electronics

MDPI

Review

A Review on the Role of Blockchain Technology in the Healthcare Domain

Haider Dhia Zubaydi [1], Yung-Wey Chong [1,*], Kwangman Ko [2], Sabri M. Hanshi [1] and Shankar Karuppayah [1]

[1] National Advanced IPv6 Centre, Universiti Sains Malaysia, Gelugor 11800, Penang, Malaysia; haidardhia@yahoo.com (H.D.Z.); Smhanshi@ieee.org (S.M.H.); kshankar@usm.my (S.K.)

[2] School of Computer and Information Engineering, Sangji University, Gangwon 220-702, Korea; kkman@sangji.ac.kr

* Correspondence: chong@usm.my

Received: 31 March 2019; Accepted: 12 May 2019; Published: 15 June 2019

Abstract: Recently, there have been increasing calls for healthcare providers to provide controls for patients over their personal health records. Nevertheless, security issues concerning how different healthcare providers exchange healthcare information have caused a flop in the deployment of such systems. The ability to exchange data securely is important so that new borderless integrated healthcare services can be provided to patients. Due to its decentralized nature, blockchain technology is a suitable driver for the much-needed shift towards integrated healthcare, providing new insights and addressing some of the main challenges of many healthcare areas. Blockchain allows healthcare providers to record and manage peer-to-peer transactions through a network without central authority. In this paper, we discuss the concept of blockchain technology and hurdles in their adoption in the healthcare domain. Furthermore, a review is conducted on the latest implementations of blockchain technology in healthcare. Finally, a new case study of a blockchain-based healthcare platform is presented addressing the drawbacks of current designs, followed by recommendations for future blockchain researchers and developers.

Keywords: blockchain; blockchain-based platform; DApp; decentralized application; healthcare; Internet of Things; IoT

1. Introduction

Blockchain is a digital-ledger-based technology developed to change the perspective of the digital transactions, or specifically, to replace them. Blockchain is defined as a distinct, decentralized distributed ledger that includes all transactions records related to participating members. Blockchain transactions are created and stored in chronological order [1], allowing digital assets (such as digital currency and digital data) to be tracked by participants without central record-keeping [2,3]. One of the key features in blockchain is that participating nodes in the network will hold a copy of the full blockchain [4]. All transactions on the blockchain must be approved because transactions are only valid under the consensus agreement of the participating members. In addition, all transactions are trackable [5], making fraudulent transactions impossible to bypass [6]. When a user (user A) wants to make a transaction to another user (user B) using blockchain, a new block is created to include the transaction. Each transaction is broadcasted across network nodes to verify it. If the new transaction is verified, the new block is added to the blockchain and distributed across network nodes so that other nodes will update their blockchain. Finally, the transaction is received by another user (user B). The full process is depicted in Figure 1.

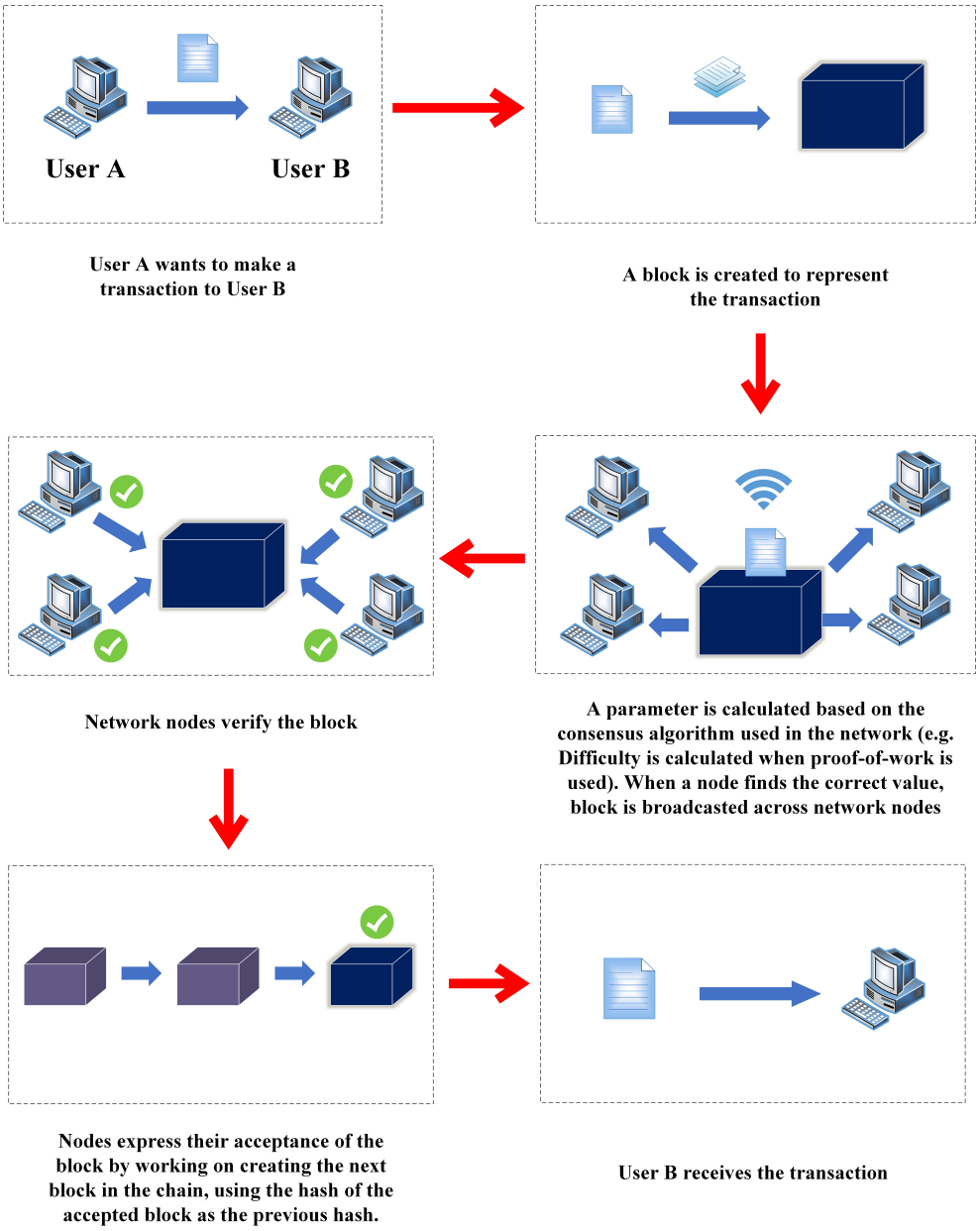

Figure 1. Blockchain process.

The launch of the Ethereum platform blockchain [7,8] enabled blockchain to support transactions in numerous applications besides cryptocurrency [9,10]. Most healthcare applications are developed on the Ethereum framework [11]. Blockchain technology is considered a promising technology for many areas such as public services [12], reputation systems [13], Internet of Things (IoT) [14], and security services [15]. Blockchain-based applications utilise smart contracts [16] to store any record or transaction of value such as currency, oil, gold, real estate contracts, energy, and intellectual property rights (IPR). Blockchain technology has two distinct characteristics: anonymity and distributed consensus [17]. Blockchain transactions provide many advantages such as security, decentralization, and instant transactions. This is because Blockchain technology (BT) eliminates the need for intermediary points such as agents or brokers. Since data is an asset in the digital economy, it is crucial to ensure that data in specific applications have not been manipulated or corrupted.

Throughout the years, Blockchain has gone through extensive development, namely digital currency (Blockchain 1.0), digital economy (Blockchain 2.0), and digital society (Blockchain 3.0). The first generation is related to the underlying technology platform (i.e., public ledger, hashing,

and mining) and overlying protocols (transaction enabling software) to support digital currency [6]. The concept of second generation Blockchain was proposed by [18] as an infrastructure for more complex application (i.e., mortgages, derivatives, stocks, and assets that can be monetized). The major innovation of the second generation relies on the usage of Blockchain in managing assets and trust agreements; thus, the concept of smart contracts was conceived. Smart contracts are an emerging use case in this generation, and are defined as computer programs that automatically execute contract terms and manage smart properties [19]. Smart contracts are faster for execution and data can be transferred faster as compared with traditional contracts [20], making it a key feature in Blockchain technology. Blockchain applications unrelated to economic activity, financial markets, commerce or money are referred to as digital society or Blockchain 3.0 [6]. This generation is associated with broader applications such as education health, science, art and governance. In this generation, several technologies are integrated with blockchain, such as cyber physical systems. In recent years, blockchain technologies have been applied in Electronic Medical Records (EMR) systems to provide control, supervision, accessibility, auditability, and interoperability over large scale data management frameworks using a comprehensive log. Current blockchain technology enables sharing and consuming computing resources, and delivering computing capabilities anytime, anywhere [9]. It is expected to revolutionize and drive industry and economics because it is secure, fast, trustworthy, immutable, and provides public and private transparent solutions. Transactions on the blockchain ameliorate the need for documentation, duplication, third-party intervention, and remediation. Although blockchain has been used in various applications for secure transactions, there are different challenges that need to be considered when implementing blockchain in healthcare application [21,22]. This is because healthcare is a regulated domain that involved patient's privacy. In this paper, problems related to implementation of blockchain technology in healthcare application and the challenges related to consensus algorithms are addressed. This paper is expected to contribute to new use case approaches for blockchain-based healthcare application.

The remainder of this paper is organized as follows. Section 2 provides an overview of blockchain technology and discusses the different consensus algorithms. Section 3 reviews the related work on blockchain technology in the healthcare domain. Section 4 presents a use-case approach for a decentralized consensus secure platform for a blockchain-based healthcare application. Finally, Section 5 is devoted to conclusions.

2. Blockchain Technology

2.1. Overview

Network architectures can be broadly categorised as centralized or distributed architecture. In centralized architecture, a central node is responsible for control and coordination of the whole network. In a distributed architecture, all nodes are connected, eliminating the need for a central point of control. A blockchain architecture functions in a peer-to-peer distributed network offering two primary advantages: greater computing power than a centralized architecture, since the computing power of all nodes is combined together; and network reliability, because there is no single point of failure [23]. Blockchain can also achieve and maintain data integrity in distributed systems due to the high level of security implemented in blockchain technology [24].

The concept of distributed ledger refers to databases that are spread across several computing devices (nodes) [25]. Each device updates itself independently through an identical saved copy of the ledger. Blockchain arises from the use of distributed ledgers. However, blockchain and a distributed ledger are not exactly the same. Although both terminologies can be defined as a cryptographically audit trail for a record of consensus of network nodes, distributed ledgers can be implemented using blockchain. Nevertheless, this process is not reversible. Distributed ledgers do not necessarily employ a chain of blocks in order to provide a valid and secure distributed consensus. Blockchain

technology manages data by grouping it into blocks and linking these blocks to one another, while using cryptography to provide security.

Blockchain works in a consensus manner where network nodes (called miners) are responsible for adding and validating blocks, which are digital records of immutable (unchangeable) data (such as transactions) stored in packages. Blockchain nodes are responsible for connecting the blockchain network, storing information on the ledger, listening to transactions and newly sealed blocks, validating newly sealed blocks (confirming transactions), passing the valid transaction to the network, and creating and passing new blocks [26]. The blockchain technology, which underlies the distributed ledger, validates the new data (transactions) in the ledger. Each block is generated after fulfilling certain and predetermined requirements. In blockchain, all network nodes receive information about every data or transactions and must verify them in order to be validated. Platforms such as Ethereum requires all nodes to receive and understand the information. However, in Corda, only involved nodes receive information about transactions. When the blockchain network contains one or more malicious user(s), unknown reliability and trustworthiness may exist in the blockchain, since unknown peers can exploit the network for their own purposes [27]. However, it is not easy to break into the blockchain network since there are huge requirements such as computing power and having more than 50% in the network.

In blockchain, each block is related to the previous block, and is digitally signed by the responsible miner using a hash function or specifically a hash algorithm (Merkle root hash [28]). The hash function is used to map every single input to a specific hash value to ensure that no duplicate hashing exists. Each block contains the data and hash of the previous block to eliminate any changes or tampering in the blockchain. New blocks are created when miners validate data using algorithms such as Proof of Work (PoW) [29] and Proof of Stake (PoS) [30] concepts. For example, PoW requires computing power to calculate the hash associated with a block to be considered valid. When a miner has more computing power, the hash will be calculated more quickly. Thus, the miner is responsible to add the block to the blockchain and receives the associated reward. The associated reward represents the type of reward the user will receive for mining a block. The time of block creation depends on the application and security mechanisms being used. For example, in Bitcoin, it takes 10 min to add a block [31] (to reduce any hyperinflation of the currency), while, in Ethereum, it takes 10 to 20 s [32].

As shown in Figure 2, blockchain can be represented as a conventional public ledger, in which a complete list of transaction (Tx) records is stored on a sequence of blocks (hashed timestamps) [33,34]. Each block has a reference that points to the previous block referred to as the parent block (i.e., block 1 is the parent block of block 2, the genesis block is the parent block of block 1). This reference is represented by a hash value, a single unique value for every block that makes the block valid. The first block of blockchain is called the genesis block, the hash value of the genesis block is straight zeros because it does not have any parent block. Another term that has been proposed by the Ethereum blockchain is the uncle block, which is created when two blocks are mined at the same time. In this situation, one block is considered the official block and added to the chain, while the other remains a stale block and it is called an uncle block (or orphan block in the Bitcoin blockchain). In the Ethereum blockchain, hashes of uncle blocks are also stored [7], unlike Bitcoin, in which the whole block is neglected.

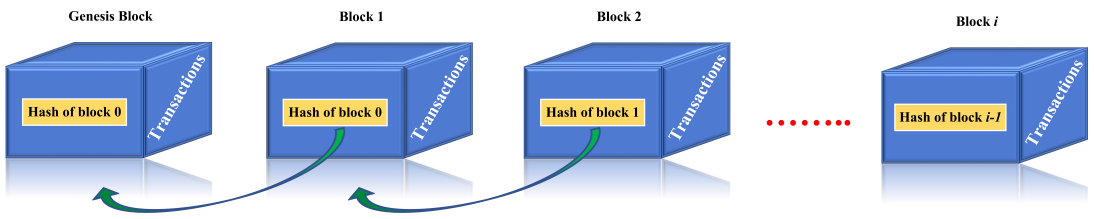

Figure 2. Blockchain architecture [34].

The block structure is shown in Figure 3. Every block consists of block version, parent block hash, Merkle tree root hash, timestamp, nBits, and nonce. Block versions illustrate the validation rules

that must be followed. Parent hash block represents the hash of the previous block to form a chain. The hash is 256-bit. A timestamp represents the time in seconds since 1970, while nBits indicate the current hashing target, which represents a threshold for the block in order to be valid [35]. nBits is an unsigned integer that the header hash must be below or equal to in order for that header to be a valid part of the blockchain. A nonce is a 4-byte random number generated to produce a hash that makes the block valid. The block hash starts with zeros and the number of zeros increase in time to increase the difficulty of figuring out the hash [36]. Thus, miners continuously calculate and guess the nonce that will produce the exact hash (including the number of zeros at the beginning), which will make the block valid. In other words, the miners must generate an output that meets certain requirements when plugging the nonce into the hashing algorithm. Miners use brute force to guess the correct value algorithm until an appropriate output value is found. Such calculation is necessary because any change in input data produces an entirely different output. Thus, these calculations must indicate an accurate output that represents a unique input.

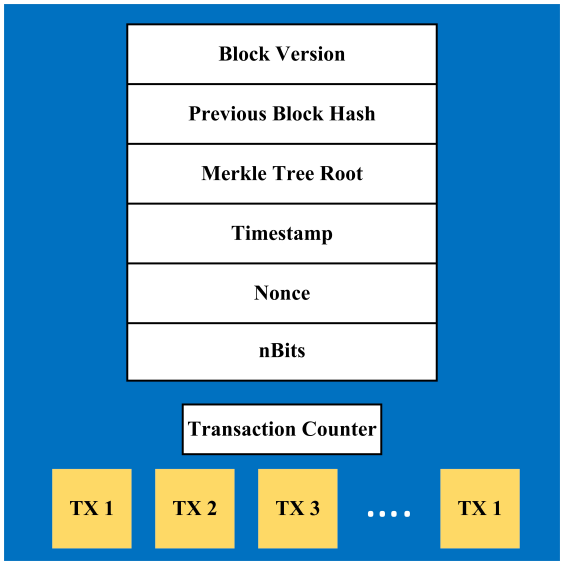

Figure 3. Block header structure.

The hash of all transactions in a block is called Merkle tree root as shown in Figure 4. Each pair of transaction hashes is merged together until a single hash is reached for all transactions, which is called Root Hash or Merkle Root. For example, the hashes of transaction A and transaction B are merged together to generate a new hash called Hash AB; the same process is performed with transaction C and D; finally, the root hash (Hash ABCD) is generated by merging Hash AB and Hash CD. The transactions and associated counters are located in the block body. Block size and transaction size are responsible for defining the number of transactions inside a single block [37].

In order to validate the authentication of transactions, blockchain uses a symmetric/asymmetric cryptography mechanism [38], in which the private key is used to sign and encrypt the data on the sender side. The public key is used to decrypt the data at the receiver side(s). The process of signing transactions produces what is known as a digital signature. The digital signature involves two phases; signing and verification. For example, when user X makes a transaction to user Y, he generates the hash value of the specified transaction. The encryption process is done using user X's (sender) private key. The original data and the encrypted hash are sent to user Y. Anyone in the network can decrypt the hash using the user X's public key. Thus, user Y decrypts the received hash and compares it with the derived hash of the received data using the hash function of user X to verify the transaction.

The Elliptic Curve Digital Signature Algorithm (ECDSA) [39] has been widely used as a digital signature algorithm in blockchains. This is because it has shorter key length as compared to Digital Signature Algorithm (DSA), Rivest-Hsamir-Adleman (RSA) and Diffie–Hellman algorithm. For IoT

devices that utilise blockchain technology, a colour spectrum chain can be used to store authentication status of the devices that can access the IoT [40]. In cloud servers, the algorithm confirms the information in the device, stores the authentication state of the identified device in the blockchain, and checks the authentication state of the stored device. When the colour spectrum chain is used in IoT sensors and multi-platforms using blockchain, the vulnerability of IoT devices can be minimised.

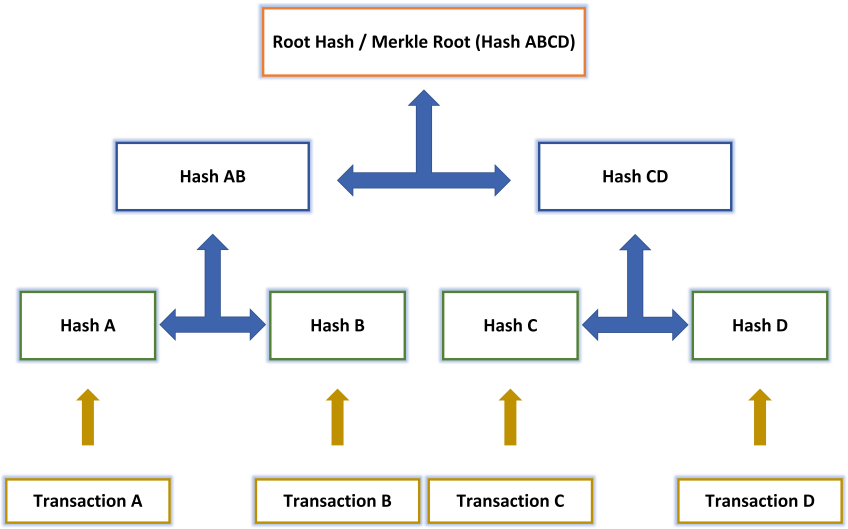

Figure 4. Blockchain Merkle tree root.

For any information system, three requirements must be fulfilled to guarantee security: confidentiality, integrity, and availability. Since blockchain is decentralized, it can guarantee the global system functionality even if one or more nodes are compromised. In blockchain, confidentiality includes securing the user's private key because it is needed along with the public key to compromise the system or impersonate someone else (stealing identity). The public and private keys are used to ensure the integrity and security when exchanging information. There is a unique private key for each user, which guarantees the ownership of information for a specific user. The user signs the information with his private key to indicate his authority to the entire network. The public key is derived from the private key based on a specific algorithm that the system uses. The public keys are distributed across the network because they are irreversible (a private key cannot be derived from public keys). Other users need to use public keys to access the information.

For example, CONIKS [41] created a key management system to control and unleash users from encryption key management. Two-step verification is performed in this system. First, the receiver's public key is verified; then, the key is checked to ensure that it is not altered over time. Integrity can be ensured in blockchain because it prevents the information from being tampered with by unauthorised parties. An integrity blockchain-based IoT framework was proposed in [42] to eliminate any trust needed for third parties. Availability is the most straightforward concept achieved by blockchain because of its distributed system design manner.

Blockchain security mechanisms prevent hacking through the distributed consensus, ensuring the safety of management systems and the centralized data storage since all transactions are required to be verified and validated by a group or community of miners. Furthermore, a blockchain network is monitored by all nodes in the network, and any malicious node (user) lacks the power to insert manipulated blocks into the public ledger because all nodes maintain a copy of the blockchain. Thus, even hacking several ledgers will not affect the blockchain, since blockchain copies provided by others are considered to be a reliable backup [43]. Blockchain systems have the ability to secure the network from certain malicious activities. However, some of them might cause problem to blockchain network [44].

Although blockchain provides an evolution to current technology, it faces many security challenges such as interoperability, scalability, and data privacy [6]. For example, in a peer-to-peer

network, when a user makes more than one payment at the same time using Bitcoins, a security concern known as a double-spending attack [6,32,43,45] arises. This occurs when the pending payments are being broadcasted and, at the same time, the network faces propagation delays or unconfirmed transactions at multiple intervals. To solve this problem, blockchain requires miners to verify the transactions by solving complex mathematical problems (mining procedure). Since it is a time-consuming process and it is hard to solve the problems, usually only one payment passes through correctly and can be registered on the blockchain. Blockchain depends on safeguarding the digital identity (the private key) to provide privacy and anonymity. However, if a key has been possessed or stolen, it is impossible to recover it by any third party, and all the information of the digital identity will vanish. There will then be no way of identifying the person behind it. This process can be very dangerous if third-party institutions are affected [6].

2.2. Consensus Algorithms

The concept behind blockchain is a secured and trusted architecture due to network consensus. Different consensus algorithms have been implemented in the past for specific applications because each domain has specific requirements. For example, some domains require low computation power, while others require faster processing of transaction. The key function of blockchain technology is consensus algorithm, which illustrates the algorithm needed to reach a total agreement between network nodes during blocks verification process [46]. Consensus algorithms aim to provide equality between miners, giving the same weight to all of them so that majority of the miners can reach a decision. However, while this approach suits controlled environments, this is not possible in a public blockchain because it might lead to Sybil attacks, in which a user can hold multiple identities and control the blockchain. In a decentralized architecture, adding a single block is done only by a single user. The user can be selected randomly or based on certain requirements. Nevertheless, random selection is prone to attacks.

The concept of consensus was conceived based on the Byzantine Generals (BG) [27] problem. During war, Byzantine generals command an army around a single city. The BG problem occurs when these generals must reach an agreement to commence an attack or not. Thus, communication is needed to ensure that there are no traitors between them because any problem in the agreement can lead to an attack failure. This challenge pervades blockchain technology because it is a distributed network, such that no central node can control the whole network. Thus, blockchain has adopted decentralized consensus algorithms to enforce the consistency and reliability of data [47]. Examples of consensus algorithms include Proof of Work (PoW) [29], Proof of Stake (PoS) [30], Delegated Proof of Stake (DPoS) [48], Transactions as Proof of Stake (TaPoS) [30], Proof of Activity [49], Proof of Capacity, Byzantine Fault Tolerance (BFT) replication [50], Practical Byzantine Fault Tolerance (PBFT) [51], Delegated BFT (DBFT), BFTRaft [52], Proof of Authority (PoA) [53], Proof-of-Stake-Velocity (PoSV) [18], Proof of Burn [54], Proof-of-Personhood (PoP) [55], Proof of Bandwidth (PoB) [56], Proof of Elapsed Time (PoET) [57], Stellar Consensus Protocol (SCP) [58], Bitcoin-NG [59], Sieve [60], Ripple [61], and Tendermint [62], among others.

Proof of Work (PoW) [29] follows a concept of work, where it is based on the fact that nodes are less likely to attack the network if they perform a lot of work. PoW-based blockchain requires miners to perform computationally expensive tasks (carried out by multiple entities) in order to add a block to the blockchain, thus making it almost impossible for Sybil attacks. PoW works in a manner called mining; nodes will perform calculations until a solution is found. For example, in Bitcoin blockchain, the calculation process aims to find a random number (called nonce) in order to generate the correct hash of block header. Thus, miners must have the ability to perform a certain amount of work in order to calculate the number. When a miner solves the problem, all other nodes are responsible for verifying that the answer is correct. PoW consumes more energy, making it inefficient to be used in low power applications. In addition, PoW nodes that participate in block verification do not correspond to the increase of block transactions; thus, it not scalable [63].

Proof of Stake (PoS) [30] divides users by their stake of the blockchain. Each node that has a certain amount of stake in the blockchain can be a miner. This consensus algorithm assumes that a user with more stake has a lower possibility to attack the network. Nodes allocate a specific amount of their stake when they become a miner. Thus, the network will hold that amount to make sure that a user is trusted and allowed to mine. PoS has lower energy consumption than PoW because it requires less computational power. The issue with PoS is that the mining process of blockchain targets the wealthiest participants, since they can own a higher stake than other nodes.

Delegated Proof of Stake (DPoS) [48] is another consensus algorithm proposed to enhance PoS. In this algorithm, instead of assigning the generation and validation of blocks to the stakeholders, certain delegates are responsible for that procedure. One of the advantages of this consensus algorithm is faster transactions since fewer nodes are involved. In addition, the chosen nodes are able to adjust block size and intervals. Dishonesty can be treated faster because delegated nodes are substituted easily. Transactions as Proof of Stake (TaPoS) [30] is a PoS variant. Unlike PoS, where certain nodes contribute to the security of the network, all nodes contribute to the security framework in TaPoS. In PoS, the limitation is due to stake age that is accumulated, even when the node is not connected to the network. Proof of Activity (PoA) [49] is proposed to reward nodes based on their activity and ownership on the blockchain.

Practical Byzantine Fault Tolerance (PBFT) [51] has been proposed for asynchronous environments to solve the Byzantine Generals Problem. It assumes that more than 2/3 of total nodes are legitimate, while less than a third are malicious. A leader is selected through each block generation, the leader is responsible for ordering transactions. In order to add a block, a minimum of 2/3 of all nodes must support the validation of block. Delegated BFT (DBFT) is a variant of BFT, and works in a similar manner to DPoS, where a certain number of nodes are responsible for validating and generating blocks. Stellar Consensus Protocol (SCP) is similar to PBFT. This algorithm is implemented based on an algorithm called Federated Byzantine Agreement (FBA) [58]. The difference between this algorithm and PBFT is that PBFT requires an agreement from majority of the nodes. SCP relies on a subset of nodes that it considers important.

Ripple [61] has been proposed to solve the issue of light latencies caused by synchronous communication between nodes. The nodes are defined as trusted to create a subset to determine network consensus, and the subset is connected to a specific server to reduce latency. BFTRaft enhances the Raft algorithm [64] by increasing its security through reformulating it into a Byzantine fault-tolerant algorithm. Tendermint [62] consensus algorithm tolerates up to 1/3 of failures, and it can host arbitrary application states. Network nodes are named validators, which create blocks and vote on whether these blocks are valid or not. To add a block, Tendermint divides the validation process into two stages: pre-vote and pre-commit. When more than 2/3 of validators commit a block, the block is committed and considered valid. BitcoinNG [59] is another consensus algorithm that aims to improve latency, throughput, and scalability. Bitcoin-NG is proved to operate optimally. However, it has limitations in terms of latency of propagation time and nodes' bandwidth.

Proof-of-Burn (PoB) is used to define how miners are committed to mining by requesting them to show a proof of their mining activities by burning cryptocurrency (or data that can be spent) to a specific address (spendable address in case of cryptocurrency), instead of consuming (burning) resources. The Proof-of-Personhood (PoP) algorithm is used to provide anonymity through binding physical to virtual identities using ring signatures [65] and collective signing [66]. The Sieve algorithm [60] is Hyperledger-Fabric implementation proposed by IBM research. It uses BFT replication in permissioned blockchain to run non-deterministic smart contracts. Non-deterministic smart contracts processes are replicated in the network and the results are compared. The results are sieved out if a divergence among results is detected within the replicated results. This design sieves out the whole operation if the divergent processes results are excessive. The advantages and drawbacks of different blockchain consensus algorithms are discussed in Table 1.

Table 1. Advantages and disadvantages of blockchain consensus algorithms.

Algorithm	Advantages	Drawbacks
Proof of Work (PoW)	* Provides comprehensive decentralization of power and control in the network * More secure network	* High processing power (expensive) * High electricity consumption * Small networks can be compromised
Proof of Stake (PoS)	* More energy efficient * Better rewards with bigger stakes * Provides faster processing of transactions	* Less decentralized network than PoW * Less security than PoW
Delegated Proof of Stake (DPoS)	* Faster processing than PoW and PoS * Better rewards distribution * Energy efficiency * Lower hardware expenses	* More susceptible to attacks * Richer people control the network * Less resiliency due to less decentralization
Transactions as Proof of Stake (TaPos)	* More security than PoS since all nodes contribute in the network * Provides a simplified PoS algorithm	* Lower speed than DPoS since all nodes included * Does not work well when there are short forks on the blockchain
Proof of Activity (PoA)	* High security * Eliminates 51% attack in blockchain network * Improve network topology *Low transaction fees	* Requires large amount of resources in mining phase * Stakeholders have the ability to double sign transactions * Difficult to implement
Practical Byzantine Fault Tolerance (PBFT)	* Ability to make transactions without the need of confirmation like in PoW * Significant energy usage reduction	* Works only in small consensus group sizes due to a high amount of communication between nodes * PBFT uses MACs which is extremely inefficient compared to the communication needed * Hard to prove the authenticity of a message to third parties * Susceptible to Sybil attacks
Delegated BFT (DBFT)	* Provides perfect finality (confirmation of transactions) * No forks with DBFT * Fast transaction execution	* Susceptible 51% attack * Still considered centralized
Steller Consensus Protocol (SCP)	* Efficient decentralized control with large network * Low latency * Flexible trust & asymptotic security	* Fits finance better than any other systems * Problem with choosing quorums and propose new arguments * Inefficient in terms of number of sent messages
Ripple	* Fast transactions * Low power consumption compared to PoW * Path dependent; the chain is uneditable * No capacity limitation for the number of transactions	* Unique Node Lists (UNLs) must be maintained, if UNLs is broken, the network might collapse * It is highly centralized
BFTRaft	* Can tolerate failure of up to 1/2 of the node count * Design simplicity and robustness	The current implementation can only be considered to guarantee liveness for one Byzantine failure
Tendermint	Similar to PoS	Similar to PoS
Proof-of-Burn (PoB)	* Encourages long-term involvement * PoB implementation can be customized * The power of burnt coins “decays” or reduces partially each time a new block is mined	* Rich get richer problem * Resource waste (the burnt coins are wasted) * High risk protocol, no coin recovery guarantee
Proof-of-Personhood (PoP)	Eliminates PoW and PoS disadvantages	Fits finance better than any other systems

3. Blockchain in Healthcare

Blockchain technology has been merged and integrated with many types of applications such as Internet of Things (IoT), healthcare, real estate and food security [7,34]. Among the different applications that use blockchain, healthcare is one of the most interesting fields in current blockchain-based research. This is because healthcare is one of the most regulated industries and blockchain can have a positive impact on the healthcare domain [67]. Blockchain technology has led to tremendous solutions for traditional healthcare domain issues [68,69], such as providing a secure infrastructure and integrated private health records [70]. Blockchain can be used to provide secure communication among stakeholders and deliver clinical reports efficiently [71].

Blockchain allows sharing an Electronic Health Record (EHR) in a secure manner since blockchain technology can be extended as a standard for stakeholders [72]. Using blockchain for EHR provides many advantages, such as preserving patient's privacy [73] and improving quality of medical care [74]. The need for patient-centric services and connecting disparate systems have triggered the usage of blockchain [75]. Blockchain provides patients full control over their medical records. Patient information is very case-sensitive and must be stored and shared in a secure and confidential manner. Therefore, it is a prime target for malicious attacks, such as Denial of Service (DoS), Mining Attack, Storage Attack and Dropping Attack [76]. Blockchain provides a secure and robust platform for healthcare against failures and attacks because it contains different mechanisms of access control [75].

3.1. Research Method

Multiple methods have been analysed in this literature. The database of this paper includes a systematic review on data sharing systems in terms of safety, efficiency, effectiveness, patient centeredness, and timeliness [77]. In addition, review on security, privacy, and efficiency for patient care management systems [71] were conducted as well. This covers access control and medical information completeness [78] and systematic review related to blockchain research [26]. Some of the papers cover proposed architecture for healthcare using blockchain. There are also future recommendations for researchers based on existing research at that time. Based on the review of many papers, a case study on best practice is constructed. The case study takes into consideration all factors and attributes such as privacy, security, effectiveness, encryption algorithms flaws, interoperability, scalability, and regulation concerns.

In this context, we focus on reviewing proposed works that were conducted in the past five years related to blockchain technology in healthcare domain. This work fills the gap for researchers to find a comprehensive review that addresses research gaps related to healthcare domain and blockchain technology.

3.2. Systematic Review

The usage of blockchain technology in healthcare does not focus on patient's privacy and security only. It is implemented to address another important issues such as interoperability. Implementing secured approaches to share medical data is challenging because of the heterogeneous data structures among diverse organizations, which results in compatibility precluding. Data comprehension can be limited due to the disparate use of the terminology "healthcare". It is required to agree on both structure and semantics of data to share medical data. However, the concerns of data consistency and security are still around because cyber attacks are attracted due to the use of centralized authority providers and data stores. Thus, establishing a consistent view of data sharing systems for patient records is problematic. Hence, many approaches have been proposed to solve these healthcare systems' issues and challenges.

The systematic review categorised the applications of blockchain technology into several key areas as shown in Figure 5. These applications are analysed to look into the fulfillment of key requirements in blockchain based healthcare systems such as data interoperability, security, integrity, cost/resources effectiveness, untrusted and transparent and complexity of the proposed work [20].

Although Blockchain has been widely deployed in cryptocurrency, most applications of blockchain in healthcare are still in conceptualization stage or implemented in testbed [79].

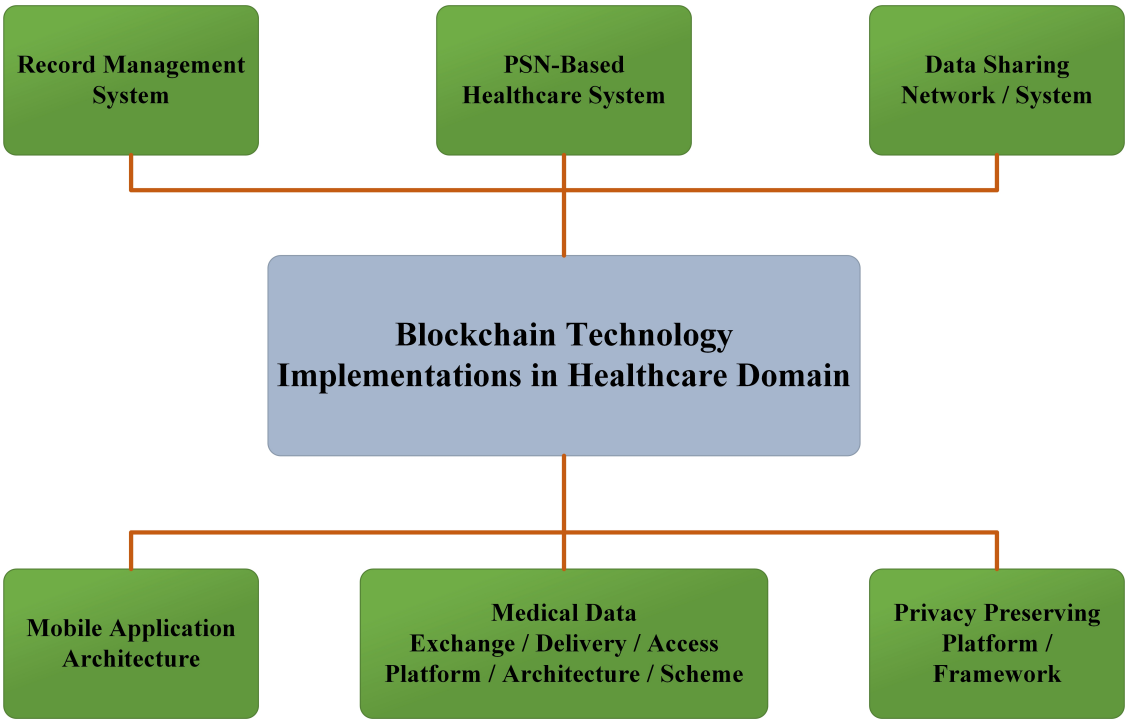

Figure 5. Blockchain implementation in healthcare.

3.2.1. Data Sharing Network/System

A secure and effective data sharing approach to sharing healthcare information is proposed in [80]. The authors used Merkle Tree-based structure to link each block with the previous block. Transactions do not include the actual patient information. Instead, they used Fast Healthcare Interoperability Resources (FHIR), an emerging standard that is designed to share Electronic Health Records (EHR) by providing public accessibility through Application Programming Interfaces (APIs). FHIR resources are indicated through a specific Uniform Resource Locator (URL) to retain operational control of patient's data and provide better security and integrity by keeping sensitive information out of the blockchain. Proof of Interoperability is used as the consensus algorithm for the process of mining blocks. Proof of interoperability relies on FHIR protocol conformance. The medical data must be verified by miners to guarantee their interoperability in terms of semantic and structural standards. This approach presents a different concept than PoW when adding blocks to the blockchain. Transactions are sent to the coordinating miner for transaction distribution. Network nodes will then verify the block after the coordinating node assemble all transactions. The coordinating miner signs the block after being returned during the signed block return phase. The block is then added and distributed. This process ensures the integrity of each block because all nodes are responsible to digitally sign the block with at least one transaction. Since the actual record data is not inserted in the block, searchability, discoverability, and data access control mechanisms are required. The value sets are stored in a repository that presents a single point of failure, thus eliminating the concept of decentralisation. Patient identification is done by assigning addresses to data, which in turn allows a single patient to hold multiple addresses on the blockchain. This might disturb and overload the system with a high number of users. The proposed system has not yet been implemented.

A data sharing framework for cloud environments based on blockchain technology has been proposed to address the access control challenges associated with sensitive data [81]. The proposed framework is based on built-in autonomy and immutability properties of permissioned blockchain

(where only verified and trusted users are allowed to access the data). The sensitive data are stored in pool(s) using permissioned blockchain, and an efficient access control is implemented via secure cryptographic techniques. A shared repository is deployed to allow users to access EMRs through a data-sharing scheme after verifying their identities and cryptographic keys. The proposed system archives user's membership by relying on identify-based authentication. It also helps to guarantee a level of security using multiple cryptographic keys. The system is separated into three layers, namely storage, system management and users. Each of these layers performs certain tasks to facilitate data sharing with secure structures. Based on authors' evaluations, the proposed framework is lightweight and scalable, while providing efficiency, identity management and distant access. However, the algorithms between entities and authentication and communication protocols were not fully investigated.

A blockchain-based system architecture is proposed to handle healthcare data access and facilitate auditable and private healthcare data sharing [82]. The proposed architecture is designed using features such as properties and smart contracts to ensure workflow automation, patient pseudonymity, shared data integrity, auditing, and accountability. The design is based on consortium blockchain, which allow all participating nodes in the network to be verified off-chain. The proposed design consists of three layers, namely WebCloud Platforms, Cloud middleware and Blockchain network. Three types of smart contracts are used, namely Registry Contract (RC), Patient Data Contract (PDC), and Permissions Contract (PC). RC is used as registry for all network nodes and maps between all network nodes. PDC is used as unique indicators to each patient, linking the hashed healthcare data to the actual data in the WebCloud Platform using URL. The PC is responsible to manage the permissions in the network because it links the PDC address and data requesting entity.

Another research that addresses the cost and interoperability issues in healthcare domain was proposed by [83]. The authors designed a blockchain-based patient centered protocol due ineffective communication between EHRs institutions when dealing with ill patients. Their research focuses on physicians and surgeons that provides critical patient care so that they can access patient's prior imaging studies, current medications, and medical history. The authors illustrated the revolution of blockchain-based healthcare data supply chain because blockchain technology can eliminate the difficulty encumbered by supporting a huge number of existing silos of patient datasets. This problem can be seen in current non blockchain-based implementations. This design addressed Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements which includes privacy, security, cloud computing guidelines. In addition, it takes into consideration HIPAA restrictions and limitations of blockchain technology. Patiotory tokens (PTOY) are used as fuel to run the blockchain. These tokens regulate network storage allocation, revenue payment cycles, and healthcare quality measurements. Such design offers minimised breaches for providers due to inherent access control properties of the system.

A user-centric architectural framework that utilizes blockchain characteristics is proposed to secure the control of information exchange [84]. The framework pairs policies that are user generated with smart contracts. This research addresses the issue of how data owners control the information after data exchange. The proposed approach employs a set of cryptographic keys to guarantee the access and security of information as well as monitor and manage violation. The system consists of users, query manager, smart contract center, processing nodes, local storage, and blockchain network. The system is constructed starting with a registration process where user credentials are stored and policies are set up. The user can send a request using private and membership keys to the query manager. Once the information has been authenticated, the processing nodes retrieve associated policies from storage and smart contracts will be generated. Smart contracts attached to the data and monitoring process will begin. The monitoring is important to make sure that the computations are conducted in a reasonable time to avoid being misused. The system provides data protection, user privacy, and complies with Health Insurance Portability and Accountability Act (HIPAA) regulations. However, scalability and efficiency are not considered.

In [85], the authors proposed an efficient approach to share continuous IoT data using blockchain. They classified the data into different categories based on data characters (static and dynamic) and data acquisition (instant and continuous). To allow control over data quality, a machine-learning-based data quality inspection module was introduced. This is crucial because IoT devices can create a large amount of data with noise. The data quality inspection can filter the noise and make sure that the data produced is reliable. By eliminating noise, accurate prediction of a user's activity can be obtained. The proposed design defines three roles in the system, namely users generating the data, key keepers that store private keys to decrypt data, and customers to provide monetary or service rewards in exchange of data. The data that have been inspected will be allowed to share or transact using blockchain module. Before the data can be uploaded in the cloud from user's application, it will be encrypted using symmetric-key algorithms such as Rijndael AES [86] together with threshold encryption schemes [87]. The symmetric key will be distributed to different key keepers to increase the complexity of decryption process. The research incorporated crypto tokens to encourage users to share their health data for research and commercial purposes. While the benefits are tempting, the proposed work is still in a conceptual design stage.

MedChain [88] is a data sharing scheme that incorporates blockchains, digest chain and structure peer-to-peer network to overcome efficiency related to metadata change when sharing data between different entities. This approach checks the integrity of shared medical IoT data stream using digest chain structure. This data sharing scheme is session-based to allow further flexibility during information sharing. MedChain network consists of two different peer nodes, namely super peers and edge peers. The super peers includes servers of entities with high computing and storage power such as national hospitals. The edge nodes are servers from small entities such as community clinics that stores actual patient data. The proposed scheme facilitates data query and access using mutable information while maintaining authenticity, integrity, and security using immutable information. Elliptic Curve Cryptography (ECC) [89] is used for key generation. This scheme offers resiliency to masquerade and replay attacks, forward secrecy, data integrity, privacy protection, and non-repudiation of unauthorized data access. MedChain reduces computation and storage overhead when new descriptions are generated. It is the only scheme that supports metadata update, storage space recycling, and data stream support.

3.2.2. Record Management System

MedRec [90,91] is a convenient and adaptable record management system. This novel Electronic Management Records (EMRs) system is designed in a decentralized manner by leveraging blockchain technology properties. MedRec aims to address several major issues related to healthcare, namely data quantity and quality, system interoperability, fragmented medical data, patient agency, and slow access to medical data. To provide interoperability, a set of APIs was built for provider database integration. Smart contracts in the Ethereum blockchain are used for data retrieval instructions and viewing permissions using a log of medical relationships between patients and providers. To ensure that the data are not tampered, a cryptographic hash is used to guarantee data integrity. Participating parties control their records by accepting or rejecting new information. A DNS-like implementation is used for identity confirmation by linking a specific Ethereum address to a specific patient's ID. Handling off-chain data exchange between the provider and patient's database is implemented by a syncing algorithm. A database authentication server is used to confirm permissions on the blockchain. The proposed system provides patients with easy access, an immutable log, and comprehensive services to medical information across treatment sites and providers. MedRec allows data sharing, confidentiality, authentication, and accountability for sensitive information. MedRec relies on multiple participants to avoid a single point of failure. However, the prototype does not include contract encryption. In addition, preserving auditability while improving obfuscation is still an issue. Scalability is an open issue in MedRec as it was not tested in large scale deployment. MedRec needs to be extended for complex scenarios regarding healthcare data since it only validates the medical records. Collecting

and sharing medical records as rewards is illegal in many countries due to privacy issues. Thus, data usage efficiency in MedRec is not satisfactory.

An implementation that uses smart contracts as mediators is proposed by [92] to access Electronic Health Records (EHRs) in large-scale information architecture. The authors address accessibility and data privacy issues in healthcare. The current version of the Ethereum platform is the base idea of the proposed architecture. Smart contracts are the core in the proposed architecture, which is used to register all access to data, process access requests, and store new transactions in the ledger. In the proposed architecture design, the data is owned by the user, not health institutions. A distributed ledger is used to execute smart contracts and record references to health transactions, store health records, store users' public and private cryptographic keys using wallets, and as a discovery service for an information index to accelerate information search. Three types of transactions are defined for specific purpose: New Record, Request Access, and Notification. For example, notification is a special transaction to indicate a public health issue. One of the advantages of such design is delegating data management to patients. Patients have full control over their medical records (control of their private key). However, if a user is not tech-savvy, or a user lost his private key, a patient's health record may be lost or compromised. The data is not stored in a centralised ledger for performance reasons, as such data retrieval process will be a challenge. The proposed design is still in the early stages of conceptualization.

MedBlock [93] is a blockchain-based information management system that has been proposed to manage medical information. An improved hybrid-consensus mechanism was implemented to address network congestion and large energy consumption issues since Delegated Proof of Stake and Practical Byzantine Fault Tolerance are not suitable. The consensus mechanism works like a board vote, one node within a region is voted as the endorser to act on behalf of other nodes. The mechanism allows effective data upload to avoid congestion in the network caused by patients performing many procedures in a centralized time. MedBlock combines symmetric cryptography and customized access control to exhibit high information security. MedBlock utilises bread crumb mechanisms, which enable users to find encrypted information that they are interested in efficiently. MedBlock provides efficient EMR access and retrieval process. It has less access times as compared to other approaches and consistent data flow in different periods, which resolves the problem of sharing information and data management in large-scale systems. Since EMRs are stored in hospitals' databases, they reduce the concept of decentralization of blockchain to avoid being targeted by malicious actors.

SMEAD [67] is a new healthcare paradigm designed for diabetic patients through an end-to-end secured system. The proposed paradigm includes three wearable devices (smart neckband, smart footwear, and smart wristband) to observe patients' statuses and predict patients' conditions. They deployed MEDIBOX (a self-served Collaborative platform for E-Distribution of Pharma and Healthcare products) to work as an alert and reminder mechanism for patients. MEDIBOX provides continuous monitoring of patients' insulin dosage. Blockchain is used to provide security and data access control for trusted parties using smart contracts. Social networks on mobile phones such as WhatsApp, Facebook, and Twitter are used as emergency mechanisms for caretakers, since these applications offer continuous communication over the internet. The proposed system is designed by integrating medication administrator, IoMT (Internet of Things in Medical Things), wearable technology and cloud computing. Public key cryptography is used to protect the data and authenticate users. Smart contracts are used to address the privacy concern by securing transactions.

MeDShare [68] is another efficient blockchain-based management system to handle medical records. This system is proposed for cloud repositories that manages shared medical records and data among medical big data entities. The proposed system ensures data provenance, security, auditing, and user verification through cryptographic keys. The MedShare data sharing mechanism is grouped into four layers, namely user, data query, data structuring and provenance, and an existing database infrastructure layer. When a user would like to access a database, a private key will be generated and digitally signed by the user. The query system will then forward the request to data structuring

and the provenance layer. A smart contract will then be executed in order to share data among cloud service providers.

Blockchain has been used to manage and share EMR data for cancer patient care. Ref. [94] use permissioned blockchain to address three main objectives: primary patient care, data aggregation for research purposes, and providing better patient care through connecting different healthcare entities. The framework consists of multiple nodes to reach network consensus, databases to handle offchain storage, membership service, and APIs for different users. The membership service is responsible for registering patients and doctors, which will be used to define the functionality of the chaincode. Patient's data are stored in two different databases, namely local database and cloud based platform. Each database stores the data in different data structures. Consensus nodes operate through a custom chaincode implemented inside them, acting as a Hyperledger validating peers through the PBFT consensus algorithm. The proposed framework aims to reduce turnaround time and reduces overall cost while improving decision-making processes. Data semantics and sensitivity must be considered in order to provide any efficient storage mechanism.

Transparency aspects make it difficult to protect data against malicious traffic analysis while maintaining accountability and transaction privacy. Hence, a novel Machine-to-Machine (M2M) messaging and rule-based beacons platform [95] has been proposed to discuss decision fusion and the role of data in seamless data management. The proposed design utilises Field-Programmable Gate Array (FPGA) based IoT sensors to monitor biological information. The data are sent wirelessly to the cloud via an IoT gateway. Blockchain is used in a distributed database to harden medical reports from being tampered. The deployed databases can be managed by disparate parties such as regulators, pharmacies, caregivers, patients, insurance companies, and hospitals. The overlay network is used between nodes to provide confidentiality for users by selecting random paths for communication. Data fusion and decision fusion are used to increase the accuracy.

In order to digitize and democratize healthcare services, privacy must be the key feature to avoid medical data being jeopardized. If a breach of medical records happens, patients will lose faith and abstain from disclosing their condition. It may produce a negative effect in all stakeholders—patients themselves, medical practitioners and scientific researchers. In order to avoid such situation, ref. [96] proposed blockchain-based data sharing system supported by a Genetic Algorithm (GA) [97] and Discrete Wavelet Transform (DWT) [98]. A genetic algorithm is used to optimize a queuing technique while DWT is used to enhance the security. The proposed system allows a fast verification process using a cryptography key generator, which in turn enhances a system's access control and immunity. Since all patients are known and their actions are stored in the blockchain records, this design allows further accountability. Shared queuing requests can only be accessed (allowing requests) only after a confirmation of identity and cryptographic keys. The proposed system is built over private blockchain and the blocks are defined based on Dual tree–complex wavelet transform (DT–CWT) and multiple watermarking schemes. Multiple watermarking schemes with blockchain technology to manage health records are used to enhance privacy, transparency, and security. Using the watermarking technique, the information of multiple physicians are embedded one after another and extracted in reverse order.

Ref. [99] introduces a blockchain-based health data ecosystem to manage high amount of health data. The proposed approach uses Exonum [100] (service-oriented architecture that works in a peer-to-peer manner) open source platform. System architecture is divided into two segments—open and closed. The medical data is stored in the closed segment while each patient unique identifier is stored in open segment. System nodes are divided into auditors and validators. Auditors check blockchain consistency because they own a full copy of blockchain ledger while network viability task is handled by validators. Validators are the entities responsible for generating new blocks using the BFT consensus algorithm. In Exonum, services module acts as smart contracts in the blockchain network while clients module are responsible for identifying customers typical functionality. The middleware module provides transactions with atomicity and ordering, realizes the interactions and replication of services with clients, accesses control, and has data consistency.

3.2.3. Medical Data Exchange/Delivery/Access, Platform/Architecture/Scheme

BlocHIE [101] is a healthcare information platform that uses blockchain as its base technology. In the proposed architecture, Electronic Medical Records (EMRs) and Personal Healthcare Data (PHD) are stored using EMR-Chain and PHD-Chain; which are loosely-coupled blockchains. In order to enhance the privacy, the EMR-Chain removes dependency on cloud services by combining on-chain verification and off-chain storage. BlocHIE uses the distributed databases of hospitals to ensure off-chain storage, while the hash value of medical records is used in a transaction for on-chain verification. Two fairness-based transaction packing algorithms, namely FAIR-FIRST and TP&FAIR, are proposed to improve fairness and throughput. BlocHIE employs PoW as its consensus algorithm. The proposed platform's proven practicability and effectiveness are based on authors' evaluations.

An operational concept of a blockchain-based platform that is built over NEM multi-signature blockchain contracts, tokens, and cryptography was proposed by [102]. Multi-signature contracts are utilised to control and administrate activity of a specific account, by establishing powers and rights to that specific account. Multi-signature contracts allow for using multiple keys to edit the medical data on the chain; thus, the entities that hold all the keys are allowed to edit the information, while others can only read or initiate transactions from the ledger. This method can handle key loss because trusted parties (i.e., governmental representatives) would receive another copy of the keypair. The data are not stored on the blockchain, but rather stored in a repository called a data lake. A data lake is characterized with scalability and storing various types of data. Only encrypted data are stored in the data lake; thus, the patient would still hold the right to read and access the data. This approach provides two main advantages from a patient's perspective. Firstly, it allows patients to manage and control their own medical records. Secondly, it enables cross-institutional sharing. Data can be easily shared from many types of devices such as home devices. However, some of the challenges towards implementing blockchain technology are not considered—for example, data access during emergency or acute treatment.

FHIRChain [103] proposed a decentralized app (DApp) prototype that functions under FHIRChain architecture. FHIRChain addresses the requirements of the Office of the National Coordinator for Health Information Technology (ONC), which are verifying identity and authenticating all participants, storing and exchanging data securely, having consistent permissioned access to data sources, applying consistent data formats, and maintaining modularity. FHIRChain encapsulates FL7's Fast Healthcare Interoperability Resources (FHIR) standard into the architecture for shared clinical data. This architecture uses context blockchains, off-chain storage and exchange reference pointers on-chain, token-based permission model and Model-View-Controller (MVC) pattern to provide a comprehensive solution. To create and manage health identities, public key cryptography is employed in the FHIRChain. The newly created DApp includes a registry smart contract to map between FHIRChain and patients, where digital identities are stored and maintained. DApp is able to provide scalable data integrity, increased modularity, fine-gained access control, and enhanced trust. Although FHIRChain demonstrates the potential of blockchain, it does not address semantic interoperability and may not be compatible with legacy systems that do not support FHIR standards.

To guarantee the encapsulated EHR validity in the blockchain, an attribute-based signature scheme has been proposed with multiple authorities [104] for EHR. In this approach, patients will endorse messages based on specific attributes without disclosing other information. The only parameter needed to access the messages is providing evidence to the verifier. Distributing the patient's public and private keys is done without the need for a central or single authority. Multiple authorities are responsible for this task. This conforms to distributed data storage mode in the blockchain, which can avoid escrow problems. Patients' information such as insurance records, consumption records, and EHRs is encapsulated in a single block when treatment is finished. When a patient goes to another healthcare service provider, the new entity needs to identify the patient and authenticate his available blockchain.

3.2.4. Mobile Application Architecture

Healthcare Data Gateways (HDG) [105] is a blockchain-based smartphone application that allows patients to manage and control their own medical records though a purpose centric access model to preserve patients' privacy. This model organizes healthcare data through a simple and unified Indicator Centric Schema (ICS). The proposed application combines a traditional database with a gateway to manage the medical data on blockchain storage system, evaluate data access requests, and utilize secure multi-party computation for further processing. HDG consists of three layers: the storage layer (lower layer), data management layer, and data usage layer (upper layer). To secure and protect the data, cryptographic techniques such as signatures, hashes, and encryption are used. Data gateways are a hybrid design of database and firewall concepts. HDG offers anonymization, efficient communication between HDGs, and data backup and recovery (using the cloud). However, one issue using HDG is how to process and compute the data while keeping the data private. It can be implemented using the MPC (Secure Multi-Party Computation) technique, a solution that can enable untrusted third-party to conduct computation over patient's data without breaching privacy trust.

A blockchain-based mobile application is designed to manage healthcare data [106]. It collects data from patients in a secure manner, then synchronizes it with cloud services and shares the data with healthcare entities and insurance providers. Cloud security is the main area that many previous works have examined and evaluated for the implementation of blockchain technology in it. However, this work provides health data sharing solutions through an innovative user-centric model. The designed application uses membership service (supported by blockchain) and a channel formation scheme to enhance identity management service and privacy protection by utilizing permissioned blockchain characteristics. Medical devices, manual input, and wearable devices are used to collect patient information using the designed mobile application. The data are shared with healthcare institutions by synchronizing them with a cloud database. Proof of integrity and validation are permanently retrievable to ensure health data integrity. Batching and tree-based data processing methods are used to ensure scalable and performance stability and handle a large amount of medical data uploaded and collected by the mobile platform.

DApp for Smart Health (DASH) [107] was proposed to allow patients to access, edit their medical records, and submit prescription requests using a web-based portal. It uses Patient Registry contract to map patient's unique identifiers and associated Patient Account contract addresses. They included multiple software pattern designs to address their challenges; abstract factory for evolvability, flyweight for data storage, proxy for secure and private data services, and publish–subscribe for scalable information filtering. The architecture design is meant to address privacy, storage, and scalability issue.

3.2.5. PSN-Based Healthcare System

Blockchain can also be implemented in Pervasive Social Network (PSN) based healthcare [70]. PSN is a system that contains a large number of medical sensors and mobile devices. [70] contributed to enhancement of two protocols. The first is enhancing the IEEE 802.15.6 version for authentication and association to address the computational requirements for resource-limited devices through establishing secure links between them in Wireless Body Area Networks (WBANs). The second protocol is a blockchain-based protocol to allow sharing medical information among PSN devices. The proposed system stores the blockchain only in specific nodes that are powerful. The proposed system was implemented using a Raspberry Pi and laptop based on a case study. Network consensus is realized by contributors of health data, and the address of each contributor is stored and shared in the designed healthcare blockchain. The address of other nodes is used to access the health data only by authorized PSN nodes. The proposed system works in the following manner: a patient presses a button installed on his sensor device to create secure links with his smartphone. The process of adding data to the blockchain is done automatically via smartphone, and the data is stored and broadcasted as a transaction to the neighbor PSN nodes (miners). Generating a new block is also done automatically

through multiple steps. Finally, an authorized person can request to view the data of the patient to create an accurate plan of treatment remotely.

The proposed design provides authentication of messages and communication across the network, confidentiality of generated secret keys, forward secrecy of the master key, and integrity of transactions. It reduces computational burden on sensor devices, and data leakage caused by the illegal acts of various parties. This is more of a cryptography point of view approach, where they focus on two main points: computational power and energy consumption. The proposed system does not fully explore the benefits of the blockchain, it has not been evaluated for large-scale environments and is designed to address challenges in PSN networks only, which is considered unsuitable for other types of implementations. Furthermore, smart contracts are one of the main points of using blockchain in healthcare, which is not included in the proposed system.

3.2.6. Privacy Preserving Platform/Framework

Medibchain [74] is a patient centric blockchain-based data management system. This system addresses storage and losing control issues using blockchain technology to encrypt health data as decentralized storage. Medibchain allows patients to have a full control over their medical data to provide pseudonymity. Data is stored on the blockchain to achieve security, integrity, and accountability. Cryptographic functions are employed to provide immutability and eliminate data protection vulnerabilities. The proposed system is divided into two levels: the first level contains a Registration Unit where the authentication is done, Private Accessible Unit (PAU) that acts as an intermediary between users and blockchain, and Graphical User Interface (GUI) for the user to interact with the system. The second level represents the system backend (the permissioned blockchain) which contains the low-level elements of the proposed system.

ModelChain [108] is a new blockchain-based framework designed for distributed privacy-preserving healthcare predictive modeling. It aims to increase network security and robustness of such modeling using blockchain technology. It also utilizes transaction metadata for model dissemination by integrating blockchains with machine learning. Since using blockchain technology in healthcare domain accelerates healthcare research, ModelChain makes use of Blockchain's characteristics to increase privacy-preserving predictive model's security and robustness among healthcare entities. This is because ModelChain disseminates predictive models. Thus, network transparency is not a critical issue. To determine the order of blockchain-based online machine learning and increase the efficiency and accuracy, a new proof-of-information algorithm is developed. This algorithm is designed over POW consensus protocol. The proof-of-information algorithm follows a concept called Boosting; the site that contains the information must have a higher priority than other sites since it cannot be predicted by partial model accurately. Thus, it must be selected as the next model-updating site.

Ancile [109] is a privacy-preserving framework proposed to offer efficient access, interoperability, and security for medical records for third parties, providers, and patients. The proposed framework focuses on preserving patient's privacy and security using cryptographic techniques and allows access control and obfuscation of data by utilizing Ethereum-based blockchain and smart contracts. They use six types of smart contracts to optimize patient's experience, minimizing any interaction between contracts and patients, and reduce privacy threats. These implemented smart contracts allow patients to manage control their own medical records. The integrity of HER databases is confirmed using query links and cryptographic hashes. The concept of Ancile was analysed and compared in terms of addressing security and privacy concerns, and interaction processes with different system entities.

Ref. [110] implemented a privacy preserving approach based on Personal Health Information (PHI) sharing (BSPP) scheme and blockchain technology to improve diagnosis in e-Health Systems. The proposed design employs two kinds of blockchains: private and consortium. Secure indexes of PHI are tracked using the consortium blockchain while the private blockchain stores the PHI. The public key is used to encrypt all data including PHI with keyword search to achieve secure search, privacy preservation, access control, and data security. System availability is guaranteed by requiring

block generators to provide proof of conformance when adding new blocks. System entities are users, medical service providers, and system manager, which keeps public key tree and generates system parameters. The system provides access control, data auditing, privacy preservation, secure search, and time controlled revocation. However, there are some issues related to modifying the URL. Since blockchain only stores the records, the location of data might be changed; thus, the old URL cannot be modified and a new URL must be generated. Furthermore, a new block is taken by the data sharing session because there is no reclaim of space after a sharing. Advantages and limitations of the existing work are discussed in Table 2.

Table 2. Advantages and limitations of related work.

Advantages	Limitations
Data Sharing Network/System [80–83]	
Ref. [80] provide high network security. Ref. [81] is lightweight, scalable, and provides efficiency, identity management and distant access.	Ref. [80] does not insert actual records in the block, and searchability, discoverability, and data access control mechanisms are required. Algorithms between entities and authentication and communication protocols were not investigated in ref. [81].
Record Management System [67,68,90–96]	
Ref. [90,91] provides easy access, immutable log, and comprehensive services. It also avoids single point of failure. Ref. [92] delegates data management to patients; thus, patients have full control over their, medical records. Ref. [93] provides efficient access and retrieval, eliminates network congestion, high information security. Ref. [68] ensures data provenancing, security, auditability, and user verification. It provides distant access and data access revocation. Ref. [94] reduces sharing time and overall cost while improving decision making. Ref. [95] maintains comprehensive patient records and provides a holistic perspective of patient's condition. Ref. [96] enhances overall security and access control, allows fast verification process and further accountability.	Ref. [90,91] does not consider contract encryption, auditability, obfuscation, and scalability. The design needs to be extended for complex scenarios regarding healthcare data. In ref. [92], problem may occurs if user is not tech-savvy, or a user's private key is lost, which might result in data loss or compromise. Ref. [93] reduces the concept of decentralization since they are stored in local databases. Ref. [68] neglected data disclosure concerns. Ref. [94] is lack of efficient storage mechanism. In ref. [96], the system can be controlled for greater expandability. This would help augment system resources and enhance the security.
Medical Data Exchange/Delivery/Access, Platform/Architecture/Scheme [101–104]	
Ref. [101] ensures off-chain storage, on-chain verification. Proved practicability and effectiveness. In ref. [102], patients have full control, allows cross-intuitional sharing. Ref. [104] provides unforgeability, high security, and perfect privacy.	In ref. [102], lack of access during emergency situation. In ref. [103], semantic interoperability is not addressed, compatibility issue with legacy systems, cannot control clinical malpractice and cost of DApp deployment. In ref. [104], when number of users increase, cost increases and the amount of medical data become large.
Application Architecture to Manage Health Records [105–107]	
Ref. [105] provides anonymization, efficient communication between HDGs and data backup and recovery using cloud. Ref. [106] ensure scalability and performance stability, and handle the large amount of medical data. Ref. [107] maintains system evolvability, data storage requirements, scalability, and balancing interoperability with privacy concerns.	Ref. [105] is unable to process data and performs computations without revealing the data. In ref. [106], the system can also be extended to accommodate the usage of health data for research purposes.
PSN-Based Healthcare System [70]	
It provides message authentication, secret keys confidentiality, secrecy of master key, and integrity of transactions. It eliminates computational burden and data leakage.	Does not explore the benefits of the blockchain (no smart contracts), it is not evaluated for large-scale environments and it is designed to address challenges in PSN networks only.
Privacy Preserving Platform/Framework [74,108,109]	
Ref. [108] adopts permissioned blockchain networks, malicious nodes could not arbitrarily participate in the network, and therefore the risk of a 51% attack is minimal. ModelChain framework utilizes a private blockchain to enable multiple institutions to contribute health data to train a machine-learning model without disclosing their individual health records.	In ref. [74], flaws in encryption algorithms or software implementations may expose the data contents. Ref. [108] requires further security improvement through encrypting transaction metadata and using Virtual Private Network (VPN). Ref. [109] consumes computational power due to high number of used smart contracts. Need to look for methods to effectively search smart contracts with large local databases or to eliminate the needs of 850 for global smart contracts.

4. Case Study in Healthcare Domain

In this section, we will introduce an approach to integrate blockchain technology with the healthcare domain. This design was developed based on our analysis from other designs' drawbacks and limitations to create a comprehensive approach. Our approach addresses the issue of privacy, security, interoperability, scalability and regularity. This approach is proposed to respond to related questions when designing a blockchain-based healthcare approach. For example:

- How authenticated parties can access and retrieve healthcare data from healthcare institutions while preserving patients' privacy
- How to ensure security of interaction between patients and the system
- How to eliminate legal and regulatory sanctions and unethical use of data when exchanging healthcare information
- How patients can access various types of data from multiple healthcare organizations using a single system.

Some of the existing work proposed complex methods for validation and authentication, which adds additional overload to the system and it is not user-friendly.

There are three main considerations in the case study, namely the blockchain network, consensus algorithm, and system design. In addition to using our blockchain network to store all logs of records of medical information when transactions are executed and grouped into blocks, it will also be used to store additional information such as requests, policies, and states of data to ensure privacy and regularity. The blockchain type that will be used in our approach is permissioned blockchain because it allows certain access control for specific identifiable participants. Using permissioned blockchain enhances network performance and security while reducing the cost and workload process for nodes that are not participating in the mining process and performs the necessary computations only for a specific application. Each transaction represents a relationship between organizational entity and a patient. It holds an identifiable number designed to be searched by the patient using mobile application. The design of our blockchain network is illustrated in Figure 6.

Cryptographic algorithms are used to ensure integrity, confidentiality, and security of data. ECC is used to encrypt the private data. This is because the algorithm employs shorter encryption keys; thus, it ensures high speed data transfer and uses less computing power as compared to other first generation algorithms. In addition, ECC is used to support cloud storage by assigning a pointer to access the data each time an authorized entity requests them. Using ECC might limit the searchability of data. As such, an identifiable number is used to address this issue. The data must be decrypted prior to the searching process; thus, exchanging public keys is an important parameter to be considered. Finding data in cloud storage includes downloading, decrypting, and searching procedures. An access control model will be created to ensure that regulation, accessing time, and cost issues are addressed. However, access control model is an effective solution for external attacks, it cannot detect internal attacks. Enhancing the access model by integrating cryptographic primitives using attribute-based encryption [73] can detect internal attacks.

The choice of consensus algorithm is one of the most important parameters to build a blockchain-based system that provides optimal performance and guarantee regularity requirements. Regularity is important because some implementations offers patients' data as rewards when adding a block to the blockchain. However, this is a serious issue that needs to be addressed because it it is illegal under HIPAA. As such, the case study concluded that the PoW algorithm should not be used. Instead, QuorumChain consensus can be used because the algorithm helps to decide the next block to be added. QuorumChain achieves consensus through a method called majority-based voting. In order to determine the next block, smart contracts are implemented in this algorithm and executed to track and identify votes from eligible nodes. The voting process on the next block starts when a possible block is found. A threshold value is chosen to compare the number of votes. If the number of votes exceeds the specified threshold, the block is appended to the blockchain. Using the threshold value

eliminates the possibility of adding multiple blocks that exist in the transactions. In addition, timeout sessions can be used to avoid creating identical blocks by multiple miners. To reduce the workload on the blockchain network, specific nodes will be responsible for the voting process, thus delegating the process of adding blocks to a specific number of nodes.

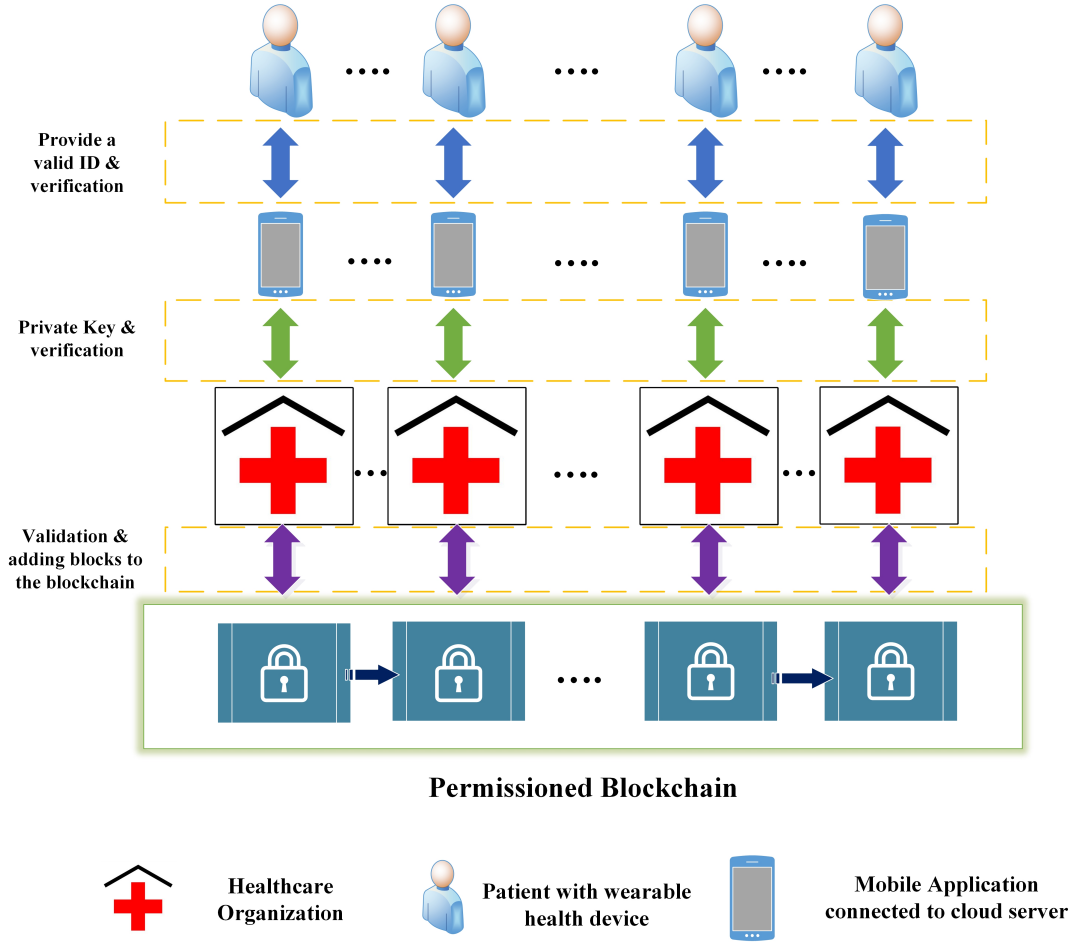

Figure 6. Blockchain network of the proposed design.

Since IoT devices can be used to obtain patient's health information, it is important to use a consensus algorithm that reduces the energy consumption to fit sensing devices' requirements. The case study proposed to integrate the Practical Byzantine Fault Tolerance (BFT) algorithm with IoT devices because it does not require high hashing power. The PBFT algorithm will be responsible for authentication through generating public and private keys for each node. It also provides a verification process by verifying the format of messages based on network agreement. It provides a low-latency storage system with sufficient throughput to support the proposed design. PBFT is suitable because it is important to provide a fast and efficient consensus convergence to allow fast transaction processing.

The design of our approach uses a multi-layer model, namely authentication layer and access layer. These layers are responsible for authentication, verification, validation, and access control. The first layer will check the information, and when the information is authenticated and verified, it is transmitted to the second layer through a secured channel. The second layer disseminates the information through the blockchain network since it is the only entity connected to the blockchain to provide an overall security through the network. Specific parameters are assigned to control network access. Smart contracts are implemented to control these parameters and handle the flow of information. Unlike other existing work, in this design, each user gets a private identification and password to ensure authorization. The received data is not sent directly to the requester. It is

converted to a 256-bit hash to allow the smart contracts to compare and verify the data to ensure that the information is not manipulated.

Common Device Metadata (CDM) for wearable sensing devices are used to aggregate data. To ensure the security and privacy of transactions, smart contracts will be built to connect the platform with smartphone applications. When wearable devices obtain data from the user, the authentication process also kicks in using smart contracts. After the data is collected, the system will incorporate it into a block to be added to the blockchain. The data are stored in cloud storage to be further processed. The process of sharing the data with healthcare institutions is handled by the users themselves when a notification is sent to their mobile phone via the designed application.

The logical execution flow is shown in Figure 7. The wearable device obtained the user's data. These data are transferred through the sensing (smart device) device to a main contract that handles data processing in order to transfer to a specific contract related to certain operation. This process between the user and the main contract is done via the authentication layer, which contains software patterns to translate the data to the sensing device. A specific contract located in the access layer directly interacts with the blockchain by adding new data. At the same time, this contract analyzes the data to check the whether these data have the correct attributes to be added to the blockchain. At this point, if an emergency case (based on certain policies in smart contracts) has occurred, the smart device will send an alert directly to the hospital to ensure patient safety.

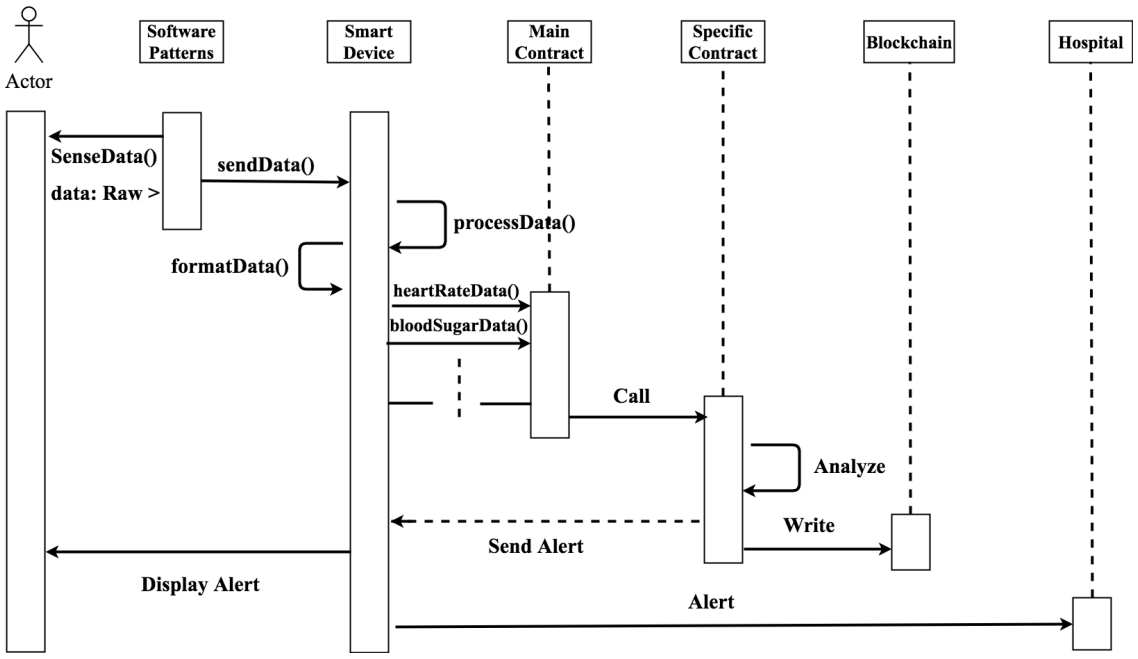

Figure 7. The logical execution flow of wearable device virtualization [111].

A smartphone application will interact with the cloud server using blockchain technology to protect patient's data collected from laboratories and wearable device to avoid any tampering or counterfeiting attempts. The application runs on a hyperledger along with the proposed platform. Performance of the decentralized secure platform and application will be evaluated and validated during the implementation procedure based on their interoperability capabilities, storage handling ability, security, and transaction speed. The workflow of the proposed blockchain-based healthcare application is shown in Figure 8. The smartphone application requests the ID and password of the user to authorize access to medical data. When sending information, ECC is used to encrypt the data. When another entity requests the data, a valid ID and password along with the correct cryptographic keys must be provided in order to make the request and access the data as shown in Figure 8. All IDs and passwords are stored in a patient registry database handled by the smart contracts. A tree-based

batching and processing method is included to provide scalable and performance considerations and handle large data sets uploaded by the mobile application.

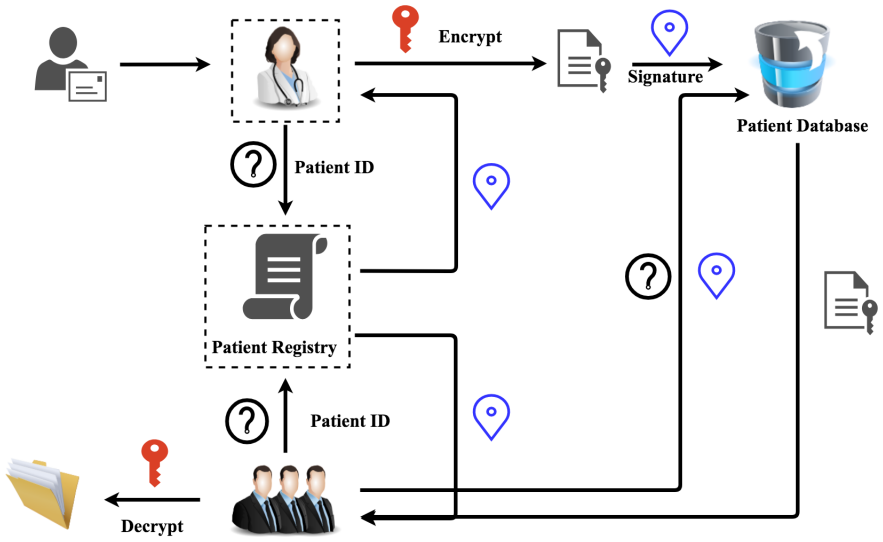

Figure 8. Blockchain-based healthcare application workflow [112].

5. Conclusions

Information and communication technology play an important role in today's world. However, the healthcare domain faces many problems due to a lack of patient-centric approaches, inability to connect disparate systems, poor interoperability between systems, and Electronic Healthcare Record (EHR) accuracy. In recent years, attention has grown towards using the blockchain in healthcare. Blockchain shows tremendous potential in the healthcare domain because it resolves issues related to medical records while providing privacy, security, interoperability, validation, and authentication. Blockchain offers solutions to real current issues such as unreported clinical trials, healthcare data breaches, and misleading data errors. In this paper, a systematic review of various consensus algorithms related to healthcare and existing work has been conducted. This paper highlights their basic ideas and challenges. Based on the systematic review, a case study that integrates blockchain into healthcare is proposed to address research gaps from existing work.

Author Contributions: The authors of this article have contributed in building this research paper as follows: Writing and preparation, H.D.Z.; Review and visualization, Y.-W.C., K.K. and S.K.; Editing and revision, Y.-W.C. and S.M.H.

Funding: This research is supported by Research University Grant (RUI) Universiti Sains Malaysia (USM) No: 1001/PNAV/8014078 and Publication Fund under Research Creativity and Management Office, Universiti Sains Malaysia.

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

References

1. Joshi, A.P.; Han, M.; Wang, Y. A Survey on Security and Privacy Issues of Blockchain Technology. *Math. Found. Comput.* **2018**, *1*, 121–147. [CrossRef]
2. Ji, S.; Cai, Z.; Han, M.; Beyah, R. Whitespace measurement and virtual backbone construction for Cognitive Radio Networks: From the social perspective. In Proceedings of the 2015 12th Annual IEEE International Conference on Sensing, Communication and Networking, SECON 2015, Seattle, WA, USA, 22–25 June 2015; pp. 435–443.
3. Han, M.; Yan, M.; Li, J.; Ji, S.; Li, Y. Generating uncertain networks based on historical network snapshots. *Lect. Notes Comput. Sci.* **2013**, *7936*, 747–758.

4. Duan, Z.; Yan, M.; Cai, Z.; Wang, X.; Han, M.; Li, Y. Truthful incentive mechanisms for social cost minimization in mobile crowdsourcing systems. *Sensors* **2016**, *16*, 481. [CrossRef] [PubMed]
5. Kostakis, V.; Giotitsas, C. The (A)political economy of bitcoin. *TripleC* **2014**, *12*, 431–440.
6. Efanov, D.; Roschin, P. The all-pervasiveness of the blockchain technology. *Procedia Comput. Sci.* **2018**, *123*, 116–121. [CrossRef]
7. Buterin, V. A *Next-Generation Smart Contract and Decentralized Application Platform*; Ethereum White Paper; 2014. Available online: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed on 15 June 2018).
8. Ethereum Community. A Next Generation Smart Contract and Decentralized Application Platform. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 1 April 2018).
9. Underwood, S. Blockchain beyond bitcoin, Commun. *ACM* **2016**, *59*, 15–17. [CrossRef]
10. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain Challenges and Opportunities: A Survey. *Int. J. Web Grid Serv.* **2016**. [CrossRef]
11. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [CrossRef] [PubMed]
12. Akins, B.W.; Chapman, J.L.; Gordon, J.M. A Whole New World: Income Tax Considerations of the Bitcoin Economy. *Pittsburgh Tax Rev.* **2015**, *12*, 24–56. [CrossRef]
13. Sharples, M.; Domingue, J. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In *Adaptive and Adaptable Learning*; Springer: Cham, Switzerland, 2016; pp. 490–496.
14. Zhang, Y.; Wen, J. An IoT electric business model based on the protocol of Bitcoin. In Proceedings of the 2015 18th Intternational Conference on Intelligence in Next Generation Networks, ICIN 2015, Paris, France, 17–19 February 2015; pp. 184–191.
15. Noyes, C. BitAV: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning. *arXiv* **2016**, arXiv:1601.01405.
16. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the 37th IEEE Symposium on Security and Privacy, San Jose, CA, USA, 23–25 May 2016; pp. 839–858.
17. Crosby, M.; Nachiappan; Pattanayak, P.; Verma, S.; Kalyanaraman, V. BlockChain Technology: Beyond Bitcoin. *Appl. Innov. Rev.* **2016**, *2*, 71.
18. Ren, L. *Proof of Stake Velocity: Building the Social Currency of the Digital Age*; Self-Published White Paper; 2014. Available online: https://www.reddcoin.com/papers/PoSV.pdf (accessed on 22 July 2018).
19. Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inf. Assoc.* **2017**, *24*, 1211–1220. [CrossRef] [PubMed]
20. Kumar, T.; Ramani, V.; Ahmad, I.; Braeken, A.; Harjula, E.; Ylianttila, M. Blockchain Utilization in Healthcare: Key Requirements and Challenges. In Proceedings of the IEEE 20th International Conference on e-Health Networking, Applications and Services, Ostrava, Czech Republic, 17–20 September 2018.
21. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media Inc: Sevastopol, CA, USA, 2015.
22. McGhin, T.; Choo, R.; Liu, C.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [CrossRef]
23. Tama, B.A.; Kweka, B.J.; Park, Y.; Rhee, K.H. A critical review of blockchain and its current applications. In Proceedings of the 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), Palembang, Indonesia, 22–23 August 2017; pp. 109–113.
24. Drescher, D. *Blockchain Basics: A Non-Technical Introduction in 25 Steps*; Apress: New York, NY, USA, 2017.
25. Rutland, E. Blockchain Byte. Available online: https://docplayer.net/57510249-Blockchain-byte-r3-research-emily-rutland-the-blockchain-byte-features-a-question-from-the-distributed-ledger-space.html (accessed on 15 September 2018).
26. Holbl, M.; Kompara, M.; Kamisali, A. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
27. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.* **1982**, *4*, 382–401. [CrossRef]
28. Merkle, R.C. A Digital Signature Based on a Conventional Encryption Function. In *Advances in Cryptology—CRYPTO 1987*; Lecture Notes in Computer Science 293; Springer: Berlin/Heidelberg, German, 1988; pp. 369–378.

29. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: www.Bitcoin.Org (accessed on 30 May 2018).
30. Larimer, D. Transactions as Proof of Stake. Available online: https://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf (accessed on 30 May 2018).
31. O'Dwyer, K.J.; Malone, D. Bitcoin Mining and its Energy Footprint. In Proceedings of the 25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies, Limerick, Ireland, 26–27 June 2014.
32. Gervais, A.; Karame, G.O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the security and performance of proof of work blockchains. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), Vienna, Austria, 24–28 October 2016; pp. 3–16.
33. Chuen, D.L.K. (Ed.) *Handbook Of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*; Academic Press: Cambridge, MA, USA, 2015.
34. Sultan, K.; Ruhi, U.; Lakhani, R. Conceptualizing Blockchains: Characteristics and Applications. In Proceedings of the 11th IADIS International Conference on Information Systems 2018, Lisbon, Portugal, 14–16 April 2018; pp. 49–57.
35. Bitcoin Project. nBits, Target Threshold. Available online: https://bitcoin.org/en/glossary/nbits (accessed on 8 September 2018).
36. Norberhuis, S.D. MultiChain: A Cybercurrency for Cooperation. Master's Thesis, Delft University of Technology, Delft, The Netherlands, 2015.
37. Burgess, K.; Colangelo, J. *The Promise of Bitcoin and the Blockchain*; Consumers' Research: Washington, DC, USA, 2015.
38. Nomura Research Institute. *Survey on Blockchain Technologies and Related Services*; FY2015 Report. Available online: https://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf (accessed on 15 September 2018).
39. Johnson, D.; Menezes, A.; Vanstone, S. The Elliptic Curve Digital Signatur e Algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63. [CrossRef]
40. Kim, S.K.; Kim, U.M.; Huh, J.H. A Study to Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security. *Energies* **2019**, *12*, 402. [CrossRef]
41. C. Team. CONIKS. Available online: https://coniks.cs.princeton.edu (accessed on 16 December 2018).
42. Liu, B.; Yu, X.L.; Chen, S.; Xu, X.; Zhu, L. Blockchain Based Data Integrity Service Framework for IoT Data. In Proceedings of the 2017 IEEE 24th IEEE International Conference on Web Services ICWS 2017, Honolulu, HI, USA, 25–30 June 2017; pp. 468–475.
43. Xu, J.J. Are blockchains immune to all malicious attacks? *Financ. Innov.* **2016**, *2*, 25. [CrossRef]
44. Cai, Y.; Zhu, D. Fraud detections for online businesses: a perspective from blockchain technology. *Financ. Innov.* **2016**, *2*, 20. [CrossRef]
45. Karame, G.O.; Androulaki, E. Double-Spending Fast Payments in Bitcoin. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, NC, USA, 16–18 October 2012; pp. 906–917.
46. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE 6th International Congress on Big Data: BigData Congress, Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
47. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2017**. [CrossRef]
48. Larimer, D. Delegated Proof of Stake. Available online: https://en.bitcoinwiki.org/wiki/DPoS (accessed on 10 January 2019).
49. Bentov, I.; Lee, C.; Mizrahi, A.; Rosenfeld, M. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. In *SIGMETRICS Performance Evaluation Reviews*; ACM: New York, NY, USA, 2014.
50. Vukolic, M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. *Lect. Notes Comput. Sci.* **2016**, *9591*, 112–125.
51. Kotla, R.; Alvisi, L.; Dahlin, M.; Clement, A.; Wong, E. Zyzzyva: Speculative byzantine fault tolerance. *ACM Trans. Comput. Syst.* **2009**, *27*, 1–39. [CrossRef]
52. Copeland, C.; Zhong, H. Tangaroa: A Byzantine Fault Tolerant Raft. Available online: http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf (accessed on 10 January 2019).
53. Parity Technologies. Proof of Authority Chains (PoA), 2017. Available online: https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains (accessed on 12 January 2019).

54. P4Titan. Slimcoin: A Peer-To-Peer Crypto-Currency with Proof-of-Burn. Available online: http://www.doc.ic.ac.uk/~ids/realdotdot/crypto_papers_etc_worth_reading/proof_of_burn/slimcoin_whitepaper.pdf (accessed on 21 January 2019).
55. Borge, M.; Kokoris-Kogias, E.; Jovanovic, P.; Gasser, L.; Gailly, N.; Ford, B. Proof-of-personhood: Redemocratizing permissionless cryptocurrencies. In Proceedings of the 2nd IEEE European Symposium on Security and Privacy, Paris, France, 26–28 April 2017; pp. 23–26.
56. Ghosh, M.; Richardson, M. A TorPath to TorCoin: Proof-of-Bandwidth Altcoins for Compensating Relays. In Proceedings of the HotPETs'14: 7th Workshop on Hot Topics in Privacy Enhancing Technologies. 2014. Available online: http://dedis.cs.yale.edu/dissent/papers/hotpets14-torpath-abs/ (accessed on 12 January 2019).
57. Intel. Proof of Elapsed Time (PoET), 2017. Available online: http://intelledger.github.io/ (accessed on 18 January 2019).
58. Mazieres, D. The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus, 2015. Available online: https://www.stellar.org/papers/stellar-consensus-protocol.pdf (accessed on 18 January 2019).
59. Metropolitana, Z.; Le, N.; California, B.; Ju, C.; Ta, C.I. Bitcoin-NG: A Scalable Blockchain Protocol. In Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, CA, USA, 16–18 March 2016.
60. Cachin, C.; Schubert, S.; Vukolic, M. Non-determinism in Byzantine Fault-Tolerant Replication. In Proceedings of the Int. Conf. Princ. Distrib. Syst. (OPODIS 2016), Madrid, Spain, 13–16 December 2016; pp. 1–20.
61. Schwartz, D.; Youngs, N.; Britto, A. *The Ripple Protocol Consensus Algorithm*; Ripple Labs Inc White Papper; 2014. Available online: https://ripple.com/files/ripple_consensus_whitepaper.pdf (accessed on 18 January 2019).
62. Kwon, J. TenderMint: Consensus without Mining; 2014. Available online: https://www.weusecoins.com/assets/pdf/library/Tendermint%20Consensus%20without%20Mining.pdf (accessed on 18 January 2019).
63. Kim, S.K.; Huh, J.H. A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective. *Energies* **2018**, *11*, 1973. [CrossRef]
64. Ongaro, D.; Ousterhout, J. In search of an Undstandable Consensus Algorithm. In Proceedings of the 2014 USENIX Annual Technical Conference, Philadelphia, PA, USA, 19–20 June 2014; Volume 37, pp. 1–16.
65. Rivest, Y.H.; Shamir, R.L.; Tauman, A. How to Leak a Secret. In Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, 9–13 December 2001; pp. 552–565.
66. Syta, E.; Tamas, I.; Visher, D.; Wolinsky, D.I.; Jovanovic, P.; Gasser, L.; Gailly, N.; Khoffi, I.; Ford, B. Keeping Authorities 'Honest or Bust' with Decentralized Witness Cosigning. In Proceedings of the 37th IEEE Symposium on Security and Privacy, San Jose, CA, USA, 23–25 May 2016.
67. Saravanan, M.; Shubha, R.; Marks, A.M.; Iyer, V. SMEAD: A secured mobile enabled assisting device for diabetics monitoring. In Proceedings of the 11th IEEE International Conference on Advanced Networks and Telecommunications Systems 2017, Odisha, India, 17–20 December 2017; pp. 1–6.
68. 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]
69. Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain technology: applications in health care, Circulation: Cardiovascular Quality and Outcomes. *arXiv* **2017**, arXiv:1706.03700.
70. Zhang, J.; Xue, N.; Huang, X. A secure system for pervasive social network-based healthcare. *IEEE Access* **2016**, *4*, 9239–9250. [CrossRef]
71. Rabah, K. Challenges & opportunities for blockchain powered healthcare systems: A review. *Mara Res. J. Med. Health* **2017**, *1*, 45–52.
72. Esposito, C.; Santis, A.D.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
73. Raseena, M.; Harikrishnan, G.R. Secure Sharing Of Personal Health Records in Cloud Computing Using Attribute-Based Broadcast Encryption. *Int. J. Sci. Eng. Res.* **2013**, *1*, 323–325.
74. Omar, A.A.; Rahman, M.S.; Kiyomoto, A.B. MediBchain A Blockchain Based Privacy Preserving Platform for Healthcare Data. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Guangzhou, China, 12–15 December 2017.

75. Karame, G.O.; Roeschlin, M.; Gervais, A.; Capkun, S.; Androulaki, E.; Čapkun, S. Misbehavior in Bitcoin: A Study of Double-Spending and Accountability. *ACM Trans. Inf. Syst. Secur.* **2015**, *18*, 2. [CrossRef]
76. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef] [PubMed]
77. Giardina, T.D.; Menon, S.; Parrish, D.E.; Sittig, D.F.; Singh, H. Patient access to medical records and healthcare outcomes: a systematic review. *J. Am. Med. Inform. Assoc.* **2013**, *21*, 737–741. [CrossRef] [PubMed]
78. Engelhardt, M.A. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technol. Innov. Manag. Rev.* **2017**, *7*, 22–34. [CrossRef]
79. Kuo, T.T.; Rojas, H.Z.; Ohno-Machado, L. Comparison of blockchain platforms: A systematic review and healthcare examples. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 462–478. [CrossRef] [PubMed]
80. Peterson, K.; Deeduvanu, R.; Kanjamala, P.; Boles, K. A Blockchain-Based Approach to Health Information Exchange Networks. *Proc. NIST Workshop Blockchain Healthc.* **2016**, *1*, 1–10.
81. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information* **2017**, *8*, 44. [CrossRef]
82. Theodouli, A.; Arakliotis, S.; Moschou, K.; Votis, K. On the design of a Blockchain-based system to facilitate Healthcare Data Sharing. In Proceedings of the 12th IEEE International Conference On Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018.
83. Mcfarlane, C.; Beer, M.; Brown, J.; Prendergast, N. *Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.0*; Entrust Inc.: Addison, TX, USA, 2017.
84. Amofa, S.; Sifah, E.B.; Kwame, O.B.; Abla, S.; Xia, Q.; Gee, J.C.; Gao, J. A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data. In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018.
85. Zheng, X.; Mukkamala, R.R.; Vatrapu, R.; Ordieres-Mere, J. Blockchain-based personal health data sharing system using cloud storage. In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018.
86. Daemen, J.; Rijmen, V. *The design of Rijndael: AES-The Advanced Encryption Standard*; Springer Science and Business Media: Berlin/Heidelberg, Germany, 2013.
87. Desmedt, Y. Threshold cryptosystems. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security 1992, QLD, Australia, 13–16 December 1992; pp. 1–14.
88. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
89. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
90. 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 Big Data, OBD 2016, Vienna, Austria, 22–24 August 2016; pp. 25–30.
91. Ekblaw, A.; Azaria, A.; Halamka, J.D.; Lippman, A. A Case Study for Blockchain in Healthcare: 'MedRec' prototype for electronic health records and medical research data. In Proceedings of the IEEE BigData 2016: IEEE International Conference on Big Data, Washington, DC, USA, 5–8 December 2016.
92. Conceiçao, A.F.; da Silva, F.S.C.; Rocha, V.; Locoro, A.; Barguil, J.M. Eletronic Health Records using Blockchain Technology. *arXiv* **2018**, arXiv:1804.10078
93. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *J. Med. Syst.* **2018**, *42*, 1–11. [CrossRef] [PubMed]
94. Dubovitskaya, A.; Xu, Z.; Ryu, S.; Schumacher, M.; Wang, F. Secure and Trustable Electronic Medical Records Sharing using Blockchain. *Am. Med. Inf. Assoc.* **2018**, *2017*, 650–659.
95. Salahuddin, M.A.; Al-Fuqaha, A.; Guizani, M.; Shuaib, K.; Sallabi, F. Softwarization of internet of things infrastructure for secure and smart healthcare. *IEEE Comput. Mag.* **2017**, *50*, 74–79. [CrossRef]
96. Hussein, A.F.; ArunKumar, N.; Ramirez-Gonzalez, G.; Abdulhay, E.; Tavares, J.M.R.S.; de Albuquerque, V.H.C. A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform. *Cogn. Syst. Res.* **2018**, *52*, 1–11. [CrossRef]
97. Holland, J.H. *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence*; MIT Press: Cambridge, MA, USA, 1992.

98. Shensa, M.J. The discrete wavelet transform: Wedding the a trous and Mallat algorithms. *IEEE Trans. Signal Process.* **1992**, *40*, 2464–2482. [CrossRef]
99. Kotsiuba, I.; Velvkzhanin, A.; Yanovich, Y.; Bandurova, I.S.; Dyachenko, Y.; Zhygulin, V. Decentralized e-Health Architecture for Boosting Healthcare Analytics. In Proceedings of the 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), Lodon, UK, 30–31 October 2018; pp. 113–118.
100. What Is Exonum? Available online: https://exonum.com/doc/getstarted/what-is-exonum/ (accessed on 19 January 2019).
101. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. Blochie: A blockchain-based platform for healthcare information exchange. In Proceedings of the SMARTCOMP 2018: The 4th IEEE International Conference on Smart Computing, Sicily, Italy, 18–20 June 2018; pp. 49–56.
102. Cichosz, S.L.; Stausholm, M.N.; Kronborg, T.; Vestergaard, P.; Hejlesen, O. How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept. *J. Diabetes Sci. Technol.* **2018**, *13*, 248–253. [CrossRef]
103. 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]
104. Guo, R.; Shi, H.; Zhao, Q.; Zheng, D. Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems. *IEEE Access* **2018**, *6*, 11676–11686. [CrossRef]
105. 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]
106. 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 PIMRC 2017: 28th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Montreal, QC, Canada, 8–13 October 2017.
107. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G. Design of Blockchain-Based Apps Using Familiar Software Patterns to Address Interoperability Challenges in Healthcare; 2015. Available online: https://www.dre.vanderbilt.edu/~schmidt/PDF/PLoP-2017-blockchain.pdf (accessed on 20 November 2018).
108. Kuo, T.; Ohno-Nachado, L. ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. *arXiv* **2018**, arXiv:1802.01746.
109. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]
110. Zhang, A.; Lin, X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J. Med. Syst.* **2018**, *42*, 140. [CrossRef] [PubMed]
111. 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] [PubMed]
112. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G. Applying Software Patterns to Address Interoperability in Blockchain-based Healthcare Apps. *arXiv* **2017**, arXiv:1706.03700.