Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges

Ruizhe Yang, F. Richard Yu, *Fellow, IEEE*, Pengbo Si, *Senior Member, IEEE*, Zhaoxin Yang, and Yanhua Zhang

***Abstract*—Blockchain, as the underlying technology of cryptocurrencies, has attracted significant attention. It has been adopted in numerous applications, such as smart grid and Internet-of-Things. However, there is a significant scalability barrier for blockchain, which limits its ability to support services with frequent transactions. On the other side, edge computing is introduced to extend the cloud resources and services to be distributed at the edge of the network, but currently faces challenges in its decentralized management and security. The integration of blockchain and edge computing into one system can enable reliable access and control of the network, storage, and computation distributed at the edges, hence providing a large scale of network servers, data storage, and validity computation near the end in a secure manner. Despite the prospect of integrated blockchain and edge computing systems, its scalability enhancement, self organization, functions integration, resource management, and new security issues remain to be addressed before widespread deployment. In this survey, we investigate some of the work that has been done to enable the integrated blockchain and edge computing system and discuss the research challenges. We identify several vital aspects of the integration of blockchain and edge computing: motivations, frameworks, enabling functionalities, and challenges. Finally, some broader perspectives are explored.**

***Index Terms*—Blockchain, edge computing, network, storage, computation.**

I. Introduction

BLOCKCHAIN emerged as the underlying technology of the digital cryptocurrency has recently attracted great attention from the tech giants to manufacturers [1]. According to market intelligence firm Tractica, the annual revenue for enterprise applications of blockchain will reach U.S.$ 19.9 billion by 2025, and the market will be composed of 29 key use cases touching at least 19 different industry sectors.

Different from the centralized digital ledger approaches, blockchain uses community validation to synchronize the distributed ledgers replicated across multiple users. It is introduced with Bitcoin [2] to deal with the double-spending problem. Beyond its original design and application, blockchain becomes a foundational technology that leads to the paradigm shift from centralized control to decentralized control. From the perspective of the information and communications technology, the ownership of assets and the rights and obligations arising from agreements can be recorded on a blockchain, for its decentralization, transparency, security, immutability, and automation. But there's still a critical flaw that prevents us from seeing these applications come to fruition: scalability. Blockchain as it stands today, is limited in the ability to scale [3].

On the other side, rapid advancement in computing technologies has enabled a wide range of applications. In this context, edge computing [4] as an extension of the cloud is introduced. Edge computing may have other names, such as fog computing, virtual cloudlet and mobile cloud. Despite the arguments of the similarities and dissimilarities of these technologies, in term of the objective they are almost the same to enable billions of devices to run applications at the edge of the network. Similar to the cloud, edge computing assists the user by providing computation power, data storage, and application services to possess location awareness, maintain low latency, support heterogeneity, and improve Quality of Service (QoS) of the applications, especially the compute-intensive and delay-sensitive ones. The distributed structure of edge computing has numerous benefits. Nonetheless, its security and privacy are significant challenges, due to the interplay of heterogeneous edge nodes and the migration of services across edge nodes [5].

Therefore, the integration of blockchain and edge computing into one system becomes a natural trend [6]–[8]. By incorporating blockchain into the edge computing network, the system can provide reliable access and control of the network, storage and computation over a large number of distributed edge nodes. Consequently, network security, data integrity and computation validity of the system can be

Manuscript received April 3, 2018; revised September 20, 2018 and November 15, 2018; accepted December 19, 2018. Date of publication January 23, 2019; date of current version May 31, 2019. This work was supported in part by the Basic Research Program of the Beijing University of Technology (BJUT), in part by the Beijing Post-Doctoral Fund, in part by the Support Project of High-Level Teachers in Beijing Municipal Universities in the Period of 13th Five-Year Plan under Grant 067175315000, and in part by the National Natural Science Foundation of China under Grant 61671029 and Grant 61571021. *(Corresponding author: Pengbo Si.)*

R. Yang, P. Si, Z. Yang, and Y. Zhang are with the Beijing Advanced Innovation Center for Future Internet Technology, Beijing University of Technology, Beijing 100124, China, and also with the Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China (e-mail: yangruizhe@bjut.edu.cn; sipengbo@bjut.edu.cn; zhangyh@bjut.edu.cn).

F. R. Yu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: richard.yu@carleton.ca).

Digital Object Identifier 10.1109/COMST.2019.2894727

considerably improved. On the other hand, the incorporation of edge computing endows the system with plenty of computational resources and storage resources distributed at the network edge, which effectively offload the blockchain storage and the mining computation from the power-limited devices. Furthermore, the off-chain storage and off-chain computation at the edges enable the scalable storage and computation on the blockchain [9].

Despite potential vision of integrated blockchain and edge computing systems, research challenges remain to be addressed before its widespread applications. Particularly, for scalability enhancement, it seems that a combination of approaches in different levels will be ultimately used. Meanwhile, the new security issues caused by outsourcing a large scale of services at the edge need to be studied further more. Besides, self-organization effectively reduces the complexity of management by adding autonomic mechanisms but also triggers new security problems. In addition, the functionalities of network, storage and computation based on blockchain and edge computing should be deeply integrated in different levels from multiple points of view with flexibility and stability. Accordingly, resource management covering different aspects needs to be broadly tackled through comprehensive research efforts. Finally, from a broader view, the directed acyclic graph, big data and artificial intelligence provide promoting relationship with blockchain and edge computing.

In this survey, we investigate the work that has already been done to enable the integration of blockchain and edge computing systems, and explore the related research challenges. The approach towards the design of the integrated blockchain and edge computing system is presented in Fig. 1, where we focus on overview, motivations, frameworks, enabling functionalities, challenges and broader perspectives.

The rest of the article is structured as follows. Section II presents an overview of blockchain and edge computing technologies. Section III discusses the motivations and requirements of the integration of blockchain and edge computing. In Section IV we explore some of the typical frameworks of the integrated blockchain and edge computing. Section V presents the integrated work from network, storage, and computation in details. Research challenges and broader perspectives are addressed in Section VI. In the end, we conclude this article in Section VII.

II. An Overview of Blockchain and Edge Computing

In this section, a brief overview of blockchain and edge computing is presented.

A. Blockchain

Blockchain is a decentralized digital ledger in a peer-to-peer (P2P) network, where a replica of the append-only ledger of digitally signed and encrypted transactions is maintained by each participant. Although it derives from early technologies, blockchain has achieved enormous popularity with Bitcoin, a worldwide electronic payment system started in 2009 [10]. As people gradually deepen the understanding of blockchain, its technology scope and applications are extended.

1) Layers: To get a better and clearer understanding of what the technical contributions and performance improvements have been done, based on the studies in [11]–[13], a decomposition of the blockchain system into separate layers is introduced, which from bottom to top are the data, network, consensus, ledger topology, incentive, contract and application, as shown in Fig. 2.

The data layer encapsulates the data generated from different applications via the transactions and blocks. Transactions between two parties are verified and packed into a block with a block header to 'chained' back to the previous block, resulting in an ordered list of blocks, see Fig. 3. The block header specifies the metadata, including hash of the previous block, hash of the current block, timestamp of the block creating time, Nonce related to the mining competition in the upper layer and Merkle root resulted from the hash tree of all transactions in the block body.

The network layer defines the networking mechanism used in blockchain. The goal of this layer is to propagate data generated from the data layer. The network can be generally modeled as a P2P network, where peers are participants. Using the networking mechanism, once a transaction is generated, it will be distributed to the neighbors and only the valid transactions will be forwarded.

The consensus layer consists of the consensus algorithm to reach consensus among the untrustworthy nodes in decentralized environments. In the existing systems, there are three major consensus mechanisms: Proof-of-Work (PoW) [10], Proof-of-Stake (PoS) [14], [15], and Practical Byzantine Fault Tolerance (PBFT) [16]. In the competition of adding blocks into Bitcoin blockchain to get rewards, PoW is required for each competitor (miners) by repeatedly running hashing functions to find a Nonce value, which is difficult to produce but easy for others to validate. Due to the computational demanding of PoW, attacks from malicious nodes are prevented as their computing power is limited compared with the total network computing power (less than 51%). In PoS [17] used in Ethereum, the hash target is per coin age, which can be simply defined as currency amount times holding period, and thus the blockchain with the highest total consumed coin age is chosen as the main chain. It eliminates the high energy consumption in PoW but prevents attacks by raising the cost of controlling a sizable stake. Different from PoW and PoS applied in the public blockchain, PBFT is ran by the validating peers in the permissioned Hyperledger Fabric to validate the transactions. PBFT works assuming that less than one third of the nodes are faulty while all others execute correctly. Some variants [18], such as Delegated PoS (DPoS), Transactions as PoS (TaPoS), PoS-Velocity (PoSV), Delegated Byzantine Fault Tolerance (DBFT) and Bitcoin-NG, select some ones to generate and validate blocks to improve the scalability, throughput and latency. Also many other consensus mechanisms, such as Proof-of-Service [19], Proof-of-Storage [20], Proof-of-Contribution (PoC) [21], [22], etc., are designed for different specific applications.

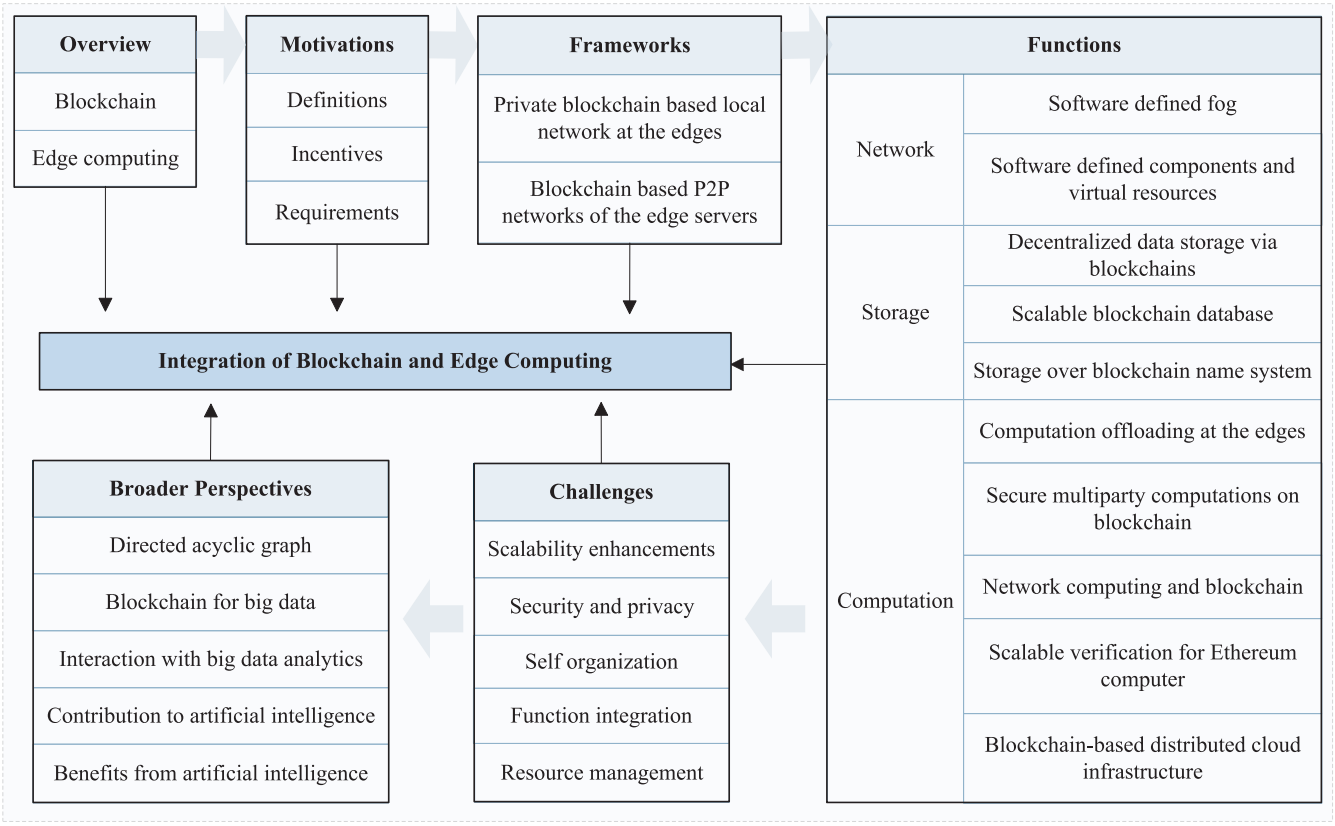


Fig. 1. Road map of the integrated blockchain and edge computing systems.

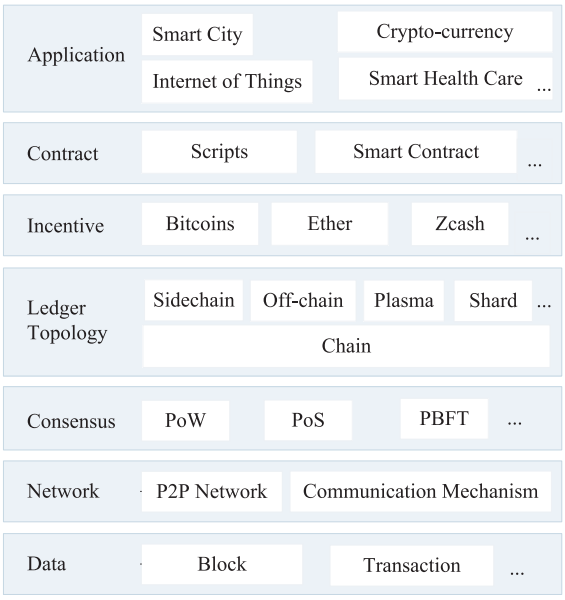


Fig. 2. Decomposition of blockchain.

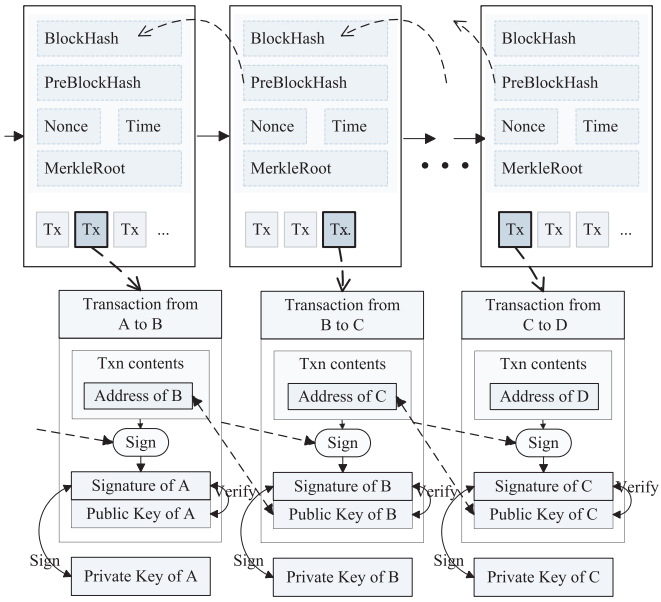


Fig. 3. Bitcoin's blockchain model.

The ledger topology layer defines the ledger topology for storing the authenticated data produced by the consensus layer. It contains the chain of blocks storing the ledger of the system and also some other states produced by consensus. Beyond the traditional block chain (main chain) structure as shown in Fig. 3, we pay special attention to some new chain topologies generated in the scalability improvement efforts. For instance, sidechains firstly proposed in [23] as a hierarchy of lower-tier 'consensus instances' can potentially have a lower degree of decentralization than the top-level chain, and permit funds moved between chains via transactions. Off-chain allows activities not to happen on blockchain. For example, lightning network [24] presents micropayment channels to send transactions, whose transfer of value occurs off-blockchain. Plasma

chains [25] composed in a hierarchy of tree, use merkleized proof to enforce child chains to maximize low-cost efficiency and net-settlement of transactions. Shard chains in Ethereum sharding [26] use on-chain state partition to gain higher throughput, where transactions are wrapped in a 'collation' and collations similar to blocks are chained using the hash value.

The incentive layer integrates economic incentives to motivate nodes to contribute their efforts to verify data. This is vital to keep the decentralized blockchain system without centralized authority working as a whole. In Bitcoin and Ethereum, bitcoins and ethers will be issued as rewards to the nodes who add blocks to the chain. Except for rewards, deposits and penalties are introduced into blockchain to secure the outsourced computation.

The contract layer brings programmable characteristics into blockchain. Scripting in Bitcoin provides a variety of ways to spend coins. Basically, each input of a transaction connects to a previous output and the connection is valid when the output's script evaluates to true given the signature provided by the input. In Ethereum, the smart contract as a powerful scripting is a group of state-response rules to automatically transfer the digital assets between users, which are far beyond just currency.

The highest layer in blockchain is the applications, including crypto-currency, Internet of Things (IoT), smart cities, etc., which could revolutionize many fields such as finance, management, and manufactures. However, blockchain is still in its infancy, academia and industry are trying to deepen the technology, particularly from the perspective of the information and communications technology, to support these advanced applications.

2) Characterization: The extension of blockchain technology scope and applications is still in progress. However, the core mechanism can be summarized as follows.

- Decentralized and transparent: A blockchain network has many validating peer nodes access to the information without a centralized authority. Therefore, transactions (records) are transparent and traceable.
- Synchronized through consensus: The consensus protocol ensures that a quorum of nodes reach an agreement on the new blocks of transactions orderly appended to the shared ledger, whose replicas maintained by participants are in sync.
- Security and immutability: The shared, tamper-proof replicated ledger guarantees the immutability and nonrepudiable through the one-way cryptographic hash functions. It is extremely difficult for adversaries to tamper with such a record, unless they control most of the miners.

B. Edge Computing

During the last decade, unlimited available resources of computing, storage and network management provided by cloud computing have resulted in lots of new cloud-based applications and rapid growth of many Internet companies, like Amazon. However, in recent years, a new trend is increasingly moving from the function of clouds towards the network edges [4], [27]. It is mainly required by some delay-sensitive applications, such as virtual reality, which has stringent delay requirements. Thus, the edge computing paradigm by pushing the cloud resources and services to the edge, enables mobility support, location awareness, and low latency. These promised gains make it a key technology for realizing various visions for next-generation Internet, such as IoT [5] and Tactile Internet (with millisecond-scale reaction time) [28].

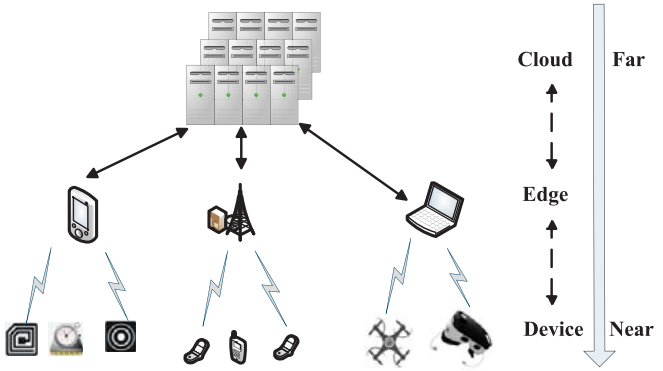


Fig. 4. The edge computing architecture.

1) Architecture: Generally speaking, the structure of edge computing can be divided into three levels: end device (front-end), edge server (near-end), and core cloud (far-end). This hierarchy represents the computing capacity of edge computing elements and their characteristics. End devices (e.g., sensors, actuators) at the front-end provide more interactive and better responsiveness for users. However, due to their limited capacity, resource requirements must be forwarded to the servers. Edge servers in the near-end can support most of the traffic flows in networks as well as numerous resource requirements, such as real-time data processing, data caching, and computation offloading. Therefore, edge servers provide better performance for end users with a small increase in the latency. Cloud servers in the far-end provide more powerful computing (e.g., big data processing) and more data storage with a transmission latency. The goal of this architecture is to execute the compute-intensive and delay-sensitive part of an application in the edge network, and some applications in the edge server communicate with the core cloud for data synchronization.

2) Characterization: The hierarchical architecture of edge computing encompasses the following attributes.

- Proximity and low latency: Near to the end of the edge computing both in a physical and a logical sense supports more efficient communication and information distribution than the far-away centralized cloud. It typically has tens of meters propagation distances for the cases of dense small-cell networks or machine-to-machine transmissions and is free from excessive delay in the backhaul network and Internet transmission. With these short propagation distances, edge computing has the potential of realizing tactile-level latency for many latency critical applications that may require tactile speed with latency approaching 1ms [29].
- Intelligence and control: The performance of a modern edge node is sufficient for the high rate transmission,

large data storage and sophisticated computing programs for a set of local users. This opens the way to the autonomous management of the application and the coordination in the edge, so that the computation and storage of end devices can be offloaded locally or delegated to other nodes or to the core selectively.
- Less concentration and privacy: Many edge computing servers could be private-owned cloudlets and these less concentration of information shall ease the concern of information leakage in cloud computing caused by the separation of ownership and management of data. For instance, the enterprise deployment of edge computing facilities sensitive information exchange within its own management, and hence has the potential to enhance the privacy.
- Heterogeneous and scalability: Edge computing that scales to a large number of sites, is a cheaper way to achieve scalability than fortifying the servers in the corporate center. Moreover, edge nodes, which could be heterogeneous platforms, provide efficiency by taking into account of the heterogeneity of devices.

III. Motivations and Requirements of Integration of Blockchain and Edge Computing

In this section, we first define the integrated system of blockchain and edge computing, then we discuss the motivation of the integration, followed by the requirements for the integration of blockchain and edge computing.

A. What Is the Integration of Blockchain and Edge Computing

To give a clear description of the integrated blockchain and edge computing system, we first demonstrate what we concentrate on blockchain and edge computing in this paper, respectively.

Blockchain concerned here pertains to its ability to allow the participant in the network to record the system in a distributed shared ledger. More attention is paid to its consensus protocol, ledger topology, incentive and contract in Fig. 2, which will be extended in the integration system to fit the different levels of edge computing systems and the combinations. The key points of blockchain are the advantages of security and privacy and the need for scalability improvement.

Edge computing considered here pertains to its capability to perform networking, storing and computing in the distributed network edge. The concentration is the service support and management. The key points of edge computing are the advantages of achieving scalability in a distributed way and the need for efficient control in a secure manner.

Therefore, the integrated frameworks and functionalities of blockchain and edge computing based systems here are aimed at providing secure services to fulfil the application requirement by taking into consideration of *network, storage and computation*, which cover the core layers of blockchain and the main capability of edge computing. The *possibility* of integration comes from both the same decentralized network infrastructure and the same functions of storage and computation, while the *necessity* of integration lies in the different advantages of blockchain and edge computing and accordingly their complementary roles. Next, we will present the details.

B. Why Do We Need Integration of Blockchain and Edge Computing

1) The Security of Edge Computing Is Challenged: The distributed structure of edge computing has numerous benefits. Nonetheless, its security is a significant challenge [5], [30], [31]. In the next-generation Internet, edge computing is in the complex interweaving of multiple and varied technologies (e.g., P2P systems, wireless networks, visualization, etc.). The interplay of heterogeneous devices as well as edge servers and the migration of services across global and local scales, create the potential for malicious behavior.

During message transmissions, some attacks (e.g., jamming attacks, sniffer attacks, and others) could be launched to disable the links by congesting the network, or to monitor the network data flow. Thus, configurations input by network administrators need to be trustworthy and validated, which actually are challenged due to the high dynamism and openness of the edge computing environment. Besides, in managing heterogeneous edge networks, it is hard to isolate the management traffic from the regular data traffic, which makes the adversaries control the network easier. In addition, decentralized controls at the edge of the Internet may bring heavy burden to the network management.

In edge computing networks, the data are separated into many parts and stored across different storage locations, which make it easier to lose data packets or store incorrectly. Thus, it is hard to guarantee data integrity. Besides, data leakage and other privacy issues could occur when the uploaded data involving several edge nodes may be modified or abused by the unauthorized adversaries. Another challenge for storage is ensuring data reliability, since traditional methods to detect and repair corrupted data using erasure codes or network coding result in heavy storage overhead in edge computing systems.

Another important security challenge in edge computing network is to maintain security and privacy in uploading computational tasks to edge computation nodes. Some verifiable computation schemes are introduced, where the computation is outsourced with the computation function or the public key to one or more servers, who return the result of the computation as well as a proof to verify the computation.

Thus, it can be seen that security issues such as secure control at the edge, secure data storage, secure computation and secure network may need new ideas to adapt to the decentralization, coordination, heterogeneity and mobility of edge computing, especially the combination of scalability with security in such massive overlays but avoiding the excessive encryption overheads.

2) Technical Challenges and Limitations of Blockchain: Despite the great potential of blockchain, it faces numerous challenges, which may limit its wide usage. There is some

kind of trilemma that blockchain systems can only at most have two of the decentralization, scalability and security [26]. Specifically, decentralization allows the network to be permissionless and censorship-resistant, security pertains to the immutability and the general resistance to attacks, and scalability concerns the ability to process transactions, respectively. Currently, the scalability issues, especially the limitations of low throughput, high latency, and resource exhausting hinder the practical feasibility of any blockchain-based solutions.

Blockchain requires increasing storage space as the number of transactions climbs up. The blockchain size of Bitcoin is about 158 GB in September 2017 whose bootstrap time is roughly four days for a new node taking part in. Ethereum seems to suffer a similar growth of applications, which is ameliorated by the fact that just the state instead of the entire blockchain history needs to be stored at the full node. Though the Internet is already massively big, it still shows a scaling limit to these kinds of decentralized networks. Besides, such a large blockchain size is a centralization risk, if only a small group of large businesses are capable to run full nodes and may cheat while the light nodes have no way of detecting this immediately [14].

Moreover, constrained by the maximum block size and the inter-block time used to generate a new block, the public blockchains, like Bitcoin (blockchain size limit of 1 MB per block) and Ethereum, can only handle on average 7-20 transactions per second, which is far below the mainstream payment processor, such as Visa credit card processing 2000 transactions per second on average [11].

Furthermore, from the perspective of users, the fee for transactions may vary since the services and miners differ the charge rate for the transaction's verification. However, the hardware cost for the mining process is non-negligible, tied with the power consumption required for the CPU calculus to be carried out [32].

To increase a blockchain's throughput, the easy ways of using many different altcoins or increasing the block size have been criticized for the cost of security and the centralization risk. Recently, on-chain scaling (sharding) and off-chain scaling (state channels) are arguably both necessary and complementary. However, all these technologies are still in the infancy stage and in need of other techniques to support, for instance, where to perform the off-chain staff.

Thus, the main goals of the research focus on increasing transaction throughput and decreasing the requirements on bandwidth, storage, and processing power for nodes while minimally sacrificing security.

3) The Benefits Brought by the Integration of Blockchain and Edge Computing: The same decentralization mechanism of both the blockchain and edge computing built on the computation, data storage, network, as well as their different complementary emphases are destined to their combination. Here, we give the benefits brought to each other from the combinations [33].

The incorporation of blockchain into edge computing enhances the *security*, *privacy*, and the *automatic resource usage*.

- Using the blockchain technique, it is possible to build a distributed control at dozens of edge nodes. Thanks to the mining process and the replication on a large number of nodes, blockchains protect the accuracy, consistency and validity of the data and rules over their life cycle in a transparent way. Thus, it is an effective solution accommodated to the larger number of heterogeneous users allocated at or moving between separated physical edges.
- Benefits of privacy in edge computing by storing data locally or small fragments of data among multiple parties are challenged for the disclosure in coordinating activities of the edges. Using the blockchain technique, each user manages its own and changeable keys to give the access and control of data without any third parties, and its pseudonymous nature allows coordinating on a peer-to-peer basis without disclosing the metadata (the source, the destination, the content) to anyone. Thus, it is possible to achieve complete privacy.
- Dynamic coordination among fog nodes involves resource borrowing and lending. Smart contract of blockchain facilitates the use of resources on demand simply by automatically running the on-demand resource algorithm for the requested service. Also the traceability of resource usage is provided in order to properly verify the service level agreement by both the client and the service provider. Thus, by blockchain and smart contracts, the resource use in edge computing is enabled with reliable, automatic and efficient executions and significantly reduced operational costs.

On the other hand, the incorporation of edge computing into blockchain brings the powerful decentralized *network* and *rich computation* and *storage resources* in the network edge.

- Blockchain consensus relies on data transmitted by the P2P network layer while edge computing paradigm originates from P2P but extends the peer to the devices at the edge and blends P2P computing with the cloud. This hierarchy architecture facilities the dissemination of information within blockchain and also physically supports some blockchain scaling approaches, for instance, the sidechain at the edge.
- The computation offloading from the end device to the edge server enables the resource-limited end users to take part in the blockchain. For example, Bitcoin's blockchain, as the most trusted immutable technique in existence but hardly ran on the mobile device or sensors, could be realized by employing the edge to process the power exhausted PoW puzzle for the users. Besides, the powerful edge introduces more economic approach for the blockchain computing resources management.
- Edge servers provide a strong storage capacity for the bulky public blockchain as well as the independent and confidential environment for the private blockchain. Furthermore, due to the limited size of data storage provided by blockchain, an off-chain data storage is necessary for some multimedia applications. The outsourcing of raw data to edge servers enables the utilization of cutting edge multimedia techniques on the blockchain.

C. The Requirements of Integration of Blockchain and Edge Computing

To implement the integration of blockchain and edge computing, several requirements need to be met [34]–[37].

- Authentication: In edge computing environments with multiple interacting service providers, infrastructures and services, it is paramount to validate the authentication of these entities, who co-work via their respective interfaces to achieve agreement by signing smart contracts. The rights and requirements of entities are recorded by blockchains during the contract establishment process. This is necessary for the establishment of secure communication channels between the elements of edge ecosystems even if they belong to different security domains.
- Adaptability: The number of devices and the complexity of applications, particularly the blockchain applied on the limited resource devices, are increasing as time goes by. Therefore, the integrated system of blockchain and edge computing should have the capability to support a fluctuating number of end users and tasks with different complexities, and the flexibility to adapt to the changing environment to allow the object or node connect or leave the network freely.
- Network security: Network security is a big concern to edge computing network due to the heterogeneity and the attack vulnerability. The integration of blockchain into edge computing networks is required to replace the heavy key management in some communication protocols, provide easy access for the maintenance of the massive scale distributed edge servers and make more efficient monitoring in the control plane to prevent malicious behaviors (like DDoS attack, packet saturating).
- Data integrity: Data integrity is the maintenance of and the assurance of the accuracy and consistency of data over its entire life-cycle. By exploiting the abundance of distributed storage resources of edge computing, replicating data over a set of edge servers as well as blockchain-based framework for data integrity service in a fully decentralized environment critically hamper the violation of data integrity (the loss or incorrectly modification of the outsourced data and the abused uploading). Therefore, a more reliable data integrity verification for both data owners and data consumers is required.
- Verifiable computation: Verifiable computation is enabling the computation offloaded to some untrusted clients, while maintaining correct results. Outsourcing computation in edge computing can scale to large numbers of computations without being constrained by the scalability of blockchain, while the incentive and autonomy of smart contract in the Ethereum blockchain should guarantee the efficient computation scheduling and the correctness of returned solutions.
- Low latency: Generally speaking, the latency of an application is the product of two components: transmission latency and computation latency. Computation latency indicates the time spent both on data processing and blockchain mining, which depend on the computation power of the system. The capacity to provide fast computing increases from end users to cloud servers but also causes a significant increase in the transmission latency. Therefore, the integration of blockchain and edge computing is to determine the mapping between what kind of the computation and where to be performed, thus to realize an ideal trade-off between transmission latency and computation latency.

IV. Frameworks of Integrated Blockchain and Edge Computing Systems

In this section, we summarize the typical frameworks (architectures) of integrated blockchain and edge computing systems. The presented frameworks are based on existing studies and reflect the basic ideas and mechanisms of the integrated systems. Unfortunately, this summary may not cover all the proposed architectures in literature, since each proposed architecture has its unique original intention, idea of design and working environment.

A. Related Work

The study of [19] proposes a distributed blockchain cloud architecture with Software-Defined Networking (SDN) enabled edge computing (fog nodes at the edge of the network), which is categorized into three layers, i.e., device, fog, and cloud. The filtered raw data is transmitted from the device layer to the SDN enabled fog layer, which is responsible for the real-time data analysis and service delivery for a set of local devices. All the SDN controllers are connected in a distributed manner using the blockchain technique, and each controller is empowered by an analysis function of the flow rule and a packet migration function to secure the network during attacks as well as a programming interface to operate the network management. A fog node reports the results of processed data to the distributed cloud and the device layers if needed, accesses the cloud to deploy the application service, and offloads computing workloads to the cloud when there are not sufficient computing resources. To approve the contributions in the performance of computation and in the transferring and storage of data in the blockchain, the consensus protocol Proof-of-Service is proposed, which uses the 2-hop technique to combine the mechanisms of PoS and PoW.

Li and Zhang [38] present a blockchain based multi-layer IoT network model. It divides the whole IoT into two parts: edge layers and high-level layers. The edge layer is defined as a local area network consisting of a certain number of objects with a central node managing them. However, this central node can also be regarded as a node of the superior layer. The edge layer here seems to be the combination of devices and fog in [19] while the high-level layers are similar to the combinations of fog nodes, fog aggregation nodes and the distributed cloud in [19]. Despite the flexible definition of edge layers, it is required to provide interfaces to the superior layer for addressing, allowing bidirectional data transfer and participating high-level layer activities as a node. Also,

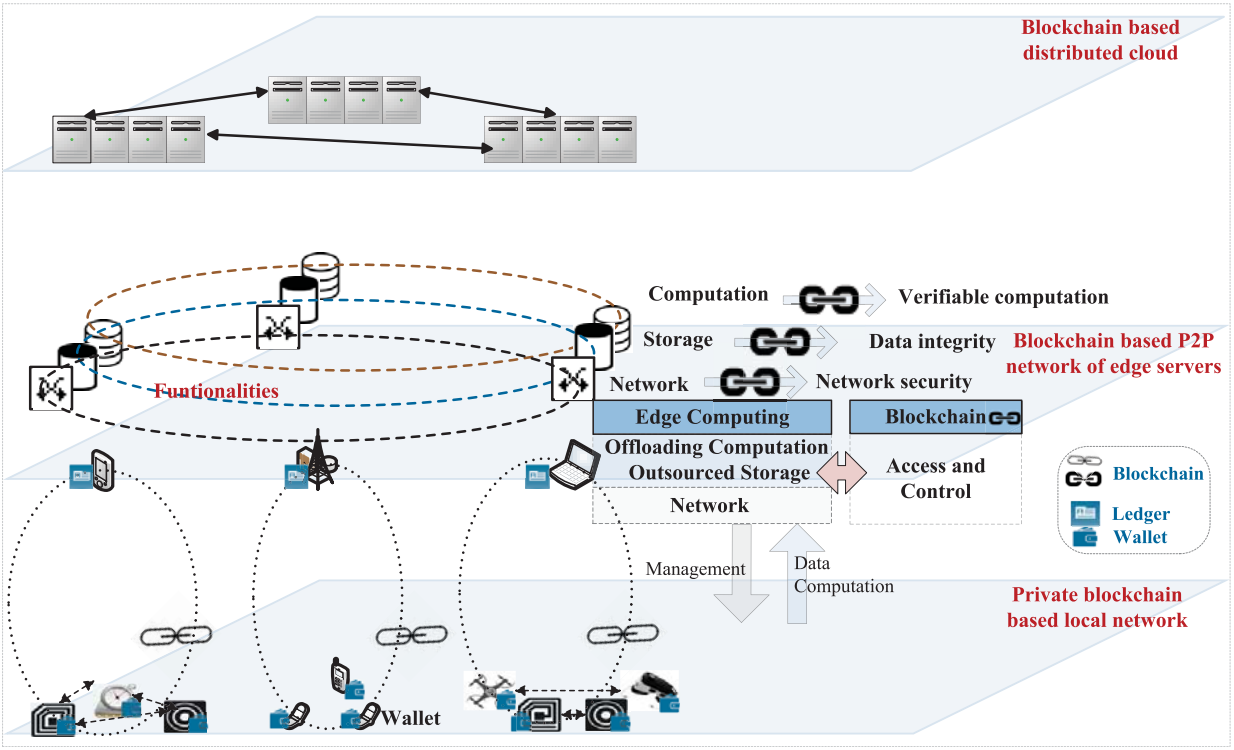


Fig. 5. Integrated blockchain and edge computing systems.

the self-independence is demanded that any object of a specified edge layer cannot communicate directly with other edge layers or higher layers. In high-level layers, except for the similar interfaces and independence requirement to edge layers, the distributed blockchain consensus is essential. Different from the management of central nodes in edge layers, nodes of high-level layers are data independent and have the full replica record of the exchanging between each other by blockchain.

Although the divisions of [19] and [38] are somewhat different due to the respective concentrating on the facility and network, the architectures are essentially in agreement with the distributed edge servers and the distributed cloud servers, both of which run on the blockchain technology.

In [8] and [39] an architecture of the blockchain based IoT virtual resources on edge host is proposed, which enables the fog as an extension of the cloud. The authors pay more attention to how the local edge network configures its P2P communicated M2M devices. Virtualization of software-defined IoT components (virtual resources) is introduced to manage the configuration of the large and heterogeneous set of devices, and the configuration of virtual resources (code or metadata) is stored in the form of encrypted blocks. Meanwhile, multiple tenants registered in the permission-based blockchain are given the capacity to define and deploy their own virtual systems and read or write in the blocks. Therefore, the permissioned blockchain manages the provisioning of virtual resources and multi-tenant access in a secure manner.

Different from the deploying of the blockchain techniques in the explicit tiers of edge computing network, IBM jointly develops with Samsung Electronics the Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) [40], [41], a foundation to build a decentralized IoT from the business view. It advocates the shift of power in the network from the center to the edges, so that devices gain greater autonomy and become points of transaction on the blockchain. Ethereum protocol is chosen in its alpha version and there are three types of peers: light peers, standard peers and peer exchanges, with the gradually increasing processing ability. Light peers (like sensors) perform messaging, retain a light wallet with their blockchain addresses and balances, and perform minimal file sharing. Standard peers retain a part of the blockchain and support light peers. Peer exchanges are potential repositories for a complete copy of the blockchain and provide blockchain analytical services.

Some other work also studies the blockchain technology as a platform for edge computing in specialized application. Without losing generality, we will also provide a quick glance on their proposed frameworks. A blockchain based distributed control system for edge computing is proposed in [42]. Emulating the three-tier edge computing model (devices, a mesh of edge nodes and cloud services), the Docker containers are deployed on edge nodes in addition to Hyperledger Fabric validating nodes on the top, which execute smart contracts to ensure that transactions are secured and properly validated. In the case of smart home, Dorri *et al.* [43] presents the local private blockchain with miners in home, which is similar to the local edge network configuration in [8]. Further, the work in [44] extends blockchain to the three tiers of smart home, overlay network and cloud storage with different types of blockchains depending on different trust, privacy and fault tolerance requirements. For vehicular communication systems, a framework for blockchain based secure key management

within the heterogeneous network is proposed [45], where Security Managers (SMs) are placed at the second layer in a geographically sparse manner (equivalent to the edge server), one for each security domain manages the cryptography materials, and the mined blocks are shared within the network for SMs to create public ledger of key transfer and management. Combined with artificial intelligence, an Ethereum based edge learning network named NeuRoNto is proposed in [46] to learn the personalized biology. The smart contract powered blockchain and multiple-agent communication technologies are used to organize the computing fogs to act as a global, distributed operating system, which can solve problems that are difficult for individual agents.

B. A General Framework

Despite the different original intention and working environment of these existing studies, *the integrated frameworks based on the general three-levels structure of edge computing can be derived as*:

1) The Private Blockchain Based Local Network Consisting of the End Nodes (Devices) and the Edge Server (Fog): Devices communicate to the central edge server, e.g., in the Wi-Fi and cellular systems, or have P2P communication with each other supported by the edge server, e.g., in the M2M IoT network. Due to the controllable access and clear identity in this local network, costly consensus mechanisms such as PoW and economic incentive are not needed and the private (permissioned) blockchain should be deployed here, which means less regulatory risk, less technical overhead, lower latency, no volatility and a wider range of consensus protocols to pick up. Generally it is cataloged into two types of structure depending on the different communication systems, processing capability and security requirements. One is the centralized management that edge server is responsible for adding new devices by creating a starting transaction and removing an existing device by deleting its ledger. Devices can communicate with each other only if the edge server permits them to do so by giving them a shared key. Each block is mined and appended to blockchain by the edge server. Another one is both devices and edge servers taking part in the blockchain, where the device performs as the light peer, receiving firmware updates or sending a transaction summary file to other peer devices. In both types, the edge server is mainly in charge of the local network control and provide the large amount of outsourced data storage and computation for the lower-ability devices based on the local blockchain in a secure manner, and some of these will be merged into the higher blockchain of servers.

2) The Blockchain Based P2P Network of Servers: For edge servers, beyond the important role in local networks, they also have the capabilities to store and forward messages to each other in order to make replications of data, share data, coordinately compute, etc. From a high-level view, the edge server perform light analytics for itself and its peers so as to realize the self-organizing that adding or deleting edge nodes adaptive to the environment. Considering the processing capability, a lightweight distributed consensus protocol should be deployed to assure the low latency and high throughput requirement. For the cloud with vast computation and storage capabilities, a distributed blockchain cloud provides low-cost, secure, and on-demand access to the most competitive computing infrastructures. Since both the scope of the P2P edge server network and the distributed cloud are much broader than the local network, the public blockchain, like Ethereum with smart contracts, is the most popular recommendations.

V. Network, Storage, and Computation of Integrated Blockchain and Edge Computing Systems

In this section, we will discuss how the integrated blockchain and edge computing systems satisfy the requirements of the network, storage, and computation, in detail. In each direction, some enabling technologies are presented.

A. Network

Ensuring security in the transmission process is one of the achievements for blockchain based edge computing network. In this integrated system, there is a typical data communication between two devices connected via their central nodes in edge layers. Besides, a blockchain (smart contract) communication [38] of the rules in data communications, such as addressing, encryption, rights and interests, validity period, etc., is set between the two edges. Therefore, data communications combined with the blockchain communications ensure the efficient and reliable cooperation of network.

During data transmission, several attacks (jamming attacks, Sybil attacks, flooding attacks, resource-depletion denial-of-service, and others [47]) at different levels could be launched to disable the links by congesting the network or could monitor network data flow. Moreover, edge computing is deployed to provide both the interfaces to subordinate (physical devices and communication) and superior layers (network and transport), and these various types of network and communication protocols, such as Mobile Wireless Networks, Wi-Fi, ZigBee and M2M, will obviously be challenging to manage network. SDN and its extension to Software-Defined Network Components (SDNC) [19] are the effective measures to mitigate the above problem. The software defined characteristics provide better network visibility by decoupling the control plane from the data plane, and the OpenFlow protocol leverages the network management and the smart contract by providing a programmable and standardized interface [48]–[50]. Besides, with the advent of SDN, Network Virtualization (NV) has gained a new traction [51]. Network virtualization rooting back in the 90s, enables the sharing and isolation of a vast resource among users as well as the constructing of a large virtual resource with small ones. This dynamic virtualized resource of network eases the network management in the context of SDNs and helps the network security and privacy realized by blockchain [8], [37], [49], [52].

1) A Software-Defined Fog: A software-defined fog [19] is composed of distributed SDN controllers, and all of the controllers in the network are interconnected in a distributed manner using the blockchain technique, so that communication can be reliable and efficient. Each SDN controller includes a

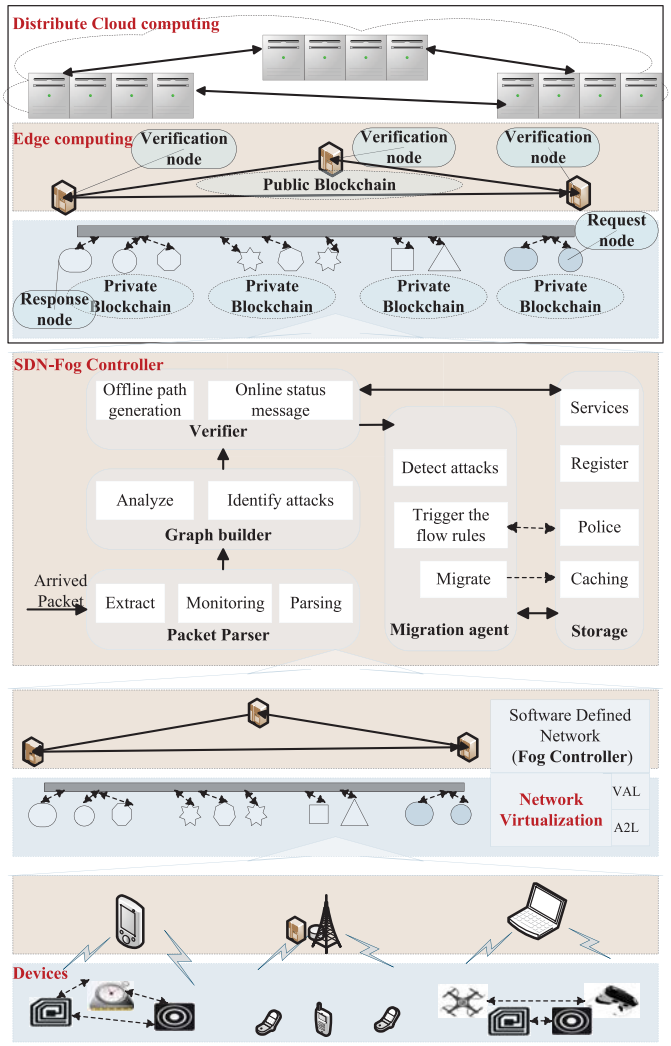


Fig. 6. Software defined & virtulization based distributed blockchain edge computing network.

flow control analyzer (parser, graph builder and verifier) and packet migration components (migration agent and data plane cache).

The analyzer is an application on the control plane, which performs the main functionality of the network infrastructure to counter saturation attacks.

- Parser monitor parses the incoming packets to extract the important metadata when attackers try to distort the network view of the controller via a subset of OpenFlow messages.
- Graph builder constructs and alters the flow diagrams connected to the network traffic based on the analysis on the parsed dataset, so that the attacks in the security policies reflected in the flowchart and the topological exchange metadata can be identified.
- In the verifier, offline path conditions are generated by navigating all the possible paths as well as collecting all the path conditions, while online reactive rules are established by monitoring and assigning the global variables' values to the status path and then parsing the paths to generate a status message.

The migration component, an application between the control plane and the data plane, sends a benign network stream to the OpenFlow controller in the attack.

- Migration agent detects attacks and makes different decisions. Against the saturation attacks, it triggers the flow rules of the parser to generate new rules and migrate the missing table packets in the data cache.
- Data plane cache is used to temporarily cache the missing packets in the case of saturation attacks and cache the flood packages during flooding attacks.

Here, the blockchain technique proposed in [7] can be directly employed to update the flow rules table in the edge computing environment, in which the software-defined fog maintains the records of flow rules table updated in its database, while the device has no database but updates its flow rules table into blockchain in the steps as follows.

- Request device updates the flow rules table by firstly broadcasting a request packet of the version verification, which demands the replies from the response device and all the fogs.
- The fog checks the version of the flow rules table in the request packet received. If it is the up-to-date version, the fog will further check its integrity, otherwise will package the latest version of the flow rules table into a response packet to be forwarded to the request device.
- The response device also checks the version consistency of the flow rules tables in the request packet and in its own records.
  (1) If both have the same version, the response device will let the other nodes in the blockchain network verify the hash value of flow rules table and cannot send the responding packet to the request device unless the confirmations from other nodes (i.e., PoW) make it believe the correctness of this flow rules table.
  (2) When the versions of flow rules tables are different, the response node have to check out the latest version. If the flow rules table of the response node is the up-to-date one, it will be packaged into a response packet and sent to the request node, otherwise the flow rules table of the response node in lower versions has to be updated.

2) The Software Defined Components and Virtual Resources: To enable the provisioning of services across cloud, fog and edge hosts, the software-defined components in the form of virtual resources are used in [8] and [49]. The virtual resources of network virtualization share many common elements in notions and interchangeably terms with SDN [53]. The view is offered by virtual resources, therefore, virtual systems on top of a physical system are created. The independent configuration of each virtual system distributing the workload to fogs in stead of constrained devices (seriously constrained in terms of energy, communications, and computation capabilities), can do real time processing or tasks and provide controlled and low latency access to physical devices. There are two layers in the resource virtualization:

- The Atomic Abstraction Layer (A2L) manages an one-to-one configuration relationship between its Atomic Virtual Resource (AVR) and the physical components (sensors,

actuators). An AVR exposes the Constrained Application Protocol (CoAP) method definitions: get, post, put and delete.
- The View Abstraction Layer (VAL) on top of the A2L manages an one-to-many relationship between its View Virtual Resources (VVR) and the lower AVR as well as a many-to-many relationship among the VVRs. In this layer, the work of services discovery and state retrieve are carried out via CoAP using the Constrained RESTful Environment (CoRE) link format (RESTful refers to the Representational State Transfer (REST) architecture).

In the scenario, where several virtual systems belong to different tenants, permission-based blockchains are deployed within each system to handle the provisioning of virtual resources and control the access to networks in a secure manner. System testing demonstrates faster response time in the implementation of Edison module connected to the Wi-Fi network with Multichain blockchain cluster hosted in the fog layer.

B. Storage

Edge computing keeps the data close to users by outsourcing the data to the edge of the network, which increases availability and reduces latency compared with the centralized cloud computing [54]. However, due to the separate storage locations, its data security, especially the data integrity is usually criticized [30]. Fortunately, integrating blockchain into edge computing extremely exploits the sameness between the P2P data storage mechanisms in edge computing and the P2P decentralized data validity of blockchain, but also their complementarity in the aspect of storage capacity and security provision.

Concerning to the combination of blockchain and edge computing for data storage, the difference between the two should be addressed firstly, since both often refer to the same term 'database'. In the sense of the ledger, sometimes blockchain is called a distributed database [54]. However, it is only capable of simple transactional logs rather than the massive amounts of data. Even with the burden of these simple logs, the scalability of blockchain is seriously challenged in the ledger size, throughput and latency. Thus, it is infeasible to store data directly in the blockchain [55]. The solution in [56] designs the off-chain storage with the Distributed Hash Table (DHT) in the blockchain, which uses the (key, value) pairs in DHT to provide the references to data, so that the blockchain turns into an automated access-control manager. This off-chain network developed into Enigma [57] overcomes data integrity issues. As a new era of petabyte scale data is coming, connecting the blockchain to the existing decentralized storage or database, which is capable of storing large scale of data off-chain, becomes more viable.

1) Decentralized Data Storage via Blockchains: Decentralized storage systems, which leverage the combined storage capacity of a network of peers to store and share content, have been widely studied in the file system and database communities for performance, availability and durability. Among the popular systems in recent years, InterPlanetary File System (IPFS) is the most robust, thought-through solution to decentralized storage. It synthesizes many of the best ideas from the most successful systems to date and proposes a novel protocol BitSwap for data exchange. The IPFS design in [58] and [59] goes through these layers, bottom-up: network, routing, exchange, merkledag, naming and applications, which are further visualized as libp2p, IPNS (name service) and IPFS stack to respectively move, define and use the data. A deeper understanding can be found from its underlying technologies, including DHT, Block Exchanges - BitSwap, Version Control Systems - Git, Self-Certified File (SFS) systems. For routing, DHT is utilized to announce added data to the network and helps locate the requested data. In particular to be efficient, IPFS DHT make a distinction for values stored based on their sizes, which directly stores small ones but only stores references for larger ones. BitSwap inspired from BitTorrent make IPFS distribute blocks quickly and robustly by adding new features with BitSwap credit and strategy. The Merkle DAG object model in Git provides facilities to capture changes to a file system tree over time in a distributed way. SFS is used to implement the IPNS name system, which generates and verifies the address of a remote filesystem.

The innovation made by IPFS extends the functionality to wider use of the decentralized data storage. On top of IPFS, Filecoin [20], similar to Bitcoin, works as an incentive layer to form an entirely distributed file storage system. Unlike Bitcoin's computation-only PoW, it introduces a class of Proof-of-Storage, in which Proof-of-Replication (PoRep) allows a prover to convince a verifier that some data has been replicated to its own uniquely dedicated physical storage and Proof-of-Spacetime (PoSt) enables a prover to convince a verifier the time of its storing data. With these novel consensus protocols, Filecoin creates powerful incentives for miners to amass as much storage as they can and rent it out to clients. On the other side, a fully decentralized blockchain based Data Integrity Service (DIS) with protocols for data integrity verification is proposed in [9], where Ethereum smart contract and IPFS are combined to facilitate the data verification. Also based on Ethereum and IPFS, a decentralized service marketplace system called Desema is presented [60], where IPFS is used for the off-chain service metadata to provide the on-chain identifier, so that data integrity can be checked by computing the identifier from the data in a smart contract and comparing it to the reference.

However, there are also other notable contenders [61], such as Ethereum Swarm, StorJ and Maidsafe. The primary objective of Swarm is to provide a sufficiently decentralized and redundant store of Ethereum's public record, and it seems an incentive platform enforced with smart contracts. StorJ creates a marketplace for buying or renting out disk space on the network with a blockchain. Maidsafe implements the 'SAFE Network', a next-generation decentralized and secure network like Ethereum, and provides similar services to Tron [62] gives a comprehensive comparison between Swarm and IPFS. It shows that as a unifying solution by integrating many existing protocols, IPFS is much further along in code maturity, scaling, adoption, community engagement and interaction with a

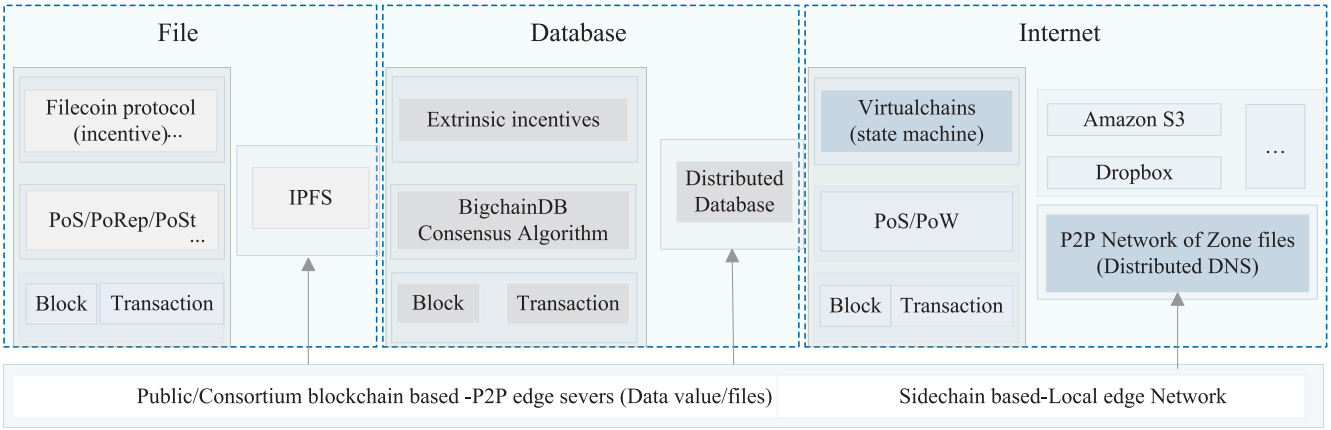


Fig. 7. Storage in the integrated blockchain and edge computing systems.

dedicated developer community. Therefore, at present IPFS seems like a great option for some projects.

2) The Scalable Blockchain Database: Since the blockchain cannot scale to handle large amounts of data in its current form, a scalable blockchain database named BigchainDB solves the scaling problem by adding the blockchain characteristics to a proven, scalable, big-data database [63], [64]. It avoids the full replication and some other technologies that plague Bitcoin, but takes the advantages of both the modern distributed databases and the blockchain. Built on the big-data distributed database, BigchainDB has these basic features: NoSQL query language, efficient querying, permissioning as well as the high throughput and capacity, which can be further increased by adding nodes. The inclusion of blockchain brings the capability of decentralized control, immutability and transfer of digital assets. Here, we list some key points of BigchainDB as follows.

- BigchainDB has two distributed databases: database S with the transaction set as a backlog and database C with the blocks to form a blockchain. There is a built-in consensus algorithm (like Paxos solving consensus among a group of unreliable processors with possible failures) in each database and a BigchainDB Consensus Algorithm between the databases, via which the transactions ordered and collected in S will be assembled into a block in the database C.
- Decentralized control is realized via the voting for the transactions in the block by a Domain Name System (DNS)-like federation of nodes (signing nodes), which are operated above the database's built-in consensus.
- Unlike a direct reference to the previous block in the typical blockchain, BigchainDB use a list of votes to provide references to the previous block, all of which should reference the same one and the exceptional may happen only if a node goes down.

Using different permissioning, the system can be a configuration from private enterprise blockchain database to open public blockchain database. The newly released version includes many fixes and tests to speak more confidently about BigchainDB's behavior in edge-case scenarios [65].

3) Storage Over Blockchain Name System: Since the DNS is a fundamental component of the Internet, Namecoin firstly focuses on some DNS defects and creates a decentralized DNS system with blockchain using PoW protocol. Afterwards, absorbing a lot of lessons from Namecoin, a global naming and storage system secured by blockchains named Blockstack [66] is proposed as a new Internet for decentralized applications. It makes great efforts in the blockchain layering, storage models, name pricing models, incentives for miners. Different from the other storage-oriented cryptocurrency blockchains, Blockstack decouples hosting data from operations of the underlying blockchain, whereby the storage systems can be more properly used.

There are three layers in Blockstack: the blockchain layer in the control plane, and the data storage layer over peer network layer in the data plane [67].

- The blockchain in control plane provides storage medium for operations and consensus on the order of operations. These operations are encoded by a special virtualchain on top of the underlying blockchain, which runs on the abstraction provided by the underlying blockchain with the complexity hidden underneath. Within the virtualchain, some new operations are defined, such as the rules for accepting or rejecting virtualchain, however, these definitions make no changes to the underlying blockchain.
- In data plane, the peer network provides a global index for discovery information by storing the routing information into zone files, which are identical to DNS zone files in the format. Whereas the actual data values are hosted in the external datastores with high-performance, which construct the storage layer. This separated storage from actual data to discovery data allows multiple storage providers to coexist, including both cloud storage (S3) and P2P systems (IPFS).

Blockchain Name System (BNS) that binds human-readable names to discovery data is built via the newly defined operations in virtualchain and the full replica of all zone files in a peer network. This decentralized naming system with distributed control gets rid of the central points of failure. In BNS, looking up data for a name is abstracted as follows.

- Find out the hash that is paired with the given name by searching for the name through virtualchain.
- Achieve the corresponding zone file in peer network by searching for this hash.
- Get the storage backend URI from the zone file to link to the storage backend.
- Read the data with access rights and verify the respective signature or hash.

Benefited from the decentralized naming system with the layered architecture, Blockstack strengthens the security and reliability of Internet services without any performances loss.

We just present the blockchain based storage from the aspect of decentralized storage, database and DNS with the representative systems. Their decentralization features all fit the geographical structure of the edge computing well. However, from the view of techniques and targets, the blockchain based decentralized data storage is the basic functionality and the blockchain based database is complementary to storage and used side by side with higher-level computing applications, and the compatibility of third-party storages and Internet support of Blockstack seems to provide a server support.

4) Use in Fog/Edge Computing Infrastructures: Due to the maturity of IPFS at present, some work of data storage in edge computing based on IPFS has been done. Confais *et al.* [68] analyze the favors of IPFS to the fog based on its immutable objects (name depending on content) and dedicated mechanisms to locate objects by Kademlia DHT. In details, it supports data locality by storing objects locally, works partially in disconnected mode when the location can be found in the Kademlia DHT and the storing node is reachable, natively enables mobility with a transparent relocation of data and scales to a large number of sites. The test of IPFS working at the edge of the network via the Yahoo Cloud System Benchmark (YCSB) illustrates the promotions of IPFS in the accessing time and the network exchange capacity between the sites, which obviously outperform Rados, an open source object storage service and Cassandra, an open-source distributed NoSQL database. The major drawback of IPFS in edge computing is the need to access the global DHT and accordingly a large amount of network traffic between the sites as well as the increasing access time for local reading. To deal with this problem, an IPFS coupled with Scale-Out NAS system is proposed in [68]. The Scale-Out NAS deployed locally and independently on each site of fog shares the object among all the IPFS nodes within this site and avoids to access the DHT when an object to read is locally stored. To realize security and privacy for IoT data, a modular consortium architecture on top of a software stack of blockchain and IPFS is proposed in [69], which includes two parts: private sidechains and the consortium blockchain. The private blockchain is maintained by the edge server (validator) for the devices in the local network and the global consortium blockchain connects edge servers.

The Local Blockchain and Data Storage: In the local private sidechain, devices encrypt the data with their own unique public and private keys and then send the encrypted data to the edge server. The edge server, which has more power in computation and storage, plays a role of a validator and authenticates any attempting to join in the sidechain. To this end, the smart contracts must have the following functions:

- Storing public keys of authorized devices and the hash of their IPFS files.
- Controlling the access, so that only the data from authorized device is allowed to connect the validator.

Once authentication is successful, the edge server logs a 'creation of data' transaction in a new block and then updates the IPFS file as well as its hash stored in the smart contract.

The Consortium Blockchain and Data Request: The decentralized consortium network with edge servers (validators) is responsible for the access control of the external requesters to a specific data within a specific sidechain. Access is authenticated by the combination of the access policies both in the consortium blockchain and in the sidechain, which includes the following steps:

- The requester signs an access request transaction with its private key.
- The validator node authenticates the requester in the consortium blockchain with the key. If the requester is unauthorized, the transaction will be dropped.
- Given the authorized requester in the consortium blockchain, the authentication in the requested sidechain will be verified.
- After passing both the authentication, the requester will receive the encrypted hash of the target IPFS file, which can be decrypted with the private key, and therefore access the target data.

To enable the data privacy and security, the smart contracts within consortium blockchain are required to be capable of modifying the access policies and the list of authorized requesters, for instance removing the requester from the authorized list to prevent its flooding if the number of its consecutive unsuccessful request goes beyond permission.

C. Computation

Besides the network control and storage, a critical role of edge computing is computation offloading of computation-intensive tasks from the less capable devices to the powerful edge servers, which can extend the battery lifetime of devices as well as speeding up the process of computation.

1) Computation Offloading at the Edges: In the local network at the edge, mobile devices or IoT devices are usually less capable of computation and low-powered. This limitation becomes critical for applications of blockchain, specifically in the mining process of PoW [70]. As a solution, edge servers near the end having sufficient resources for blockchain computing are used for offloading jobs from adjacent devices, so that blockchain deployment on devices is enabled with a local computing power supporting hashing, encryption algorithms, and possibly consensus like PoW.

For efficient edge computational resources management for the blockchain, some optimization models are proposed. Luong *et al.* [71] study the edge resources allocation for mobile blockchain and develop a deep learning-based auction scheme, where a multi-layer neural network architecture is constructed based on an analytical solution. The neural

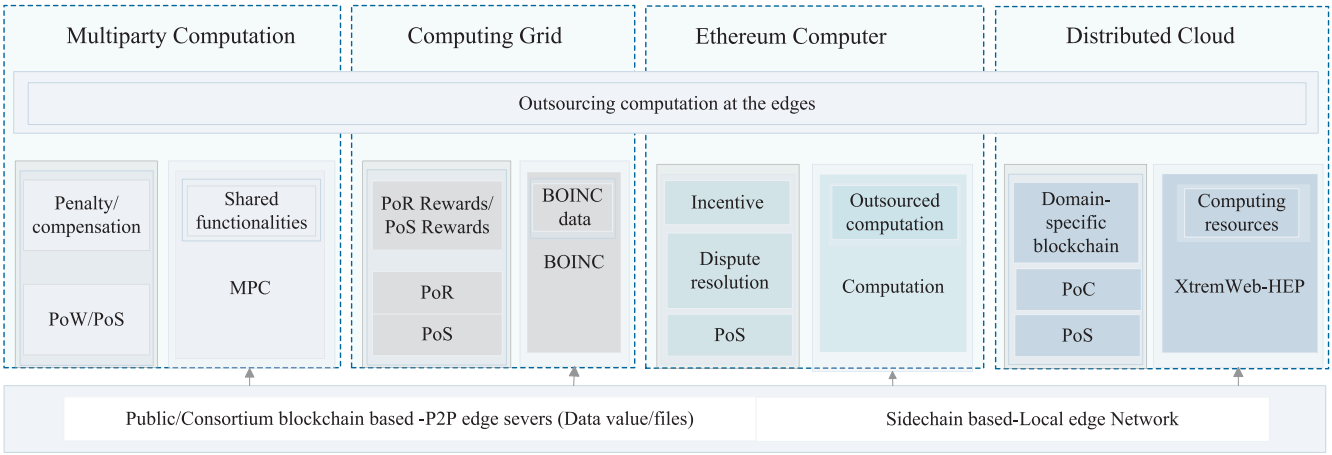


Fig. 8. Computation in the integrated blockchain and edge computing systems.

networks are trained using the valuations of the miners, and the network parameters are optimized by a Stochastic Gradient Descent (SGD) solver to minimize the loss function that is the expected, negated revenue of the computing provider.

In [72], based on blockchain mining experiment results, a hash power function is defined, which characterizes the probability of successfully mining a block per the amount of resources. Considering the competition among devices for the computational resources, the allocative externalities are considered in the model. In the auction mechanism, the social welfare is maximized while guaranteeing the truthfulness, individual rationality and computational efficiency.

A two-stage Stackelberg game is proposed to model the interaction between the computing provider and miners [73]. The edge server with computational resources playing the role of the leader in the game sets the price of the service per computing unit to maximize its profit in the upper stage. Based on the price set by the provider, the devices in need of mining blocks, being the followers in the lower stage, make a decision on the optimal amount of computing service for their offloading mining task.

On the other side, due to the less computation power of a single edge node compared with cloud computing, the computation tasks usually need to be assigned to several edge nodes. In this decentralized computing, both the efficiency and security are the key problems. Thus, distributed computing running on the blockchain becomes the most promising approach, where blockchain works as incentive as well as verification.

2) Secure Multiparty Computations on Blockchain: An early work on the integration of blockchain and computation in [74] studies how to do Multiparty Computation (MPC) on Bitcoin. Secure MPC is a subfield of cryptography that allows a group of mutually distrusting parties to jointly compute a function over their private inputs, and Bitcoin is used to construct a version of timed commitments for MPC. The committer is responsible for starting the MPC with a secret value but also forced to back the commitment with deposit to be deducted if the reveal of the secret is unfinished within the time specified. Therefore, fairness of certain multiparty protocols is obtained. Meanwhile, Kumaresan and Bentov [36] use Bitcoin to incentivize the correct computations. In its verifiable computation scheme, the solver can submit a proof of correctness along with the answer, which will be checked by miners or a designated verifier. A secure MPC protocol with compensation is put forth in [75], where the adversary has to suffer a monetary penalty if he mounts a denial of service attack while the honest ones collects a compensation, so that not only fairness is guaranteed but also the robustness. Later in [76], penalties are used to improve the efficiency, where the script complexity in both the non-reactive setting and the reactive setting is effectively reduced. An efficient protocol for amortized secure MPC with penalties and secure cash distribution is recently presented in [77]. After an initial phase of cryptocurrency, the parties are enabled to interact only among themselves over the course of playing many poker games, within which money changes hands. In a specific application, MPC is used for data queries in Enigma [57], a platform of both storing and computing for the data using blockchain. To reduce the communication complexity, hierarchical secure MPC is proposed at the cost of increased parallelizing computation complexity. In this research line, due to the original secure and verifiable features of MPC, blockchain mainly solves the fairness and privacy problem.

In the practical application, MPC is challenged by the unavailability of stability and preliminary configuration in dynamic environments. As a solution, the gateway is defined to perform coordination in [78], which can be considered as a virtual server at the edge. On the other side, enhancement of privacy and interactivity with end users is an advocated feature of the edge computing involved in performing computation and storing data locally, but currently in the lack of suitable computational platform. Recently, some studies have considered MPC as a suitable option to offer the basic block for building decentralized privacy preserving computational frameworks [79]. In [80], a threshold secure MPC (TSMPC) protocol is proposed, which enables the servers (edge severs) performing homomorphic computation on the data but without learning anything from them. Based on this TSMPC, a blockchain-based threshold IoT system called BeeKeeper

records the data in blockchain and let the nodes perform significantly less verification than TSMPC. All these preliminary research results show that the integration of blockchain, MPC and edge computing is a good choice to realize the scalable, secure and private computation.

3) Network Computing and Blockchain: Berkeley Open Infrastructure for Network Computing (BOINC) [81] is a platform for network computing, developed at U.C. Berkeley Spaces Sciences Laboratory. It is a generalized implementation of the client-server, Internet-scale model that SETI@home made famous. Note that SETI@home makes use of machines at the edges of the Internet, from which the edge-centric computing cloud takes inspiration. It is an open-source software for volunteer computing at first, where each project operates its own servers and the participants (clients), ranging from general purpose GPUs, to multiple powerful CPUs, to ubiquitous smart phones with the Application Programming Interfaces (APIs) and tools. In order to improve systems response time, virtualization is introduced into the combination of BOINC with clouds to create a volunteer cloud system [82]. Further to break through the inherent limitations of volunteers, scalable cloud resources are used for short on demand projects [83], in which the client side is changed from a volunteer computing architecture to an infrastructure as a service based on cloud computing. In the progress of developing a BOINC-based big data mining applications [84], a high-speed local network is required for connecting the computational resources and releasing the huge data sets to be transferred between clients. It can be seen that the BOINC platform is developing from a P2P scientific computing to a P2P cloud computing/edge computing for high computation task, particularly the big data applications.

However, BOINC is always challenged for its inadequate security [82], [84]. Recently as a solution, rewarding BOINC computation using blockchain [85], [86] on top of Proof-of-BOINC is proposed. Proof-of-BOINC is a hybrid proof of work consensus including the blockchain PoS and the BOINC contribution named Proof-of-Research (POR), which can be seen from the minting and verification process in Fig. 9.

4) A Scalable Verification for Ethereum Computer: Ethereum can be viewed as a decentralized computing platform or virtual machine to run the auto-executing programmed smart contract. However, it is not a complete virtual machine that most developers would need [55]. Miners in Ethereum collectively comprise the most powerful computational resources but offer very limited computation capacities for processing and verifying transactions, which are almost equal to the level of a smart phone.

To solve this bottleneck, a framework of computation through a scriptable cryptocurrency [87], called Ethereum computer, allows users to outsource computations to the network, which will receive incentive payments for the correct computation results.

TrueBit system in [88] amplifies the capabilities of Ethereum computer. It makes computing affordable by drastically reducing the superfluous network node required in traditional smart contracts and secures the computation task over trustless smart contracts by a novel two-layer verification mechanism.

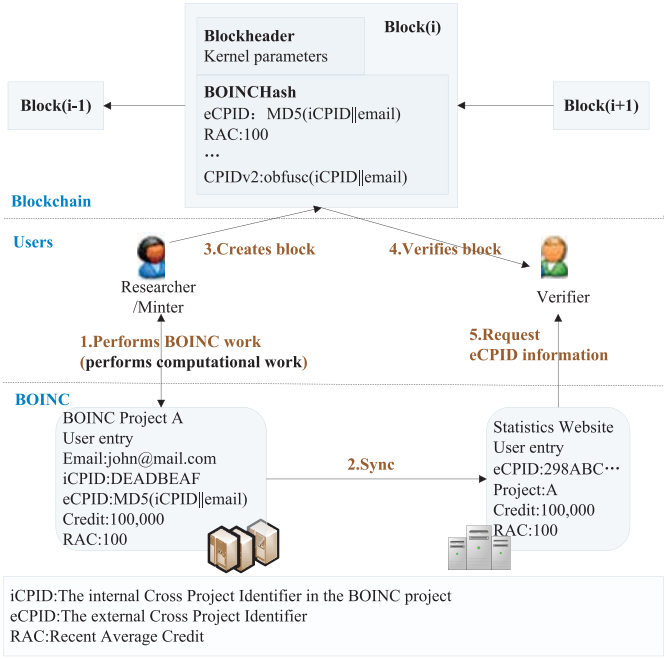


Fig. 9. Minting and verification process [86]. 1. A minter (Researcher) joins in a BOINC project A and carries out the computation. The project server (A) stores the minter's information and pay for the work by increasing the users Total Credit value. 2. Statistical websites download the statistics for all users from the project server (A). 3. The user earns credits with his RAC increasing and is able to create (mint) a block to be broadcasted to the network. 4. The Investor and Researcher in the network will verify the block by extracting the values from the BOINCHash data structure inside the received block, among which the eCPID is utilized to request the RAC and other information from a statistics website. 5. The Investor and Researcher compare the reply information from the statistics website to the ones derived from BOINCHash structure. If they are equal and the cryptographic puzzle is solved, the block is accepted.

- The dispute resolution layer with the verification game, solves the Verifier's Dilemma, in which the miner stops donating its limited resources to thankless verification tasks. This verification game proceeds in rounds among the solver who performs computational task to obtain the solution, the challenger who disputes the correctness of the solution, and the judger who decides on the correctness of the output. In each round of the game, the portion of computation in dispute is narrowed down.
- The financial incentive lay atop the dispute resolution layer, encourages anonymous parties to not only contribute CPU cycles but also perform requested computational tasks correctly. To incentivize correct computations, it periodically imposes forced errors to ensure the Verifiers' diligently searching for errors, and requires deposits from solvers and verifiers to thwart Sybil attacks.

The Golem project [89] to build decentralized supercomputer, which is crowdfunded 820,000 Ether (ETH) in 2016, cites TrueBit as a verification mechanism for their outsourced computation network. Golem connects computers in a peer-to-peer network, enabling direct payments between computing requesters, computing providers, and software developers with dedicated Ethereum-based transaction. Computing providers could be anyone, from an individual user renting out idle

CPU cycles of a portable computer, to a large datacenter contributing their entire capacity.

5) A Blockchain-Based Fully Distributed Cloud Infrastructure: Relying on XtremWeb-HEP and Ethereum smart contracts, a blockchain-based fully distributed computing infrastructure, named iEx.ec [21], [22] is proposed. XtremWeb-HEP [90] middleware similar to BOINC project, is an open-source desktop grid software to harvest computing power, providing the required features of fault-tolerance, multi-applications, multi-users, hybrid public/private infrastructure, etc. On top of XtremWeb-HEP, the development of smart contract supports distributed applications by incentiving the acquisition and provisioning of computing resources. For better performances, several technology innovations are made, especially the Proof-of-Contribution (PoC) consensus protocol and a domain-specific blockchain [21].

The consensus protocol PoC proves the correctness of the contribution out of blockchain, such as providing a data set, transferring a file, and performing a computation so as to enable the corresponding token transactions in the blockchain. It allows a consensus between the off-chain resources and blockchain. To prevent malicious users to fake the contributions, a decentralized network of trusted nodes is built using several certification mechanisms like reputation mechanism, PoS and transaction backward mutability window.

Domain specific blockchain (sidechain) is used to meet the case of transactions arriving en masse when tasks are submitted or the case of low latency required during communication and acknowledgement. Normally, an application would go through the standard blockchain, however, in the case of a large amount of tasks, some of the tasks can be offloaded to sidechains for tracking and feedback. This offloading can reduce the traffic on the generalized blockchain.

Within the interaction between the XtremWeb-HEP and the blockchain layer, smart contracts of matchmaking and multi-criteria scheduling play important roles in coordination. The matchmaking contract describes the demands for a task or a virtual machine instance in the terms of minimum amount of disk space, Random Access Memory (RAM), Graphics Processing Unit (GPU), etc. And then the scheduling contract according to these requirements is able to distribute the proper computational resources to execute tasks.

The research edition of iEx.ec will build block for fog/edge computing and make it the Heroku/Docker for blockchain computing by developing some advanced methods over iEx.ec ready DApps, which includes the integration with IPFS, the energy positive worker for micro-services and the container supporting trusted computing [21].

We just discuss the computation related to blockchain and edge computing from different aspects with different concerns. It firstly focuses on the need of edge computing for the blockchain, which offloads the computation needed by the consensus layer of PoW-based blockchains to the edges/fogs. The resource management and its pricing based optimization with intelligent algorithms are the core contributions. Next, high performance computations in need of blockchain and edge computing environment are deeply surveyed. Security and privacy are the outstanding features of MPC, which can be enhanced further by the blockchain and extended to dynamic IoT environment by using gateway at the edge, and certainly blockchain based MPC is a good choice to realize the privacy decentralized computation in edge computing. The combination of BOINC network computing and blockchain highlights the high-performance computation (big data mining) with efficient resource scheduling mechanism brought by BOINC and the complementarity of blockchain in security, both of which can be realized by an integrated proof of work at the consensus layer. Ethereum computer (TruBit) incentives correct decentralized computation with a sophisticated verification mechanism that solves the Verifier's Dilemma by imposing forced errors to ensure the diligently verifying. Finally, a blockchain distributed cloud infrastructure is built (iEx.ec) based on XtremWeb-HEP with a comprehensive designing from the sidechain storage, proof of work in the consensus layer, task scheduling to the integration with other technologies.

D. Remarks

1) Blockchain-Based Control: Through the discussion on the network, storage and computation, the role of blockchain as access and control of the integrated system becomes sharper. Particularly, integrated networks are mostly studied based on SDN, which is employed as the control unit in traditional networks. Also, the network virtualization decoupling the virtual networks from the dedicated hardware provides flexible network resource. Both the functionalities meet the access and control requirements from the blockchain. Besides, the programmability and software manner inherited from SDN and NV facilitate the implementation of blockchain. In the storage and computation, blockchain is combined with the existing P2P file systems, distributed databases, desktop grid software, etc., which create distributed storage resources and distributed computational resources on top of the physical hardware. The responsibility of the blockchain is to make sure the secure and effective use of these resources. Even in the Blockstack architecture, there is a clear definition of the blockchain layer in the control plane.

2) The Off-Chain Resource Provided at the Edge: Due to the scalability limits, it is impossible to store a large amount of data or run complex computation directly in blockchain, although it is to some extent a database and a virtual machine. The off-chain approach becomes one of the most promising solutions [91], particularly for the off-chain storage and off-chain computation in edge computing, whose large quantity of the idle computation power and storage space distributed near the end can yield sufficient capacities for performing computation-intensive and latency-critical tasks for the devices. In the iEx.ec project, the new PoC protocol enables DApps to access the off-chain computing resources, and the verification game in Truebit is also a solution that uses off-chain computations. There are several other similar implementations using a consensus between the blockchain and off-chain resources, like Filecoin, Fatcom [21], etc.

3) Latency and Resource-Constrained IoT Devices: The joint design of edge computing and blockchain can be

beneficial in addressing the latency issue in blockchain systems. It is well known that the low transaction rate of blockchain systems is related to the latency issue. With edge computing and 5G cellular networks, the latency can be reduced to the order of 1-10 milliseconds for low-latency application such as the Tactile Internet. For instance, considering the less powerful edge computing compared to cloud computing, a low-complexity blockchain consensus named proof of contribution with adaptive hash target is proposed in [92]. To save the storage of edge servers, futile transactions whose output are all referenced out and hence useless can be deleted, while the full history of transactions is kept in the cloud. Moreover, the transaction can be propagated before verification by giving the deposit, so that the latency is greatly reduced with edge computing. In addition, the joint design can be beneficial to resource-constrained IoT devices as well. With edge computing, the computation-intensive tasks in blockchain systems can be offloaded to the edge computing servers with low latency, then the shortcoming of IoT devices can be mitigated.

Finally, the enabling technologies discussed above are summarized in Table I.

VI. Challenges and Broader Perspectives

Despite the promising prospect of the integration of blockchain and edge computing, some significant research challenges remain to be addressed. In this section, we present some of these research challenges, followed by a discussion on broader perspectives.

A. Challenges

1) Scalability Enhancements: As we discussed in Section III-B2, scalability can be considered as alongside ideas of decentralization and security, to form the scalability trilemma. As a solution, outsourcing the storage and computation at the edge combined with the off mainchain protocols in the integration of blockchain and edge computing systems in Section IV and Section V effectively provides the scalable data storage and computation. In the local network, the private blockchain or the sidechain is employed. The sidechain scheme permits developers to connect new sidechains to the mainchain (e.g., Ethereum) with to-and-from transferring of the ledger assets [6]. However, the efficiency is criticized for the incurred high latencies for crossing chains, especially the crossing over the mainchain for spending funds between sidechains [93].

A special mention here is Plasma [25], a very recently proposed solution to the scalable computation on the blockchain, which supports potentially billions of state updates per second. It constructs blockchain computation in a MapReduce format, proposes a consensus mechanism to do PoS token bonding on top of existing blockchains and therefore composes blockchains into a hierarchical tree of child chains that periodically transfers information back to the root chain. Thus, the efficient matching of this hierarchical ledger topology and the hierarchical tiers of edge computing may provide an effective solution. However, Plasma increases scalability only by a constant factor with fixed withdrawal delays, otherwise its security level decreases with flexible withdrawal delays.

Unlike the layer 2 scaling approaches (e.g., sidechain, Plasma), blockchain sharding [26] splits the entire state of the network into partitions called shards, where each shard contains its own independent state and transaction history, and certain nodes would process transactions only for certain shards, allowing the throughput of transactions to be much higher. However, the problem with sharding is the cross-shard latency, which is likely to be on the order of minutes in Ethereum [94].

Concerning on the issues of cross-chain, in the Web3 stack [94], Interledger protocol enabling cross-chain interoperability becomes an important layer and some other optional components are suggested. However, there is no silver bullet that will solve all problems. It is likely that a combination of approaches fitted in the edge computing environment will ultimately be used, e.g., a combination of off-chain (Lightning Network), and Plasma atop Ethereum, or atop the base-layer PoS and sharding as recommended by Vitalik Buterin [95].

2) Security and Privacy: Despite the original security and privacy issues of blockchain [96], outsourcing services at the edges in the integrated system of blockchain and edge computing presents new security and privacy challenges. The off-chain solutions, which are most commonly used in the existing work, are still controversial for the lost transactions in the extreme case of nodes crashing over a channel [93], although strategies like the verification game in Truebit and PoC in iEx.ec are currently under development to address these problems.

In Plasma, the line between on-chain and off-chain is blurred by the tree hierarchy, and a series of fraud proofs that share a great degree of similarity with TrueBit are constructed to enforce the deposit and withdrawal between the child and the parent. But it may suffer adversarial mass withdrawal attack to prevent fraud proofs [25]. In its future research, withdrawals from Plasma chains could be secured by some other forms of non-interactive compact proofs, like Zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs), which is a valuable tool for verifiable computation and privacy preserving protocols [97]. However, due to the challenge in Common Reference String (CRS) model and slow software implementations, its concrete security of the deployment is lower than originally intended [98].

3) Self-Organization: The management of the network and the application will become a huge challenge with the growth of edge computing nodes. To facilitate the deployment of edge computing, self-organization is introduced to add the autonomic mechanisms so that the complexity of the technology can be masked from operators and users [99]. It is defined as the planning, configuration, management, optimization and healing of radio access networks in Self Organizing Network (SON). In IoT environments, the proposed self-organizing Fog of Things (FoT) [100] includes self-organizing monitoring, gateway deployment, failure recovery service, management and balancing of profiles. Some other self-properties, like

TABLE I
NETWORK, STORAGE, AND COMPUTATION OF INTEGRATED BLOCKCHAIN AND EDGE COMPUTING SYSTEMS

	Ref.	Applications	Purposes	Contributions
Network	[7]	IoT network	Detect attacks in the IoT network in real time	Distributed network architecture based SDN, using blockchain-based flow rule updating
	[8]	IoT network	Reduce the response time	A Multichain blockchain cluster in a Fog network to handle the provisioning of the virtual resources onto edge devices
	[37]	Smart Healthcare	A softwarized IoT infrastructure for secure and smart healthcare	A softwarized infrastructure (SDN and NVF) embracing cloud and fog computing, blockchain, Tor, and message brokers
	[19]	IoT network	Reduce delay and response time, increase throughput and detect real-time attacks	A blockchain-based distributed cloud architecture with SDN enabled controller of fog nodes
	[38]	IoT network	Secure IoT network	A multi-layer IoT network model based on blockchain technology
	[39]	IoT network	Reduce the communication delay	Cloud-hosted permission-based blockchains (Bluemix) for distributing usage
	[40] [41]	IoT network	Support P2P messaging, distributed file sharing and autonomous device coordination	Telehash for messaging, BitTorrent for file sharing and Ethereum, a blockchain protocol for autonomy (peer exchange, standard peer, light peer)
	[42]	Control systems	Blockchain-based distributed control system for edge computing	The Docker containers are deployed on edge nodes in addition to Hyperledger Fabric validating nodes
	[43]	Smart home network	Prevent DDOS attack and linking attack in smart home	Blockchain-based smart home framework: a miner in each smart home responsible for all communication within and external to the home
	[44]	Smart home network	A secure, private, and lightweight (eliminate the overhead of BC) architecture for IoT	A hierarchical blockchain-based architecture for IoT, including a private blockchain at local
	[45]	Transportation systems	Efficiency and robustness of key management	Blockchain-based distributed key management and a dynamic scheme to reduce the key transfer time
	[48]	IoT network	Prevent the attacks in SDN based IoT clouds	An overview of security issues of SDN based IoT clouds and the reasons of adding the blockchain-based security layer
	[49]	IoT network	Provisioning IoT services on the IoT edge devices	Use virtual resources in combination with a Multichain blockchain for provisioning IoT services on edge hosts
	[50]	Internet service providers network	Provide the content sessions quickly over the Internet	A system where each content session is brokered on the blockchain
	[52]	IoT network	Edge computing enable resilient wireless network virtualization	Leverage the blockchain protocol to prevent double spending of same wireless resources between mobile virtual network operator
Storage	[9]	IoT network	Ensure data integrity for cloud-based IoT	A blockchain-based framework providing the data integrity verification for both the data owners and the data consumers
	[20]	Internet network	Build a decentralized storage network	Turn cloud storage into an algorithmic market running on blockchains with the consensus Proof-of-Replication
	[56]	Storage network	Ensure users own and control their data in security	A decentralized data management system using blockchains as access-control managers
	[60]	Service system	Decentralized service marketplaces	Service marketplaces based on the Ethereum blockchain in combination with IPFS
	[63]–[65]	Database network	A scalable blockchain database	A distributed database added blockchain characteristics, fixed for edge-case scenarios
	[66], [67]	Internet network	A global naming and storage system	An architecture with one blockchain layer in the control plane and the peer network layer and data-storage layer in the data plane
	[69]	IoT network	IoT data privacy	A modular consortium architecture for IoT and blockchains

Continued on next page

self-maintain [18], [41] and self-awareness [101] share the similar ideas with self-organization. We can conclude from these studies that the first and important step is monitoring (awareness) [102], which is responsible for maintaining updated all critical information about FoT components, so as to automatically deploy the gateways or servers and cooperate for new applications [102].

And currently it seems that the integration of blockchain into edge computing is the best way to realize this self-organizing mechanism by using the auto-enforceable smart contracts to associate the related functions, which used to be separately realized [99]. It also enables the network to achieve consensus based coordination and validating operations to guard against routing or denial of service attacks [41], [103]. In [104], a self-evolving decentralized network is proposed with Cellular Automata (CA) powered consensus and Proof-of-Relay (PoRe) consensus. CA is a state machine with a collection of nodes, where each node changes its state following a local rule that only depends on its neighbors, and these local states eventually affect the global behavior by

TABLE II
NETWORK, STORAGE, AND COMPUTATION OF INTEGRATED BLOCKCHAIN AND EDGE COMPUTING SYSTEMS (CONTINUED)

Continued from previous page

	Ref.	Applications	Purposes	Contributions
Computation	[21] [22]	Internet network	A blockchain-based fully distributed cloud	A blockchain-based fully distributed cloud infrastructure with the Proof-of-Contribution (PoC) consensus protocol and a domain-specific blockchain (sidechain)
	[36]	Internet network	Incentivize correct computations	A model of incentivizing correct computations to realize verifiable computation, fair computation and secure computation
	[70]	IoT network	Mobile blockchain meets edge computing	An economic approach for edge computing resource management
	[71]	IoT network	Efficient edge computing resource management for the blockchain	An optimal auction based on deep learning algorithm for allocating edge resource for PoW
	[72]	IoT network	Edge computing as an enabler for mobile blockchain	A hash power function is defined and the social welfare is maximized with auction mechanism
	[73]	IoT network	Edge computing as an enabler for mobile blockchain	Formulate a two-stage Stackelberg game to jointly consider the edge service provider profit and the miners utilities
	[74]	Internet network	The fairness in certain multiparty protocols	Use Bitcoin to construct a version of timed commitments for MPC
	[75]	Internet network	Realize the fairness and robustness for MPC	A formal model of secure MPC with compensation
	[76]	Internet network	Secure MPC	Penalties are used to improve the efficiency of protocols
	[77]	Internet network	Amortized secure MPC	Stateful contracts enable richer forms of interaction between secure computation and a cryptocurrency
	[78]	Internet network	Flex secure MPC in IoT environments	Stateful contracts enable richer forms of interaction between secure computation and a cryptocurrency
	[80]	Internet network	A blockchain based threshold IoT system: BeeKeeper	A threshold secure MPC (TSMPC) protocol and a blockchain-based threshold IoT system based on TSMPC
	[82]- [84]	Internet network	Support a P2P cloud computing/edge computing	The combination of BOINC with clouds and high-speed local networks
	[85], [86]	Internet network	Securely reward volunteer computing in a decentralized manner	An open source cryptocurrency upon the BOINC platform
	[87]	Internet network	Computation through a scriptable cryptocurrency	Formalize the security model and implement the consensus computer in Ethereum with trade-offs in latency and accuracy
	[88] [89]	Internet network	A scalable verification solution for blockchains	Propose a dispute resolution layer with the verification game and a financial incentive layer to encourage parties to contribute the computation
Others	[46]	Artificial intelligence	Protect user data and incentive the artificial intelligence for the greater good of humanity	Decentralized artificial intelligence and distributing deep learning to the edge of the network
	[57]	Internet network	Jointly store and run computations on data	External blockchain is utilized as the controller of the network to enable the off-chain data storage and proofs of correct computations

propagating through local interactions. PoRe encourages participants to contribute to blockchain network by sharing their connectivity and band-width to get rewards. However, despite the general scalable and security problems, self-organization may trigger a cooperative attack. For instance, some attackers slow down the system performance, potentially reducing the amount of network connectivity and data transfer speed or claim large amounts of data, when the data are actually smaller than the amount of relay data.

4) Function Integration: Edge computing incorporates the combination of various platforms, network topologies, and servers. It is difficult to manage data and resources for diverse applications running on varying and heterogeneous platforms.

Regarding data management, various storage servers are running with various operating systems. In last section, we described the generalized frameworks of blockchain based IPFS, blockchain database (BigchainDB) and blockchain DNS (Blockstake). The combination of blockchain and IPFS gains much attention for the broader use of P2P file storage; BigchainDB, complementary to P2P file systems (IPFS, Enigma), are more geared to large-scale database-style decentralized storage; and Blockstake shows that decentralized control in the form of federations can work at Internet scale. They should be put into different applications according to their different strength or be revised to adapt to the edges structure. It has the same demand for the integrating of computations. For example, BOINC and XtremWeb-HEP can be integrated by the EDGeS bridge technology to provide a worldwide grid [105]. Therefore, the integration of these blockchains based computation systems becomes a natural trend.

Moreover, the integration of network, storage and computation functionalities into one system can provide not only support for highly scalable data retrieval but also powerful capability of data processing, hence reducing duplicate data transmissions and enabling computationally intensive

tasks [106], [107]. However, most of the present blockchain based studies and projects mainly focus on a single aspect. Enigma proposed in [57] is an early exploration of using blockchain to enable different parties to jointly do the task of data storage and data computation. Similar to the work in [69] and [85], the external blockchain in Enigma conducts as the controller of the network, through which the data off-chain stored on the client-side is accessible with the distributed hash-table and the Proofs of Correct computations are stored and audited. In particular to enable more demanding computations, only a small subset of the network performs each computation over different parts of the data instead of the full replication of the computation and storage in the network. Just recently, a data-oriented computing and networking paradigm named HyperNet is proposed [108], with the Private Data Center (PDC) featuring control over user data, concentration of computation and storage resources. Requesting data within a PDC is controlled by access control strategies with the help of SDN technology, and the interaction process between PDCs follows rules regulated by smart contracts. However, collaborative mechanisms between different kinds of blockchains in HyperNet are the future research challenged.

Thus, for the sake of the blockchain based storage and computation infrastructures to coexist with the edge computing network infrastructure, the different infrastructure type, topology, QoS requirement, service type and security level across these three need to be integrated with flexibility and stability.

5) Resource Management: Resource management as a dominating technique in networks has been widely investigated in various scenarios. A set of issues, challenges, and future research directions for edge computing are discussed in [5] and [29], for instance, the adaption to the dynamic environments and the large-scale optimization for the collaboration of multiple edge servers. These problems are more serious in the integration of blockchain and edge computing, since the collaboration of servers is much more tightly in the blockchain based secure manner, and the considerations are much broader [21]. In this distributed integration system, a matchmaking contract for resource provisioning is used to pair a resource request to a resource offer. It describes the computational resources characteristics in terms of the amount of RAM, CPU type and disk space, and implements the pairing with different kind of policies. Besides, to properly distribute tasks to run on a set of computing resources, a multi-criteria scheduler is required, which collects the computing resources and schedules the tasks using several strategies. A challenge is to design such multi-criteria scheduler on top of blockchain for the jointly optimization of integrated computation, storage and network functions. Moreover, the resources consumed by blockchain are non-negligible so that the edge computing resource management for the PoW has been studied in [70]–[73]. However, the quantitative analysis of the resources required for other consensus protocol is seldom studied so far.

B. Broader Perspectives

1) Directed Acyclic Graph: Directed Acyclic Graph (DAG) is a graph that flows in one direction, which has some similarity to the tree hierarchy but allows a block or transaction to reference multiple parents, leading to a DAG instead of a chain. A DAG structure of blocks (the block DAG) is proposed in [109], which incorporates the contents of off-chain blocks into the ledger and provides an increased throughput and a better payoff for weak miners. Another DAG structure without blocks but composed of transactions appears in Dagcoin [110], then followed by IOTA Tangle [111] and finally Byteball [112]. These three have some technical differences in the consensus protocol and transaction finality, due to their respective strength in their application areas. However, they are similar in using the DAG structure without miners. For example, in IOTA Tangle, when a new transaction joins the Tangle, it chooses two previous transactions to approve, thus, users who issue a transaction are contributing to the network's security. Each transaction directly involved in maintaining the sequences makes it blockless and more efficient and therefore outperforms the block DAG or general blockchains in the speed and the scalability. However, IOTA Tangle may be criticized for a centralized coordinator to do checkpointing, which is supposed to be shut down when the network is large enough. Since Tangle offers interaction with any blockchain technologies, a collaborative system of multiple blockchains to develop more robust decentralized consensus system is desirable.

2) Blockchain for Big Data: In the era of information explosion, the value of data greatly promotes the development of big data technology. However, facing an expansion in quantity and diversity of digital data, big data technologies still have challenges in control, authenticity and privacy, especially in the context of the distributed edge computing, which complementary to the cloud provides real-time big data analytics [113], [114]. The blockchain technology happens to be the solution to this problem with non-tampering, traceable and automatically executed smart contracts. Nevertheless, the combination research is still new and in experimenting phase. As we discussed in Section V-B2, BigchainDB design starts with a distributed database and adds blockchain characteristics, which enable the shared control of big data infrastructure, the audit trails on data and universal data exchange. It achieves the performance of 1 million writing per second, sub-second latency, petabyte capacity as well as the easy-to-use and efficient querying. Nevertheless, to realize the large scale data storage, BigchainDB avoids some key technologies of Bitcoin, such as the full replication. Abdullah *et al.* [115] study the Kerberos, which is the authentication protocols for Big Data. Security problems associated with Kerberos in large networks are presented, and the enhancement authentication and authorization are proposed based on the blockchain. In [116], from a view of business, a blockchain based ecosystem for big data exchange is proposed, where the blockchain is used to protect the copyright and privacy. Similarly, a credible big data sharing model is presented in [117] with the smart contact of purchasing between the two data owners. In [118], several blockchain solutions for big data are reviewed in different applications, which are especially important in the healthcare industry with the accuracy and time-sensitive need for data.

3) Interaction With Big Data Analytics: In addition to the trust data and universal exchange, blockchain integrated with

edge computing greatly improve the transparency and the real time in big data analytics. It is theoretically possible to get a hold of each transaction that has ever happened, and therefore, the trends and patterns are analyzed at the near-end edges. In other words, analytical results derived from the big data systems based on blockchain and edge computing are likely to be a lot more accurate and faster than they are today.

From another perspective, however, blockchain and edge computing may benefit from the use of big data analytics. Big data mining applications can run pattern recognition for thousands to millions of blockchain interactions, which contain various information of the system control, particularly the real-time analysis on the distributed techniques and models for data stream mining. Therefore, evil users and vicious behaviors are quickly identified and prevented so that the high performance is guaranteed. A successful example is Ripple, which reduces the cost of real-time transactions among banks by using the big data analytics to identify patterns in consumer spending and identify risky transactions a lot quicker.

4) Contribution to Artificial Intelligence: Owing to the huge amounts of data and computing power required, most of the Artificial Intelligence (AI) algorithms perform on cloud servers rather than at the edge. But the far placement of cloud makes current AI algorithms useless or inefficient for the time-critical applications. For now, the emerge of blockchain makes it possible to bring AI closer to the edge, with a high qualitative-large quantity of sharing data and a superpower blockchain based distributed computing [119]. Blockchain's decentralized/shared control and incentivization encourage data sharing, which in turns lead to high profits for participants as well as guarantee the data integrity for the whole data life [120]. Besides, blockchain and smart contracts take the traditional distributed computing to a new level. As we discussed in Section V-C, platforms, like iEx.ec, Golem, which integrate the blockchain into distributed computing, enable scalable off-chain computation outsourced at the distributed edges. Using these super powerful computing near the end, the blockchain based edge computing can be used for various use cases, including distributed machine learning and deep learning. For instance, in our ongoing work, the problem of training deep networks using lots of CPU cores is transformed to the collective learning approach using the deep Q-learning in each edge node and securely blockchain to share and improve the learning results. Some projects already combine AI and blockchain, such as SingularityNET [121], which is aiming to create a networking AI with blockchain to power the robot brain, and DeepBrain Chain [122], which is building a computing platform to support the creation of AI algorithms. Moreover, some work on machine learning and deep learning algorithms to lower their data and computation requirements is underway, such as the Gamalon project [123], TraneAI, Neureal, etc. [124]. This will be one of the possible paths to bring the AI closer to the edge. Currently, an edge based decentralized AI network named NeuRoN [46], allows the users with data ownership to train the neural network models based on smart contracts among the incentivizing developers, end users, and research organizations using a token.

5) Benefits From Artificial Intelligence: On the other side, AI brings great benefits to blockchain and edge computing integrating systems. In [125], a security model is proposed based on Markov Decision Processes (MDP) to effectively evaluate the impact of network-layer parameters onto the blockchain security, facing the double-spending and selfish mining of PoW. Accordingly, the optimal adversarial strategies are devised by taking into account of the adversarial mining power, the impact of eclipse attacks, block rewards, and real-world network and consensus parameters. IBM also recently announced plans to launch cognitive blockchain [126], in which AI agents perform tasks and make recommendations for updates to smart contracts, associated analytics and specific processes by analyzing the changes to data, regulations, interactions, suspect activity, etc., across the broader network. In the project of MATRIX [127], AI is leveraged to design a new generation blockchain, which supports automatic generation of smart contacts, enhanced security under malicious attacks, and highly flexible operations.

In the integrated blockchain and edge computing systems, the benefits of smart services as well as automatic operation support brought by AI are enlarged. As we discussed in Section V-C, deep learning algorithms and Stackelberg game are used to solve the efficient edge computing resource management for the blockchain PoW consensus in [71]–[73]. Stackelberg game is also used to analyze the security attacks by outsiders of the blockchain-based share systems in [128]. In [129], an intelligent blockchain-based resource management in cloud data centers is realized by reinforcement learning, which is embedded in the smart contracts to get the historical knowledge and executes the migration of requests to lower the total energy cost in a distributed way. In [130], the view change, access selection, and computational resources allocation in the blockchain based software-defined IoT are jointly optimized by a dueling deep Q-learning approach. Tsai [131] apply the Google federated learning and transfer learning to transform blockchain smart contract into a distributed parallel computing architecture. The individual learned models returned from individual local systems are composed and optimally updated globally by federated learning, and the distributed learned models are extended into the other models by distributed transfer learning. Pokrovskaia [132] give an example of building a tax, financial and social regulatory mechanisms with the tool of AI, blockchain, and controlling instruments of fog computing.

VII. Conclusion

This article addressed the integration of blockchain and edge computing, which is becoming an important concept that leverages their decentralized management and distributed service to meet the security, scalability and performance requirements in future networks and systems. Our discussion began with an overview of blockchain and edge computing, in which the basic theory and recent advances of each were briefly introduced. We then presented the motivations and requirements of the integration of blockchain and edge computing. Next, we discussed the frameworks of the integrated system based on

three-layer architecture of edge computing and put eyes on the private blockchain based local network and blockchain based P2P of the servers. We then discussed the network control, storage and computation at the network edges and the realization of the network security, data integrity and computation verification by the integration of blockchain into the edge computing. We also discussed the significant research challenges of the integrated system in the scalability enhancement, security and privacy, self-organization, function integration and resource management. Finally, the broader perspectives were explored.

In summary, research on the integrated blockchain and edge computing systems is quite broad, and some challenges lay ahead. Nevertheless, it is favorable for the network community to address the challenges and go forward. This article attempts to briefly explore the technologies related to the integration of blockchain and edge computing at a very preliminary level, which may open a new avenue for the development of integrated systems.

REFERENCES

[1] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, Sep. 2017.

[2] T. Florian and S. Björn, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

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

[4] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017.

[5] W. Yu *et al.*, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2017.

[6] 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, 2017.

[7] 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.

[8] M. Samaniego and R. Deters, "Virtual resources & blockchain for configuration management in IoT," *J. Ubiquitous Syst. Pervasive Netw.*, vol. 9, no. 2, pp. 1–13, 2017.

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

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

[11] K. Croman *et al.*, "On scaling decentralized blockchains," in *Proc. ICFCDS*, Feb. 2016, pp. 106–125.

[12] 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.

[13] F. R. Yu and Y. He "A service-oriented blockchain system with virtualization," *Trans. Blockchain Technol. Appl.*, vol. 1, no. 1, pp. 1–10, Jan. 2019.

[14] V. Buterin. (2014). *A Next Generation Smart Contract and Decentralized Application Platform*. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[15] P. L. Seijas, S. Thompson, and D. McAdams. (2016). *Scripting Smart Contracts for Distributed Ledger Technology*. [Online]. Available: http://eprint.iacr.org/2016/1156

[16] C. Cachin. (2016). *Architecture of the Hyperledger Blockchain Fabric*. [Online]. Available: https://pdfs.semanticscholar.org/

[17] S. King and S. Nadal. (2012). *PPcoin: Peer-to-Peer Crypto-Currency With Proof-of-Stake*. [Online]. Available: http://peercoin:net/assets/paper/peercoin-paper:pdf

[18] 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.

[19] 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, 2017.

[20] Protocol-Labs. (2017). *Filecoin: A Decentralized Storage Network*. [Online]. Available: https://filecoin.io/filecoin.pdf

[21] (2017). *The iEx.ec Project*. [Online]. Available: https://iex.ec/app/uploads/2017/04/iExec-WPv2.0-English.pdf

[22] (2018). *iEx.ec*. Accessed: Apr. 2, 2018. [Online]. Available: https://iex.ec

[23] A. Back *et al.* (2014). *Enabling Blockchain Innovations With Pegged Sidechains*. [Online]. Available: https://blockstream.com/sidechains.pdf

[24] J. Poon and T. Dryja. (2016). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. [Online]. Available: https://lightning.network/lightning-network-paper.pdf

[25] J. Poon and V. Buterin. (2017). *Plasma: Scalable Autonomous Smart Contracts*. [Online]. Available: https://plasma.io/plasma.pdf

[26] V. Buterin. (2017). *On Sharding Blockchains*. [Online]. Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ

[27] P. Garcia Lopez *et al.*, "Edge-centric computing: Vision and challenges," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 37–42, Oct. 2015.

[28] A. Aijaz, M. Dohler, A. H. Aghvami, V. Friderikos, and M. Frodigh, "Realizing the tactile Internet: Haptic communications over next generation 5G cellular networks," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 82–89, Apr. 2017.

[29] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 82–89, 4th Quart., 2016.

[30] M. Mukherjee *et al.*, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.

[31] S. Yi, Z. Qin, and Q. Li. (2015). *Security and Privacy Issues of Fog Computing: A Survey*. [Online]. Available: http://www.cs.wm.edu/∼zhengrui/papers/wasa15-fog.pdf

[32] F. Maughelli. (2016). *Security-Related Experiences With Smart Contracts Over the Ethereum Blockchain*. [Online]. Available: http://amslaurea.unibo.it/13991/1/francesco_maughelli_tesi.pdf

[33] P. De Filippi, "The interplay between decentralization and privacy: The case of blockchain technologies," *J. Peer Prod.*, vol. 7, Sep. 2016, pp. 1–19.

[34] M. Conoscenti, A. Vetrò, and J. C. D. Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE AICCSA*, Agadir, Morocco, Nov. 2016, pp. 2161–5330.

[35] E. Gaetani *et al.*, "Blockchain-based database to ensure data integrity in cloud computing environments," in *Proc. Ital. Conf. Cybersecurity*, Venice, Italy, Jan. 2017, pp. 146–155.

[36] R. Kumaresan and I. Bentov, "How to use Bitcoin to incentivize correct computations," in *Proc. ACM SIGSAC CCS*, Scottsdale, AZ, USA, Nov. 2014, pp. 30–41.

[37] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of Internet of Things infrastructure for secure and smart healthcare," *Computer*, vol. 50, no. 7, pp. 20–27, Jul. 2017.

[38] C. Li and L.-J. Zhang, "A blockchain based new secure multi-layer network model for Internet of Things," in *Proc. IEEE ICIOT*, Honolulu, HI, USA, Jun. 2017, pp. 33–41.

[39] M. Samaniego and R. Deters, "Hosting virtual IoT resources on edge-hosts with blockchain," in *Proc. IEEE CIT*, Nadi, Fiji, Dec. 2016, pp. 116–119.

[40] IBM. (2015). *Empowering the Edge: Practical Insights on a Decentralized Internet of Things*. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03662USEN

[41] S. Panikkar, S. Nair, P. Brody, and V. Pureswaran, *ADEPT: An IoT Practitioner Perspective*, IBM, Armonk, NY, USA, 2015.

[42] A. Stanciu, "Blockchain based distributed control system for edge computing," in *Proc. IEEE CSCS*, Bucharest, Romania, May 2017, pp. 29–31.

[43] 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 PerCom Workshops*, Kona, HI, USA, Mar. 2017, pp. 618–623.

[44] A. Dorri, S. S. Kanhere, and R. Jurdak. (2016). *Blockchain in Internet of Things: Challenges and Solutions*. [Online]. Available: https://arxiv.org/abs/1608.05187

[45] A. Lei *et al.*, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[46] W. D. Brouwer and M. Borda. (2017). *NeuRoN: Decentralized Artificial Intelligence, Distributing Deep Learning to the Edge of the Network*. [Online]. Available: https://s3-us-west-1.amazonaws.com/ai.doc.static/pdf/whitepaper.pdf

[47] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[48] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," in *Proc. IEEE NFV-SDN*, Berlin, Germany, Nov. 2017, pp. 303–308.

[49] M. Samaniego and R. Deters, "Using blockchain to push software-defined IoT components onto edge hosts," in *Proc. BDAW*, Blagoevgrad, Bulgaria, Nov. 2016, pp. 1–9.

[50] N. Herbaut and N. Negru, "A model for collaborative blockchain-based video delivery relying on advanced network services chains," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 70–76, Sep. 2017.

[51] D. Drutskoy, E. Keller, and J. Rexford, "Scalable network virtualization in software-defined networks," *IEEE Internet Comput.*, vol. 17, no. 2, pp. 20–27, Mar./Apr. 2013.

[52] D. B. Rawat, M. S. Parwez, and A. Alshammari, "Edge computing enabled resilient wireless network virtualization for Internet of Things," in *Proc. IEEE CIC*, San Jose, CA, USA, Dec. 2017, pp. 155–162.

[53] N. Bizanis and F. A. Kuipers, "SDN and virtualization solutions for the Internet of Things: A survey," *IEEE Access*, vol. 4, pp. 5591–5606, 2016.

[54] D. Neumann, C. Bodenstein, O. F. Rana, and R. Krishnaswamy, "STACEE: Enhancing storage clouds using edge devices," in *Proc. ACM/IEEE ACE Workshop*, Karlsruhe, Germany, Jun. 2011, pp. 19–26.

[55] S. Raval, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. Sebastopol, CA, USA: O'Reilly Media, 2016.

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

[57] G. Zyskind, O. Nathan, and A. S. Pentland. (2015). *Enigma: Decentralized Computation Platform With Guaranteed Privacy*. [Online]. Available: https://www.enigma.co/enigma_full.pdf

[58] J. Benet. (2014). *IPFS-Content Addressed, Versioned, P2P File System (DRAFT 3)*. [Online]. Available: https://arxiv.org/abs/1407.3561

[59] M. Pors. (2017). *Understanding the IPFS White Paper Part 2*. [Online]. Available: https://decentralized.blog

[60] M. Klems *et al.*, "Trustless intermediation in blockchain-based decentralized service marketplaces," in *Proc. ICSOC*, Málaga, Spain, Nov. 2017, pp. 731–739.

[61] M. Pors. (2017). *Picking a Decentralized Storage System*. [Online]. Available: https://decentralized.blog

[62] V. Tron. (2017). *IPFS & SWARM*. [Online]. Available: https://github.com/ethersphere/go-ethereum/wiki/IPFS-&-SWARM

[63] BigchainDB-GmbH. (2017). *A BigchainDB Primer*. [Online]. Available: https://www.bigchaindb.com/whitepaper/bigchaindb-primer.pdf

[64] T. McConaghy *et al.* (2016). *BigchainDB: A Scalable Blockchain Database*. [Online]. Available: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

[65] T. Daubenschütz. (2017). *BigchainDB Version 0.10 Released*. [Online]. Available: https://blog.bigchaindb.com/bigchaindb-version-0-10-released-9684fdb2a8ff

[66] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *Proc. USENIX ATC*, Denver, CO, USA, Jun. 2016, pp. 181–194.

[67] M. Ali, J. Nelson, R. Shea, and M. J. Freedman. (2017). *Blockstack Technical Whitepaper*. [Online]. Available: https://blockstack.org/whitepaper.pdf

[68] B. Confais, A. Lebre, and B. Parrein, "Performance analysis of object store systems in a fog and edge computing infrastructure," in *Transactions on Large-Scale Data and Knowledge-Centered Systems*. Heidelberg, Germany: Springer, Aug. 2017, pp. 40–79.

[69] M. S. Ali, K. Dolui, and F. Antonelli. (2017). *IoT Data Privacy via Blockchains and IPFS*. [Online]. Available: https://koustabh.eu/PDF/IoT_2017_paper_18.pdf

[70] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han. (2017). *When Mobile Blockchain Meets Edge Computing: Challenges and Applications*. [Online]. Available: https://arxiv.org/abs/1711.05938

[71] N. C. Luong, Z. Xiong, P. Wang, and D. Niyato. (2017). *Optimal Auction for Edge Computing Resource Management in Mobile Blockchain Networks: A Deep Learning Approach*. [Online]. Available: https://arxiv.org/abs/1711.02844

[72] Y. Jiao, P. Wang, D. Niyato, and Z. Xiong. (2017). *Social Welfare Maximization Auction in Edge Computing Resource Allocation for Mobile Blockchain*. [Online]. Available: https://arxiv.org/abs/1711.02844

[73] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han. (2017). *Edge Computing Resource Management and Pricing for Mobile Blockchain*. [Online]. Available: https://arxiv.org/abs/1710.01567

[74] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multiparty computations on bitcoin," in *Proc. IEEE Symp. SP*, San Jose, CA, USA, May 2014, pp. 443–458.

[75] A. Kiayias, H.-S. Zhou, and V. Zikas, "Fair and robust multi-party computation using a global transaction ledger," in *Proc. ACM ACAC*, New York, NY, USA, May 2016, pp. 705–734.

[76] R. Kumaresan, V. Vaikuntanathan, and P. N. Vasudevan, "Improvements to secure computation with penalties," in *Proc. ACM SIGSAC CCS*, Vienna, Austria, May 2016, pp. 406–417.

[77] I. Bentov, R. Kumaresan, and A. Miller, "Instantaneous decentralized poker," in *Proc. ASIACRYPT*, Hong Kong, Nov. 2017, pp. 410–440.

[78] M. von Maltitz, S. Smarzly, H. Kinkelin, and G. Carle, "A management framework for secure multiparty computation in dynamic environments," in *Proc. IEEE/IFIP Netw. Oper. Manag. Symp.*, 2018, pp. 1–7.

[79] 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.

[80] L. Zhou, L. Wang, Y. Sun, and P. Lv, "Beekeeper: A blockchain-based IoT system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, 2018.

[81] D. P. Anderson. (2004). *BOINC: A System for Public-Resource Computing and Storage*. [Online]. Available: https://boinc.berkeley.edu/grid_paper_04.pdf

[82] A. Marosi, J. Kovács, and P. Kacsuk, "Towards a volunteer cloud system," *Future Gener. Comput. Syst.*, vol. 29, no. 6, pp. 1442–1451, 2013.

[83] D. Montes, J. A. Añel, T. F. Pena, P. Uhe, and D. C. H. Wallom, "Enabling BOINC in infrastructure as a service cloud systems," *Geosci. Model Develop.*, vol. 10, no. 2, pp. 811–826, 2017.

[84] A. Jurgelevičius and L. Sakalauskas, "Big data mining using public distributed computing," *Inf. Technol. Control*, vol. 47, no. 2, pp. 236–248, 2018.

[85] R. Halford. (2014). *Gridcoin: Crypto-Currency Using Berkeley Open Infrastructure Network Computing Grid as a Proof of Work*. [Online]. Available: https://bravenewcoin.com/assets/Whitepapers/gridcoin-white-paper.pdf

[86] M. Grothe, T. Niemann, J. Somorovsky, and J. Schwenk. (2017). *Breaking and Fixing Gridcoin*. [Online]. Available: https://www.ei.rub.de/media/nds/veroeffentlichungen/2017/08/14/paper-woot.pdf

[87] L. Luu, J. Teutsch, R. Kulkarni, and P. Saxena, "Demystifying incentives in the consensus computer," in *Proc. ACM SIGSAC CCS*, Denver, CO, USA, Oct. 2015, pp. 706–719.

[88] J. Teutsch and C. ReitwieBner. (2017). *A Scalable Verification Solution for Blockchains*. [Online]. Available: https://people.cs.uchicago.edu/teutsch/papers/truebit.pdf

[89] (2016). *The Golem Project: Crowdfunding Whitepaper*. [Online]. Available: http://golemproject.net/doc/DraftGolemProjectWhitepaper.pdf

[90] H. He *et al.*, "Extending the EGEE grid with XtremWeb-HEP desktop grids," in *Proc. IEEE/ACM CCGrid*, Melbourne, VIC, Australia, May 2010, pp. 685–695.

[91] P. Kasireddy. (2017). *Blockchains Don't Scale. Not Today, at Least. But There's Hope*. [Online]. Available: https://hackernoon.com/@preethikasireddy

[92] C. Xu *et al.*, "Making big data open in edges: A resource-efficient blockchain-based approach," *IEEE Trans. Parallel Distrib. Syst.*, pp. 1–13, Sep. 2018.

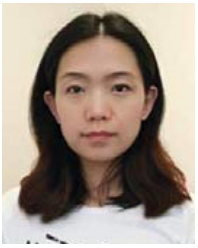
[93] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. USENIX Conf. NSDI*, Santa Clara, CA, USA, Mar. 2016, pp. 45–59.

[94] K. Samani. (2018). *The Web3 Stack*. [Online]. Available: https://multicoin.capital/2018/07/10/the-web3-stack/

[95] A. Akentiev. (2017). *Plasma in 10 Minutes*. [Online]. Available: https://medium.com/chain-cloud-company-blog/

[96] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[97] A. Chiesa, E. Tromer, and M. Virza, "Cluster computing in zero knowledge," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Sofia, Bulgaria, May 2015, pp. 371–403.
[98] S. Bowe, A. Gabizon, and I. Miers. (2017). *Scalable Multi-Party Computation for ZK-SNARK Parameters in the Random Beacon Model*. [Online]. Available: https://eprint.iacr.org/2017/1050.pdf
[99] (2017). *Edge Intelligence*. [Online]. Available: http://www.iec.ch/whitepaper/pdf/IEC_WP_Edge_Intelligence.pdf
[100] C. Prazeres and M. Serrano, "SOFT-IoT: Self-organizing FOG of things," in *Proc. WAINA*, May 2016, pp. 803–808.
[101] J. S. Preden *et al.*, "The benefits of self-awareness and attention in fog and mist computing," *Computer*, vol. 48, no. 7, pp. 37–45, Jul. 2015.
[102] M. A. Ferrag *et al.* (2018). *Blockchain Technologies for the Internet of Things: Research Issues and Challenges*. [Online]. Available: https://arxiv.org/pdf/1806.09099.pdf
[103] F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, "From bitcoin to cybersecurity: A comparative study of blockchain application and security issues," in *Proc. IEEE ICSAI*, Hangzhou, China, Nov. 2017, pp. 975–979.
[104] NKN Lab. (2018). *NKN: A Scalable Self-Evolving and Self-Incentivized Decentralized Network*. [Online]. Available: https://www.nkn.org/doc/NKN_Whitepaper.pdf
[105] P. Kacsuk, J. Kovacs, Z. Farkas, A. C. Marosi, and Z. Balaton, "Towards a powerful European DCI based on desktop grids," *Grid Comput.*, vol. 9, no. 2, pp. 219–239, Mar. 2011.
[106] C. Wang, Y. He, F. R. Yu, Q. Chen, and L. Tang, "Integration of networking, caching and computing in wireless systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 7–38, 1st Quart., 2018.
[107] K. Toczé and S. Nadjm-Tehrani. (2018). *A Taxonomy for Management and Optimization of Multiple Resources in Edge Computing*. [Online]. Available: https://arxiv.org/abs/1801.05610
[108] H. Yin *et al.*, "Hyperconnected network: A decentralized trusted computing and networking paradigm," *IEEE Netw.*, vol. 32, no. 1, pp. 112–117, Jan./Feb. 2018.
[109] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *Proc. Int. Conf. Financ. Cryptography Data Security*, San Juan, Puerto Rico, Jan. 2015, pp. 528–547.
[110] S. Lee. (2018). *Explaining Directed Acylic Graph (DAG), the Real Blockchain 3.0*. [Online]. Available: https://dagcoin.org/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/
[111] S. Popov. (2017). *The Tangle*. [Online]. Available: https://iota.org/IOTA_Whitepaper.pdf
[112] A. Churyumov. (2016). *Byteball: A Decentralized System for Storage and Transfer of Value*. [Online]. Available: https://byteball.org/Byteball.pdf
[113] J. Chen *et al.*, "A parallel random forest algorithm for big data in a spark cloud computing environment," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 4, pp. 919–933, Apr. 2017.
[114] S. Yu, M. Liu, W. Dou, X. Liu, and S. Zhou, "Networking for big data: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 531–549, 1st Quart., 2017.
[115] N. Abdullah, A. Hakansson, and E. Moradian, "Blockchain based approach to enhance big data authentication in distributed environment," in *Proc. IEEE ICUFN*, Milan, Italy, Jul. 2017, pp. 887–892.
[116] J. Chen and Y. Xue, "Bootstrapping a blockchain based ecosystem for big data exchange," in *Proc. IEEE ICBC*, Honolulu, HI, USA, Sep. 2017, pp. 460–463.
[117] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in *Proc. IEEE BIGCOM*, Chengdu, China, Aug. 2017, pp. 117–121.
[118] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *Proc. IEEE EUROCON*, Aug. 2017, pp. 763–768.
[119] B. Dickson. (2017). *How Do You Bring Artificial Intelligence From the Cloud to the Edge?* [Online]. Available: https://thenextweb.com/contributors/2017/08/21/bring-artificial-intelligence-cloud-edge/
[120] M. Swan, "Blockchain thinking: The brain as a decentralized autonomous corporation," *IEEE Technol. Soc. Mag.*, vol. 34, no. 4, pp. 41–52, Dec. 2015.
[121] (2017). *Singularitynet: A Decentralized, Open Market and Inter-Network for AIs*. [Online]. Available: https://public.singularitynet.io/whitepaper.pdf
[122] (2017). *Deepbrain Chain: Artificial Intelligence Computing Platform Driven by Blockchain*. [Online]. Available: https://dlc0uvc36o5o6.cloudfront.net/assets/pdf/DeepBrainChainWhitepaper_en.pdf
[123] B. Vigoda *et al.* (2016). *Idea Learning*. [Online]. Available: https://gamalon.com/technology/
[124] F. Corea. (2017). *The Convergence of AI and Blockchain: What Is the Deal?* [Online]. Available: https://medium.com/@Francesco_AI/
[125] A. Gervais *et al.*, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC CCS*, Vienna, Austria, Oct. 2016, pp. 3–16.
[126] J. Groopman. (2017). *Four Examples of Blockchain-Artificial Intelligence Deployments*. [Online]. Available: https://www.tractica.com/artificial-intelligence/four-examples-of-blockchain-artificial-intelligence-deployments/
[127] L. Tzu. (2017). *Matrix Technical Whitepaper*. [Online]. Available: https://www.matrix.io/html/MATRIXTechnicalWhitePaper.pdf
[128] D. B. Rawat, L. Njilla, K. Kwiat, and C. Kamhoua, "iShare: Blockchain-based privacy-aware multi-agent information sharing games for cybersecurity," in *Proc. IEEE ICNC*, Mar. 2018, pp. 425–431.
[129] C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," *IEEE Cloud Comput.*, vol. 4, no. 6, pp. 50–59, Nov./Dec. 2017.
[130] C. Qiu *et al.*, "Blockchain-based software-defined industrial Internet of Things: A dueling deep Q-learning approach," *IEEE Internet Things J.*, pp. 1–14, Sep. 2018.
[131] J. Tsai, "Transform blockchain into distributed parallel computing architecture for precision medicine," in *Proc. IEEE ICDCS*, Vienna, Austria, Jul. 2018, pp. 1290–1299.
[132] N. N. Pokrovskaia, "Tax, financial and social regulatory mechanisms within the knowledge-driven economy. Blockchain algorithms and fog computing for the efficient regulation," in *Proc. IEEE ICSCM*, St. Petersburg, Russia, May 2017, pp. 709–712.



Ruizhe Yang received the B.S. degree from the Beijing University of Technology in 2004 and the Ph.D. degree from the Beijing University of Posts and Telecommunications in 2009. She joined the Beijing University of Technology in 2009, where she is currently a Lecturer. From 2017 to 2018, she visited Carleton University, Ottawa, Canada. Her research interests include blockchain, resource management, and channel estimation.

F. Richard Yu (S'00–M'04–SM'08–F'18) received the Ph.D. degree in electrical engineering from the University of British Columbia in 2003. From 2002 to 2006, he was with Ericsson, Lund, Sweden, and a start-up in CA, USA. He joined Carleton University in 2007, where he is currently a Professor. His research interests include wireless cyberphysical systems, connected/autonomous vehicles, security, distributed ledger technology, and deep learning. He was a recipient of the IEEE Outstanding Service Award in 2016, the IEEE Outstanding Leadership Award in 2013, the Carleton Research Achievement Award in 2012, the Ontario Early Researcher Award (formerly, Premiers Research Excellence Award) in 2011, the Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from the Canada Foundation of Innovation in 2009, and the Best Paper Awards at IEEE ICNC 2018, VTC 2017 Spring, ICC 2014, Globecom 2012, IEEE/IFIP TrustCom 2009, and International Conference on Networking 2005.

He serves on the editorial boards of several journals, including the Co-Editor-in-Chief for *Ad Hoc & Sensor Wireless Networks*, and a Lead Series Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, and the IEEE COMMUNICATIONS SURVEYS & TUTORIALS. He has served as the technical program committee co-chair of numerous conferences. He is a registered Professional Engineer in the province of Ontario, Canada and a fellow of the Institution of Engineering and Technology. He is a Distinguished Lecturer, the Vice President (Membership), and an Elected Member of the Board of Governors of the IEEE Vehicular Technology Society.

Pengbo Si (SM'15) received the B.S. and Ph.D. degrees from the Beijing University of Posts and Telecommunications in 2004 and 2009, respectively. He joined the Beijing University of Technology in 2009, where he is currently a Professor. From 2007 to 2008, he visited Carleton University, Ottawa, Canada. From 2014 to 2015, he was a Visiting Scholar with the University of Florida, Gainesville, FL, USA. His research interests include blockchain, SDN, resource management, and cognitive radio networks.

Zhaoxin Yang received the B.S. and M.S. degrees from the Beijing University of Technology in 2015 and 2018, respectively, where he is currently pursuing the Ph.D. degree. His current research interests include big data, blockchain, and machine learning.

Yanhua Zhang received the B.E. degree from the Xi'an University of Technology in 1982 and the M.S. degree from Lanzhou University in 1988. From 1982 to 1990, he was with Jiuquan Satellite Launch Center, China. In 1990, he was a Visiting Professor with Concordia University, Montreal, Canada. He joined the Beijing University of Technology in 1997, where he is currently a Professor. His research interests include QoS-aware networking and radio resource management in wireless networks.