electronics

Article

Blockchain-Based Secure Storage Management with Edge Computing for IoT

Baraka William Nyamtiga [1], Jose Costa Sapalo Sicato [2], Shailendra Rathore [2], Yunsick Sung [3] and Jong Hyuk Park [2,*]

[1] Department of Electrical and Information Engineering, Seoul National University of Science and Technology, Seoul 01811, Korea
[2] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 01811, Korea
[3] Department of Multimedia Engineering, Dongguk University-Seoul, Seoul 04620, Korea
* Correspondence: jhpark1@seoultech.ac.kr; Tel.: +82-2-970-6702

Received: 27 May 2019; Accepted: 21 July 2019; Published: 25 July 2019

Abstract: As a core technology to manage decentralized systems, blockchain is gaining much popularity to deploy such applications as smart grid and healthcare systems. However, its utilization in resource-constrained mobile devices is limited due to high demands of resources and poor scalability with frequent-intensive transactions. Edge computing can be integrated to facilitate mobile devices in offloading their mining tasks to cloud resources. This integration ensures reliable access, distributed computation and untampered storage for scalable and secure transactions. It is imperative therefore that crucial issues of security, scalability and resources management be addressed to achieve successful integration. Studies have been conducted to explore suitable architectural requirements, and some researchers have applied the integration to deploy some specific applications. Despite these efforts, however, issues of anonymity, adaptability and integrity still need to be investigated further to attain a practical, secure decentralized data storage. We based our study on peer-to-peer and blockchain to achieve an Internet of Things (IoT) design supported by edge computing to acquire security and scalability levels needed for the integration. We investigated existing blockchain and associated technologies to discover solutions that address anonymity, integrity and adaptability issues for successful integration of blockchain in IoT systems. The discovered solutions were then incorporated in our conceptual design of the decentralized application prototype presented for secure storage of IoT data and transactions.

Keywords: blockchain; IoT; edge computing; peer-to-peer; security

1. Introduction

Blockchain has recently become so popular as a technology that makes use of community validation to synchronize contents of replicated ledgers across multiple users [1]. Operating as a decentralized ledger that verifies and stores records of transactions; blockchain performs better than counterpart approaches that are based on centralized digital ledgers. In blockchain, data records are stored as blocks whose logical relations are structured as a linked list of data blocks chained together [2]. Using the consensus mechanism; updates made in data blocks are reflected across the entire network resulting into a tamper-proof platform for storing and sharing data [3]. With this automated data sharing in blockchain; no intervention of an intermediary entity is needed and thus creating a paradigm shift from centralized to decentralized management. It was initially introduced to solve double spending problems in Bitcoin [4] but it has extended with time in deploying other applications such as smart grid, healthcare, delivery networks and logistics systems. It is however, not without flaw, and its limited capability to scale and handle frequency-intensive tasks is identified to be the greatest [5].

Such platforms as Internet of Things (IoT) containing numerous physical objects connected to the internet may reap the security benefits of blockchain to achieve privacy in its services. The many connected systems in IoT communicate with each other over the internet, and thus, producing and exchanging massive amounts of data, which may be of a sensitive nature [6]. The decentralized nature of blockchain makes it a potential candidate in safeguarding privacy of such systems in a Peer-to-Peer (P2P) fashion guaranteeing security of the exchanged information. However, because of its intensive consumption of resources in the mining and consensus processes and the limited resources of nodes in IoT makes it difficult to directly utilize blockchain in IoT and other mobile services [2].

In this view, mobile edge computing provides a complimentary way to handle proof-of-work (PoW) puzzles and facilitates the use of blockchain in IoT systems. Edge computing is introduced at the edge of the network as an extension for distributing resources and services on the cloud [7]. It provides a multiple access environment for subscribers to enjoy cloud-like facilities of elevated computing, application and storage services. The resource-constrained mobile devices can therefore boost their computing powers by offloading their mining and storage tasks to the edge servers. The integration of blockchain and edge computing shall create a decentralized environment for outsourced computation and secure storage for scalable and secure transactions. The main stumbling blocks that remain for this integration to be realized is largely related to security aspects and the decentralized management in edge computing [8].

Along with resource management issues, integration of features and scalability improvement among others; most crucial aspects of security must be well addressed for the integration to be realized. Several research efforts have been made to investigate resolutions for these issues and we learnt from these studies that issues regarding anonymity, adaptability and integrity must be addressed for the effective utilization of blockchain in decentralized data storage for IoT. As only pseudonymity is guaranteed by blockchain; integrity is only dependent on the number of honest miners and PoW's complexity and with adaptability contrary being limited by the complexity; investigation for mitigations of these issues is called for [6].

We focus our study in investigating factors that affect blockchain's anonymity, integrity and adaptability by leveraging our private IoT design on P2P and blockchain integrated with edge computing. The P2P architecture principally provides a robust decentralized storage system with ensured data privacy and no single points of failure. Blockchain handles controlled access and authentication of transactions whereas edge computing avails communication and computing resources to facilitate the less capable IoT devices participating in the blockchain. We investigate existing blockchain technologies to attain an architectural integrated design that can achieve the needed security and scalability as well as addressing issues of data integrity. We further explore various protocols and technologies that can enhance privacy in IoT applications by achieving anonymity further beyond just pseudonymity.

The lack of a publicly agreed platform to deploy blockchain in IoT has prompted us to carry out this study considering the great potentials brought by IoT to individuals and institutions with the many devices being interconnected and massive data being exchanged. By exploring edge computing attributes and blockchain's securities our study seeks to discover a secure and scalable environment to deploy blockchain for IoT and the key contributions for our research work are as follows:

- Based on the edge computing layered architecture and blockchain's P2P distributed ledger, we provide a thorough account of the typical stumbling blocks to be overcome to enable deployment of blockchain in IoT systems.
- We propose a novel framework to solve the identified issues of anonymity, integrity and adaptability in order to achieve successful integration of blockchain and edge computing for IoT systems. We further provide description of how these solutions can be implemented in the different layers of edge computing architecture.
- We present a practical approach towards the implementation of a decentralized application on the blockchain and give conceptual analysis of the protocols and operating environments for a

prototype to achieve implementation of scalable and secure blockchain data storage in edge computing platforms for IoT applications.

The rest of our article is organized with related works being first explained in Section 2. Requirements and considerations for the proposed framework are then given in Section 3. The model of the proposed framework is presented in Section 4. Section 5 contains system prototype design, implementation setup, framework conceptual evaluation and discussions. We finally conclude our study in Section 6.

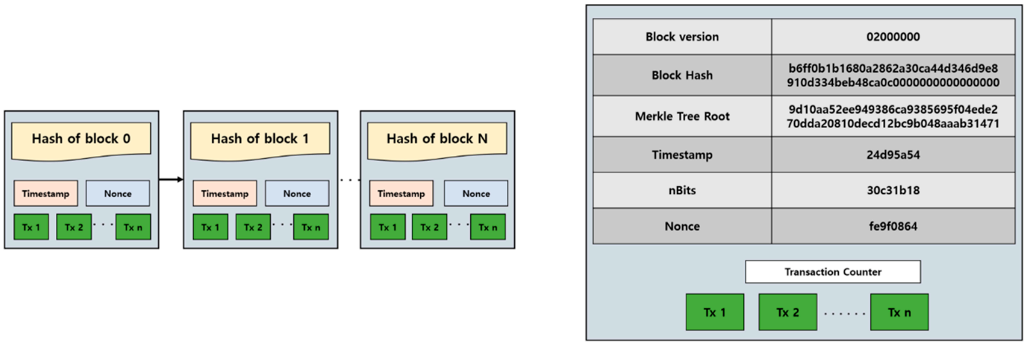
2. Related Works

2.1. Core Technologies

2.1.1. Blockchain Technology

Blockchain is a technology that uses secure cryptographic mechanisms to provide decentralized electronic ledger formed by a sequence of chronologically connected blocks of transactions [9,10]. Blockchain is made up of immutable and publicly verifiable records maintained by nodes of a P2P network to ensure tamper-proof transmission and storage of approved transactions [3]. Participants in the blockchain network use a certain agreed-on consensus protocol to confirm or dismiss every transaction before it is appended to the blockchain in the same order as they are verified [9]. Figure 1a,b below illustrates the general configuration of blockchain and the internal structure of its block respectively. A participant in blockchain, commonly known as a miner is only allowed to append a new data block to the chain after performing a "mining" process in order to guarantee data validity and integrity. Mining process is computationally intensive, and a miner has to solve a puzzle known as proof-of-work (PoW) and obtain a hash value, which, after being validated by majority of miners, can successfully be added to the blockchain.

The approved transactions are stored in the blockchain as a continuously growing chain of blocks, (hence the name blockchain) whereby each block is connected to the previous. Starting from the initial block, which is commonly referred to as a genesis block; each block in the chain contains a hash value as a link to the preceding block, a timestamp and some transactional details. The hash value of the previous block is computed during the creation of a new block and the genesis block has no link to any previous blocks because it is the first in the chain. Upon a successful addition of a new block; the public ledger is synchronized among all participants in the network and thus, being visible to all prevents modification by some entities with malicious intents.



Block version	02000000
Block Hash	b6ff0b1b1680a2862a30ca44d346d9e8 910d334beb48ca0c0000000000000000
Merkle Tree Root	9d10aa52ee949386ca9385695f04ede2 70dda20810decd12bc9b048aaab31471
Timestamp	24d95a54
nBits	30c31b18
Nonce	fe9f0864

(**a**) (**b**)

Figure 1. (**a**) Configuration of the blockchain; (**b**) internal structure of a block in the blockchain**.**

According to the desired permission attributes; an entity has three options to interact with a blockchain; namely public, private or consortium blockchain [3]. In a public blockchain; all participants are involved in reading, submitting, verifying and getting consensus for transactions without any central entity to manage memberships or ban illegitimate readers or writers [11,12]. Contrary to the public; a private blockchain is administered by restricting access to data through the centralization of write permission to only one entity and keeping read permissions public or restricted to some specific entities in the network [11]. As for consortium; only a pre-selected set of peers are involved in the consensus process. It can be viewed as a partially decentralized network in which read permission may be open, or restricted to specific peers while blocks' validity are confirmed by those few chosen in advance [3].

The key attributes characterizing blockchain as general decentralized ledgers include autonomous, distributed, immutable, anonymous and contractual [3,11]. It is autonomous in the sense that the network is governed and controlled collectively by all participants through a consensus mechanism. Blockchain is distributed by operating in a P2P fashion where new approved transactions are broadcasted to all other peers in the system for validation and storage without intervention of any central entity. Being immutable means records in a blockchain always remain accurate and unchanged as a consequence of demanding verification by other nodes to make any modifications. Moreover, transactions and data transfers among peers in a blockchain network are kept anonymous. Trust is ensured by blockchain and the sender's or receiver's blockchain address is sufficient for authentication [13,14]. Another significant attribute of blockchain is the established rules and policies in smart contracts that are correctly and timely executed in the network without intervention of any central authorizing entity [3].

2.1.2. Internet of Things

The internet of things (IoT) is a network paradigm in which physical devices such as actuators, sensors, vehicles and other smart technologies are connected to communicate with data centers and exchange information [15]. IoT constitutes a heterogeneous environment to allow interactions among various systems; both hardware and software systems. Being continuously integrated in their surroundings; devices in IoT are embedded with low-cost sensors for a range of applications including smart grids, smart healthcare and smart transportation. It is structured with three main levels identified as the device layer, gateway layer and the cloud layer. The cloud forms the back end layer on the internet where data is stored (and possibly the heavy computation is done). The gateways are deployed in the middle layer for linking IoT devices to the internet providing access to data and services. Low-powered IoT devices form the third layer and they are characterized by less computational resources, less powered and lacking sufficient memory for storage [10,16].

To overcome the limited capabilities in computation power and storage while ensuring security; IoT devices can incorporate low-powered hardware accelerators to establish a new class of secure applications [17]. The use of symmetric pre-shared key is still utilized in IoT as a conventional solution for security, but this simple approach cannot be adapted for a massive number of devices in IoT. Blockchain offers a promising venture to suit the stringent needs of the less capable IoT devices in a typical decentralized topology. Efforts are being made to adopt blockchain to secure communications in IoT using public key schemes and approaches of deploying blockchain in IoT environments draw so much attention in research communities [10,18].

2.1.3. Edge Computing

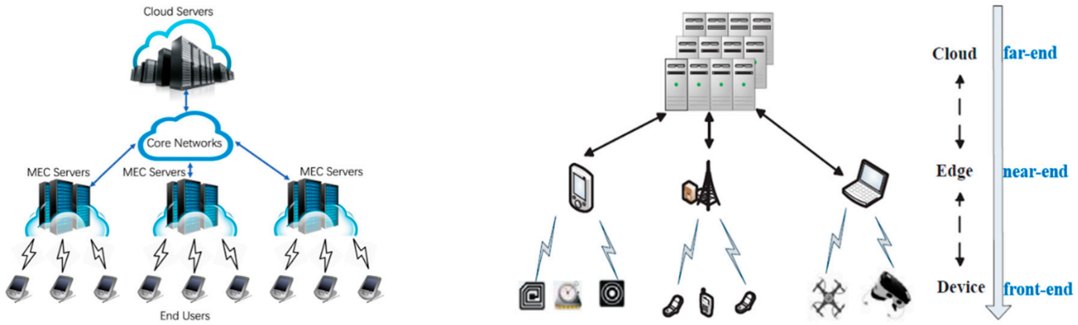
Mobile edge computing (MEC) defines a technology that, "provides an IT service environment and cloud-computing capabilities at the edge of the mobile network, within the Radio Access Network (RAN) and in close proximity to mobile subscribers" [19]. It is a new paradigm; an outcome from the rapid growth in technology that have seen computing services and resources which were originally serviced in the cloud now being moved towards the "edge" of the mobile network [8]. The steep growth of the number of mobile devices has rendered traditional centralized cloud computing ineffective in fulfilling the quality of services (QoS) for many applications. In MEC, computing and storage resources namely cloudlets, fog nodes or micro data centers are deployed at the base station at the internet's edge nearby end devices [7] to avoid obstructions and system failures [20]. The main intention is to achieve high network efficiency, to minimize latency, and ensure reliable delivery of services for better user experience [19]. By directly connecting to the closest cloud service-enabled edge network [21], users of delay-sensitive applications such as virtual reality (VR) and augmented reality (AR) can meet their strict delay specifications. Pushing resources to the edge enables increased mobility, low latency and provides location awareness [8]. MEC forms a key technology for realizing many visions for the next-generations of cellular networks (5G [19]) and the Internet (IoT [15] and tactile internet [22]) to allow increased deployment of new applications. It bestows the satisfaction of stringent requirements of 5G and IoT through increased throughout, automation, minimal latency and enhanced scalability. "It enables a new value chain, fresh business opportunities and a myriad of new use cases across multiple sectors" [19].

The structure of edge computing is illustrated in Figure 2a whereby the edge servers are closer to users than to servers on the cloud. Its architecture can broadly be separated into three distinct levels namely front-end constituting end devices, near-end constituting edge servers and the far-end, which is made up of the core cloud [8,15]. The hierarchy structure illustrated in Figure 2b directly reflects computing capabilities of the elements in the different levels.

The end devices such as actuators and sensors are deployed at the front-end to provide interactivity and greater responsiveness for end users. Devices found in this level have limited capacities to satisfy most requirements and thus, forward them to edge servers to be accomplished.

The edge servers deployed as gateways in the near-end convey and distributes the traffic flowing through the networks [15]. The edge servers can also fulfill resources requirements of real-time data processing, data caching and computation offloading. Most computation and storage tasks will thus be offloaded to the near-end to attain better performance and more storage.

Cloud servers are found in the far-end with more powerful computing and more storage capabilities but faced with significant transmission latency because of its deployment farther away from end users. At this level we find provisions for massive parallel data processing, machine learning, big data mining and management to mention but a few [15].



(**a**) (**b**)

Figure 2. (**a**) Basic edge computing architecture [13]; (**b**) typical architecture of edge computing network.

This architectural design is tailored for the execution of mission-critical, compute-intensive and delay sensitive tasks of customers at the edge while applications in the edge servers synchronize the data with the core cloud for long-term storage.

2.2. Existing Research Works

In their work that is based on the usage of blockchain as a service for IoT; Samaniego et al. in [10] stipulate that blockchain can potentially benefit IoT devices for untampered storage and authenticated transactions. They identify a hosting environment to be the key challenge in successfully deploying blockchain in IoT devices. They proceed to perform evaluations on the usage of fog and the cloud as candidate platforms for deployment and reveal that the fog performs better than the cloud.

Xiong et al. in [2] present a prototype of using edge computing for blockchain in devices with constrained resources. They demonstrated the possibility of mobile devices to access and utilize computing resources in the edge network to facilitate usage of blockchain in their applications. Their testbed and experimental results exhibit that the integration is beneficial both to miners and service providers as more miners joins the network.

Liu et al. [23] proposed a framework for resource distribution in using edge computing to facilitate the use of blockchain in video streaming systems for transcoding. They designed an incentive mechanism and consider two approaches to offload the burden of transcoding tasks in edge computing environment. Their simulation results verified the model to bear good results in maximizing average profits in the offloading and adaptive schemes for resource allocation.

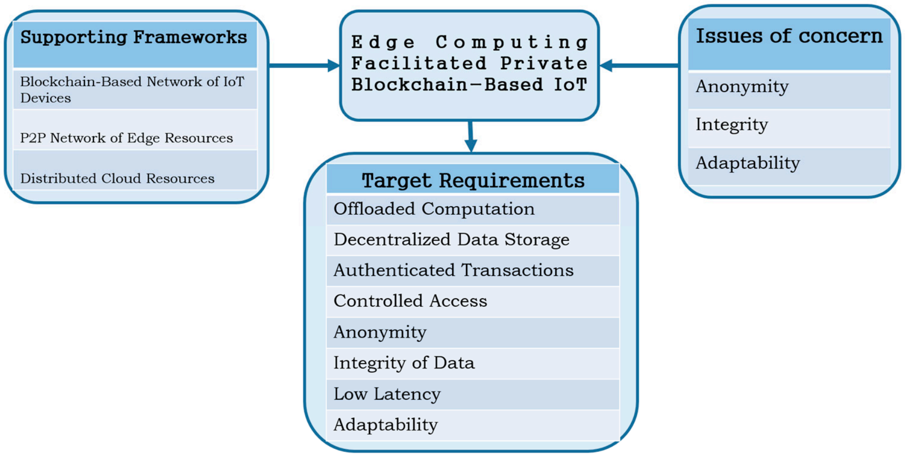
Performing a systemized review of literature on the usage blockchain for IoT; Conoscenti et al. in [6] set out to establish the feasibility of employing blockchain and P2P in achieving a decentralized private design for IoT applications. Their findings identified three issues of anonymity, adaptability and integrity to be obstacles for a successful integration. They found that anonymity is only guaranteed by pseudonyms, integrity relies on the complexity of PoW and massive numbers of honest miners whereas the adaptability is coincidentally limited by PoW's complexity.

Mitigations for such issues have been separately studied by different research works in [3,24–30]. Yu et al. [30] and Liu et al. [26] tackled the issue of integrity; Feng et al. [3], Miers et al. [27] and Sasson et al. [28] have given propositions on addressing anonymity. As for addressing scalability; works by Kasireddy [25], Yeow et al. [29] and Eyal et al. [24] suggest possible solutions to enable the adaptability of blockchain for IoT.

The above described studies have collectively portrayed the feasibility of integrating edge computing in blockchain for IoT applications. While some have focused in the general architectural issues needed for the integration; some are general studies on mitigation of specific issues in blockchain and others have applied the integration as a platform to deploy specific applications. While the hosting environment is perceived as a challenge for deploying the desired scheme; some studies have identified specific issues of anonymity, integrity and scalability to be fundamental for achieving successful integration. We based our study on the design of a suitable platform to deploy blockchain services in IoT with a focus on how to address the identified crucial aspects of adaptability and security to guarantee secure decentralized storage.

3. Requirements and Considerations for the Proposed Framework

The building blocks that achieve our privately designed blockchain-based IoT with edge computing for secure data management are summarized in Figure 3**Error! Reference source not found.**. In this block diagram, the supporting frameworks, areas of concern to be addressed along with target requirements for the proposed model are illustrated. The supporting frameworks were integrated together in the design to address the issues of concern and meet the targeted requirements.



Supporting Frameworks
Blockchain-Based Network of IoT Devices
P2P Network of Edge Resources
Distributed Cloud Resources
Edge Computing Facilitated Private Blockchain−Based IoT
Issues of concern
Anonymity
Integrity
Adaptability
Target Requirements
Offloaded Computation
Decentralized Data Storage
Authenticated Transactions
Controlled Access
Anonymity
Integrity of Data
Low Latency
Adaptability

Figure 3. Building blocks and target requirements for the edge computing leveraged private blockchain-based internet of things (IoT) architecture.

3.1. The Need for Integration

Beside the promising potentials that are availed by these individual technologies; blockchain, edge computing and IoT each have their own limitations and challenges that can complement each other in their integration. On one hand, despite the benefits blockchain brings to the technological world; stringent requirements by the nodes for computation, storage and bandwidth need to be met to achieve higher throughputs of transactions while maintaining high security standards. On the other hand, while the distributed structure of edge computing is desirable; its mobility and dynamism to support heterogeneous devices in an openly coordinated computing environment is susceptible to potential malicious attacks. This brings security challenges in the outsourced storage, decentralized network control and offloaded computation of tasks that need attention. Furthermore, even though IoT provides a convenient platform that makes the world highly connected, smarter and more efficient; its devices are characterized by confined computing capabilities, low power and limited storage capacities.

By integrating all these technologies, thus, blockchain's mining and replication processes ensure valid, consistent and accurate transactions in a heterogeneous edge computing environment. Pseudonyms and smart contracts in blockchain enable privacy and enhance efficient, reliable and automated resource coordination for edge computing at minimal running expenses. Moreover, edge computing's P2P originality facilitates information distribution in blockchain's consensus protocol. Edge computing also serves as a bridge to enable IoT's resource-restrained end devices to participate in blockchain by offloading their heavy computation tasks to edge servers. Additionally, edge computing creates a confidential and independent environment for blockchain to outsource storage burdens to servers on the edge network and meet its storage requirements.

3.2. Issues Affecting Blockchain Adoption for IoT

Anonymity: The pseudonyms in blockchain that are responsible to handle anonymity of transactions is rendered insufficient [6] because of the demonstrated possibility to de-anonymize participants. By performing analysis of the traffic flow or the ledger itself, identities of users in the blockchain network can be revealed. Several techniques to achieve de-anonymization are summarized in [6] as change address, multiple inputs, associations with IP and usage of some centralized services. The detailed description of these techniques will not be provided here but they all involve disclosing users' identities by either revealing ownership of input addresses, linking back multiple addresses owned by the same participant [31], associating IP addresses by analyzing traffic patterns [32] or using some centralized entity for service administration [31,33].

Integrity: Integrity issues arise in blockchain when either of the reliability, accuracy and consistency aspects of transactions in the network is compromised. In spite of being vulnerable to other attacks on integrity as described in [6] including selfish mining attack, history-revision attack and stubborn mining attack; these are trivial attacks and were not covered in our study. The most outstanding attack posed on integrity is the misbehaving of a dishonest miner that may be in possession of high ratios of processing capabilities in the blockchain network. This kind of miners may corrupt the consensus protocol and also lead to losses of past data.

Adaptability: As stated in [26,34,35], scalability issues are caused by blockchain's mode of operating, which demands that all participants in the network must verify and permanently store each added block and every generated transaction. When the number of transactions grow so high and gets more complex; requirements for bandwidth, computation power and storage also increase [25] consequentially obstructing blockchain's scalability. The many transactions result in larger sized ledgers that are too expensive to be stored by end devices with finite resources in IoT. Moreover, the complex PoW puzzles and the upper limit specification of 1 MB [6] for a maximum size of a block in blockchain yield longer delays and reduced throughput. Eventually, this prohibits its adaptability in practical blockchain-based solutions.

3.3. Problem Statement

Despite the ongoing efforts for a suitable platform for blockchain deployment in IoT applications; anonymity, adaptability and data integrity are crucial issues that are yet to be solved to ensure safe storage of data. Since only pseudonyms are guaranteed in blockchain, and integrity relies only on massive numbers of honest miners and PoW's complexity (which also affects the scalability); investigation for appropriate technologies to provide stronger anonymity than just pseudonymity and achieve adaptable data integrity must be done.

3.4. Design Requirements

As it was illustrated earlier in Figure 3, the design principles that must be fulfilled by the designed architecture to ensure successful integration of edge computing and blockchain for IoT applications include:

- Decentralized data storage, the integrated architecture of edge computing and blockchain should complement each other to extend storage capacities of IoT devices by combining the storage capacities of participating entities in a P2P basis in storing and sharing the transactions.
- Offloaded computation, the processing tasks outsourced to the edge servers by end devices should be verifiable and guaranteed to produce accurate results.
- Data integrity, the integrated system requires built-in reliable mechanisms to verify actions of both the data owners and consumers to ensure consistent and accurate modification of the outsourced data in the decentralized environment.
- Authenticity of transactions, to establish secure communication channels in the mobile, decentralized and heterogeneous environments of edge computing; validity of the involved entities and their respective transactions must be adequately authenticated.
- Anonymity, to ensure user data privacy in the blockchain network and allow participants in the network to conveniently perform their desired transactions without worry about being tracked or their identity being traced on the network. Their identity should not be mandatory for authentication, instead, only the transaction address shall suffice [13,14].
- Adaptability, the architecture must be flexible enough to support fluctuating environments and meet future growth in the number of devices and increasing amounts of transactions continuously generated and stored. It should adapt to these growing needs and increased complexities in future applications while maintaining acceptable levels of system throughput, delays and security.
- Low latency, the model should strike a balance and achieve optimal levels in the amounts of delays incurred during the computation and transmission of transactions from one entity to another. Identification of what computation tasks are involved and decision on where they should be performed between the end devices and servers on the cloud are important in ensuring minimal latencies in the system.
- Controlled access, it is imperative that access policies are enforced in the framework to regulate which data of a user can be shared and be viewed by whom.

4. Proposed Framework

Presented in this section is the conceptual design for blockchain integration with edge computing for IoT processing and storage requirements. The scheme is structured in layers to migrate blockchain's intensive operations in a separate layer outside the application layer containing IoT devices having constrained resources. We then proceeded to provide a description of the operations involved in each of the framework's layers. As three IoT fundamental requirement categories: Computation offloading, outsourced data storage and control and management of network traffic, and their deployment in the framework was discussed next. The services deployment description was also accompanied with an illustration of how anonymity, integrity and adaptability solutions were implemented in the framework.

4.1. Design Overview

Our design was composed of three layers identified as the cloud layer, the edge layer and the device layer as illustrated in Figure 4 below. This framework adopts the same layers as those found in the edge computing architecture but enhanced with a P2P connectivity of devices in each layer to provide additional storage and computation capabilities. The device layer constitutes P2P connected IoT end users from whom data originates and they utilize resources in the edge network. The edge layer is comprised of servers and storage facilities that are connected in P2P fashion to provide additional storage, ensure robustness and avoid risks of single points of failure. This layer is responsible for short-term data storage, real-time data processing and analytics and handling communications for various data and messages exchanged among the different nodes. The cloud layer is made up of more powerful facilities to provide long-term data analytics and storage as well enterprise level reporting and communication. The resources in the cloud can also be configured as nodes on blockchain to ensure privacy and integrity of data in the system.

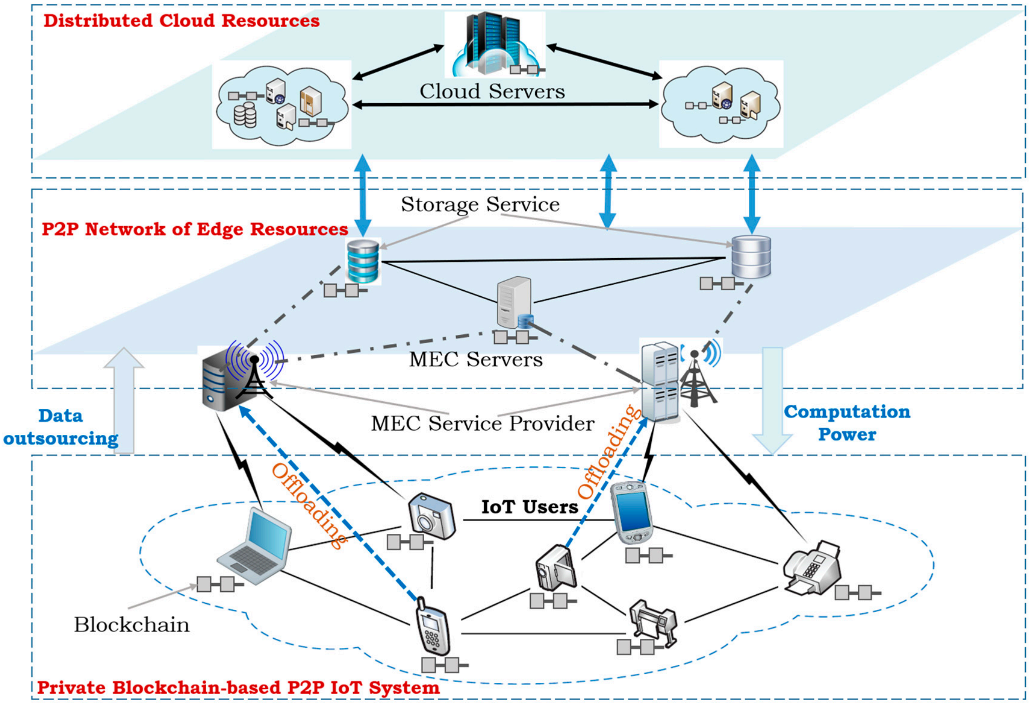


Figure 4. Blockchain-based IoT framework with edge computing.

4.2. The Layered Architecture of the Proposed Framework

In this section, we described all three layers of the proposed framework namely decentralized IoT device layer, P2P network of edge servers and distributed cloud resources in addressing the described issues and meeting the target requirements.

4.2.1. Decentralized IoT Device Layer

This layer is comprised of P2P networks of user devices capable of participating in blockchain system to exchange messages among each other as sources and consumers of IoT data. Such devices include smart devices with sensors and actuators to collect data and share with other peers or forward to upper layers. Communication mechanisms for smart devices to access the system can either be centralized through edge servers or decentralized through a P2P network. In the centralized communication, a private blockchain is enforced whereby interactions among the peers are controlled by the server—addition of new peers, mining of blocks and removal of an existing peer.

In this mode, communication between peer devices is facilitated only through a shared secret key issued to devices by the server.

On the other hand, devices and servers both can participate in public blockchain through the P2P mode of communication. For this case, because of finite resources in end devices, their participation in blockchain was facilitated by more capable servers found in upper layers, at the edge and on the cloud. The heavier operations are thus performed by servers while end devices only performed lighter tasks such as sharing summary file of transactions with peer nodes or accepting firmware updates. As illustrated in Figure 5 below, edge servers securely provide massive outsourced storage and high computation capacities per-demand to IoT devices with constrained resources in both centralized and decentralized modes of communication. Moreover, edge servers being closer to end users can offer fast responses in their IoT applications.

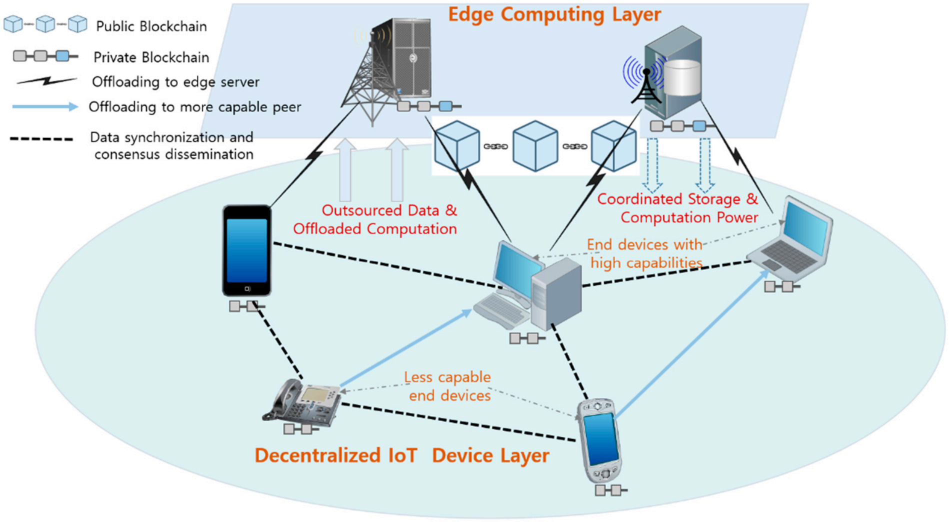

Public Blockchain
Private Blockchain
Offloading to edge server
Offloading to more capable peer
Data synchronization and consensus dissemination
Edge Computing Layer
Outsourced Data & Offloaded Computation
Coordinated Storage & Computation Power
End devices with high capabilities
Less capable end devices
Decentralized IoT Device Layer

Figure 5. Operations involved in the IoT device layer.

The decentralization brought by the P2P connection of devices enable them to flexibly offload their intensive tasks—be it storage or computation to either an edge server or a nearest more capable peer for even faster response time. By offloading, the devices store only a section of the chain useful in their own transactions instead of the whole thing and they are relieved of intensive computation. Furthermore, due to a lack of standardization for smart devices from different vendors to cross-operate, blockchain enables these devices all to participate in the same blockchain network.

4.2.2. P2P Network of Edge Servers

The edge layer extends the cloud to bring services closer to end devices for improved performance and low latency. On top of availing desired resources to smart IoT devices, edge servers can also distribute messages among themselves to create replicated storage of data and coordinated data processing. To achieve this, blockchain is deployed in servers at the edge layer to establish a distributed platform with guaranteed secure transmission of data and across the network. Along with message conveyance in the network, edge nodes conduct light analytics for other peers and for themselves to achieve self-organization in dynamically addition and removal of edge nodes. They also process the data and forward real-time data analytics either to distributed cloud for long term storage or back to end devices as per respective requirements. The P2P architecture in this layer creates a pool of mobilized resources for short-term storage, speedy computation and the analytics.

In case the computing requirements are more intensive than what edge servers can handle; the servers can also offload their workloads and request services from the cloud. Blockchain avail consensus protocols that are utilized to validate devices' requirements for computation and storage claims. Smart contracts with lightweight consensus protocols in such a public blockchain as Ethereum are most appropriate to ensure lower latency and higher throughputs for broader scopes of P2P networked edge servers and distributed resources on the cloud.

4.2.3. Distributed Cloud Resources

The cloud layer is primarily meant to provide "services" for storage and computation but in our framework, it can also be treated as a node on the blockchain network capable of participating in the mining process. Hosting massive storage and computation facilities, consensus mechanism in distributed blockchain is crucial for the cloud layer to provide secure, inexpensive and timely access to offer best quality computing services. Resources configured as blockchain nodes can be incentivized when well behaved and are punished accordingly when they misbehave through the incorporated data integrity service.

Unlike nodes in the edge layer, the cloud layer nodes are independent of data and by using blockchain, complete replication of all records being shared among them is maintained.

4.3. Deployment of Services and Fulfillment of Design Requirements for IoT Applications

Discussed in this section is how the different services are deployed in the framework to meet IoT demands as well as how they can be practically realized in the implementation. Later in the section, an account regarding satisfaction of previously defined design principles for the proposed scheme is given.

4.3.1. Deployment of Services for IoT Requirements

Computation offloading, the first service deployed in our framework plays the role of relieving the heavy and intensive computation tasks from the less capable end devices onto powerful servers found on the edge network. Due to high computing power required in solving such puzzles as PoW during the mining process in blockchain, the resource-disadvantaged mobile devices running IoT applications are incapable of executing them on their own. With edge servers deployed at the edge of the network closer to end devices, their abundant resources can take the processing load from the devices and enable them to participate in the blockchain network. Such tasks involving computations of hashes, encryption and decryption as well as PoW are offloaded from the devices and outsourced to edge servers for execution. Blockchain safeguards the security aspects of this module in a case when a computation operation requires assignment to multiple edge nodes. Having been relieved of such operations increases the battery lifetime for devices and speeds up the execution of tasks with efficiency and assured security.

For offloading computation in our framework we adopt the off-chain state channels proposed by Kasireddy in [25]. This approach offers extensibility for blockchain to store more data and perform more complex operations. With this scheme implemented in our model, the issue of adaptability will be addressed and blockchain's ability to scale with increasing number of transactions will improve. Tools to implement off-chain state channels in our model include a smart contract powered decentralized Lightning Network (https://lightning.network/) presented in [36] or its Ethereum equivalent, Raiden Network (https://raiden.network/) that extends Ethereum with scalable and timely transactions.

The off-chain state channels provide a mechanism of interaction in blockchain whereby events that were supposed to be carried out on blockchain are conducted off the blockchain instead. As illustrated in Figure 6 below, the procedure was achieved in three steps using cryptographically secure mechanisms to achieve significant enhancements with increased speed and lowered costs. After locking part of the blockchain state in step 1 using smart contracts, participants were then able to make updates to their desired transactions in step 2 without committing to the blockchain. Afterwards, the participants submitted the state back to blockchain in step 3, which provided settlement by closing the state channel and unlocking the state again. In this proceeding, only step 1 and 3 involved executions that were published on the blockchain network while step 2 at which most of the intensive tasks were executed did not involve blockchain at all.

Utilizing the off-chain state channels, the less capable IoT devices could lock portions of the blockchain that was needed by their own transactions in step 1 above. Then in step 2, these devices could either download firmware updates or upload data and files with summary of their transactions to be shared with other devices without having to deal with the entire blockchain. Finally, in the last step, the updates made in the locked states were committed back to the main chain where the state channel was closed, and locked state was unlocked.

There is also a proposition by Yeow et al. in [29] and Eyal et al. with their Bitcoin-NG (Bitcoin-next generation) protocol in [24] of using side chains. The target is to improve performance using a protocol that allows connections of new side chains to the main chain with back-and-forth transfers of transactions between the main chain and different other side chains. This scheme, however, incurs high delays in crossing the side chains across the main chain to get the funds to destined side chains where such funds need to be spent and will not be suitable for our model.

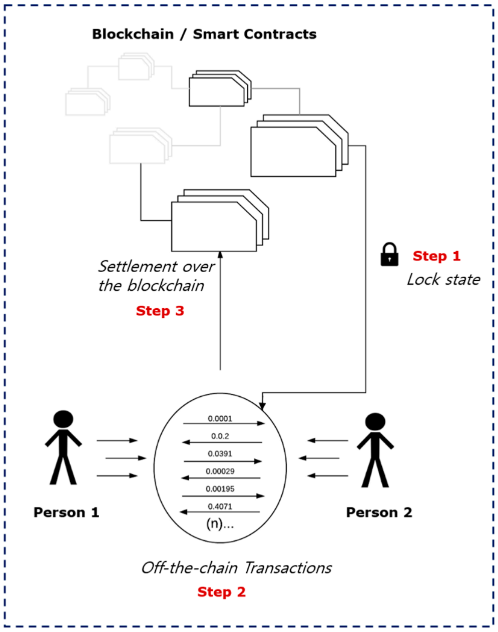
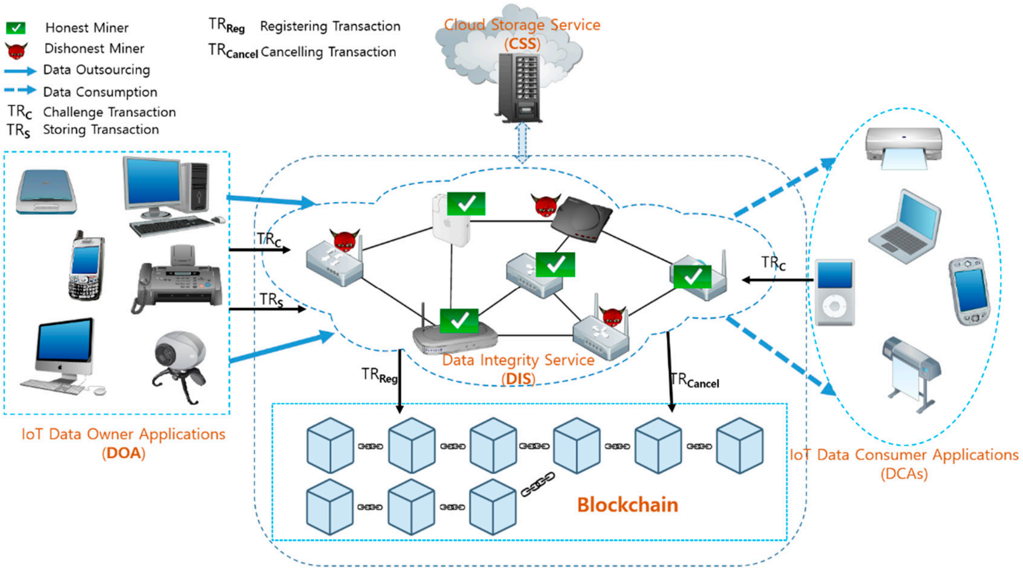


Figure 6. Off-chain state channel procedures.

Outsourced decentralized data storage, compared to the centralized storage mechanisms in cloud computing, the decentralized storage achieved by the integration of edge computing and blockchain exploits the benefits of both to provide increased storage sizes, high security of stored data and keeps data closer to users. Storing data on edge servers close to owners and consumers decreases the communication latency and elevates the system availability, durability and performance. The large storage capacity offered by edge computing complements the validated security in blockchain to ensure a decentralized storage management in P2P basis without entrusting the data to any centralized entity. Additional mechanisms of Proof-of-Space and Proof-of-Spacetime were also introduced for prover participants to convince verifier participants of their replicating capabilities and times of their data storage. These additional features were combined to attain a data integrity service that facilitated data verification to ensure integrity of the stored data along with utilization of Ethereum and smart contracts. With this service, IoT applications were enabled to attain more storage capacities by outsourcing their storage to higher capacity servers on the edge and other peers whereby blockchain was there to guarantee secure storage. We utilized the Data Integrity Service originally formulated by Dziembowski et al. in [26] and the off-chain state channels explained in computation offloading deployment above to realize secure outsourced data storage in our framework.

The blockchain-based Data Integrity Service (DIS) as illustrated in Figure 7 is detailed in [26] as a potential solution for data integrity. In DIS, users were identified as data owners and consumers running their respective data owner applications (DOA) and data consumer applications (DCA). The cloud storage service (CSS) can either be provided as just a service on the cloud or can also practically be treated as a node on the blockchain. Both the owners and consumers were uniquely identified by their corresponding public keys in the blockchain system. Upon joining the blockchain network, both the DOA and DCAs got a key pair generated for them, a private key and a corresponding public key. While the public key would be used to identify each node's account, the corresponding private key would be used in accessing the node's account. All transactions could only be completed in the system when the node's account had enough deposit. While both DOAs and DCAs could flexibly join the network as miners, it was normally challenging and mostly needless for the DOAs to get their deposit by being miners because of their deficient computing power. As for DCAs, based on their hardware facilities and finances, they could also flexibly act as miners or not.

The practical solution for the data integrity service for outsourcing storage in our integrated framework was realized by utilizing a combination of Ethereum and smart contracts. This solution requires that data originating from end devices to be encrypted before being outsourced to safeguard data confidentiality. Using Proof-of-Space (PoSpace), peers involved in a P2P network must legitimize their claims of making deposits and commit the space they possess [30]. PoSpace in this context described a means for a prover to express valid interest when requesting a service by investing significant amount of memory or disk space to solve a challenge administered by a verifier. It is important to note that in solving the issued challenge for PoSpace, apart from dedicating the required space, huge amounts of files need to be exchanged between the prover and verifier, which renders this approach pretty much impractical, but again, security always comes at a price.



✓ Honest Miner
Dishonest Miner
Data Outsourcing
Data Consumption
TR_C Challenge Transaction
TR_S Storing Transaction
TR_{Reg} Registering Transaction
TR_{Cancel} Cancelling Transaction
Cloud Storage Service
(CSS)
TR_C
TR_S
TR_C
TR_{Reg}
TR_{Cancel}
Data Integrity Service
(DIS)
IoT Data Owner Applications
(DOA)
Blockchain
IoT Data Consumer Applications
(DCAs)

Figure 7. Framework for data integrity using blockchain.

To generate and link a transaction in blockchain, peers need to register and validate their transactions by solving the verification challenges as set in proof of space. A smart contract was utilized by IoT users when storing transactions in this framework. After locally encrypting the information to prevent unauthorized access, a transaction was created and then announced by owner clients to the P2P network and made claims for requirements and inquired costs to be incurred. In turn, the miners (peers in the P2P network) checked the users' requirements and available service in transactions to offer clients the needed storage for rent. With adequate incentives and punishments being enforced through smart contracts, IoT devices can thus outsource their data to be stored in a decentralized P2P storage system.

To check integrity of the outsourced data; IoT users generate a new challenge transaction for which the miners hosting the data need to compute a proof (to be verified by users) and put it on blockchain. In the case when the computed proof fails the verification, the miners as data hosts are punished by rewarding the deposit initially committed by them when registering to the IoT users. Miners can revoke, when needed, the committed space by producing a cancelling transaction and withdraw the deposit that was committed during registration.

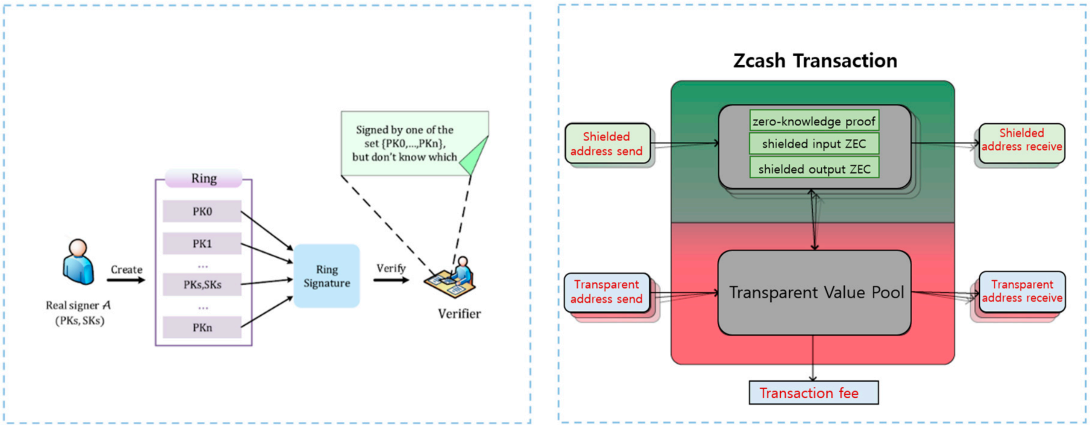
Network traffic control, along with the two described services, assured security in transmission of data from one entity to another is of great importance. This service is deployed to provide network control mechanisms to carry data between devices in those transactions traversing the network across some intermediate nodes. This extends to protect communications of the smart contracts themselves carrying rules that govern various transactional aspects. The contracts could be exchanged by nodes that are likely located at opposite edges of the network and this transmission must be protected. It is imperative therefore, that, both data and contracts communications be protected to achieve reliable and efficient coordination in the network. Such details as rights and privileges, user addressing, cryptographic information and transactions validity period are carried in these messages. As the messages are transported among the devices in the network, security attacks at different levels need to be well addressed in the design. As edge computing bridges subordinate layers and the superior and interfaces with various other systems and protocols (Wi-Fi, M2M and cellular networks for instance), management of the network in this heterogeneous environment becomes inevitably a challenge. The effective measures for this deployment is the use of software-defined networks (SDN) and its extension to SDN components (SDNC) as described by Sharma et al. in [37] through provision of better network visibility by dissociating the control plane from the data plane. Ultimately, the use of dynamic virtualization of network resources in the context of SDNs simplifies management of the network management and facilitates realization of privacy and security in the network through blockchain [38,39]. Measures involving blockchain technologies have been fused in our framework to enable access control, authentication of users and transactions, integrity and data privacy in the framework.

To practically realize enhanced anonymity in the traffic flowing across network nodes in our framework we utilize Zerocash—Zcash (https://z.cash/), its predecessor Zerocoin (http://zerocoin.org/), and linkable ring signature schemes (https://github.com/sorrge/LSAG) presented in [40] and [41]. Zerocash provides a strong privacy-preserving digital currency, Zerocoin offers a cryptocurrency that conceals details of the transaction whereas linkable ring signature avails means to verify whether same signer generated two different signatures, but yet no way to tell the signer's identity.

We discovered three possible approaches to preserve anonymity for blockchain, mixing services, ring signatures and non-interactive zero-knowledge proof from Feng et al. in [3]. The mixing services can offer protection against anonymity attacks by obscuring relationships in a transaction between senders and receivers. The obfuscation allows concealment of entity's identity that is involved in the communication along with contents being transmitted. A ring signature is formed from a set of chosen members that joins the ring without intervention of any central entity and one of the members anonymously signs the message on everyone's behalf. The ring signature produces a valid but anonymous digital signature from the ring of participants without revealing the identity of the signature's producer. As for zero-knowledge proof (ZKP), a cryptographic scheme is provided in which a transaction can be validated without leakage of any extra information.

Despite its spontaneity in mixing transactions for blockchain, the mixing services incur a lot of delay when participants discover one another before their transactions are able to be mixed. The ring signature as illustrated in Figure 8a and initially designed by [42], without going in a lot of details; uses a public key infrastructure (PKI) to generate valid signatures for all members in the ring, which the verifier can validate without discovering the true identity of the real signer. The linkable ring signature is a scheme formed when an entity in the ring is able to sign the same message twice using the same tag whereas the used signatures can be linked using PKI mechanisms, but the signer's identity stays anonymous [3]. In spite of the strong anonymity availed by ring signatures, the large size of its transactions, the direct proportionality between its signature's size to the number of entities in the ring, and its difficulty in auditability are key limitations that it still suffers from.

ZKP on the other hand offers a suitable protocol to anonymously verify transactions in blockchain using its non-interactive zero-knowledge proof (NIZK) variant. In NIZK proof, the connection between the prover and verifier is removed to enable anonymity during transactions. Without diving into detailed explanation of how they operate, zerocoin and zerocash both utilize cryptographic procedures in NIZK proof to prevent transaction analysis and enhance anonymity. Zerocoin is presented by Miers et al. in [27] to counter graphic analysis of transactions and allow full anonymous transactions of currency. It employs NIZK proof procedures to authenticate minted coin before being redeemed later with equal-valued new coin that possess no prior information and hence unlinking the transactions from their origins of payment. Furthermore, zerocash described in [28] provides even a higher level of privacy for blockchain by enabling participants to anonymously pay each other directly without revealing origin, destination and amounts involved in transactions. Figure 8b below illustrates mechanisms to send and receive Zcash in a transaction using shielded addresses and through generated ZKP, other participants are able to verify encrypted data in the transaction without revealing the address.



(**a**) (**b**)

Figure 8. (**a**) Ring signature anonymity; (**b**) high-level view of a ZCash (ZEC) transaction.

4.3.2. Fulfillment of Design Requirements in the Framework

Summarized in Table 1 below are brief descriptions of how the defined target requirements are satisfied in our proposed framework using different tools and other deployed services.

Table 1. Satisfaction of target design principles in the proposed scheme.

Target Requirement	Fulfillment in the framework
Offloaded Computation	Through the use of off-chain state channels implemented by raiden networks, complex and heavy computational loads are relieved from IoT devices onto powerful servers at the edge.
Decentralized Data Storage	By utilization of the data integrity service (DIS) and the off-chain state channels, secure and large storage capacities are obtained through blockchain and edge computing and data is managed in P2P basis without entrusting to any centralized authority.
Authenticated Transactions	To ensure validity of transactions in the system, nodes are required to solve a predefined challenge as set in the smart contracts of the DIS when storing the transactions. A transaction is valid only when the computed proof for the issued challenge is verified by users.
Controlled Access	Through the use of private and public key pairs generated for data owners and consumers when being registered in the DIS, nodes' accounts are identified by the public keys whose access is governed by the corresponding private keys. This ensures controlled access to the stored data in the system.
Anonymity	A hybrid of cryptographic mechanisms in such tools as linkable ring signatures, zerocoin and zerocash are utilized in achieving stronger anonymity of transactions

	beyond the pseudonyms in blockchain in ensuring privacy of users and their respective data.
Integrity of Data	By the use of incentive and punishment schemes enforced through smart contracts to data owners and consumers in the DIS, integrity is guaranteed for IoT devices to outsource their data to be decentrally kept in a P2P storage.
Low Latency	Fast responses (hence low delays) to IoT applications through deployment of edge servers at the edge of the network closer to end devices.
Adaptability	Enhanced ability to scale in the scheme through the off-chain state channels availed by the use of Lightning or Raiden networks to allow future growth of more devices and massive transactions.

5. Experimental Evaluation

5.1. Prototype Design of the Proposed Framework

In this section we presented a detailed experimental design and tools required for implementation of a prototype for our proposed framework. As an initial proof-of-concept to verify practicality of our decentralized storage scheme; we used a setup shown in Figure 9**Error! Reference source not found.** below to perform the experiments. A powerful workstation, for example one containing an Intel Xeon Processor E5-1630 v3 (10 MB SmartCache and operating 3.70 GHz) was used as an edge computing server. In actual operation, P2P network of edge servers was to be implemented but this setup should suffice to run our initial tests. On the other hand, android empowered devices were used as IoT end nodes. Moreover, among the many cloud service providers such as Amazon's S3, Digital Ocean and IBM's BlueMix, we used Microsoft Azure from Microsoft to build, deploy and test our framework. A summary of tools, equipment and technologies required for development of our prototype are presented in Table 2**Error! Reference source not found.** below along with their respective description.

Table 2. List of tools, equipment and technologies for prototype development and testing.

Serial #	Item Name	Item Description
1	Android Mobile Devices	End nodes on which IoT applications run.
2	Edge Computing Server	A powerful server to host offloaded tasks.
3	Wireless Access Point	A network hub to provide connectivity between devices.
4	Microsoft Azure Cloud	Provision of cloud services.
5	TestRPC	Simulation of Ethereum blockchain.
6	Truffle	Framework for development of smart contracts.
7	MetaMask	Ethereum client for web browser.
8	web3 API	Ethereum JavaScript API.
9	npm	JavaScript's Node Package Manager.
10	Node.js	JavaScript's run-time environment.
11	Data integrity service	Smart contracts-based framework for data integrity.
12	Raiden network	Ethereum extension to provide off-chain scaling.
13	Linkable ring signatures	A digital signature scheme to verify anonymous message signer.
14	Zerocash	A cryptocurrency to enable selective transparency of transactions.

The endgame was for IoT end nodes to act as miners and perform mining operations on the edge computing server whose computation and storage capabilities could be elevated by services on the Microsoft azure cloud. Using an Ethereum JavaScript API, web3 (https://github.com/ethereum/web3.js/), we developed a data storage decentralized application (*DApp*) whose client module could be installed and run on IoT nodes and operated by Ethereum platform running on the edge workstation. Three basic tools were needed to develop this application, namely TestRPC, Truffle and MetaMask.

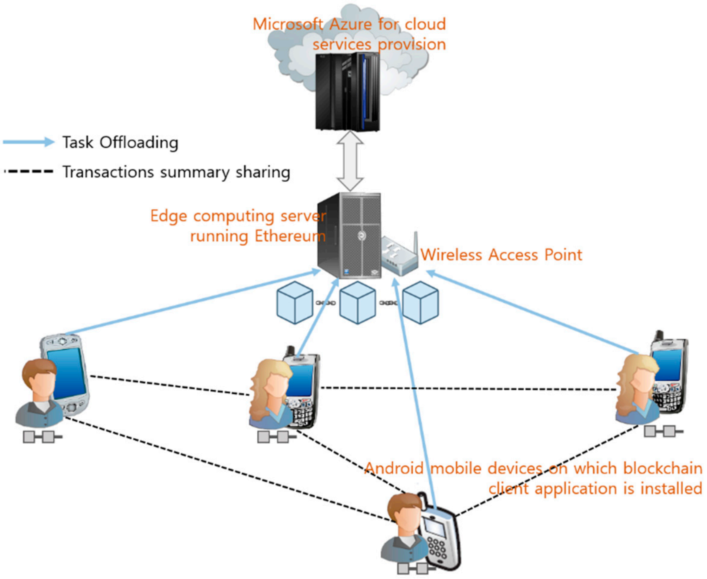

Microsoft Azure for cloud services provision
Task Offloading
Transactions summary sharing
Edge computing server running Ethereum
Wireless Access Point
Android mobile devices on which blockchain client application is installed

Figure 9. Prototype implementation setup.

TestRPC as one of Ethereum clients can be used to locally simulate an Ethereum network to run and test the smart contracts before being deployed on the main network. It is available on npm package manager, the default package manager for Node.js.

Through Node.js, the Ethereum network can then be locally created and started with some default accounts, private keys and listening on a designated port (say 8545 for example).

Truffle is used as a toolsuite for development of Ethereum's solidity-based smart contracts. Having similar syntax to JavaScript, solidity is an object-oriented, high-level programming language highly used in development of smart contracts. Equipped with built-in compilation for smart contracts, their testing and deployment, truffle also offers a JavaScript abstraction to simplify communications between smart contracts and user application interfaces. It is also available on npm and it is compatible with TestRPC and web3 API without any additional installation or configurations.

In a project tree created, truffle service can then be initialized to host the smart contracts, to manage deployment files and house test files, which are useful for testing the contracts and the applications under development.

As a final tool piece, MetaMask provides a lightnode Ethereum client that runs in the web browser to expose the web3 API to the developed DApp and enable the user to interact with Ethereum network by running it on the browser. MetaMask tool is offered as an extension in Google chrome with which a user can connect various Ethereum networks, ranging from the main network, some online test networks or the implemented local network on TestRPC. From the designated port, the user is able to change network and connect MetaMask to the Ethereum network operated locally by TestRPC.

Using the above described environmental setup we developed our decentralized application integrating it with the zerocash project (https://github.com/zcash/zcash) along with the linkable ring signature scheme (https://github.com/sorrge/LSAG) for stronger privacy. An extension of the Ethereum network, the raiden network was also utilized for scalable and instant transactions. The smart contracts in the DApp were implemented through the Ethereum network to realize the data integrity service. Using the developed DApp, the mobile devices could connect to the edge server through a wireless access point (AP) and perform mining processes. In this case, the miners were assisted by Ethereum services to request storage and computational services from the edge server. The mined blocks of transactions could then be accessed and distributed through the Ethereum network.

For measuring framework's performance, we aimed at conducting experiments using a combination of the TestRPC running on Node.js to simulate the Ethereum network and our developed DApp for smart contracts and other incorporated features. Using Node.js, we first created an initial, say 5000 blocks and then proceeded using the mobile nodes to initiate mining of blocks on top of the main blockchain. Varying the number of mining devices, we considered three different cases—using three, four and five miners in the three cases. We fixed the number of transactions in each block being mined (say 20 transactions) and through smart contracts we could adjust the "difficulty" targets for PoW puzzles. We used Central Processing Unit (CPU) utilization afterwards to measure miner's computation demands trends for all the three cases. At this initial stage of our model development, we only targeted to evaluate successful mining of blocks. We used edge server's CPU utilization to measure computation service demands by varying number of miners and their respective demands. The service demand then reflected the success probability in mining the blocks. Similarly, we aimed to run our experiments to evaluate energy and memory consumption, as well as a full scale deployment of incentivized outsourced storage with optimized offloading models.

5.2. Conceptual Evaluation and Discussion

Our investigation for blockchain technologies to meet our design goals of anonymity, integrity and adaptability levels in our framework had discovered potential solutions. These solutions need to be incorporated together in a unified decentralized application developed based on the blockchain network to verify its smooth operation. In this section we discussed our research findings and the conceptual analysis of our initial practical implementation for the framework.

The limitations to scale and interoperate brought by heterogeneity of IoT devices and the various protocols involved in edge computing environment was addressed by introducing a layered architecture in the blockchain system. This entails dividing blockchain deployment into separate layers and excluding it from the application layer, thus, allowing the less capable IoT devices to store only the portion of blockchain that is required by their own transactions. Storage of entire blocks, which is very expensive for devices with low capacities, will then be avoided. The operations and interactions of the different entities in the individual layers were given in detail in the proposed framework section. As explained earlier, the off-chain state channels scheme allows some operations of the blockchain to execute off the chain. This enables the separation of blockchain intensive operations into another separate layer. In our model, the massive data storage and intensive transactions can be outsourced from IoT devices as off-chain storage and off-chain computation to off-chain resources at the edge layer and other peers in the system. Facilitated with large amounts of storage and computation capabilities accumulated in a P2P network, the framework can avail enough capacities for storage and processing to enable blockchain's adaptability for IoT applications. Since the heavy tasks have been outsourced off-the-chain, a more secure and efficient IoT system could be realized that is capable of adapting to changes in the environment and increased users and transactions.

As for a crucial aspect of anonymity in a decentralized system that ensures reliable access and control, distributed computation and secure data storage with validated transactions, just blockchain's pseudonyms are not enough. Some applications require stronger anonymity and just pseudonyms will not cut it, a hybrid of several cryptographic schemes should be used instead to achieve full anonymity. As explained earlier, using tools like linkable ring signatures enables us to conceal the identity of the sender in a transaction and allow users in the network to anonymously and trustily perform transactions. Moreover, zerocoin and zerocash employ non-interactive zero-knowledge proof to create perfect tools for obfuscating information contained in transactions. By converting information bits in a transaction into some unintelligible random bit sequence with no linkage to original information, these tools make it impossible for an adversary to bleach anonymity. This resilience to stop ill-intended entities to recover even a single bit of information about the transaction makes these protocols more suitable for guaranteeing anonymity in our model.

Furthermore, the data integrity service that makes use of Ethereum and smart contract facilitated by proof-of-space offers an adequate solution for data integrity. This combination brings together the data owners and consumers to interact in a P2P fashion to meet their requirements for storage and data respectively. The smart contracts create incentive and punishment mechanisms in the system to encourage more miners to join the network and commit their storage space and punish those who fail to verify their actions to ensure authenticity and integrity of data. We therefore find this mechanism to be suitable in safeguarding data integrity in our decentralized framework and achieve the needed security for data storage. Moreover, through the use of different tools and various combination of cryptographic mechanisms as was presented earlier in Table 2; the target requirements of our integrated scheme were fulfilled.

With these findings, we were developing a system prototype and integrated the uncovered solutions to achieve a secure blockchain storage system in an edge computing platform to serve IoT devices. Our solution was utilizing the Ethereum's JavaScript API to create a decentralized application that we then tested on a TestRPC Ethereum simulated network. Using smart contracts from the truffle framework and MetaMask Ethereum web client, we were able to deploy and test our application. Utilizing the raiden network to extend Ethereum, smart contracts in our application were deployed being equipped with zerocash and linkable ring signatures schemes, as well as the data integrity service. With this combination we were able to achieve adaptability through the raiden network, which was an off-chain scaling solution whose primary purpose was to offer instant, low-cost and scalable transactions. With this network we could implement a layered architecture in which end devices running IoT applications stored only portions of the blockchain and performed light computations. Meanwhile the large storage requirements and intensive computations were offloaded to more powerful servers on upper layers. The data integrity service was addressed in the application through rules defined in Ethereum smart contracts and we finally achieved strong anonymity of user and transactions in IoT through zerocash protocol and linkable ring signatures scheme.

6. Conclusion and Future Directions

Our study was set to seek a secure data storage and a highly performing design of IoT by integrating two highly trending technologies, blockchain and edge computing. We proposed an integrated IoT framework based on P2P network to enable edge computing and blockchain complement one another with their large storage capacity and strong security features respectively. To meet the security and performance requirements of our model, we investigated the suitable existing technologies to address issues of integrity, adaptability and anonymity that are crucial for integration of blockchain and edge computing.

We adopted a Proof-of-Space based solution in smart contracts-based data integrity service to authenticate stored transactions and fortify data integrity with no central authority involved. To enhance scalability in our design, we adopted a layered architecture that separates blockchain from the application layer realized through raiden network that extends Ethereum with instant and scalable transactions. The separation enables resource-restrained IoT devices to only store portions of blockchain needed for their own transactions. As for anonymity, we found linkable ring signatures, zerocoin and zerocash to be adequate tools for concealing user identity and obscuring information contained in transactions. We therefore utilized zerocash and linkable ring signatures in the prototype of our framework to strengthen anonymity. From our study, we have designed a practical system prototype for implementation of integrated system of blockchain and edge computing with secure and decentralized data storage. Conceptual evaluations of the individual solutions incorporated indicate feasibility in successful integration sufficient for safely storage of massive information shared among diverse IoT devices.

Future works: In this article we have only provided a conceptual design of a system prototype and provided a concise evaluation mostly based on the strengths of the individual solutions adopted. Our future endeavors are focused in using the decentralized application developed to evaluate the successful operation of our proposed scheme and optimize the different parameters involved. Starting with simple patterns of CPU utilization, memory usage and power consumption on the edge server to evaluate system's performance, we envision achieving a full scale deployment across all layers. Afterwards we shall formulate some optimized models for outsourcing along with offloading (e.g., what to offload, when to offload and where to offload) and then evaluate performance for all associated aspects of network latency and bandwidth consumption to achieve a higher throughput and fast responding system.

Author Contributions: Conceptualization, B.W.N. and J.C.S.S.; Methodology, B.W.N. and J.C.S.S.; Writing—Original Draft Preparation, B.W.N. and J.C.S.S.; Supervision, S.R. and J.H.P.; Funding Acquisition, J.H.P and Y.S.

Funding: This research was supported by the MSIT (Ministry of Science, ICT), Korea, under the High-Potential Individuals Global Training Program) (2019-0-01585) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

Conflicts of Interest: The authors declare no conflict of interest regarding the design of this study, analyses and writing of this manuscript.

References

1. Kubendiran, M.; Singh, S.; Sangaiah, A.K. Enhanced Security Framework for E-Health Systems using Blockchain. *J. Inf. Process. Syst.* **2019**, *15*, 239–250.
2. Xiong, Z.; Zhang, Y.; Niyato, D.; Wang, P.; Han, Z. When Mobile Blockchain Meets Edge Computing. *IEEE Commun. Mag.* **2018**, *56*, 33–39.
3. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2018**, *13*, 45–58.
4. Kim, H.W.; Jeong, Y.S. Secure Authentication-Management human-centric Scheme for trusting personal resource information on mobile cloud computing with blockchain. *Hum. Centric Comput. Inf. Sci.* **2018**, *8*, 11.
5. Vukolić, M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security*; Springer: Berlin, Germany, 2015.
6. Conoscenti, M.; Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016.
7. Satyanarayanan, M. The emergence of edge computing. *Computer* **2017**, *50*, 30–39.
8. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1508–1532.
9. Meng, W.; Tischhauser, E.W.; Wang, Q.; Wang, Y.; Han, J. When Intrusion Detection Meets Blockchain Technology: A Review. *IEEE Access* **2018**, *6*, 10179–10188.
10. Samaniego, M.; Deters, R. Blockchain as a Service for IoT. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016.
11. Lin, I.C.; Liao, T.C. A Survey of Blockchain Security Issues and Challenges. *IJ Netw.Secur.* **2017**, *19*, 653–659.
12. Wüst, K.; Gervais, A. Do you need a Blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018.
13. Brickell, E.; Li, J. Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities. In Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, Alexandria, VA, USA, 29 October 2007.
14. Jiao, Y.; Wang, P.; Niyato, D.; Xiong, Z. Social welfare maximization auction in edge computing resource allocation for mobile blockchain. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Beijing, China, 16–18 August 2018.
15. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A Survey on the Edge Computing for the Internet of Things. *IEEE Access* **2018**, *6*, 6900–6919.
16. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411.
17. Shafagh, H.; Hithnawi, A.; Burkhalter, L.; Fischli, P.; Duquennoy, S. Secure sharing of partially homomorphic encrypted iot data. In Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems, Delft, The Netherlands, 6–8 November 2017.
18. Hummen, R.; Shafagh, H.; Raza, S.; Voig, T.; Wehrle, K. Delegation-based Authentication and Authorization for the IP-based Internet of Things. In Proceedings of the 2014 Eleventh Annual IEEE

International Conference on Sensing, Communication, and Networking (SECON), Singapore, 30 June–3 July 2014.

19. Hu, Y.C.; Patel, M.; Sabella, D.; Sprecher, N.; Young, V. Mobile edge computing—A key technology towards 5G. *ETSI White Pap.* **2015**, *11*, 1–16.
20. Jararweh, Y.; Doulat, A.; AlQudah, O.; Ahmed, E.; Al-Ayyoub, M.; Benkhelifa, E. The future of mobile cloud computing: Integrating cloudlets and mobile edge computing. In Proceedings of the 2016 23rd International Conference on Telecommunications (ICT), Thessaloniki, Greece, 16–18 May 2016.
21. Abbas, N.; Zhang, Y.; Taherkordi, A.; Skeie, T. Mobile edge computing: A survey. *IEEE Int. Things J.* **2018**, *5*, 450–465.
22. Aijaz, A.; Dohler, M.; Aghvami, A.H.; Friderikos, V.; Frodigh, M. Realizing the Tactile Internet: Haptic Communications over Next Generation 5G Cellular Networks. *IEEE Wirel. Commun.* **2017**, *24*, 2–9.
23. Liu, M.; Yu, F.R.; Teng, Y.; Leung, V.C.M.; Song, M. Distributed Resource Allocation in Blockchain-Based Video Streaming Systems With Mobile Edge Computing. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 695–708.
24. Eyal, I.; Gencer, A.E.; Sirer, E.G.; Van Renesse, R. Bitcoin-ng: A scalable blockchain protocol. In Proceedings of the 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16), Santa Clara, CA, USA, 16–18 March 2016.
25. Kasireddy, P. Blockchains don't Scale. Not. Today, at Least. But there's Hope. 2017. Available online: https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a (accessed on 19 May 2019).
26. Liu, B.; Yu, X.L.; Chen, S.; Xu, X.; Zhu, L. Blockchain based data integrity service framework for IoT data. In Proceedings of the 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, 25–30 June 2017.
27. Miers, I.; Garman, C.; Green, M.; Rubin, A.D. Zerocoin: Anonymous distributed e-cash from bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013.
28. Sasson, E.B.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized anonymous payments from bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–21 May 2014.
29. Yeow, K.; Gani, A.; Ahmad, R.W.; Rodrigues, J.J.; Ko, K. Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. *IEEE Access* **2017**, *6*, 1513–1524.
30. Yu, Y.; Li, Y.; Tian, J.; Liu, J. Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wirel. Commun.* **2018**, *25*, 12–18.
31. Möser, M.; Böhme, R.; Breuker, D. An. inquiry into money laundering tools in the Bitcoin ecosystem. In Proceedings of the 2013 APWG eCrime Researchers Summit, San Francisco, CA, USA, 17–18 September 2013.
32. Koshy, P.; Koshy, D.; McDaniel, P. An. analysis of anonymity in bitcoin using p2p network traffic. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin, Germany, 2014.
33. Valenta, L.; Rowan, B. Blindcoin: Blinded, accountable mixes for bitcoin. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin, Germany, 2015.
34. Wörner, D.; Von Bomhard, T. When your sensor earns money: Exchanging data for cash with Bitcoin. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, Seattle, WA, USA, 13–17 September 2014.
35. Zyskind, G.; Nathan, O.; Pentland, A. Enigma: Decentralized Computation Platform with Guaranteed Privacy. *arXiv*, 2015, arXiv:1506.03471.
36. Poon, J.; Dryja, T. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*; Draft Version 0.5; 2015. Available online: http://www.bitcoinlightning.com (accessed on 19 May 2019).
37. Sharma, P.K.; Chen, M.Y.; Park, H.J. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access* **2018**, *6*, 115–124.
38. Salahuddin, M.A.; Al-Fuqaha, A.; Guizani, M.; Shuaib, K.; Sallabi, F. Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare. *arXiv* **2018**, arXiv:1805.11011.
39. Samaniego, M.; Deters, R. Virtual resources & blockchain for configuration management in IoT. *J. Ubiquitous Syst. Pervasive Netw.* **2017**, *9*, 1–13.
40. Liu; K.J.; Wei; K.V.; Wong; S.D. Linkable spontaneous anonymous group signature for ad hoc groups. In *Australasian Conference on Information Security and Privacy*; Springer: Berlin, Germany, 2004.

41. Wang, L.; G. Zhang; Ma, C. A survey of ring signature. *Front. Electr. Electron. Eng. China* **2008**, *3*, 10–19.
42. Rivest, R.L.; Shamir, A.; Tauman, Y. How to leak a secret. In *International Conference on the Theory and Application of Cryptology and Information Security*; Springer: Berlin, Germany, 2001.