Computers, Materials & Continua
DOI:10.32604/cmc.2021.014753
Article

Tech Science Press

Blockchain-as-a-Utility for Next-Generation Healthcare Internet of Things

Alaa Omran Almagrabi[1], Rashid Ali[2], Daniyal Alghazzawi[1], Abdullah AlBarakati[1] and Tahir Khurshaid[3,*]

[1]Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]School of Intelligent Mechatronics Engineering, Sejong University, Seoul, 05006, Korea
[3]Department of Electrical Engineering, Yeungnam University, Gyeongsan, 38541, Korea
[*]Corresponding Author: Tahir Khurshaid. Email: tahir@ynu.ac.kr
Received: 13 October 2020; Accepted: 24 January 2021

Abstract: The scope of the Internet of Things (IoT) applications varies from strategic applications, such as smart grids, smart transportation, smart security, and smart healthcare, to industrial applications such as smart manufacturing, smart logistics, smart banking, and smart insurance. In the advancement of the IoT, connected devices become smart and intelligent with the help of sensors and actuators. However, issues and challenges need to be addressed regarding the data reliability and protection for significant next-generation IoT applications like smart healthcare. For these next-generation applications, there is a requirement for far-reaching privacy and security in the IoT. Recently, blockchain systems have emerged as a key technology that changes the way we exchange data. This emerging technology has revealed encouraging implementation scenarios, such as secured digital currencies. As a technical advancement, the blockchain network has the high possibility of transforming various industries, and the next-generation healthcare IoT (HIoT) can be one of those applications. There have been several studies on the integration of blockchain networks and IoT. However, blockchain-as-a-utility (BaaU) for privacy and security in HIoT systems requires a systematic framework. This paper reviews blockchain networks and proposes BaaU as one of the enablers. The proposed BaaU-based framework for trustworthiness in the next-generation HIoT systems is divided into two scenarios. The first scenario suggests that a healthcare service provider integrates IoT sensors such as body sensors to receive and transmit information to a blockchain network on the IoT devices. The second proposed scenario recommends implementing smart contracts, such as Ethereum, to automate and control the trusted devices' subscription in the HIoT services.

Keywords: blockchain; next-generation IoT; privacy and security; healthcare IoT; complex healthcare applications

1 Introduction

The Internet of Things (IoT) has widely evolved and undergone rapid advancements, leading to several complex applications, for example, smart cities, smart industries, and smart healthcare. It is expected that more than 30 million smart devices will be part of the IoT by 2020 [1]. The blend of billions of connected devices equipped with sensors and actuators improves the user's quality of experience (QoE). The IoT is expected to contribute more than USD 7 trillion to the world economy by 2020 [1]. Although the IoT improves users' QoE, it faces various privacy and security challenges because of the numerous connected smart devices utilizing existing wireless communication technologies. For example, Wi-Fi, ZigBee, and Bluetooth [2], particularly for security-related applications, such as healthcare IoT (HIoT). Fig. 1 shows a typical HIoT architecture, where the information created in a healthcare framework by different sensors goes to the handling layer with varying communication assistance technologies. The privacy and security issues to such a piece of information are known to the researchers. However, they are either ignored or observed as a reconsideration. It is significant for the HIoT to improve its operational structure from an expensive, unreliable, and centralized design to an intelligent, more reliable, and decentralized framework [3]. Such a decentralized model guarantees reduced network deployment costs, network scalability, system self-sufficiency, protection and privacy in a trustless setting, user-level safety, and most significantly, a network attack control infrastructure.

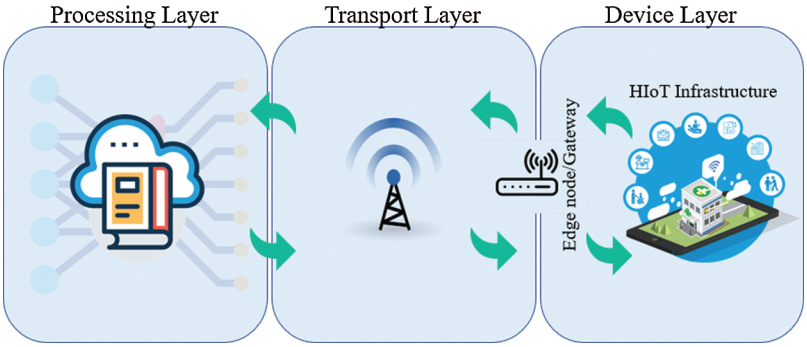

Figure 1: A typical layered architecture of an IoT-based healthcare system

Today, the information is easily trusted from industrial and government institutions, such as hospitals and healthcare centers, without guaranteeing that the data has not been manipulated or falsified by the attackers. It usually happens if data security systems are centralized. The attackers exploit data as per their advantages, bringing a threat to sensor device reliability. Consequently, privacy and security frameworks are essential to ensure that the data have never been altered. One of the potential arrangements in the HIoT to bring trust is to execute a distributed model, where all the participating healthcare devices trust and assure that the data stays unchanged. For instance, if all the healthcare devices have the data and demonstrate to one another that the data have not been altered, it is conceivable to accomplish trustworthiness and security. For this reason, blockchain systems are now being considered by researchers as one of the potential frameworks [4–9] to acknowledge the required decentralized trustworthiness in the IoT.

Recently, blockchain technology arose as a decentralized, trustless verification system for monetary exchanges of Bitcoin cryptographic money (digital currency). The cryptographic security advantages of blockchain inspire researchers to utilize IoT systems to address privacy and security

issues, such as pseudonymous identities (PIDs), decentralization, variation to non-critical failure, the openness of the transactions, and access [6]. Thus, blockchain as a distributed setup and alteration-free system can handle security issues, fundamentally in the HIoT [10] for information privacy and reliability. Usually, the HIoT structures are distributed, and the decentralized peer-to-peer (P2P) condition of the blockchain network is in a perfect form for the HIoT systems. The comprehensive record-keeping blockchain systems keep track of the transactions (TXs) in the HIoT network among numerous devices in a decentralized way. It leads to an agile system setup and lessens the risks of single point network failure. In a few of the related research works [11,12], the researchers propose solutions for specially selected vehicular ad hoc networks (VANETs). The blockchain network also holds TXs in a certain inconclusive way to ensure validity. Specifically, the receiving user's signature in TXs guarantees the legitimacy and non-repudiation of the TXs. This hashed chain structure of a blockchain network insists the data integrity. Consensus mechanisms in a blockchain system ensure the integrity and precision of the hashed chain.

Additionally, consensus contracts tolerate attacks and failures in the network. For instance, as detailed in [13], the proof-of-work (PoW) consensus protocol suffers attacks from twelve hash power attackers, and a similar situation occurs from thirteen attackers using a practical Byzantine fault tolerance (PBFT) consensus protocol. These issues are serious for the HIoT applications, where the heterogeneous kind of sensor devices with heterogeneous system situations produce the diverse type of IoT information.

Table 1: List of abbreviations and acronyms used in this paper

Abbreviations	Definition
BaaU	Blockchain-as-a-utility
PBFT	Functional Byzantine fault tolerance
IoT	Internet of things
HIoT	Healthcare IoT
PID	Pseudonymous identity
P2P	Peer-to-peer
PoW	Proof of work
PoS	Proof of service
LPoS	Leased proof of stake
PoB	Proof of burn
PBFT	Practical Byzantine fault tolerance
QoE	Quality of experience
SC	Smart contract
TX	Transaction
VANET	Vehicular ad hoc network

Furthermore, because of its capacity to utilize alterable open keys as client PIDs to shield privacy and security [14], a blockchain network has a high degree of encryption. Therefore, a blockchain network can be linked to the IoT applications and services, especially those requiring reliable communication [15], such as the HIoT applications. However, current blockchain systems have constraints on flexibility, TX affirmation, higher capacity prerequisites, high power consumption, and computational requirements, and, most essentially, security leakage because of the

trustless supporting structure. These barriers mean a comprehensive challenge of the blockchain network before being utilized for a trustworthy HIoT in a protected and effective manner.

Similarly, to encourage the selection of blockchain systems for reliable HIoT networks, a significantly out-of-the-way investigation is expected to explore how current blockchain systems can be utilized as a reliability tool for the HIoT. Moreover, the difficulties confronted by HIoT applications are exploiting the blockchain system's privacy and security issues. This paper outlines a precise overview of the blockchain network technology to solve threats to HIoT privacy and security necessities. We propose the use of two of the blockchain innovations in detail; smart contracts (SCs) and the consensus mechanisms, to assess a viable blockchain-as-a-Utility (BaaU) framework for security assurance in the HIoT systems. We propose using the BaaU framework in cloud network administration and correspondence layers to meet the numerous security needs of the HIoT systems, for example, validation of the healthcare devices, support, authorization, data assurance, and low latency in critical data transmission. Tab. 1 lists all the abbreviations and acronyms used in the paper.

2 An Overview of Blockchain

2.1 Blockchain: A Definition

The trustworthiness in the distributed data frameworks is critical because of the absence of confirmation mechanisms, mainly on account of sensitive information, for example, the utilization of digital currencies in direct money TXs. Nakamoto [16] presented Bitcoin as a virtual digital currency that works in a decentralized way without any centralized server. Bitcoin stores money TXs securely in a decentralized P2P system of verifiable nodes (known as actors). In addition to Bitcoin, Nakamoto sets forth the idea of blockchain, the adoption of which gained significantly more popular than the cryptographic digital currency. The blockchain checks currency-related TXs performed by untrustworthy actors. The blockchain network is distributed in its nature, everlasting, open, steady, and auditable. The genuine significance is that a client can transparently look at the entirety of the system's previous exchanges. Similarly, every activity of the frameworks can be verified at any time and can be approved by any actor.

2.2 Structure of a Blockchain

A basic blockchain structure can be divided into three layers: A fundamental P2P working layer, an overall ledger layer, and various application layers, as shown in Fig. 2. The essential first layer of P2P connected devices ensures unconstrained contact among the geographically distributed actors. Although such actors are physically distributed devices, the application of the actors has proportional privileges. Such devices engage in the routing measure by finding and keeping up the associations between neighboring devices, thus inducing and affirming the network TXs. As such, devices in the framework synchronize the blockchain's information blocks (data structure), which are the characteristics of a distributed blockchain network.

The data structure in a blockchain network enlists information on TXs performed at a given time. Every block within a blockchain is referenced by the previous block's header hash, as shown in Fig. 3. The framework's peers include the functionalities of routing, limit, wallet association, and TX mining to facilitate the blockchain system [17]. The devices are placed into four categories based on these functionalities: Core devices, maximum functionality devices, private minor devices, and light wallet devices. The entire blockchain's replication and lighter devices form a portion of the connected devices' chain. The security keys are kept in the wallet allowing devices to perform network TXs, for instance, managing Bitcoins. Finally, authorizing the PoW agreement

to include new blocks is the mining feature of a device. The miners are the devices that execute these functionalities through mining. The miners gather recently created Bitcoins and are provided with digital currency as a compensation fee for their services. The PoW is the core of a trustless consensus technique in a blockchain network, which comprises a computationally rigorous task that is very complicated for new blocks to solve. The miners in a blockchain network finish the PoW to distribute a new block; at that point, the remaining devices in the network affirm its legitimacy before adding to the chain; due to different miners' simultaneous association with the chain of the blocks, blockchain forks into various branches. The miners include the lengthiest legal extension of blocks to determine this circumstance. These steps bring about an advanced, distributed calculation of trustless consensus. In that case, a malicious attacker must get hold of at least 51% of the framework's computational resources. Thus, corrupting blocks in a blockchain is nearly impossible.

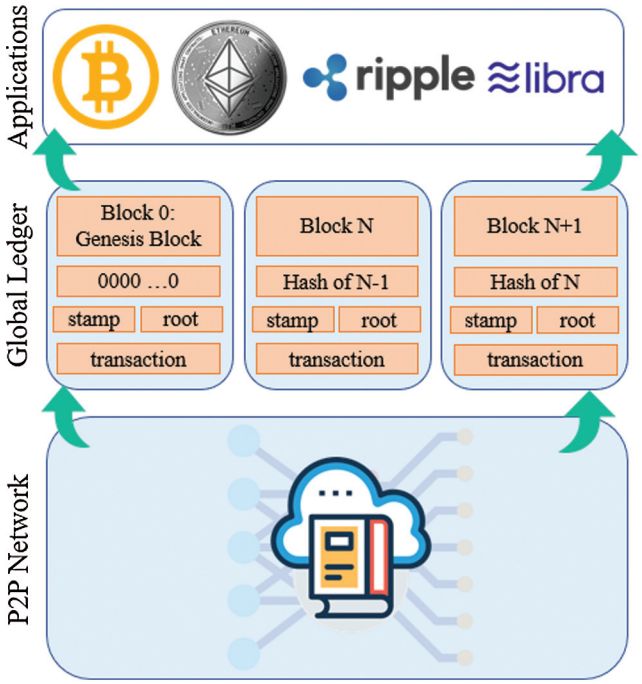

Figure 2: A conventional layered architecture of the blockchain network

The SC is a technological advancement in the form of a digital protocol presented by the blockchain, which permits the programmed implementation of a contract based on predefined conditions. An SC decides the reason for the execution of an exchange with the digital currency substitute. A typical SC indicates limits and necessities outside digital currency exchange, such as acknowledging benefits in a specific extent of interactions with non-monetary segments, making it an ideal part for a blockchain advancement in different research areas. Ethereum [18] was one of the first blockchain networks to implement SCs.

2.3 Types of a Blockchain Network

The blockchain networks are partitioned into two groups; permissioned blockchain networks or permissionless blockchain networks. There are numerous kinds of blockchain networks

dependent on such definitions, for example, public, private, hybrid, and consortium blockchain networks. Tab. 2 shows the critical difference between different types of blockchains. A blockchain network can be characterized as permissioned or permission-less based on the limitations to connect new blocks of TXs. A permission-less blockchain network includes new blocks of TXs by any of the users; however, only authorized devices can deal with TXs in a permissioned blockchain network [19].

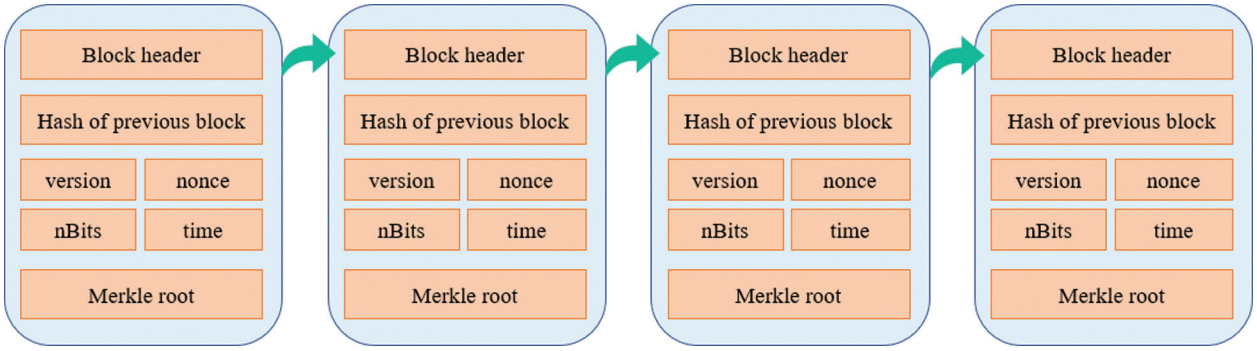

Figure 3: Connected blocks in a typical blockchain network

Table 2: Comparison between permissioned and permission-less blockchain networks

Permissioned	Permission-less
Requires permission before participation	Does not require permission before participation
Participants are already known	Participants are unknown
A limited number of participants	Unlimited number of participants
Data security	Less data privacy
Instant consensus inevitability	Week consensus inevitability
High transaction throughput	Low transaction throughput
Less scalable	Highly scalable
Vulnerability for participant collusion	Vulnerable to 51% attack

2.3.1 Public Blockchain

A public blockchain network exists in the permission-less blockchain category, which gives free and open access to the digital ledger from any device in the system [20]. The mining of new blocks is often focused on the ultimate rewards to incentivize the miners. In a public blockchain network, the correspondence between the devices takes more time to add the TXs. System transparency is protected by making all TXs accessible to shared devices. Thus, user information security concerns and issues are rising in such a blockchain network. Since there is a weak TX certainty, there is a low TX throughput in the public blockchain, generally determined in transactions per second (TPS). A few examples of public blockchains include Bitcoin, Ethereum, Litecoin [21], and Lisk [22].

2.3.2 Private Blockchain

A typical private blockchain is an approved ledger with a limited number of known miners. This type of blockchain has restricted handling of TXs for the predefined miners. Moreover, miners have access to their directly connected TXs [19]. One example of a private blockchain, Hyperledger-Fabric [23], ensures the secrecy of TXs utilizing multiple private channels. Such private channels are called restricted communication methods that one-of-a-kind miners use to secure TX protection and confidentiality. The private blockchains are unquestionably looser as compared to the public blockchains. Since private blockchains have a low quantity of approved miners, they are faster than public blockchains and have a higher throughput [20]. However, some private blockchains utilizing Byzantine fault tolerance (BFT) consensus experience low versatility issues due to the limited number of validators. Zheng et al. [10] depict that the partially incorporated TX blocks can be altered in a private blockchain. Examples of private blockchain models include Hyperledger, Multichain [24], and Quorum [25].

2.3.3 Hybrid/Consortium Blockchain

A hybrid blockchain network is a partially decentralized blockchain that balances between a private and a public blockchain [18]. In this type of blockchain network, the consensus technique is overseen by a portion of the pre-chosen devices. For instance, in the Hyperledger blockchain, miners maintain a mining device in the blockchain network. Approval of a block in the Hyperledger includes signing in from at least seven devices. In this situation, the explicit network devices may have free perusal access to the blockchain or maybe restricted otherwise [19]. Subsequently, this form of the blockchain network is called partially decentralized. In any case, a consortium blockchain is relatively easy to tamper with [10] because of reduced decentralization.

3 Major Blockchain Technologies

In this section, we first present a recently rising blockchain network innovation, that is, the SC, that performs random measurements rather than moving digital money. At the end of the section, we explain the consensus mechanism's primary mechanism to utilize a trustless blockchain network.

3.1 Smart Contract

An SC is a determination to set out the terms and conditions for an agreement's digital TXs. It presents contractual provisions in the structure. In the beginning, the idea of an SC was considered unviable. However, the blockchain included SC as one of its critical features after the realization of its strengths. As a part of the blockchain network, the SC has significant commitments and moved blockchain to its next generation, known as Blockchain 2.0. These automatically executed contracts promise to change the way current TXs work in a decentralized environment. Fig. 4 illustrates SC's workings in a standard blockchain network between a buyer and a seller. The SC code exists in the blockchain, and a specific ID (address) has been established. The users use an SC address to request their transactions. The blockchain's trust process governs the contract (see the next section for further details). The implementation of the SCs in a blockchain provides advantages, including openness, lowered costs, smoother transaction delivery, consistency, and experience. It supports the association of numerous imaginative advancements over an assortment of research areas of this study. Bitcoin utilizes a primary scripting language; thus, it is not essential to embrace the SC framework. It prompts the usage of next generation blockchain networks where SC innovation is being applied, for example, Ethereum. The users view Ethereum as one of the most dependable SC blockchain networks. It contains an advanced

Turing-machine programming language that determines SCs and the delivered resources. The SCs access information about various states and activities utilizing the oracles. These artifacts are essential to the significant consolidation of the SCs. However, they bear additional complexity due to the certainty provisioning in the oracles [26]. The SCs are yet helpless against many network attacks, such as [27] explains the fascinating new difficulties and issues faced by the SCs. Another problem with the SC is the resultant concern when vulnerabilities are found in the agreement code since it is irreparable and unchangeable. The real-world agreements typically incorporate terms and conditions that are not recent. Subsequently, an SC requires a great deal of exertion in checking the agreements' details, intending to perceive and measure execution by a network framework [28].

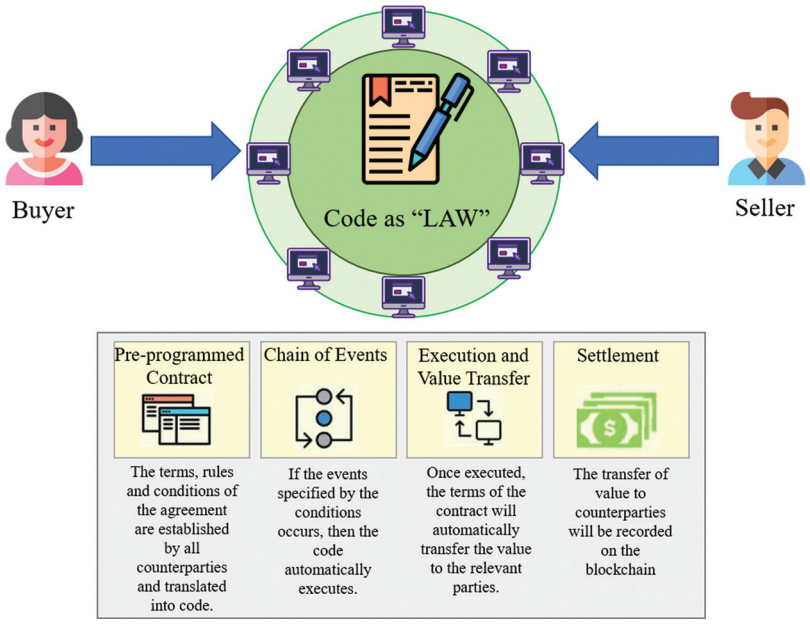

Figure 4: The working of the smart contracts in a blockchain network

3.2 Consensus Mechanism

The consensus mechanism is one of the fundamental parts of the blockchain network and is liable for blockchain information [29]. The consensus mechanism's essential motivation is to apply the SC rules in a decentralized, trustless network. Various blockchain networks utilize a few authentication strategies, including proof of work (PoW), proof of service (PoS), leased proof of stake (LPoS), proof of burn (PoB), and Practical Byzantine fault tolerance (PBFT). In the following subsections, we outline some noticeable consensus mechanisms, also summarized in Fig. 5.

3.2.1 Proof of Work (PoW)

Initially, PoW was the essential consensus mechanism for Bitcoin, which expects miners to comprehend a computationally expensive challenge that is simple to verify before adding a new block. The arrangement of these undertakings is written in a PoW consensus protocol before comparing blockchain with any node. Later, the nodes confirm and associate this recently added block with the blockchain over the network [30]. The technique for including new blocks happens

simultaneously in numerous parts of the network, resulting in a hierarchical structure in the chain. Accordingly, the blockchain network frequently incorporates a few separate divisions simultaneously. Before embedding another node in the network, each peer in the network checks this branch as the longest part of the blockchain, which should be legitimate. The main issue with such a consensus mechanism is that it requires thorough computation. The standard form of attack on Bitcoin, as previously mentioned, is the 51% attack. Inducements from the PoW expressly support centralism as the distribution of mining pool endorsement. Several drawbacks, such as higher latency, lower TX rate, and higher power consumption, make the PoW unacceptable for various applications, particularly energy-constrained applications. Several researchers have proposed numerous endeavors to change the PoW.

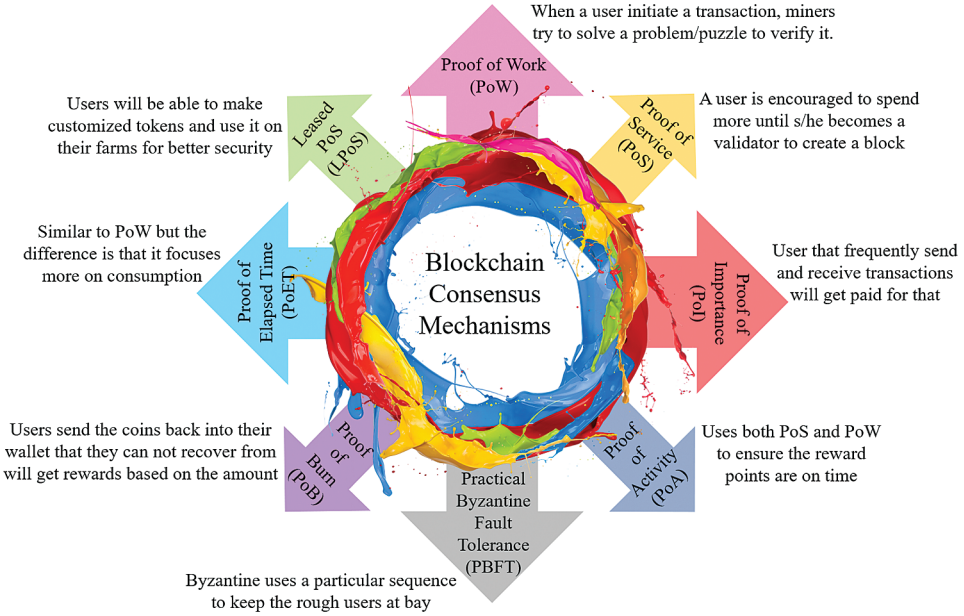

Figure 5: Some of the prominent consensus mechanisms used in the blockchain networks

3.2.2 Proof of Service (PoS)

The PoS algorithm is a notable alternate strategy to the PoW consensus mechanism in a blockchain network. The PoS framework executes the algorithm since the node with more compensation is concerned with the chain's presence and the blockchain network's specific activity, thereby establishing an additional fitting solution for network security. The fundamental motivation behind utilizing a PoS technique is to move forthcoming external costs into the network's inwardness. One of the PoS consensus technique issues is the absence of chances for miners to establish themselves. It empowers the redesign of the current consensus initiatives. Examples of the blockchains utilizing this sort of consensus are PeerCoin [31] and Ethereum. One of the blockchain network, Bitshare [32] uses the PoS variant known as DPoS delegates. In the DPoS, different observers access TX marks and timestamps in the blockchain network. The client is compensated each time a block is effectively added to the blockchain. Affirmation of the TXs is made more accessible by permitting users to set the blocks' latency and size.

3.2.3 Leased Proof of Stake (LPoS)

In the LPoS [33], a client can rent assets to different clients to be trusted and selected to make new establishments. This technique expands the number of selectable individuals in the organization, diminishing the risk of a specific group of users limiting the blockchain network. In such a consensus mechanism, all the participating users divide their incentives relatively. The Waves-blockchain [33] is one example of LPoS consensus protocols.

3.2.4 Proof of Burn (PoB)

Another type of blockchain consensus is PoB [34], which proposes consuming coins to construct a new block in the chain. The PoB is similar to a PoW consensus mechanism, that is, hard to evaluate and simple to check. However, it has higher energy consumption [34]. It also incorporates strategic suggestions that can add to a better environment. In this consensus mechanism, clients consume their coins so they can mine blocks onto the blockchain. A PoB moves the cost of the consumer onto the miner. As clients are focused on consuming their coins in the blockchain network to gain more advantages from mining, PoB supports a task's long-term consumer interest. A high percentage of long-term users of a blockchain network will ultimately influence such coins' price stability. One of the problems facing the PoB is that there is a lot of resource wastage and that much of the mining capacity belongs to those miners who consume more coins. Slimcoin [35] makes use of PoB as the consensus network protocol.

3.2.5 Proof of Importance (PoI)

The PoI [36] links a significant rate for building a stable interface for each user's blockchain network. The likelihood that the consumer will be chosen to create a block depends on this significance limit. The estimation of this critical rate often considers the sum of the coins used and the number of positive TXs. This consensus system determines all the eligible users to add a block to a blockchain network through harvesting. The user that inserts a block into the blockchain network earns the block-relevant transaction fees. The higher the significant factor is, the higher the probability that a customer will be picked to collect the blocks. The PoI protocol is a user-based support network where users can deposit their coins and transfer them across the network. It is a non-PoS algorithm that is known to help collectors. This consensus protocol was applied to the blockchain networks by NEM [36].

3.2.6 Proof of Activity (PoA)

A new version of the PoW and the PoS protocol for cryptocurrencies called proof of activity (PoA) has been introduced in [37]. A PoA consensus mechanism indicates reasonable protection against potential realistic attacks on a blockchain network, which has somewhat limited storage connectivity repercussions. In a PoA, the conventional PoW algorithm uses block mining continues, with miners competing to be the first to crack a puzzle and seeking their rewards [37]. The only distinction is that the successfully mined blocks do not enclose TXs. Instead, they are merely templates that include header and reward address information. After practical mining of this virtually blank block, the PoA nodes use the PoS protocol. The header information is used to select a random group of validators to sign the blockchain block. If some or more of the chosen validators remain unsigned after a given amount of time, the nodes discard a block as incomplete. The PoA consensus protocol was criticized, yet a single block of mining always requires a lot of expense. A double signing of the block by a single miner is still a challenge for a PoA algorithm [37]. The Espers cryptocurrency [38] uses the PoA form of consensus.

3.2.7 Proof of Elapsed Time (PoET)

An Intel-developed blockchain network known as the PoET consensus system was implemented by Intel SawtoothLake (also known as IntelLedger) [30]. The PoET was designed to run in a time execution environment (TEE), such as the Device Protection Extension SGX for Intel [39]. The PoET uses a random leader election model (also known as a lottery-based electoral model), where the protocol chooses the next member randomly to finalize the sequence. Later, it deals with the untrusted and open-ended users of the consensus algorithm. In this consensus method, both miners can run the TEE using Intel SGX to request a wait time from the TEE code. The leader is the miner with the shortest remaining time. A certified miner claiming to be the block formation leader can also produce verifiable proof created by all other users using the TEE. This compromise method has the downside of being based on expensive high-performance computing hardware.

3.2.8 Practical Byzantine Fault Tolerance (PBFT)

Hyperledger-Fabric [23] is a famous blockchain that offers a scalable framework with a consensus plug-in mechanism. Hyperledger-Fabric supports PBFT, which executes non-deterministic blockchain codes. The PBFT was introduced in [40,41] as the first practical solution for Byzantine weaknesses. A PBFT uses the concept of a replicated state computer and replica voting for block validation. It has several optimization functions, such as validating and encrypting TXs between replicas and users. The scale and number of TXs the system would face in practical terms with Byzantine faults. A representation of $3f+1$ is needed to tolerate f nodes that fail, according to the PBFT consensus mechanism. In this phase, the overhead on the output of the repeated resource is reduced. However, the overhead TXs substantially rise as the number of replicas increases [42]. A comprehensive study on creating consensus structures for different blockchain networks was carried out. Nevertheless, there is a shortfall of work seeking to use these two tools to protect IoT privacy, especially for HIoT applications.

4 Related Research Overview

Researchers from universities and industries have recently published several research works on blockchain-based IoT innovation [5–10,43]. This theoretical framework either focuses on the blockchain network's general uses in the IoT or only examines specialized viewpoints on computerized digital currency forms. Their studies lack insight into the blockchain network's problems with IoT privacy protection. Frankenfield [34] provide issues from the cryptocurrency's viewpoint, such as a distributed denial-of-service (DDoS) attack, 51% attack, data elasticity, verification, and ease of use. In [44], the authors performed an in-depth study of blockchain technology and its impacts on the developments. This work further highlights Bitcoin's issues and call for a focus on the future applications of decentralized networks. However, this study addresses the IoT as a short subcategory in the long list of blockchain technologies' potential use cases. In [45], the authors address numerous blockchain versions, such as Ethereum [46], Ripple [47], and Gridcoin [48], and detail some of the core blockchain-based solutions. However, they do not consider the issues around blockchain networks and IoT amalgamation in their study. The authors of [49] propose a lightweight blockchain protocol for IoT implementations in smart home applications. Their theoretical work includes preventing intensive computing, TX validation delay, and the Bitcoin network's blockchain scalability. Conoscenti et al. [50] suggest one use case for blockchain and IoT convergence, which uses SC blockchains to customize and control IoT devices. Their proposed architecture is designed to resolve security and synchronization concerns within an IoT client-server network. All the connected IoT devices in their proposed solution are vulnerable to security attacks if the server is malicious. In [48], the authors proposed Ethereum SCs as a

secure open framework for IoT applications to take advantage of the blockchain networks. Pham et al. [51] performed a comprehensive literature review of the blockchain implementations outside cryptocurrencies and discussed their integration with IoT-based performance. Several systems have proposed different ways of integrating the blockchain networks on privacy sites to accommodate IoT applications. However, most architectures need many computing rounds to protect privacy and end up with massive energy usage and high device costs. Our proposed architectures increase the system's efficiency to suit an essential IoT function such as the HIoT.

Table 3: Summary of related research works

Reference	Framework	Summary
Yli-Huumo et al. [43]	Bitcoin	DDoS attacks, 51% attack, data pliability, authentication
Buterin [45]	Smart contracts	Next-generation smart contracts and decentralized framework
Dorri et al. [48]	Blockchain	Challenges and solutions for blockchain-based IoT applications
Huh et al. [49]	Blockchain	Managing IoT devices using blockchain framework
Conoscenti et al. [50]	Systematic framework	Review of blockchain-based frameworks for IoT applications
Pham et al. [51]	Smart contracts	A smart contract-based secure system for the HIoT
Chakraborty et al. [52]	Centralized framework	A centralized e-healthcare system involving healthcare providers, healthcare facilities (hospitals and clinics), doctors, and patients
Talukder et al. [53]	Consensus: proof of disease	A consensus mechanism for medical decisions
Abdullah et al. [54]	eHealth framework	Ethereum to address requirements for critical healthcare services: participatory, customized, accurate, predictive, proactive, and preventive
Kuo et al. [55]	Distributed Ledger framework	Saddled conditions of patient health through the integration of blockchain and the IoT into a healthcare system
Badr et al. [56]	IoT-HER framework	A general blockchain framework for use in future biomedical and eHealth services
Yu et al. [57]	IoTChain framework	Proposal of the multilayered pseudonym-based encryption (PBE) definition, allowing a user to access, verify, and update health-related information on a multilayered IoT
Rahman et al. [58]	Spatial blockchain-based framework	Proposed an IoT-based blockchain-assisted mobile platform for dyslexia healthcare
Salahuddin et al. [59]	Softwarization framework	A softwarized blockchain-IoT platform for e-healthcare services with improved adaptability, cost viability, and stability

Chakraborty et al. [52] suggested a centralized e-healthcare system that involves healthcare providers, healthcare facilities (hospitals and clinics), doctors, and patients. In their proposed solution, numerous sensors collect health-related information from patients in real-time and use the Ethereum SC model to store information in the blockchain, known as TESTRPC. However, health-related information requires absolute protection and privacy; thus, the authors of [53] propose moderating this problem. Recently, Ethereum has been used to address high-profile online healthcare services; participatory, customized, accurate, predictive, proactive, and preventive [54] features. Kuo et al. [55] explored patient health's loaded conditions by integrating a blockchain network and the IoT into a healthcare system. A general blockchain framework was used to provide future biomedical and eHealth services. Badr et al. [56] propose the multilayered pseudonym-based encryption (PBE), allowing a user to access, verify, and update health-related information on a multilayered IoT. Yu et al. [57] propose a framework called IoTChain to provide healthcare and information to patients with blockchain and IoT technology's assistance. In [58], authors propose an IoT-based blockchain-assisted mobile platform for dyslexia healthcare in which dyslexic patients and their caregivers use, store, and access dyslexic design in a multimodal data allocation method. Salahuddin et al. [59], on the other hand, propose a softwarized blockchain-IoT platform for e-healthcare services with improved adaptability, cost viability, and stability. For this purpose, the authors of [60] developed an IoT-based patient-centric agent to encourage end-to-end services using a blockchain for consistent patient observations.

The related research work explored a few significant research issues and challenges in the HIoT integration of the existing IoT-blockchain, which should be understood and used effectively to harness the BaaU for the HIoT. Tab. 3 summarizes the key contributions of the authors from the related research works. We note a shortage of research studies that address the importance of using a blockchain network for the next-generation HIoT. In such a scenario, there is no discussion of the blockchain consensus mechanisms. Methodological use cases for the IoT-enabled blockchain for the HIoT have also not been discussed. In this article, we propose two solutions for the next-generation HIoT that uses BaaU.

5 Blockchain-as-a-Utility (BaaU) Model for Privacy Preservation in the HIoT

In this paper, we outline a BaaU model for the protection of privacy within the HIoT systems. We suggest two circumstances in which the blockchain networks can be used to ensure HIoT trustworthiness (as shown in Fig. 6). The first recommendation indicates that a healthcare provider in the HIoT integrates IoT sensors, such as body sensors, to receive and transmit information and interfaces it to a blockchain network on these devices. The blockchain network now gives the linked HIoT devices the capacity to exchange data, process orders, and complete TXs. Thus, the blockchain network's privacy protection capability mitigates the security assaults, as the attacker uses trustless indirect access to target the network [52]. The sensor devices directly send their information to the central gateway, which provides adequate energy and memory resources. The blockchain network is updated at the edge device in this scenario, which keeps records of all the sensor devices that join the network and are approved for sending and receiving information. Thus, the blockchain networks may detect a malicious attack to mimic a system that has been approved. All sensor devices also track the information they send and update the data accordingly. Since the gateway keeps track of the amount of data sent and received from the devices, it can easily distinguish data anomalies and restrict the problem's source. Additionally, the cloud maintains a more extensive blockchain network, which executes similar standards to improve the

framework's flexibility. Therefore, the collected information is optimized using big data analysis. The Blockchain traffic flow analysis at the gateway helps to identify security threats in real-time.

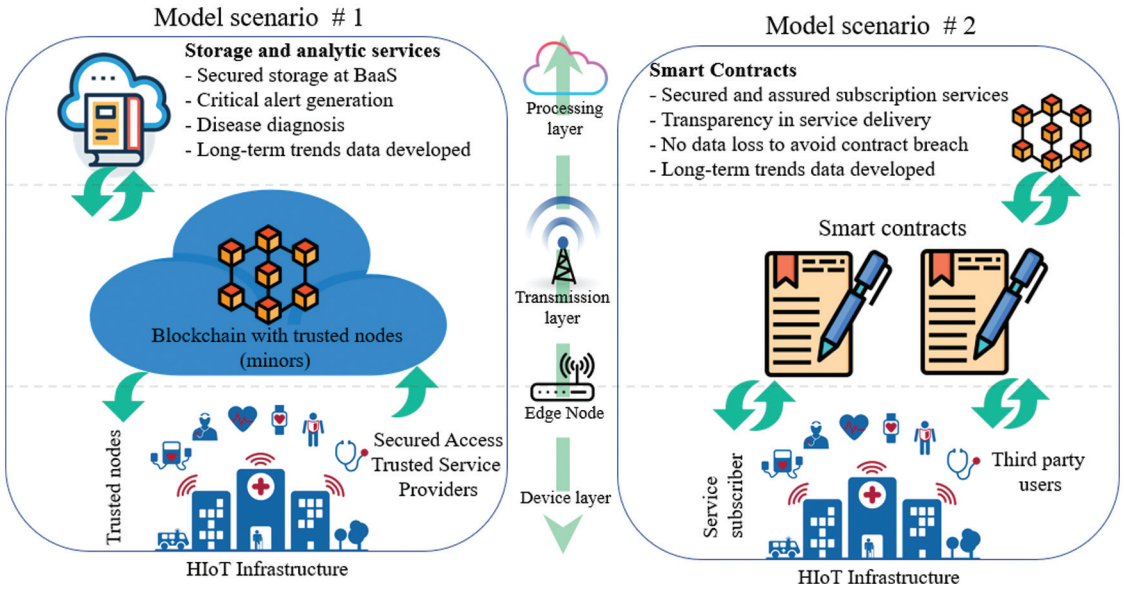

Figure 6: Proposed blockchain-as-a-utility (BaaU) model scenarios for privacy preservation in the healthcare IoT (HIoT) infrastructures

This paper's second proposed scenario suggests implementing SCs (such as Ethereum) to automate and control the HIoT services subscribed by the trusted devices/nodes. The Ethereum, as discussed earlier, is a worldwide, open-source blockchain SC for decentralized IoT systems that gives the ability to compose code that controls digital data, runs exactly as it is customized, and can be accessed over the Internet. The rationale for the proposed solution is that using an Ethereum for security preservation issues in the HIoT frameworks will provide a consistent and stable exchange of the TXs between associated devices, similar to how it works blockchain-based digital cryptocurrencies [9]. The facilities provided by the customer are governed by the terms and conditions of the SC. If there are any violations of the terms and conditions, counteractive measures can be automatically carried out. Our proposed BaaU framework uses a private blockchain. It is possible to base the consensus process on the PoS for such applications with extended facilities like proof of healthcare stack (PoHS) or proof of medical stack (PoMS) [61]. In this consensus mechanism, device stakeholders who define their initial tokens, depending on the quantity of healthcare data they contribute, are the SCs. The tokens can then be dynamically updated based on their behavior (willingness to verify transactions) [62]. By implementing high sanctions, malicious actions will be tackled. Suppose a breach of the HIoT safety and dignity can specifically affect patients' health or have legal and legislative implications. In that case, the authorization for misuse of voting power can be effect-related, for example, depending on the tokens retained and the potential effects of the violation in the worst case. It is important to note that authorizations can be represented in multiple ways; economic or reputational. The reputational might mean that the device's voting power (impact) is halved (and equally compensated for good conduct over time) for each breach.

6 Conclusion

The HIoT consists of a multi-sensor system that periodically tracks the physio-synthetic information provided by the body's physiological reactions. A massive amount of health-related information is transmitted to the cloud continues to analyze further and treat patients. The information shared is susceptible and vital, requiring immunity to unauthorized alterations. The blockchain networks have recently emerged as a critical technology that transforms the way we exchange information. This technology has exhibited promising application scenarios, such as protected digital currencies. As a technical development, the blockchain network has the drastic potential to transform many industries, and a HIoT could be one of the next generations of such applications. There have been various studies on the convergence of the blockchain networks and the IoT; however, these lack a formal structure for using blockchain-as-a-utility (BaaU) for HIoT privacy and security systems. In this paper, we overview the blockchain networks in the HIoT applications for privacy preservation. Besides, we suggest using blockchain's decentralized and robust capabilities as a utility (BaaU) in a system to mitigate these protection and privacy issues for the HIoT applications. Our proposed architecture proposes two BaaU scenarios to execute the blockchain in the HIoT for security and privacy conservation. The first recommendation suggests that a healthcare service provider integrates IoT sensors such as body sensors to transmit information to a blockchain network on the IoT devices. The second proposed scenario recommends implementing smart contracts, such as Ethereum, to automate and control the HIoT services.

Acknowledgement: The authors gratefully acknowledge DSR technical and financial support for RG-2-611-41.

Funding Statement: This work was supported by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under Grant No. RG-2-611-41 (A.OA. received the grant).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. Lund, C. MacGillivray, V. Turner and M. Morales, "Worldwide and regional internet of things (IoT) 2014-2020 forecast: A virtuous circle of proven value and demand," *International Data Corporation*, Technical Report, 2014. [Online]. Available: http://branden.biz/wp-content/uploads/2017/06/IoT-worldwide_regional_2014-2020-forecast.pdf.

[2] Y. B. Zikria, S. W. Kim, O. Hahm, M. K. Afzal and M. Y. Aalsalem, "Internet of things (IoT) operating systems management: Opportunities, challenges, and solution," *Sensors*, vol. 2019, no. 19, pp. 1793, 2019.

[3] J. Wurm, K. Hoang, O. Arias, A. Sadeghi and Y. Jin, "Security analysis on consumer and industrial IoT devices," in *21st Asia and South Pacific Design Automation Conf.*, Macau, pp. 519–524, 2016.

[4] R. Ali, Y. A. Qadri, Y. B. Zikria, F. Al-Turjman, B. S. Kim *et al.,* "A blockchain model for trustworthiness in the internet of things (IoT)-based smart-cities," in *Trends in Cloud-based IoT, EAI/Springer Innovations in Communication and Computing*. Switzerland, AG, Cham: Springer International Publishing, pp. 1–9, 2020.

[5] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things*, vol. 1, no. 2, pp. 1–13, 2018.

[6] A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, no. 3, pp. 173–190, 2018.

[7] I. Makhdoom, M. Abolhasan, H. Abbas and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *Journal of Network and Computer Applications*, vol. 125, no. 9, pp. 251–279, 2019.
[8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[9] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli *et al.,* "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.
[10] Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
[11] P. K. Sharma, S. Y. Moon and J. H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city," *Journal of Information Processing Systems*, vol. 13, no. 1, pp. 184–195, 2017.
[12] B. Leiding, P. Memarmoshrefi and D. Hogrefe, *Self-Managed and Blockchain-based Vehicular Ad-hoc Networks*. Heidelberg, Germany: UbiComp Adjunct, pp. 137–140, 2016.
[13] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *3rd Symp. Operating Syst. Des. Implementation*, New Orleans, USA, pp. 173–118, 1999.
[14] M. C. K. Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoinlike digital cash systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2543–2585, 2018.
[15] X. Zha, K. Zheng and D. Zhang, "Anti-pollution source location privacy preserving scheme in wireless sensor networks," in *13th Annual IEEE Int. Conf. on Sensing, Communication, and Networking*, London, UK, pp. 1–8, 2016.
[16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Online Unpublished paper, pp. 1–9, 2018. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
[17] A. M. Antonopoulos, "Mastering bitcoin: Unlocking digital cryptocurrencies," in *Gravenstein Highway North*. Sebastopol CA: O Reilly Media, Inc, 2014.
[18] Q. Feng, D. He, S. Zeadally, M. K. Khan and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, no. 1, pp. 45–58, 2019.
[19] J. Garzik, "Public vs. private blockchains Part 1. Permissioned blockchains," *Semantic Scholar*, 2015. [Online]. Available: https://www.semanticscholar.org/paper/Public-versus-Private-Blockchains-Part-1-n%3A/f5c596ada0674449879965c5cc4c347c2b2b3180.
[20] K. Lukas, "In-depth on differences between public, private and permissioned blockchains," Online Unpublished, 2015. [Online]. Available: https://medium.com/@lkolisko/in-depth-on-differences-between-public-private-and-permissioned-blockchains.
[21] Litecoin, "The cryptocurrency for payments," *Litecoin homepage*, 2011. [Online]. Available: https://litecoin.org/.
[22] Lisk, "Lisk documentation," *Lisk homepage*, 2018. [Online]. Available at: https://lisk.io/documentation.
[23] Hyperledger-fabric, "Hyperledger-fabric documentation, Hyperledger-fabric homepage," 2019. [Online]. Available: https://media.readthedocs.org/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf.
[24] G. Gideon, "Multichain private blockchain," *Whitepaper*, pp. 1–17, 2015. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf.
[25] Quorum, "Quorum whitepaper," *Whitepaper*, pp. 1–8, 2016. [Online]. Available: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorumn%20Whitepapern%20v0.1.pdf.
[26] F. Zhang, E. Cecchetti, K. Croman, A. Juels and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *The 2016 ACM SIGSAC Conf. on Computer and Communications Security*, Vienna, Austria, pp. 270–282, 2016.
[27] K. Delmolino, M. Arnett, A. Kosba, A. Miller and E. Shi, *Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab*. Berlin Heidelberg: Springer, 2016.
[28] C. K. Frantz and M. Nowostawski, "From institutions to code: Towards automated generation of smart contracts," in *IEEE Int. Workshops on Foundations and Applications of Self Systems*, Augsburg, Germany, pp. 1–6, 2016.

[29] C. Cachin and M. Vukoli, "Blockchains consensus protocols in the wild," arXiv preprint, pp. 1–24, 2017. [Online]. Available: https://arxiv.org/pdf/1707.01873.pdf.
[30] A. Baliga, "Understanding blockchain consensus models," *Persistent Systems: Whitepaper*, pp. 1–14, 2017. [Online]. Available: https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Block-chain-Consensus-Models.pdf.
[31] S. King and S. Nadal, "Peercoin-secure & sustainable cryptocoin," *Whitepaper*, pp. 1–15, 2015. [Online]. Available: https://peercoin.net/whitepaper.
[32] F. Schuh and D. Larimer, "Bitshares 2.0: General overview," *Cryptonomex: Whitepaper*, pp. 1–10, 2017. [Online]. Available: https://cryptorating.eu/whitepapers/BitShares/bitshares-general.pdf.
[33] Cryptographic, "Leased proof-of-stake (LPoS) homepage," *Cryptographic*, 2017. [Online]. Available: https://cryptographics.info/cryptographics/blockchain/consensus-mechanisms/leased-proof-stake/.
[34] J. Frankenfield, "Proof of burn (cryptocurrency) homepage," *Investopedia*, 2018. [Online]. Available: https://www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp.
[35] P4Titan, "Slimcoin: A peer-to-peer crypto-currency with proof-of-burn mining without powerful hardware," *Whitepaper*, pp. 1–6, 2014. [Online]. Available: http://www.doc.ic.ac.uk/ids/cryptopapersetcworth-reading/proofofburn/slimcoinwhitepaper.pdf.
[36] A. Nember, "NEM technical reference," *Whitepaper*, pp. 1–58, 2018. [Online]. Available: https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf.
[37] I. Bentov, C. Lee, A. Mizrahi and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," *SIGMETRICS Performance Evaluation Review*, vol. 42, no. 1, pp. 34–37, 2014.
[38] Batysta, "Espers: Cryptocurrency with hybrid PoW/PoS and unique algorithm homepage," *Espers*, 2017. [Online]. Available: https://blog.espers.io/espers-cryptocurrency-with-hybrid-pow-pos-and-unique-algorithm-63da942e307d.
[39] Intel Corporation, "Intel's software guard extensions (SGX): The control of protecting your data," *Intel Corporation*, 2019. [Online]. Available: https://www.intel.com/content/www/us/en/architecture-and-technology/.
[40] V. Gramoli, "From blockchain consensus back to byzantine consensus," *Future Generation Computer Systems*, vol. 1, no. 1, pp. 1–10, 2017.
[41] F. Knirsch, A. Unterweger, G. Eibl and D. Engel, "Privacy-preserving smart grid tariff decisions with blockchain-based smart contracts," in *Sustainable Cloud and Energy Services: Principles and Practices*. Cham: Springer, pp. 85–116, 2017.
[42] J. Zhu, P. Liu and L. He, "Mining information on bitcoin network data," in *IEEE Int. Conf. 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)*, Exeter, pp. 999–1003, 2017.
[43] J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, pp. 163477, 2016.
[44] M. Pilkington, "Blockchain technology: Principles and applications," in F. Xavier Olleros, M. Z. Edward Elgar (Eds.), *Research Handbook on Digital Transformations*, pp. 1–39, 2016.
[45] V. Buterin, "A next-generation smart contract and decentralized application platform," *Whitepaper*, 2014. [Online]. Available: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.
[46] Ripple, "XRP: The digital asset for payments homepage," *Ripple*, 2013. [Online]. Available: https://ripple.com/xrp/.
[47] Gridcoin, "The computational power of a blockchain driving science & data analysis," *Whitepaper*, 2018. [Online]. Available: https://gridcoin.us/assets/img/whitepaper.pdf.
[48] A. Dorri, S. S. Kanhere and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," *CoRR*, 2016. [Online]. Available: http://arxiv.org/abs/1608.05187.
[49] S. Huh, S. Cho and S. Kim, "Managing IoT devices using blockchain platform," in *IEEE 19th Int. Conf. on Advanced Communication Technology*, Bongpyeong, Republic of Korea, pp. 464–467, 2017.

[50] M. Conoscenti, A. Vetro and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in *2016 IEEE/ACS 13th Int. Conf. of Computer Systems and Applications*, Agadir, pp. 1–6, 2016.

[51] H. L. Pham, T. H. Tran and Y. Nakashima, "A secure remote healthcare system for hospital using blockchain smart contract," in *2018 IEEE Globecom Workshops*, Abu Dhabi, United Arab Emirates, pp. 1–6, 2018.

[52] S. Chakraborty, S. Aich and H. Kim, "A secure healthcare system design framework using blockchain technology," in *2019 21st Int. Conf. on Advanced Communication Technology*, PyeongChang Kwangwoon-Do, Republic of Korea, pp. 260–264, 2019.

[53] A. K. Talukder, M. Chaitanya, D. Arnold and K. Sakurai, "Proof of disease: A blockchain consensus protocol for accurate medical decisions and reducing the disease burden," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*, Guangzhou, pp. 257–262, 2018.

[54] T. Abdullah and A. Jones, "eHealth: Challenges far integrating blockchain within healthcare," in *2019 IEEE 12th Int. Conf. on Global Security, Safety and Sustainability*, London, United Kingdom, pp. 1–9, 2019.

[55] T. T. Kuo, H. E. Kim and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.

[56] S. Badr, I. Gomaa and E. A. Elrahmanb, "Multi-tier blockchain framework for IoT-EHRs systems," *Procedia Computer Science*, vol. 141, pp. 159–166, 2018.

[57] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu *et al.,* "IoTChain: Establishing trust in the internet of things ecosystem using blockchain," *IEEE Cloud Computing*, vol. 5, no. 4, pp. 12–13, 2018.

[58] M. A. Rahman, E. Hassanain, M. M. Rashid, S. J. Barnes and M. S. Hossain, "Spatial blockchain-based secure mass screening framework for children with dyslexia," *IEEE Access*, vol. 6, pp. 61876–61885, 2018.

[59] 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. 74–79, 2017.

[60] I. Tomi and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, 2017.

[61] A. Kiayias, A. Russell, B. David and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," *Lecture Notes in Computer Science*, vol. 10401, pp. 357–388, 2017.

[62] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye *et al.,* "Incentivizng consensus propagation in proof-of-stake based consortium blockchain networks," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 157–160, 2019.