architecture for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 3–16, Sep. 2015.

[164] N. Kshetri, "1 Blockchain's roles in meeting key supply chain management objectives," *Int. J. Inf. Manag.*, vol. 39, pp. 80–89, Apr. 2018.

[165] F. Imbault, M. Swiatek, R. De Beaufort, and R. Plana, "The green blockchain: Managing decentralized energy production and consumption," in *Proc. IEEE Int. Conf. Environ. Elect. Eng. IEEE Ind. Commercial Power Syst. Europe*, 2017, pp. 1–5.

[166] S. Kikitamara, M. C. J. D. van Eekelen, and D. I. J.-P. Doomernik, *Digital Identity Management on Blockchain for Open Model Energy System*, Inst. Comput. Inf. Sci., Radboud Univ., Nijmegen, The Netherlands, 2017.

[167] M. Samaniego and R. Deters, "Hosting virtual IoT resources on edge-hosts with blockchain," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, 2016, pp. 116–119.

[168] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *Proc. Glob. Internet Things Summit*, 2017, pp. 1–6.

[169] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 464–467.

[170] J.-H. Lee, "BIDaaS: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2018.

[171] J. Hughes and E. Maler, "Security assertion markup language (SAML) V2.0 technical overview," OASIS SSTC, Burlington, MA, USA, Working Draft sstc-saml-tech-overview-2.0-draft-08, pp. 29–38, 2005.

[172] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," in *Proc. 2nd ACM Workshop Digit. Identity Manag.*, 2006, pp. 11–16.

[173] D. Hardt, "The OAuth 2.0 authorization framework," Internet Eng. Task Force, Fremont, CA, USA, Rep. 6749, 2012.

[174] H. A. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of namecoin and lessons for decentralized namespace design," in *Proc. WEIS*, 2015.

[175] D. Shrier, W. Wu, and A. Pentland, *Blockchain & Infrastructure (Identity, Data Security)*, MIT Connection Sci., Cambridge, MA, USA, 2016, pp. 1–18.

[176] N. Rückeshäuser, "Typology of distributed ledger based business models," in *Proc. 25th Eur. Conf. Inf. Syst. (ECIS)*, Guimarães, Portugal, 2017, pp. 2202–2217.

[177] A. Act, "Health insurance portability and accountability act of 1996," *Public Law*, vol. 104, p. 191, 1996. [Online]. Available: jhswestern.homestead.com

[178] *European CommissionDirective 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal of the European Communities Number L 281/31*. Accessed: Dec. 20, 2018. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[179] T. Fan and Y. Chen, "A scheme of data management in the Internet of Things," in *Proc. 2nd IEEE Int. Conf. Netw. Infrastruct. Digit. Content*, 2010, pp. 110–114.

[180] F. Khodadadi, R. N. Calheiros, and R. Buyya, "A data-centric framework for development and deployment of Internet of Things applications in clouds," in *Proc. IEEE 10th Int. Conf. Intell. Sensors Sensor Netw. Inf. Process. (ISSNIP)*, 2015, pp. 1–6.

[181] Q. Xu, K. M. M. Aung, Y. Zhu, and K. L. Yong, "A large-scale object-based active storage platform for data analytics in the Internet of Things," in *Advanced Multimedia and Ubiquitous Engineering*. Heidelberg, Germany: Springer, 2016, pp. 405–413.

[182] A. J. J. Valera, M. A. Zamora, and A. F. G. Skarmeta, "An architecture based on Internet of Things to support mobility and security in medical environments," in *Proc. 7th IEEE Consum. Commun. Netw. Conf. (CCNC)*, 2010, pp. 1–5.

[183] C. C. Cerbulescu and C. M. Cerbulescu, "Large data management in IoT applications," in *Proc. 17th Int. Carpathian Control Conf. (ICCC)*, 2016, pp. 111–115.

[184] T. Li, Y. Liu, Y. Tian, S. Shen, and W. Mao, "A storage solution for massive IoT data based on NoSQL," in *Proc. IEEE Int. Conf. Green Comput. Commun. (GreenCom)*, 2012, pp. 50–57.

[185] Y. Zhou, S. De, W. Wang, and K. Moessner, "Enabling query of frequently updated data from mobile sensing sources," in *Proc. IEEE 17th Int. Conf. Comput. Sci. Eng. (CSE)*, Chengdu, China, 2014, pp. 946–952.

[186] X. Hao, P. Jin, and L. Yue, "Efficient storage of multi-sensor object-tracking data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 10, pp. 2881–2894, Oct. 2016.

[187] T. Lu, J. Fang, and C. Liu, "A unified storage and query optimization framework for sensor data," in *Proc. 12th Web Inf. Syst. Appl. Conf. (WISA)*, 2015, pp. 229–234.

[188] I. P. Zarko, K. Pripužić, M. Serrano, and M. Hauswirth, "IoT data management methods and optimisation algorithms for mobile publish/subscribe services in cloud environments," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, 2014, pp. 1–5.

[189] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *Proc. IEEE Mil. Commun. Conf.*, 2017, pp. 261–266.

[190] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. Int. Conf. Open Big Data (OBD)*, 2016, pp. 25–30.

[191] Q. Xu, K. M. M. Aung, Y. Zhu, and K. L. Yong, "A blockchain-based storage system for data analytics in the Internet of Things," in *New Advances in the Internet of Things*. Cham, Switzerland: Springer, 2018, pp. 119–138.

[192] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati, "Mind my value: A decentralized infrastructure for fair and trusted IoT data trading," in *Proc. 7th Int. Conf. Internet Things*, 2017, p. 15.

[193] F. Wang, S. Liu, P. Liu, and Y. Bai, "Bridging physical and virtual worlds: Complex event processing for RFID data streams," in *Proc. Int. Conf. Extending Database Technol.*, 2006, pp. 588–607.

[194] M. Ma, P. Wang, and C.-H. Chu, "Data management for Internet of Things: Challenges, approaches and opportunities," in *Proc. Green Comput. Commun. (GreenCom) IEEE Internet Things (iThings/CPSCom) IEEE Int. Conf. IEEE Cyber Phys. Soc. Comput.*, 2013, pp. 1144–1151.

[195] A. Asin and D. Gascon, *50 Sensor Applications for a Smarter World: Libelium White Paper*, Libelium, Zaragoza, Spain, 2012.

[196] *Huawei: IoT, Driving Verticals to Digitization*. Accessed: Dec. 12, 2018. [Online]. Available: http://www.huawei.com/minisite/iot/en/

[197] *Qualcomm: IoT Solutions*. Accessed: Dec. 12, 2018. [Online]. Available: https://www.qualcomm.com/solutions/internet-of-things

[198] *LG IoT SmartThinQ*. Accessed: Dec. 12, 2018. [Online]. Available: http://www.lg.com/us/discover/smartthinq/thinq

[199] *Samsung IoT Solutions*. Accessed: Dec. 12, 2018. [Online]. Available: https://goo.gl/fHtMm7

[200] *Cisco IoT Products and Services*. Accessed: Dec. 12, 2018. [Online]. Available: https://goo.gl/6z8o4c

[201] *Carriots by Altair*. Accessed: Dec. 12, 2018. [Online]. Available: https://www.carriots.com/

[202] *Eurotech M2M/IoT Software and Services*. Accessed: Dec. 12, 2018. [Online]. Available: www.eurotech.com/en/products/software+services

[203] *IBM Watson IoT*. Accessed: Dec. 12, 2018. [Online]. Available: https://www.ibm.com/internet-of-things

[204] *BlueApp*. Accessed: Dec. 12, 2018. [Online]. Available: https://www.blueapp.io

[205] *IoT Monetization: Ericsson*. Accessed: Dec. 12, 2018. [Online]. Available: https://goo.gl/kh8e3R

[206] *Deutsche Telekom M2M*. Accessed: Dec. 12, 2018. [Online]. Available: https://m2m.telekom.com/

[207] *Vodafone M2M/IoT Services*. Accessed: Dec. 12, 2018. [Online]. Available: www.vodafone.com/business/iot

[208] M. Westerlund, S. Leminen, and M. Rajahonka, "Designing business models for the Internet of Things," *Technol. Innov. Manag. Rev.*, vol. 4, no. 7, pp. 5–14, 2014.

[209] T. Keskin and D. Kennedy, "Strategies in smart service systems enabled multi-sided markets: Business models for the Internet of Things," in *Proc. 48th Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2015, pp. 1443–1452.

[210] *Internet of Things Companies: The Biggest IoT Directory*. Accessed: Dec. 12, 2018. [Online]. Available: http://http://www.iot-directory.com/

[211] *Fortinet Reveals 'Internet of Things: Connected Home' Survey Results*. Accessed: Dec. 12, 2018. [Online]. Available: http://www.fortinet.com/press_releases/2014/internet-ofthings.html

[212] C. Perera, R. Ranjan, L. Wang, S. U. Khan, and A. Y. Zomaya, "Big data privacy in the Internet of Things era," *IT Prof.*, vol. 17, no. 3, pp. 32–39, May/Jun. 2015.

[213] L. Xu *et al.*, "Enabling the sharing economy: Privacy respecting contract based on public blockchain," in *Proc. ACM Workshop Blockchain Cryptocurrencies Contracts*, 2017, pp. 15–21.

[214] M. Samaniego and R. Deters, "Using blockchain to push software-defined IoT components onto edge hosts," in *Proc. Int. Conf. Big Data Adv. Wireless Technol.*, 2016, p. 58.

[215] Z. Nehaï and G. Guerard, "Integration of the blockchain in a smart grid model," in *Proc. 14th Int. Conf. Young Scientists Energy Issues (CYSENI)*, 2017, pp. 127–134.

[216] E. Münsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *Proc. IEEE Conf. Control Technol. Appl. (CCTA)*, 2017, pp. 2164–2171.

[217] *Dajie Ltd. Website*. Accessed: Dec. 12, 2018. [Online]. Available: www.dajie.eu

[218] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *Proc. Int. Conf. Financial Cryptography Data Security*, 2015, pp. 528–547.

[219] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *Proc. Int. Conf. Financial Cryptography Data Security*, 2015, pp. 507–527.

[220] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "SPECTRE: A fast and scalable cryptocurrency protocol," in *Proc. IACR Cryptol. ePrint Archive*, vol. 2016, 2016, p. 1159.

[221] S. Popov, "The tangle," Budapest, Hungary, IOTA, White Paper, 2017.

[222] A. Churyumov, "Byteball: A decentralized system for storage and transfer of value," Moscow, Russia, Byteball, White Paper, 2016. [Online]. Available: https://byteball.org/Byteball.pdf
[223] N. Narula. (2017) *Cryptographic Vulnerabilities in IOTA*. Accessed: Dec. 12, 2018. [Online]. Available: https://goo.gl/jFKYPp
[224] F. R. Yu, J. Liu, Y. He, P. Si, and Y. Zhang, "Virtualization for distributed ledger technology (vDLT)," *IEEE Access*, vol. 6, pp. 25019–25028, 2018.
[225] K. Croman *et al.*, "On scaling decentralized blockchains," in *Proc. Int. Conf. Financial Cryptography Data Security*, 2016, pp. 106–125.
[226] *Ethereum Transaction Chart*. Accessed: Dec. 12, 2018. [Online]. Available: https://etherscan.io/chart/tx
[227] J. Herrera-Joancomartí, "Research and challenges on bitcoin anonymity," in *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*. Cham, Switzerland: Springer, 2015, pp. 3–16.
[228] S. Meiklejohn *et al.*, "A fistful of bitcoins: Characterizing payments among men with no names," in *Proc. Internet Meas. Conf.*, 2013, pp. 127–140.
[229] J. Barcelo. (2014). *User Privacy in the Public BitCoin BlockChain*. Accessed: Dec. 12, 2018. [Online]. Available: https://goo.gl/mN2y6V
[230] S. Feld, M. Schönfeld, and M. Werner, "Analyzing the deployment of bitcoin's P2P network under an as-level perspective," *Procedia Comput. Sci.*, vol. 32, pp. 1121–1126, Jun. 2014.
[231] P. Koshy, D. Koshy, and P. Mcdaniel, "An analysis of anonymity in bitcoin using P2P network traffic," in *Proc. Int. Conf. Financial Cryptography Data Security*, 2014, pp. 469–485.
[232] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Proc. IEEE Symp. Security Privacy (SP)*, 2013, pp. 397–411.
[233] E. B. Sasson *et al.*, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Security Privacy (SP)*, 2014, pp. 459–474.
[234] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash protocol specification," Lakewood, CO, USA, Zerocoin Electric Coin Company, White Paper, 2016.
[235] K. Naganuma, M. Yoshino, H. Sato, and T. Suzuki, "Auditable zerocoin," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS&PW)*, 2017, pp. 59–63.
[236] A. Kumar, C. Fischer, S. Tople, and P. Saxena, "A traceability analysis of Monero's blockchain," in *Proc. IEEE Eur. Symp. Res. Comput. Security*, 2017, pp. 153–173.
[237] S. Noether and A. Mackenzie, "Ring confidential transactions," *Ledger*, vol. 1, pp. 1–18, 2016.
[238] H. Kopp, D. Mödinger, F. Hauck, F. Kargl, and C. Bösch, "Design of a privacy-preserving decentralized file storage with financial incentives," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS&PW)*, 2017, pp. 14–22.
[239] G. Maxwell, "Coinjoin: Bitcoin privacy for the real world," in *Proc. Bitcoin Forum*, 2013.
[240] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "CoinShuffle: Practical decentralized coin mixing for bitcoin," in *Proc. Eur. Symp. Res. Comput. Security*, 2014, pp. 345–364.
[241] J. Bonneau *et al.*, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proc. Int. Conf. Financial Cryptography Data Security*, 2014, pp. 486–504.
[242] M. Möser and R. Böhme, "Anonymous alone? Measuring bitcoin's second-generation anonymization techniques," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS&PW)*, 2017, pp. 32–41.
[243] *Ethereum Light Client Protocol*. Accessed: Dec. 12, 2018. [Online]. Available: https://github.com/ethereum/wiki/wiki/Light-client-protocol
[244] *Segregated Witness Benefits*. Accessed: Dec. 12, 2018. [Online]. Available: https://bitcoincore.org/en/2016/01/26/segwit-benefits/
[245] *Raiden Network: Fast, Cheap, Scalable Token Transfers for Ethereum*. Accessed: Dec. 12, 2018. [Online]. Available: https://raiden.network
[246] *Swarm Documentation*. Accessed: Dec. 12, 2018. [Online]. Available: https://swarm-guide.readthedocs.io
[247] J. Kwon and E. Buchman, "Cosmos: A network of distributed ledgers," Cosmos, Washington, DC, USA, Rep. [Online]. Available: https://cosmos.network/resources/whitepaper on 20 Dec 2018
[248] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Gener. Comput. Syst.*, vol. 92, pp. 357–373, Mar. 2019.
[249] J. Vermeulen. *Bitcoin and Ethereum vs Visa and PayPal: Transactions Per Second*. Accessed: Dec. 12, 2018. [Online]. Available: https://goo.gl/31yXJ0
[250] A. Kiayias and G. Panagiotakos, "Speed-security tradeoffs in blockchain protocols," in *Proc. IACR Cryptol. ePrint Archive*, vol. 2015, 2015, p. 1019.
[251] V. K. Gurbani, V. Hilt, I. Rimac, M. Tomsu, and E. Marocco, "A survey of research on the application-layer traffic optimization problem and the need for layer cooperation," *IEEE Commun. Mag.*, vol. 47, no. 8, pp. 107–112, Aug. 2009.
[252] A. Akhunzada *et al.*, "Securing software defined networks: Taxonomy, requirements, and open issues," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 36–44, Apr. 2015.
[253] 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, Sep. 2017.
[254] C. Xu *et al.*, "Making big data open in collaborative edges: A blockchain-based framework with reduced resource requirements," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2018, pp. 1–6.

Muhammad Salek Ali received the B.Eng. degree in electrical (telecommunications) engineering from the National University of Sciences and Technology, Pakistan, in 2012 and the M.Sc. degree in data communication networks from Aston University, U.K., in 2015. He is currently pursuing the Ph.D. degree in electronics, telecommunications and information technologies from the University of Bologna. He is also researching with the OpenIoT Research Unit, FBK CREATE-NET, Italy. His research interests include blockchains and their applications within the Internet of Things, data science, and machine learning techniques.

Massimo Vecchio received the M.Sc. degree (*magna cum laude*) in information engineering from the University of Pisa, Pisa, Italy, and the Ph.D. degree (with Doctor Europaeus mention) in computer science and engineering from the IMT Institute for Advanced Studies, Lucca, Italy, in 2005 and 2009, respectively. In 2015, he is an Associate Professor with eCampus University. In 2017, he has also joined FBK CREATE-NET, Trento, Italy, to coordinate the research activities of the OpenIoT Research Unit. He is the Project Coordinator of AGILE, a project co-founded by the Horizon 2020 programme of the European Union. His current research interests include computational intelligence and soft computing techniques, Internet of Things paradigm and effective engineering design and solutions for constrained and embedded devices. Regarding his most recent editorial activity, he is an Editorial Board Member of *Applied Soft Computing* and the *IEEE Internet of Things Magazine*, besides being the Managing Editor of the IEEE IoT newsletters.

Miguel Pincheira received the Diploma degree in computer and informatics engineering and the master's degree in computer science from the University of Bío-Bío, Chillán, Chile, in 2007 and 2011, respectively. He is currently pursuing the Ph.D. degree in information and communication technology with the University of Trento. He was a full-time Lecturer and a Mentor for the students robotics group with the Computer Sciences and Information Technologies Department, University of Bío-Bío. He is also researching with the OpenIoT Research Unit, FBK CREATE-NET, Trento, Italy. His current research interest includes blockchain technology and its applications in the Internet of Things domain, embedded systems, and robotics.

Koustabh Dolui received the M.S. degree in telecommunications engineering from the Politecnico di Milano, Italy. He is currently pursuing the Ph.D. degree in computer science with the imec-DistriNet Department, Katholieke Universiteit Leuven, Belgium. He was a Research Engineer with FBK-Create-Net, Trento, Italy, for the EU H2020 project AGILE. He has published and delivered talks in multiple conferences since 2013. His current research interests are focused on scalable data processing in multitier IoT architectures and distributed machine learning techniques.

Fabio Antonelli received the master's degree in electronics engineering from the Politecnico di Milano, Milan, Italy. He is the Head of the OpenIoT Research Unit, FBK CREATE-NET, Trento, Italy. He worked for over 15 years in the telco sector (within Alcatel and Telecom Italia groups) gaining extensive knowledge in experimental research, design, software development, and management of ICT projects. In FBK, his interests have shifted on applied research in multimedia networking, architectures and platforms for the Internet of Things, where he has contributed and coordinated applied research activities in different European research projects in the Future Internet, multimedia, and Internet of Things domains.

Mubashir Husain Rehmani (M'14–SM'15) received the B.Eng. degree in computer systems engineering from the Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2004, the M.S. degree from the University of Paris XI, Paris, France, in 2008, and the Ph.D. degree from the University Pierre and Marie Curie, Paris, in 2011. He is currently with the Telecommunications Software and Systems Group, Waterford Institute of Technology, Waterford, Ireland. He served as an Assistant Professor with the COMSATS Institute of Information Technology, Wah Cantonment, Pakistan, for five years. He has authored/edited two books published by IGI Global, USA, one book published by CRC Press, USA, and one book with Wiley, U.K. He is currently an Area Editor of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. He served as an Associate Editor for the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS from 2015 to 2017. He currently serves as an Associate Editor for *IEEE Communications Magazine*, the *Journal of Network and Computer Applications* (Elsevier), and the *Journal of Communications and Networks*. He is also serving as a Guest Editor for *Ad Hoc Networks* (Elsevier), *Future Generation Computer Systems* (Elsevier), the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and *Pervasive and Mobile Computing* (Elsevier). He was a recipient of the "Best Researcher of the Year 2015 of COMSATS Wah" Award in 2015, the certificate of appreciation, "Exemplary Editor of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS for the year 2015" from the IEEE Communications Society, the IEEE ComSoc Technical Committee on Communications Systems Integration and Modeling, in IEEE ICC 2017, the Research Productivity Award in 2016 and 2017 and also ranked #1 in all Engineering disciplines from Pakistan Council for Science and Technology, Government of Pakistan, and the Best Paper Award in 2017 from Higher Education Commission, Government of Pakistan.