sustainability

MDPI

Article

MedShard: Electronic Health Record Sharing Using Blockchain Sharding

Faiza Hashim [1,*], Khaled Shuaib [1] and Farag Sallabi [2]

[1] Department of Information Systems and Security, College of Information Technology, United Arab Emirates University, Khalifa Bin Zayed Street, Asharej, Al Ain, United Arab Emirates; k.shuaib@uaeu.ac.ae
[2] Department of Computer and Network Engineering, College of Information Technology, United Arab Emirates University, Khalifa Bin Zayed Street, Asharej, Al Ain, United Arab Emirates; f.sallabi@uaeu.ac.ae
* Correspondence: 201890063@uaeu.ac.ae

Abstract: Electronic health records (EHRs) are important assets of the healthcare system and should be shared among medical practitioners to improve the accuracy and efficiency of diagnosis. Blockchain technology has been investigated and adopted in healthcare as a solution for EHR sharing while preserving privacy and security. Blockchain can revolutionize the healthcare system by providing a decentralized, distributed, immutable, and secure architecture. However, scalability has always been a bottleneck in blockchain networks due to the consensus mechanism and ledger replication to all network participants. Sharding helps address this issue by artificially partitioning the network into small groups termed shards and processing transactions parallelly while running consensus within each shard with a subset of blockchain nodes. Although this technique helps resolve issues related to scalability, cross-shard communication overhead can degrade network performance. This study proposes a transaction-based sharding technique wherein shards are formed on the basis of a patient's previously visited health entities. Simulation results show that the proposed technique outperforms standard-based healthcare blockchain techniques in terms of the number of appointments processed, consensus latency, and throughput. The proposed technique eliminates cross-shard communication by forming complete shards based on "the need to participate" nodes per patient.

Keywords: healthcare; blockchain; sharding; electronic health record (EHR); scalability

Citation: Hashim, F.; Shuaib, K.; Sallabi, F. MedShard: Electronic Health Record Sharing Using Blockchain Sharding. *Sustainability* **2021**, *13*, 5889. https://doi.org/10.3390/su13115889

Academic Editor: Fabrizio D'Ascenzo

Received: 18 March 2021
Accepted: 20 May 2021
Published: 24 May 2021

1. Introduction

Technology has revolutionized and improved healthcare systems in the last few years. Sharing electronic health records (EHRs) is a key aspect of the healthcare ecosystem, which drives the interoperability of patients' data across multiple entities in healthcare for better treatment and diagnosis. Patients may visit more than one healthcare provider such as general practitioners, specialists, clinics, and pharmacies within few days for various needs. Each entity that a patient visits stores the record in its private database. This record should be shared among entities to enable access to a patient's medical history for better diagnosis and treatment. When patients visit other healthcare providers, they are unable to provide a detailed record of their medical history as it is stored in a private database. Patients might be required to undertake the same laboratory tests because previous records are unavailable. Additionally, interoperability trials among different healthcare providers pose obstacles to data sharing [1]. EHRs sharing is an important research topic as it has a powerful impact on patients and healthcare providers. Several cloud-based solutions [2–4] have been proposed, but the credibility of a third-party cloud service poses a challenge [5]. Recently, blockchain technology was adopted in the healthcare domain to improve the quality of healthcare providers and make the healthcare systems smarter by eliminating the engagement of a third party.

Blockchain is considered a revolutionary technology for implementing distributed ledgers with high security and decentralization. It was introduced in 2008 by Satoshi Nakamoto as a decentralized peer-to-peer payment method in the digital currency Bitcoin [6], paving the way for other areas such as finance, supply chain, banking, education, and marketing to adopt the technology. Blockchain can distinctively transform the healthcare ecosystem in a smart and safe manner by allowing a secure, private, and decentralized network among peers to collaborate without a third party through consensus. It is founded on a shared, distributed, and immutable digital ledger of transactions, which appends blocks to the ledger in chronological order once the transactions within the block are verified by most network participants. The block's data are then hashed and linked to the previous block via the previous block's hash value, thus providing immutability in the ledger [7]. Although blockchain can transform the healthcare ecosystem in a smart and safe manner, its scalability has been a challenge in the healthcare domain when managing large-scale networks in terms of the number of nodes and transaction throughput. A node represents a component (participant) on a blockchain-based system and it is the foundation of the technology that represents each entity connected to the network [8]. Healthcare is a fast-growing and dynamic network of nodes because nodes may join at a high rate which can lead to network degradation and transaction delays due to the consensus mechanism used among them. Thus, healthcare blockchain networks should be scalable as the number of nodes increases in the network.

Sharding has been widely investigated and discussed to address the scalability issue in blockchain [9–12]. Sharding is a horizontal partitioning technique that artificially divides the network into shards (committees), with each shard processing transactions in parallel [13]. This technique improves the network throughput and latency by running a consensus within the shard with a subset of blockchain nodes. Sharding has not been investigated in the healthcare domain for improving the performance of a healthcare blockchain. Cross-shard communication has been a hurdle in network performance in sharded blockchain systems. In cross-shard communication, a node in one shard communicates with a node in another shard. The proposed transaction-based sharding for healthcare blockchain eliminates cross-shard communication by forming complete shards for each patient appointment or request for a service to be provided by a participating entity.

2. Motivation and Contribution

Recently, blockchain technology has been prominently adopted for sharing EHRs securely among healthcare participants. The shared ledger is replicated among all the participating nodes, which creates scalability issues as new nodes enter the network and get a complete state of the ledger. This delays the verification of transactions, which cannot be tolerated in a sensitive environment such as healthcare.

Patients with multiple caregivers need to share their medical history effectively for better service. Thus, it is important to share health records among various stakeholders of the healthcare ecosystem, including individuals (patients and their doctors) and individual and a stakeholder (patients to insurance companies/research centers). Sharing EHRs is an important step in expanding the interoperability of healthcare providers and making the healthcare system smart and efficient.

This study contributes to the literature by resolving the scalability issue in healthcare blockchain and providing an efficient solution to a secure sharing of EHRs among various entities. The following are the contributions of this study:

- Scaling out healthcare blockchain-based systems using sharding.
- Eliminating cross-shard communication overhead by forming complete shards for each appointment such that nodes in one shard do not need to communicate with nodes in other shards.
- Using Proof-of-Authority (PoA) for consensus within the shards, having only the previously visited caregivers as validating nodes to minimize the consensus latency of appointment processing in the healthcare network.

- Using "transaction-based shard formation" based on the patient's ID represented by a cryptographic public key where all previously visited caregivers participate in the shard. Hence, a patient does not need to keep a record of his/her visits to caregivers.

The rest of the paper is organized as follows. Section 3 investigates related work, Section 4 discusses the proposed sharding technique, Section 5 presents a theoretical analysis of the proposed technique, Section 6 provides performance evaluation, and Section 7 concludes the paper.

3. Related Work

Blockchain technology is projected to transform the healthcare ecosystem with its distinct characteristics, which include decentralization, security, immutability, persistency, anonymity, and auditability. Blockchain can reshape traditional EHR sharing across multiple healthcare entities to improve the quality of healthcare making it smarter and more efficient. Accordingly, some previous research contributions in EHR sharing are discussed in this section.

MedRec [14] was among the first to look into implementing blockchains in the healthcare system. It was developed by researchers at the Massachusetts Institute of Technology (MIT) in 2016 to improve handling and sharing of EHRs. MedRec addressed four major issues in healthcare in its first release: disjointed data, interoperability, patient centricity, and research data. The work addressed interoperability challenges among the healthcare and research communities. Proof-of-Work (PoW), a consensus scheme, was implemented to secure EHRs from tampering. However, the computational cost of PoW increases as the network participants grow in blockchain, resulting in low throughput in a high-transaction-volume network. In this regard, MedRec did not provide a solution for scaling out the technology.

In 2018, MedRec 1.0 [15] was issued as a usable system in healthcare and addressed the flaws of its first release, including pseudonymity for communication, security, scalability, and privacy issues. MedRec 1.0 attempted to resolve the scalability issue by bypassing the blockchain for patient notification and restricted blockchain storage for the creation and modification of identities and relationships. This method resolved the storage issue; however, the transaction throughput was still affected by high transaction volumes of new node identity creation and modification. Moreover, there was no mention of any mechanism for patients' notification, although it must be maintained in the blockchain for tracing previous records.

MedicalChain [16] is another blockchain implemented in healthcare, providing a transparent and patient-centered system for healthcare providers and patients to share EHRs in a secure and auditable environment. MedcalChain enables patients to control who accesses their health data. In this system, transactions can be viewed only by the participants associated with the transactions. In such a scenario, a patient and an associated practitioner with direct input are allowed to access the patient's records. However, for external access, an external practitioner should go through a series of steps to be added to the patient's authorized asset to access the record. In a healthcare environment, this procedure slows down transaction throughput and leads to critical issues caused by delay in case of an emergency.

A blockchain-based logging system was proposed in an earlier study [17] to facilitate the exchange of EHRs across countries in Europe in an OpenNCP. This work ensures security, traceability, liability, and an audit mechanism in sharing healthcare data across nations. However, to deal with the scalability of a large network, this system used a private blockchain to store audit logs and claimed to store any number of streams by each node. However, the scheme lacked important details about how a private blockchain is implemented for cross-border exchange of EHRs. To deal with the mining process for a private blockchain that suffers from a single-node monopolization issue, the authors implemented a diversity mechanism. In such a mechanism, a single miner can create a specified number of blocks only. The mechanism performed better than PoW, but

having a single miner may produce a source and a target for adversarial attacks, seriously threatening the healthcare environment.

The Healthcare Data Gateway (HGD) [18] application was proposed and developed to ensure the ownership of patient data based on the blockchain. This architecture allowed patients to possess, monitor, and communicate their data effortlessly and securely while preserving their privacy in the network. This application provided patients complete ownership of EHRs and data sharing relied on patients' willingness to share. This system used a database schema to store all types of data in tables. However, assembling a summarized EHR for one patient from various hospital databases in a single location is a challenge. This also raises the issue of a single point of failure of EHRs being stored in one location. As this system completely authorizes patients to store their medical records and preverves their rights to maintain secrecy and prevent recorded confidential information from being shared with any entity during a medical treatment for personal interests. A more efficient system will allow for the ownership and access of EHRs to be appropriately balanced with defined rights among the participating entities.

MedBlock [1] provides a solution to large-scale EHR management and sharing in healthcare systems using blockchains by enabling efficient data sharing and collaboration that facilitates hospitals to obtain patients' therapeutic history before a consultation. This scheme divides tasks among the nodes in the blockchain network such that a single node can take a solo task to achieve efficiency and scalability. However, these tasks are performed sequentially rather than parallelly. Hence, some nodes remain idle until the completion of a single task. The distributed ledger in this scheme contains the encrypted summary (diagnostic information), which is considered extra storage on the ledger in the presence of record pointers and hash values of EHR. This consumes storage on the ledger and slows down the throughput of a high volume of transactions.

In a study [19], researchers developed a medical image-sharing framework using blockchains for a cross-domain environment and proposed a distributed data store to generate a ledger of radiological studies and patient-defined authorization. This work addresses the interoperable healthcare ecosystem and the result can be generalized to further medical domains. However, the proposed framework had certain drawbacks, including complex privacy and security prototypes and an uncertain regulatory environment.

A study [20] presented a multilevel patient location-sharing scheme based on blockchains for telecare medical information systems. It defined the primary requirements of blockchain-based location sharing, including decentralization, unforgeability, confidentiality, multi-level privacy protection, retrievability, and verifiability. The system model was comprised of three entities: location data owner (LDO), location data requester (LDR), and miners. The mining process was based on a PoW mechanism, resulting in a high computational time and high energy consumption making it not a suitable fit for a healthcare network.

Medchain [5] researchers presented a healthcare blockchain-based data-sharing scheme by achieving high efficiency and security through dual network architecture, a session-based data-sharing scheme, and a digest chain structure. This scheme successfully addresses the efficiency issues of existing systems, such as those reported in earlier studies [1,14]. Two types of events are recorded on the blockchain in Medchain: data generation (write operation) and session creation (read operation). Each blockchain participant maintains a full state of the distributed ledger. However, the ledger only contains fingerprints to retrieve information from the directory nodes. This mechanism optimizes the storage overhead in the block but affects the network's throughput because an involved transaction of the consensus process runs by the blockchain nodes, followed by a routing process run by the directory nodes.

In the area of cloud computing-based healthcare systems, EHRs have been stored on the cloud. Cloud computing offers various advantages, including fast communication, advanced sharing, storage facility, low cost, simple access, and dynamic association [21]. However, cloud-based healthcare systems are vulnerable to privacy and security issues from safe and illicit users. Several studies have integrated blockchains with existing

cloud-based healthcare infrastructure to improve the privacy, security, scalability, and sharing systems [22–27]. However, most cloud-based medical record handling systems are vulnerable to the single point of failure issue and rely on the credibility of a third party, that is, a cloud service provider, which can pose a major challenge.

Scalability poses a major challenge and it should be addressed for efficient and speedy data sharing in healthcare. Scalability is defined as follows: as the number of transactions grows, the system becomes slower, more expensive, and less sustainable over the long term. Sharding helps address the issue of scalability. The following subsection focuses on several scalability solutions adopted in a healthcare blockchain environment using sharding mechanisms.

Sharding-Based Healthcare Blockchain

Sharding is a database technique successfully adopted in blockchain technology to resolve the scalability issue. This technique splits processing transactions overhead among various small groups of nodes (called committees or shards). These groups work in parallel to improve the network performance with significantly smaller communication, computation, and storage per node, thus permitting the network to scale to large-size networks [9]. Sharding is a practical solution adopted in several projects from various domains. Elastico [10] was among the first in the implementation of sharding techniques in blockchain, followed by Omniledger [11], Chainspace [12], Rapidchain [9], and Monoxide [28].

Healthcare has welcomed the blockchain technology for EHR management and secure sharing across the participating entities in its ecosystem, including patients, doctors, hospitals, laboratories, insurance companies, and pharmaceuticals, ensuring distribution of EHRs and providing patients' data ownership [29]. Scalability is a critical challenge in the healthcare blockchain domain as it affects the network throughput and latency. Considering that the healthcare system is sensitive to real-time delay, transactional delay causes a serious threat to human life, especially in case of emergencies. Sharding plays a vital role in addressing scalability challenges in healthcare by processing patients' appointments in parallel and by minimizing the consensus time as consensus is done within each shard. This has a significant impact on the latency and throughput of the healthcare blockchain network.

Researchers have been examining the use of sharding in blockchain-based healthcare systems. A multi-domain IoT blockchain that focuses on blockchain sharding in the healthcare IoT domain was proposed in a study [30]. Each shard included an entity such as a hospital and number of wearable smart devices for medical data collection and distribution among multiple shards (cross-shard communication). The key limitation of this system is the consensus mechanism that runs twice, first within the shard and then via the main shard, resulting in more energy consumption and transaction delay.

To address the scalability challenge in blockchain, a lightweight blockchain was proposed by a study [31], which divided the network participants into demographic clusters. Each cluster maintained a single copy of the ledger for the healthcare domain system. The transactions in each cluster were verified by a single miner (Head Blockchain Manager). Although a single miner saves time and energy consumption in the mining process, a single miner acting maliciously may lead to shard takeover attacks and cause loss of shard transaction data. Therefore, the mining process should include some trusted nodes to safeguard the shard.

Lightweight blockchain maximizes the throughput of transactions and reduces energy computation by parallel processing in healthcare blockchain, but it does not effectively address communication among clusters.

Although sharding has not been thoroughly investigated in the healthcare domain, various other domains using sharding to address scalability issues have shown promising results as well as various challenges. Currently, the main challenges of sharding relate to communication (cross-shard communication) and security. This study applies a sharding

technique in the healthcare blockchain domain to efficiently scale out healthcare blockchain-based systems and further enhance their security and scalability.

4. Proposed Scheme

This study proposes a transaction-based shard formation technique for an EHRs sharing system. The shards are formed for patients' appointment and are processed in parallel. The proposed scheme eliminates the issue of cross-shard communication in a sharded healthcare blockchain system. As mentioned in a study [32], 95% of the transactions in a sharded blockchain are based on cross-shard, which is responsible for transactional delays and degrading the system throughput. Figure 1 shows the proposed architecture for a sharded blockchain-based healthcare data-sharing system. It shows the different architectural entities along with their responsibilities and the flow of data among various modules in the network.

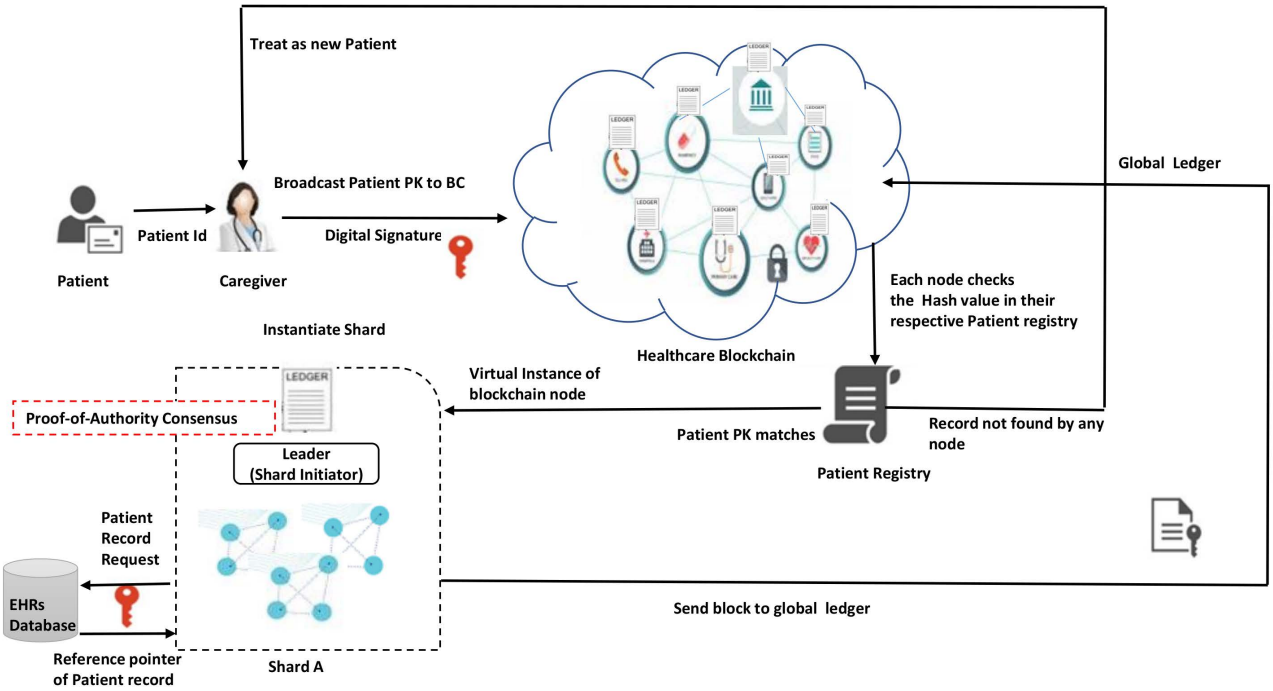

Figure 1. Proposed sharded blockchain-based EHR sharing system workflow.

The workflow of the proposed EHR sharing using sharding-based blockchain is as follows:

- A patient visits a caregiver, a node, participating in the blockchain network.
- The caregiver creates a digital signature (DS) that includes the patient's public key and broadcasts it to registered nodes in the blockchain network.
- Nodes that received the patient's digital signature verify it and use the patient's public key to search their local database for any previous records.
- Nodes, previously visited by the patient, respond by sharing previous records with the requesting caregiver through a secure communication channel off the chain. In doing so, nodes need to adhere to any signed consent by the patient.
- The caregiver instantiates a shard containing blockchain nodes from which responses were received. A participating node could assign a virtual instance of itself to the shard being formed while the shard initiator, current caregiver, assumes the leadership role for the shard.
- Transactions for the patient's appointment are performed among the shard nodes only, rather than all nodes in the blockchain.
- Transactions are added to a block by the shard leader.

- The PoA consensus algorithm is used to reach an agreement for the validity of the block within the shard.
- Once the block is validated, it is added to the global ledger.
- A shard is discarded once the appointment ends and all virtual instances of participating nodes are released.

Each step is discussed in detail in the following subsections using a layered model of the proposed shard-based healthcare blockchain network.

4.1. Healthcare Blockchain Layered Model

The proposed healthcare blockchain technique adopts a sharding mechanism. Figure 2 shows a sharded blockchain layered model to illustrate different components of the proposed solution. Each component is discussed in detail. Table 1 lists the abbreviations used in this study.

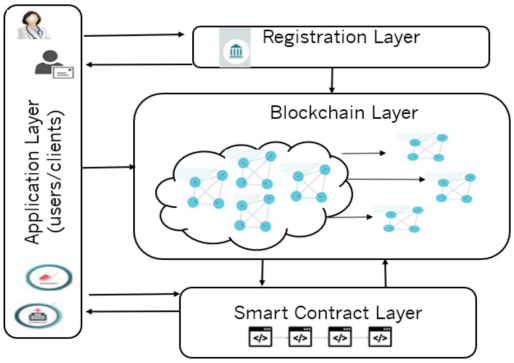

Figure 2. Sharded healthcare blockchain layered model.

Table 1. List of abbreviations.

Abbreviations	Meaning
EHR	Electronic Health Record
SM	System Manager
BN	Blockchain Nodes
PK	Public Key
DS	Digital Signature
P	Patient
C	Caregiver
S	Shard
SN	Shard Node
VN	Virtual Node
Trans	Transaction
NS(in)	Shard Initiator Node
Qtxn	Queue holding Transactions

4.1.1. Registration Layer

The registration layer authenticates the participants in the blockchain and generates a cryptographic public–private key pair using public-key cryptography such as the Rivest–Shamir–Adleman (RSA) algorithm [33] for the requested participant. Although RSA is being used in this work, other public-key cryptography can be used, such as elliptic curve cryptography (ECC). The algorithm uses two keys, public and private, forming a relevant pair [34,35]. Public keys are typically used as an address, account number, or id of an entity and can be shared with other users on the network [35,36], through a trusted third party. Our proposed technique uses the patient's public key as a patient ID on the blockchain. However, private keys are used for signing transactions to authenticate the signer and provide nonrepudiation. In the proposed solution, this is system manager (SM),

which could be a certification authority, as was proposed earlier [37]. The SM does not impose centralization when transactions are performed within the peer-to-peer network of participating nodes in the blockchain. All involved entities, such as hospitals, laboratories, pharmacies, and insurance companies, are registered through the SM off-chain. This process provides authentication and secure transfer of EHRs transactions among trusted entities in the blockchain. The registration information is then stored in a registry pool to be used to verify registered nodes for future transactions. Smart contracts are used to maintain health users' identifiability without exposing personal information to the blockchain. The use of public/private cryptographic key pairs replaces the need for a traditional username/password authentication scheme through smart contracts. If a new node plans to join the network, it registers through the following steps:

- Sends a request for registration by triggering the smart contract.
- Provides its participant ID, role (patient/doctor/hospital/laboratory), and affiliated organization.
- If the identity is legitimate, the SM computes the new node's encryption keys using an algorithm such RSA.
- The SM sends the keys to the node through a secure channel.
- The SM stores the registration information in the registry pool to be used for future authentication.

Figure 3 presents the sequence diagram of the registration layer.

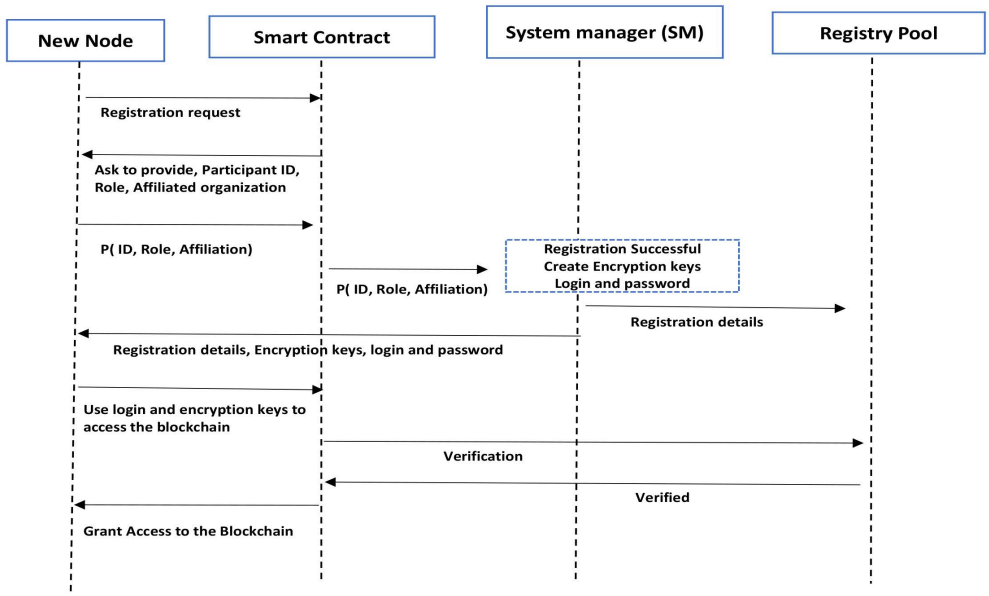

Figure 3. Sequence diagram for registration process in the proposed healthcare blockchain.

4.1.2. Application Layer

The application layer provides a user interface to the registered participating entities in the network. This layer comprises all nodes intending to access/share EHRs via the blockchain. Examples of such nodes include healthcare providers, hospitals, laboratories, insurance companies, patients, and government bodies. These nodes use their registration information to access the network and share records via encryption keys allocated in the registration layer.

4.1.3. Blockchain Layer

The objective of a blockchain network is to deliver peer-to-peer access without a central authority in a transparent and decentralized mode. In some cases, only a certain group of participants need to interact in the blockchain network, for example, logistics supply chains, healthcare, and financial institutions. Based on the requirements of any domain,

different types of blockchain frameworks can exist to meet the desired degree of control and restrictions among members. A public blockchain maintains user anonymity and publicly broadcasts transactions. Anyone can join the network and participate in the consensus process. Thus, a public blockchain is unsuitable for a healthcare domain [38]. Therefore, several studies on healthcare environment have adopted private [7,39] or consortium blockchain-based designs [30,38,40] wherein data privacy can be controlled. In our proposed solution, we use a consortium blockchain for healthcare data sharing among various registered entities depending on the permissions granted by an administering authority.

Among the various registered entities in the network, the blockchain layer is the actual EHR transactions sharing layer. All transactions occurring in the blockchain are stored in a distributed ledger, which is replicated to all other nodes in the network in a classical blockchain environment. This leads to the issue of scalability. In the proposed architecture, the blockchain uses the sharding technique to scale out the healthcare blockchain following a horizontal partitioning method.

Healthcare Blockchain Sharding

Scalability has been a challenge in the deployment of any fast-growing technology, as in the case of healthcare blockchain-based networks. In such networks, not all entities need to have a complete blockchain ledger. Therefore, our proposed techniques focus on interactions only among concerned parties in the network, i.e., on a need-to-know basis. The proposed solution uses the sharding technique to achieve this purpose and thus effectively resolves the scalability issue. As mentioned earlier, sharding is a technique that follows partitioning and parallel processing of transactions. Classical blockchain implementation can be grouped into multiple groups/committees called "shards." Each shard processes its own transactions and maintains a single view of the distributed ledger. Adding all shard transactions in parallel scales out the entire network.

Shard Formation

Shard formation is an important task in a sharded blockchain network. Various clustering algorithms are used for shard formation in the literature, including peer discovering algorithms, user assignment algorithms, smart contract-based shard formation, demographic clustering algorithms, and nearest neighbor algorithms. Initially, these algorithms exhibited good performance in shard formation but could not make the process efficient because of increased cross-shard communication overhead. According to a study [32], 95% of the communication in a sharded blockchain is performed as a cross shard, which degrades the network throughput. This study eradicates cross-shard transactions to increase network throughput. This is addressed using an efficient shard formation process such that all interacting nodes forming a shard do not need to communicate with the nodes in any other shard. In our proposed architecture, "transaction-based sharding" is used such that shards are formed based on patients' records present in the corresponding nodes. Shard formation starts with the transaction proposal to access a patient's history from the last visited entities among the healthcare blockchain participating entities. The query node, i.e., the node that the patient is currently visiting, prepares a transaction proposal using the patient's public key and a timestamp for the transaction. The transaction proposal is hashed using a secure hash algorithm such as SHA-256 that generates a unique 256-bit output for a given input [41,42]. The hashed value is encrypted using the query node private key to generate a digital signature. Digital signature (DS) is a mathematical technique that verifies the authenticity and ensures the integrity of the transaction [34,43]. A valid DS shows that the content is original as was sent and the sender is authentic [36]. The DS generated by the query node is broadcast to all nodes in the blockchain and a shard, say A, is instantiated by the current caregiver. Figure 4 shows the sequence diagram of the shard formation process.

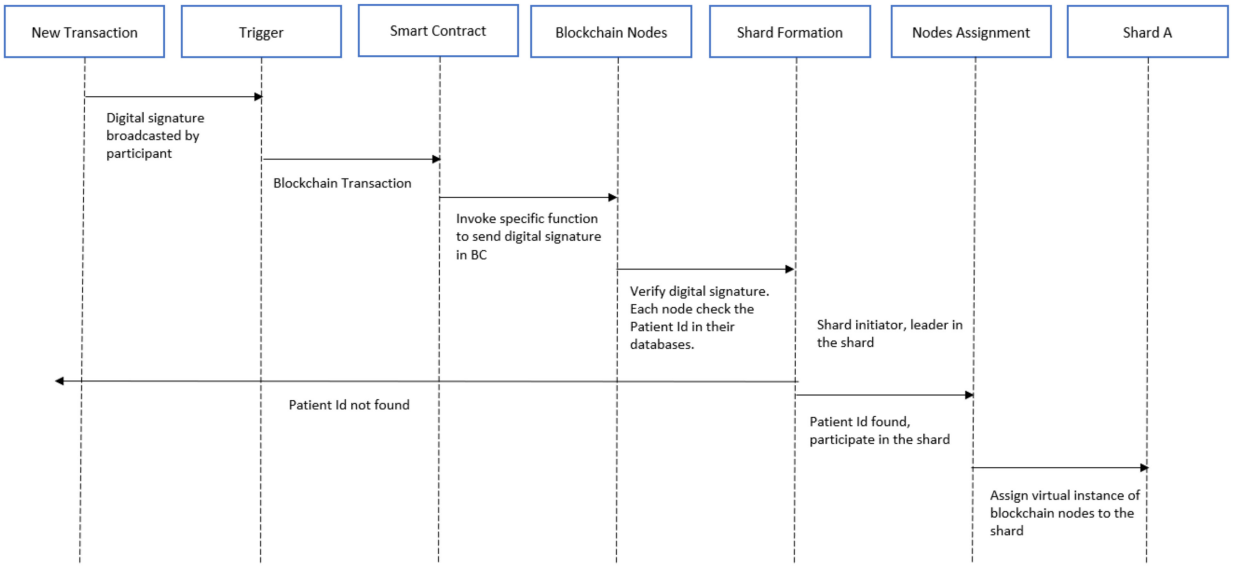

Figure 4. Sequence diagram for shard formation in proposed healthcare blockchain.

Shard Participants

In the above example, node assignment to a shard is based on the matching of the patient's public key, Ppk, by the nodes in the network, i.e., the B_N verifies the DS they received and checks their patient's registry for a match of the broadcasted Ppk. Nodes that do not find a record for Ppk discard the request. Nodes that find a match for Ppk in their registry assign a virtual instance of the node to the shard being formed. Thus, if a patient previously visited a hospital and needs to share the medical history with his/her current caregiver, a complete shard is formed based on the Ppk to include all previously visited entities by the patient. The size of each shard depends on the patient's history (the number of entities the patient visited previously). Algorithm 1 presents steps used for shard formation and nodes assignment in the proposed technique.

Algorithm 1. Shard Formation and Nodes Assignment to the Shard

1: A patient P_i visit a caregiver C_i
2: C_i(DS) $\rightarrow B_N$ # Ci broadcast DS of Ppk to Blockchain nodes
3: C_i instantiate a shard S_i
4: **if** (B_N finds Ppk) **then**
5: $S_i \rightarrow \mathrm{VN}_{Ppk}$ # Assign virtual instance of B_N to the shard
6: **else**
7: Discard transaction
8: **end if**
9: $Si = NS(in) U\{V\ NPpk\}$
10: $Leader \leftarrow N_{S(in)}$ # Shard initiator node is selected as Leader of the shard

Number of Shards

This section examines the number of shards that can be created in the proposed healthcare blockchain architecture. In the literature, there is no consensus on the optimal number of shards in a sharded blockchain network. In a public blockchain setup, shard formation is based on each epoch; therefore, it cannot be fixed to an optimal number as the models are public and it can grow or shrink depending on the number of nodes contributing to the network. In a permissioned blockchain setup, as in an earlier study [44], the authors used $N/(3f + 1)$ shards in their network, where N is the total number of nodes in the blockchain and f denotes the number of failed nodes. Two types of failure nodes are discussed in another study [45]: crash failure, wherein nodes may fail anytime

unintentionally and byzantine failures, wherein nodes may act maliciously to interrupt the network.

In the proposed technique for sharing EHRs, the number of shards formed in the healthcare blockchain network is directly proportional to the number of active patients' appointments in the network. Forming permanent shards may result in a large number of active appointments, which may lead to low throughput. Thus, in our proposed model, shards are discontinued at the end of a patient's appointment/service with his/her caregiver who initiated the creation of a shard. Thus, resources of other participating nodes are released and there is no throughput degradation within the network.

Query Processing within a Shard

A transaction-based sharding technique results in a complete shard comprising all concerned nodes where the patient's EHRs are stored. Hence, sharing these EHRs among the nodes within a shard is faster than sharing within the classical blockchain. The proposed solution does not oblige the healthcare provider to transfer the actual patient record to the new system. Instead, it only delivers a reference point to the data in the system for access. The node that broadcasts the DS is considered a "leader" within the formed shard. A shard maintains a single ledger shared by all participating nodes, and thus, optimizing the storage boosts the transaction throughput. The current caregiver (shard initiator) can now request a patient's medical history, prescription history, and test reports from the entities within the shard. The concern nodes provide access to patient's EHRs in their respective premises (off-chain data storage) through a reference pointer. The data are transmitted off-chain via a secure channel. This process of EHR sharing eliminates cross-shard transactions because all concerned nodes reside within the same shard. Algorithm 2 is used for query processing within a shard.

Algorithm 2. Query Processing within Shard

```
Smartcontract: DataRequest(Ppk)
DataRequest(Ppk)
if msg.sender = Authorized B_N then
    if Patientid == true then
        returen(recordRP)
    else
        AbbortSession
    end if
end if
PoA Consensus
End Appointment
Discard S_i
S_i ← Null
```

PoA Consensus

A consensus algorithm is a procedure responsible for ensuring a common agreement is reached among all network participants in a decentralized distributed system about the current state of the distributed ledger. Various consensus algorithms are used in the blockchain ecosystem, including Proof-of-Work (PoW), Proof-of-Stake (PoS), Byzantine Fault Tolerance (BFT), Practical Byzantine Fault Tolerance (PBFT), and Proof-of-Authority (PoA). PoA gained rapid acceptance in various blockchain applications ranging from software applications [46–50] to the healthcare domain [51–53]. Our proposed scheme uses a PoA consensus algorithm for its relatively simple and fast processing of transactions. PoA is a modified version of the BFT consensus algorithm [45], with a lighter message exchange mechanism between participating nodes (n). In PoA consensus, a set of honest nodes called "authorities" are responsible for reaching a consensus for the validity of transactions with a minimum of $(n/2 + 1)$ authorities' agreement; therefore, it can tolerate up to 50% of the byzantine failures. PoA works in rounds during which a leader is elected to propose a new

block to a set of authorities on which the consensus is achieved. In the proposed technique, the leader election process is simplified as the shard initiator is automatically appointed as the leader node in the shard. According to a study [45], the screening process from the administrator is arduous in general PoA consensus algorithms. However, in the proposed technique, the screening process for all nodes joining the blockchain network is completed in the registration layer, which minimizes the screening time.

The proposed sharded healthcare blockchain uses Aura, which is a PoA algorithm implemented in an earlier study [54]. It works in two rounds [45]. In the first round, the leader proposes the new block to the authority nodes within the shard. The second round is the block acceptance step wherein each authority node sends the block to its peers within the shard and receives a minimum $(n/2 + 1)$ acceptance and the block is validated and ready to append to the distributed ledger. Algorithm 3 presents the modified algorithm for the proposed technique.

Algorithm 3. PoA Consensus within Shard

1: *Leader* $\leftarrow N_{S(in)}$ # Shard initiator is selected as leader of the shard
2: $Q_{txn} \leftarrow$ *Null* #Transactions queue
3: *Trans(Qtxn)* $\rightarrow$ *block*
4: **for** step i **do**
5: *Leader(block)* $\rightarrow V_{N(i)}$
6: $V_{N(i)} \leftarrow$ *block* # Shard node receives block from leader
7: $V_{N(i)} \rightarrow S_N - 1$ # Each node sends block to its peer nodes
8: **end for**
9: **if** (all shard nodes receive the same block) **then**
10: *BlockAccept*
11: **else**
12: *Discardblock*
13: **end if**
14: block $\rightarrow$ *global ledger*

4.1.4. Smart Contract Layer

Smart contracts are executable codes that process the requests occurring in the blockchain network. Smart contracts trigger all processing in the blockchain network because the blockchain itself does not execute any code. In the proposed network, smart contracts trigger the various events that serve as a bridge among various layers in layered models, ranging from node registrations, shard formation, query transactions, data search, responding to the query node, triggering the consensus process, and appending block to the blockchain network. The functions to be performed by the smart contracts include the following:

- Determining the validity of the participating nodes
- Initiating a shard
- Assigning nodes to the specific shard
- Determining whether a specific node has the permission to access data
- Notifying the relevant nodes about data-sharing requests
- Forwarding requests to the owner of the data source
- Granting access to the EHR in the respective storage via the obtained hash of the record
- Sending EHR reference pointer to the query node.

5. Theoretical Analysis of the Proposed Solution

In this section, we analyze our proposed scheme from the following three aspects: security and privacy, scalability, and cross-shard communication exclusion.

5.1. Security and Privacy

The proposed solution uses a consortium blockchain model, which is a permissioned network among healthcare organizations, allowing only legitimate nodes in the network

to participate. The process of registration through SM provides security and privacy to the network nodes. At the time of registration, the participating nodes (hospital, doctor, patient) are verified to ensure that the nodes are legitimate and provided the required encryption keys. The nodes proceed with their pseudo identities instead of true identities. Thus, user privacy is protected in the network.

The proposed scheme uses a static setting for configuring the shard membership. Shard formation refers to the criteria used to allocate nodes to join a shard. The patient's public key is used for shard formation, which refers to the static sharding. In a static shard formation setting, the shard members are not intermittently assigned, and they have known and trusted identities; therefore, it is not vulnerable to Sybil attacks [13]. If any of the participating nodes act maliciously, the SM is authorized to discard the node from the network. Moreover, the transactions are processed within the shard among the concerned nodes only, which can prevent unauthorized nodes from accessing medical information. Therefore, the proposed scheme provides better security and privacy measures in a healthcare ecosystem.

5.2. Scalability Performance Analysis

Scalability is a major concern in any fast-growing technology. In the case of blockchain networks, scalability is defined in terms of throughput, latency, storage, and block size. This section analyzes the proposed scheme using a performance matrix in blockchain network, such as throughput, consensus latency, and the number of transactions processed for each appointment. The analysis is performed based on the proposed sharding technique compared with the unsharded techniques used in healthcare blockchain. The more verifiers involved in the block verification phase, the higher is the level of security; however, it also increases latency (owing to verification delay). Healthcare requires security with minimal delay in the verification process. Therefore, the proposed system using PoA, which ensures security by deploying honest verifiers in the consensus and number of verifiers, is reduced by the sharding technique.

Consensus Latency: Latency refers to the delay between the time when a transaction is added in a block by a consensus participant and the block is validated by a majority of the consensus nodes. As the number of transactions increases in the blockchain, the verification and confirmation time of transactions increase rapidly. In an unsharded blockchain, several nodes participate in the consensus step for a transaction to be verified. In a healthcare blockchain, the network latency should be reduced for faster processing of transactions. The proposed sharded blockchain runs a PoA consensus among the shard nodes locally with S_N number of nodes (where $S_N \subset B_N$); therefore, the waiting time for the verification of a transaction is minimized by carefully choosing the number of verifiers within the shard. Our scheme eliminates the leader selection step as the shard initiator is appointed as the leader of the shard. We analyze the consensus latency of each appointment. By increasing the number of shard nodes, the consensus latency also increases based on the number of validating nodes in each shard. Let C_T be the confirmation time and S_T the submission time of the transaction for consensus, respectively, with a network delay N_D. Then, the consensus latency L_T per shard is represented by Equation (1) which is used for the calculation of latency in our proposed blockchain network.

$$L_T = ((C_T + N_D) - S_T) \tag{1}$$

Throughput: Blockchain throughput is defined as the successful transactions per second (TPS) given a particular network size. Transaction latency and throughput are inversely proportional to each other as the confirmation in blockchain depends on the consensus mechanism. Considering an unsharded blockchain network processing T_c number of transactions per second, as the transactions are broadcasted to the entire network nodes, B_N, the throughput drops as time evolves. This is because the computing complexity of block validation increases as more blocks are appended to the network. As the number of appointments in the network increases, the number of transactions increases as well. In this

case, the number of transactions reaching the maximum threshold of the network capacity causes a delay in processing the remaining transactions. However, in the proposed scheme, the entire network is divided into K shards, where K depends on the number of active appointments in the healthcare consortium model. Each shard processes a distinct set of transactions; therefore, as the number of transactions increases in the network, they are processed in parallel within the shards. Thus, all transactions are processed in the shards within a unit time and the overall network capacity to process transactions improves. The number of shards is not constant in the network, as it depends on the number of active appointments/requests for service. When an appointment is completed, the shard is discarded. Hence, our proposed solution ensures a scalable network with high throughput compared with unsharded models in blockchain-based healthcare.

5.3. Cross-Shard Communication

The proposed sharding-based healthcare blockchain uses a sharding mechanism to share a patient's EHR within the shard. The sharding technique has been used successfully in many domains for a scalable blockchain development. However, resolving the scalability issue has an overhead of cross-shard communication where a node in one shard needs to communicate with the nodes in another. Cross-shard communication overhead is more complex, which makes the verification process more challenging [31]. The proposed sharding technique in healthcare uses a transaction-based shard formation technique to minimize the network overhead. The shards are formed based on the presence of patients' records in the participating nodes. Therefore, all nodes having the same patient's public key are grouped in a shard. During the appointment between a caregiver and patient, any record can be requested through transactions within the shard only. As a result, it forms complete shards for an appointment; therefore, the shard nodes do not need to communicate with nodes in other shards.

6. Performance Evaluation

This section evaluates and compares the performance of our proposed sharded blockchain healthcare algorithm with previous work (unsharded blockchain-based healthcare systems). A discussion on the results obtained by varying the parameters is also presented with regard to the number of appointments processed, consensus latency, and throughput to analyze the scalability of the proposed architecture.

6.1. Experimental Setup

The experiments were performed by simulating the proposed sharded and unsharded healthcare blockchain using Python 3.6 on Windows 10, Intel(R)® Core(TM) i5-8256U CPU, 64-bit operating system. Table 2 presents the simulation parameters. The caregiver nodes are the authorized blockchain nodes and participate in the consensus step to validate the transactions for each appointment. In this setup, the appointment follows a Poisson distribution, such that each appointment arrives at an arbitrary positive time. We simulated a minimum of 50 caregiver nodes and examined the scalability of the network by increasing the number to 100, 150, 200, and 250. A block size of 1 MB was used, which consists of transactions for each appointment. A block in blockchain is comprised of a header and the body. The block header includes the metadata information (previous block's hash value, Merkle root hash value, block number, and timestamp) and the body part of the block includes the transactions related to patient's EHR. SHA 256 was used as a hashing algorithm in our experiments. For each appointment a random number of shard sizes were generated in the range of 2 to 20. The shard size implies the number of caregivers previously visited by the patient; therefore, we used a random shard size for each patient.

Table 2. Simulation parameters.

Parameters	Values
Simulation time	100,000 units
Caregiver nodes	{50, 100, 150, 200, 250}
Patient nodes	40
Hashing algorithm	SHA 256
Block size	1 MB
Transactions delay	60 Time units
Min nodes in a shard	2
Max nodes in a shard	20

6.2. Scenario 1

In this scenario, we tested the scalability of the proposed sharded healthcare blockchain against the unsharded network to check the number of appointments processed in both networks in a fixed simulation time. Figure 5 shows the number of appointments processed by our proposed technique against the unsharded within the same simulation time with 50 caregivers. It shows that the sharded healthcare blockchain processed 112 appointments and the unsharded healthcare blockchain processed 28 appointments with the same simulation settings. There is a significant increase in the number of appointments processed in the proposed sharded healthcare blockchain because the block validation time is reduced when using the PoA consensus algorithm and multiple appointments are being processed in parallel using the sharding technique.

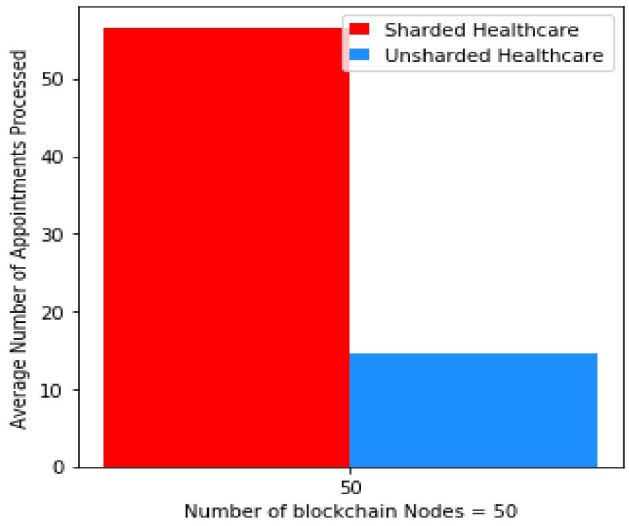

Figure 5. The average number of appointments, within the same time period, processed in the proposed sharded healthcare blockchain versus unsharded healthcare blockchain with the total number of blockchain nodes = 50.

In the same scenario, we increased the number of blockchain nodes (caregiver nodes) from 50 to 150, 200, and 250 nodes to check the scalability performance of our proposed technique. Figure 6 shows a comparative result of sharded healthcare blockchain against the unsharded. We examined the effect of increasing the number of caregivers in the proposed network on the number of processed appointments and found it to be insignificant as long as the patient has not previously visited the added caregiver nodes. Transactions are processed within the shards that are formed based on the patient's medical history. Only shard nodes participate in the block validation for each appointment; therefore, increasing the blockchain nodes has no effect on the performance because not all nodes participate in the consensus process. However, as the number of blockchain nodes increases, the number of processed appointments in the unsharded healthcare system decreases as the new nodes

joining the network participate in the consensus step for block validations; therefore, the performance of the unsharded network in terms of the number of appointments processing is degraded.

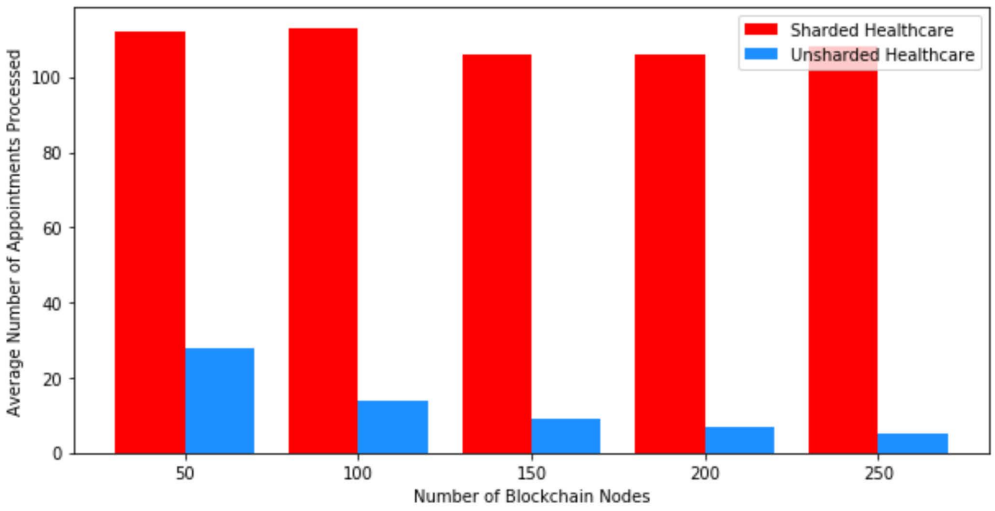

Figure 6. Average number of appointments processed using sharded healthcare and unsharded healthcare blockchain with increasing number of blockchain nodes.

6.3. Scenario 2

In the second scenario, we measured the consensus latency of our proposed technique. Consensus latency measures the delay between the time a transaction is added to the block by a leader (current caregiver) until the block is validated by blockchain nodes. Figure 7 shows the consensus latency for query transactions in a proposed sharded healthcare blockchain against previous work, with the same simulation setting of 50 caregiver nodes. It shows that the consensus latency of the sharded healthcare blockchain is significantly less than that of the unsharded healthcare approach. This is because in the proposed sharded healthcare blockchain, only the shard nodes participate in the consensus mechanism to reach an agreement for validating the block. However, in unsharded healthcare models, all network nodes are involved in the consensus step, resulting in high consensus latency.

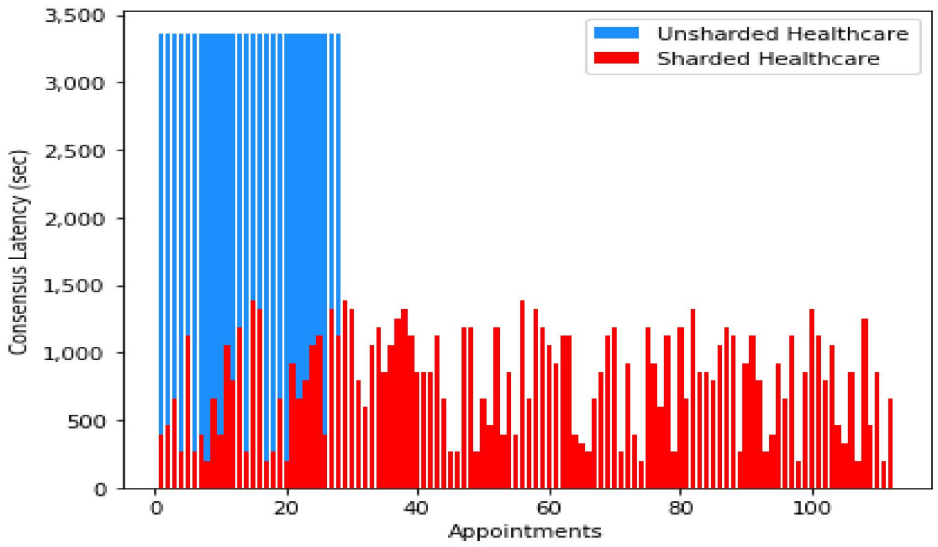

Figure 7. Consensus latency of proposed sharded healthcare blockchain versus unsharded healthcare blockchain.

This setup shows that consensus latency is directly proportional to shard size in the proposed model. As the size of the shard increases, the consensus latency also increases linearly. This increase depends on the number of validating nodes participating in the shard.

Figure 8a,b show that consensus latency is inversely proportional to the number of appointments processed in the blockchain network. The average number of appointments in Figure 8a decreases as consensus latency increases in the unsharded healthcare model by increasing the number of blockchain nodes. However, the impact of consensus latency on the number of appointments in our proposed sharded healthcare blockchain is insignificant. The variation in Figure 8b is due to the shard size when the number of blockchain nodes increases.

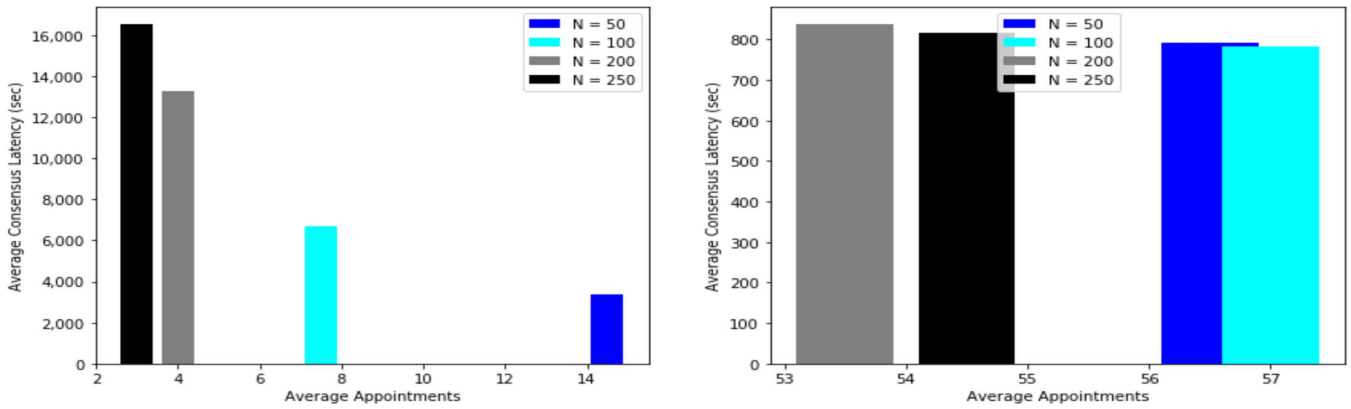

Figure 8. Appointments processing and consensus latency, (**a**) Average number of appointments processed in unsharded healthcare model with average consensus latency. (**b**) Average number of appointments processed in the proposed sharded healthcare blockchain with average consensus latency.

Figure 9 shows the average consensus latency of our proposed sharded healthcare blockchain against that of the unsharded healthcare models for query transactions with an increasing number of blockchain nodes from 50 to 100, 150, 200, and 250. As the number of nodes increases in the network, there is a significant increase in the consensus latency of the unsharded healthcare blockchain. This is because the new nodes joining the network are directly involved in the consensus step. However, increasing the blockchain nodes in the proposed sharded model is insignificant as the consensus is run by only the shard nodes within the shard.

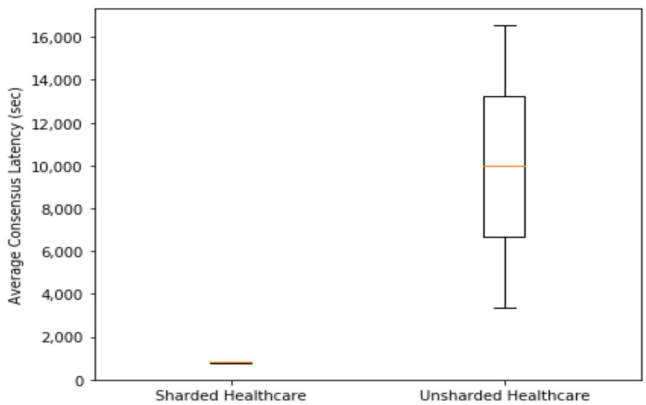

Figure 9. Average consensus latency of sharded healthcare blockchain versus unsharded healthcare blockchain with an increasing number of blockchain nodes.

6.4. Scenario 3

Next, we evaluated the throughput scalability of our proposed technique. Figure 10 shows the average network throughput of both models, sharded and unsharded, with an increasing number of blockchain nodes. A significant decrease in the network throughput of unsharded healthcare blockchain was observed compared with our proposed sharded healthcare model. This is because the network throughput is inversely proportional to the consensus latency, which in turn is directly proportional to the number of nodes participating in the consensus mechanism. Increasing the number of network nodes results in higher consensus latency and leads to lower throughput. However, in the sharded healthcare blockchain, appointments are handled in independent shards. Increasing the number of network nodes is insignificant on sharded models as consensus runs within the shard and depends on the number of shard nodes instead of network nodes, resulting in low consensus latency and high throughput. Furthermore, the appointments in a sharded healthcare blockchain are processed in parallel as shards process appointments independently. Therefore, in unit time, a sharded healthcare blockchain can process multiple appointments compared with unsharded healthcare models, resulting in high throughput with a factor K, where K is the number of shards in a blockchain network.

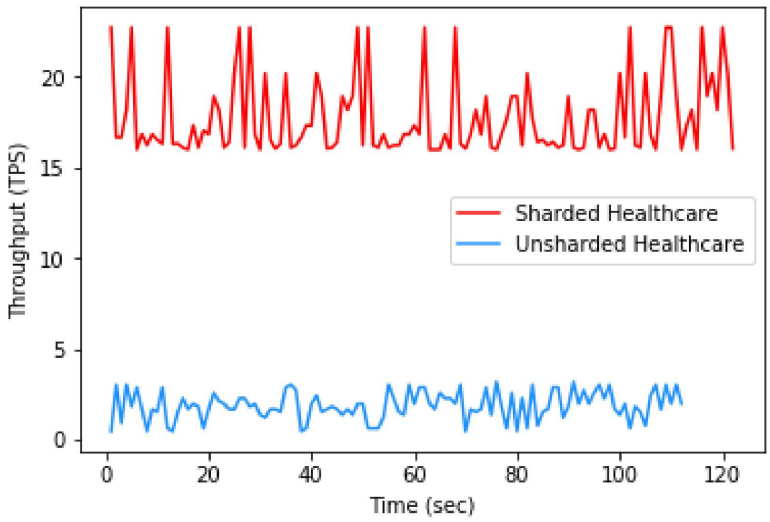

Figure 10. Throughput of the proposed sharded healthcare blockchain and unsharded healthcare blockchain.

To summarize the obtained results from the various simulated scenarios, we examine the impact of our proposed sharding technique on the performance of a healthcare blockchain and compared the results against the unsharded model. The performance of the proposed sharded-based model was examined in terms of the number of appointments processed, consensus latency, and throughput. The results demonstrated a significant increase in appointment processing in sharded-based healthcare as compared to the unsharded network. Our proposed technique processed appointments in parallel within shards, resulting in low latency and high throughput. Next, we analyzed the scalability of our proposed technique when increasing the number of blockchain nodes. The obtained results showed that our proposed model is more scalable as increasing the number of nodes had no significant impact on the performance since transactions were processed within each shard with the minimal number of shard nodes participating in the consensus process.

7. Conclusions

EHRs are important assets in a healthcare ecosystem and should be shared among healthcare entities to ensure better treatment and diagnosis. The use of blockchain technology in healthcare can revolutionize EHRs sharing. Many researchers have adopted

blockchain in the healthcare ecosystem to improve interoperability. Blockchain can enhance EHRs sharing because of its distributed, immutable, decentralized, and secure architecture. However, scalability is a significant bottleneck in blockchain network owing to its replication of distributed ledger among all participating nodes and consensus mechanisms and it must be carefully managed in a healthcare blockchain. This study proposes a sharding technique in healthcare blockchain to resolve scalability issues. A "transaction-based sharding" technique is used to form shards depending on patients' previously visited entities. The proposed model improves the performance of healthcare blockchain by parallel processing of a patient's appointments within shards.

In this study, we present a sharding-based healthcare blockchain model and compare its performance with an unsharded healthcare blockchain model. The simulation results showed improved performance of our proposed model in terms of consensus latency, throughput, and number of appointments processed. The proposed work eliminates cross-shard communication, which degrades system performance in any sharded model. With the successful implementation of sharding in healthcare blockchain, many refinements from a practical perspective should be considered in future research, including modeling associated security threats, emergency case handling, EHRs management, and efficient patient record updates.

Author Contributions: This work was designed and implemented by F.H. under the supervision of K.S. and F.S. F.S. contributed to the initial implementation of the simulation. As the principal investigator, K.S. provided technical guidance and funding acquisition. F.H. wrote the original draft of the paper, K.S. and F.S. proofread and edited the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Zayed Center for Health Sciences, the United Arab Emirates University, Grant number 31R180.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, *42*, 136. [CrossRef] [PubMed]
2. Bahga, A.; Madisetti, V.K. A cloud-based approach for interoperable electronic health records (EHRs). *IEEE J. Biomed. Health Inform.* **2013**, *17*, 894–906. [CrossRef] [PubMed]
3. Fernández-Cardeñosa, G.; De La Torre-Díez, I.; López-Coronado, M.; Rodrigues, J. Analysis of cloud-based solutions on EHRs systems in different scenarios. *J. Med. Syst.* **2012**, *36*, 3777–3782. [CrossRef] [PubMed]
4. Zangara, G.; Corso, P.P.; Cangemi, F.; Millonzi, F.; Collova, F.; Scarlatella, A. A cloud based architecture to support electronic health record. *Stud. Heal. Technol. Inform.* **2014**, *207*, 380–389.
5. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
6. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: http://www.bitcoin.org (accessed on 22 May 2021).
7. Ismail, L.; Materwala, H. Blockchain paradigm for healthcare: Performance evaluation. *Symmetry* **2020**, *12*, 1200. [CrossRef]
8. Mosakheil, J.H. Security Threats Classification in Blockchains. 2018. Available online: http://repository.stcloudstate.edu/msia_etds/48 (accessed on 22 May 2021).
9. Zamani, M.; Movahedi, M.; Raykova, M. Rapidchain: Scaling blockchain via full sharding. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018.
10. Luu, L.; Narayanan, V.; Zheng, C.; Baweja, K.; Gilbert, S.; Saxena, P. A secure sharding protocol for open blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016.
11. Kokoris-Kogias, E.; Jovanovic, P.; Gasser, L.; Gailly, N.; Syta, E.; Ford, B. Omniledger: A secure, scale-out, decentralized ledger via sharding. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018.
12. Al-Bassam, M.; Sonnino, A.; Bano, S.; Hrycyszyn, D.; Danezis, G.J. Chainspace: A Sharded Smart Contracts Platform. Available online: https://arxiv.org/pdf/1708.03778.pdf (accessed on 22 May 2021).

13. Wang, G.; Shi, Z.J.; Nixon, M.; Han, S. Sok: Sharding on blockchain. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies, Zurich, Switzerland, 21–23 October 2019.
14. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016.
15. MedRec. MedRec Technical Documentation. 2018. Available online: https://medrec.media.mit.edu/ (accessed on 22 May 2021).
16. Albeyatti, A.J.M.S.-P. White Paper: Medicalchain. 2018. Available online: https://medicalchain.com/en/team/ (accessed on 22 May 2021).
17. Castaldo, L.; Cinque, V. Blockchain-based logging for the cross-border exchange of ehealth data in europe. In *International ISCIS Security Workshop*; Springer: New York, NY, USA, 2018.
18. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
19. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2019**, *25*, 1398–1411. [CrossRef]
20. Ji, Y.; Zhang, J.; Ma, J.; Yang, C.; Yao, X. BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems. *J. Med. Syst.* **2018**, *42*, 147. [CrossRef]
21. Wang, H.; Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *J. Med. Syst.* **2018**, *42*, 152. [CrossRef]
22. Liu, W.; Zhu, S.; Mundie, T.; Krieger, U. Advanced blockchain architecture for e-health systems. In Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, 12–15 October 2017.
23. Al Omar, A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Rahman, M.S. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Gener. Comput. Syst.* **2019**, *95*, 511–521. [CrossRef]
24. Kaur, H.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *J. Med. Syst.* **2018**, *42*, 156. [CrossRef]
25. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
26. Liu, J.; Li, X.; Ye, L.; Zhang, H.; Du, X.; Guizani, M. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018.
27. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017.
28. Wang, J.; Wang, H. Monoxide: Scale out blockchains with asynchronous consensus zones. In Proceedings of the 16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19), Boston, MA, USA, 26–28 February 2019.
29. Shuaib, K.; Saleous, H.; Zaki, N. Blockchains for secure digitized medicine. *J. Pers. Med.* **2019**, *9*, 35. [CrossRef]
30. Tong, W.; Dong, X.; Shen, Y.; Jiang, X. A hierarchical sharding protocol for multi-domain IoT blockchains. In Proceedings of the ICC 2019–2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019.
31. Ismail, L.; Materwala, H.; Zeadally, S. Lightweight blockchain for healthcare. *IEEE Access* **2019**, *7*, 149935–149951. [CrossRef]
32. Nguyen, L.N.; Nguyen, T.D.; Dinh, T.N.; Thai, M.T. Optchain: Optimal transactions placement for scalable blockchain sharding. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019.
33. Milanov, E. *The RSA Algorithm*; RSA Laboratories: Hebron, CT, USA, 2009; pp. 1–11.
34. Lepore, C.; Ceria, M.; Visconti, A.; Rao, U.P.; Shah, K.A.; Zanolini, L. A survey on blockchain consensus with a performance comparison of PoW, PoS and Pure PoS. *Mathematics* **2020**, *8*, 1782. [CrossRef]
35. Hellman, M. An overview of public key cryptography. *IEEE Commun. Mag.* **2002**, *40*, 42–49. [CrossRef]
36. Aydar, M.; Cetin, S.C.; Ayvaz, S.; Aygun, B. Private key encryption and recovery in blockchain. *arXiv* **2019**, arXiv:1907.04156.
37. Liu, X.; Wang, Z.; Jin, C.; Li, F.; Li, G. A blockchain-based medical data sharing and protection scheme. *IEEE Access* **2019**, *7*, 118943–118953. [CrossRef]
38. Mikula, T.; Jacobsen, R.H. Identity and access management with blockchain in electronic healthcare records. In Proceedings of the 2018 21st Euromicro Conference on Digital System Design (DSD), Prague, Czech Republic, 29–31 August 2018.
39. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **2018**, *42*, 130. [CrossRef]
40. Theodouli, A.; Arakliotis, S.; Moschou, K.; Votis, K.; Tzovaras, D. On the design of a blockchain-based system to facilitate healthcare data sharing. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018.
41. SHA-256. Cryptographic Hash Algorithm. Available online: https://www.movable-type.co.uk/scripts/sha256.html (accessed on 12 December 2020).

42. Python Pool. SHA-256: Implementation in Python. Available online: https://www.pythonpool.com/python-sha256/ (accessed on 20 December 2020).
43. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [CrossRef] [PubMed]
44. Amiri, M.J.; Agrawal, D.; Abbadi, A.E. On sharding permissioned blockchains. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019.
45. Christodoulou, K.; Iosif, E.; Inglezakis, A.; Themistocleous, M. Consensus crash testing: Exploring ripple's decentralization degree in adversarial environments. *Future Internet* **2020**, *12*, 53. [CrossRef]
46. Ekparinya, P.; Gramoli, V.; Jourjon, G. The attack of the clones against proof-of-authority. *arXiv* **2019**, arXiv:1902.10244.
47. Weber, I.; Lu, Q.; Tran, A.B.; Deshmukh, A.; Gorski, M.; Strazds, M. A platform architecture for multi-tenant blockchain-based systems. In Proceedings of the 2019 IEEE International Conference on Software Architecture (ICSA), Hamburg, Germany, 25–29 March 2019.
48. Ethereum Proof-of-Authority Consortium Azure. Available online: https://docs.microsoft.com/en-us/azure/blockchain/templates/ethereum-poa-deployment (accessed on 1 February 2021).
49. AWS. *Launch Enterprise-Ready Blockchain Networks on AWS in Minutes with Kaleido—A ConsenSys Solution*; AWS: Seattle, WA, USA, 2018; Available online: https://aws.amazon.com/blogs/apn/launch-enterprise-ready-blockchain-networks-on-aws-in-minutes-with-kaleido-a-consensys-solution/ (accessed on 22 May 2021).
50. Ethereum. Rinkeby: Ethereum Testnet. Available online: https://www.rinkeby.io//#stats (accessed on 22 May 2021).
51. Daraghmi, E.-Y.; Daraghmi, Y.-A.; Yuan, S.-M. MedChain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access* **2019**, *7*, 164595–164613. [CrossRef]
52. Zhu, X.; Shi, J.; Lu, C. Cloud health resource sharing based on consensus-oriented blockchain technology: Case study on a breast tumor diagnosis service. *J. Med. Internet Res.* **2019**, *21*, e13767. [CrossRef]
53. Dwivedi, A.D.; Malina, L.; Dzurenda, P.; Srivastava, G. Optimized blockchain model for internet of things based healthcare applications. In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019.
54. Ethereum; Parity. Blockchain Infrastructure for the Decentralized Web. Available online: https://www.parity.io/ (accessed on 5 January 2021).