big data and cognitive computing

MDPI

Article

ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain

Pratik Thantharate [1,†] and Anurag Thantharate [2,*,†]

[1] Independent Researcher, Jersey City, NJ 07304, USA
[2] School of Computing and Engineering, University of Missouri, Kansas City, MO 64112, USA
* Correspondence: adtmv7@mail.umkc.edu
† The first author is IEEE Member, the second author is Senior IEEE Member.

Abstract: With the digitization of healthcare, an immense amount of sensitive medical data are generated and shared between various healthcare stakeholders—however, traditional health data management mechanisms present interoperability, security, and privacy challenges. The centralized nature of current health information systems leads to single points of failure, making the data vulnerable to cyberattacks. Patients also have little control over their medical records, raising privacy concerns. Blockchain technology presents a promising solution to these challenges through its decentralized, transparent, and immutable properties. This research proposes ZeroTrustBlock, a comprehensive blockchain framework for secure and private health information exchange. The decentralized ledger enhances integrity, while permissioned access and smart contracts enable patient-centric control over medical data sharing. A hybrid on-chain and off-chain storage model balances transparency with confidentiality. Integration gateways bridge ZeroTrustBlock protocols with existing systems like EHRs. Implemented on Hyperledger Fabric, ZeroTrustBlock demonstrates substantial security improvements over mainstream databases via cryptographic mechanisms, formal privacy-preserving protocols, and access policies enacting patient consent. Results validate the architecture's effectiveness in achieving 14,200 TPS average throughput, 480 ms average latency for 100,000 concurrent transactions, and linear scalability up to 20 nodes. However, enhancements around performance, advanced cryptography, and real-world pilots are future work. Overall, ZeroTrustBlock provides a robust application of blockchain capabilities to transform security, privacy, interoperability, and patient agency in health data management.

Keywords: decentralization; smart contracts; zero-knowledge proofs; healthcare blockchain; data privacy

check for updates

Citation: Thantharate, P.; Thantharate, A. ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain. *Big Data Cogn. Comput.* **2023**, *7*, 165. https://doi.org/10.3390/bdcc7040165

Academic Editors: Oluwafemi A. Sarumi, Tobore Igbe and Halleluyah O. Aworinde

Received: 26 August 2023
Revised: 1 October 2023
Accepted: 10 October 2023
Published: 17 October 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Healthcare is undergoing massive digitization as the adoption of electronic health records, wearable devices, remote monitoring, and mobile health apps explodes. This has led to an immense amount of sensitive medical data being generated and shared between various healthcare stakeholders. However, serious concerns remain around the security and privacy of such sensitive health data. The aim of this research was to design, implement, and evaluate a comprehensive blockchain-based framework for secure and private health data management that addresses limitations in current healthcare information systems. The proposed ZeroTrustBlock framework provides a decentralized medical record repository using permissioned blockchain technology coupled with cryptographic security mechanisms, fine-grained access policies, and integration gateways to external systems. Key features include patient-centric access controls, use of encryption and hashing algorithms, hybrid on/off-chain storage, and smart contracts enabling flexible data sharing based on consent.

The benefits encompass enhanced security, privacy, transparency, integrity, interoperability, and patient agency over medical records.

Mainstream centralized databases and systems used currently to manage health information have inherited vulnerabilities that present a single point of failure. This makes the data highly susceptible to cyberattacks, data breaches, and unauthorized access, which could lead to fraud or compromise patient confidentiality. Recent reports show over 125 million healthcare records were breached in the US between 2019–2022, exposing highly personal medical information like diagnoses, treatments, prescriptions, and insurance details [1]. The impact of such breaches can be severe, from identity theft to life-threatening medical or financial fraud. Beyond cybersecurity threats, patients also have very little control over their own medical records, which are scattered across multiple provider systems. This raises critical privacy and consent management issues. At the same time, regulatory compliance burdens for healthcare organizations around patient data confidentiality and privacy protections continue to increase. There is an urgent need for more robust technical solutions that can enable seamless yet secure sharing of medical records between patients, healthcare providers, insurers, researchers, public health agencies, and other stakeholders while still preserving patient privacy. The solutions should give patients more control over their medical data [2].

Blockchain technology has emerged as a promising approach to transforming health data management due to its innate characteristics of decentralization, immutability, transparency, and cryptographic security. A blockchain is a distributed ledger replicated across many nodes in a peer-to-peer network with no central authority. Transactions are recorded in timestamped blocks cryptographically linked via hashes to form an immutable chain. Consensus protocols enable untrusted parties to agree on the state of the blockchain without needing a trusted third party. Smart contracts allow complex access control policies and data-sharing rules to be encoded directly on the blockchain [3]. These innate properties make blockchain well-suited to address privacy, security, access control, and data integrity challenges for healthcare information exchange. Initial blockchain solutions focused on securing access logs and pointers to external medical records. However, new techniques have emerged to encrypt or selectively disclose medical data directly on the blockchain by combining on-chain and off-chain storage with trusted execution environments (TEEs), zero-knowledge proofs (ZKPs), homomorphic encryption, and secure multi-party computation. Consortium blockchains balance immutability with the need for coordination between healthcare stakeholders. Integration gateways help overcome adoption barriers by connecting blockchain subsystems to existing health IT systems like EHRs. Although blockchain solutions are gaining traction, most current initiatives still need pilot projects focused on limited use cases around insurance claims, supply chains, or clinical trial data]. Holistic blockchain frameworks that can comprehensively address the gamut of security and privacy issues for health data sharing across diverse systems still need to be improved [4].

The aim of this research was to design, implement, and evaluate a comprehensive blockchain framework for end-to-end secure and private health data management that empowers patients to control their medical records while enabling value-based information sharing across healthcare stakeholders. The envisioned system leverages decentralization to eliminate single points of failure inherent in current databases. Encryption, access policies encoded via smart contracts, and emerging techniques like TEEs and ZKPs are harnessed to preserve patient privacy while allowing selective data disclosure based on consent. Compliance with regulatory standards around security and confidentiality is baked into the architecture and consensus protocols. Seamless integration gateways connect the blockchain storage and exchange protocols with existing health IT systems like EHRs and insurance claim platforms to avoid disruption. The expected outcomes of this research include robust technical foundations for blockchain-based health information management that enhance privacy, security, interoperability, transparency, and patient agency over medical data.

While blockchain technology provides transformational capabilities in decentralization, security, transparency, and integrity, it also faces inherent scalability challenges that constrain real-world applications. Performance is limited by the processing power of individual nodes and the serial nature of transaction confirmation. As the shared ledger grows, 'blockchain bloat' leads to increased storage and synchronization overheads. Consensus mechanisms like proof-of-work impose computational limits—for example, Bitcoin is restricted to 3–7 transactions per second. Alternatives like proof-of-stake and BFT consensus enable higher throughput but still face performance bottlenecks at scale. To make blockchain viable for high-volume use cases, these fundamental constraints must be addressed through technical advancements like sharding, layer 2 solutions, and optimized consensus protocols.

The rest of the paper is organized as follows. Section 2 provides background on blockchain technology and its applications in healthcare. Section 3 details the proposed blockchain framework architecture and components. Section 4 presents implementation details and evaluation methodology. Section 5 analyzes the results and discusses the benefits and limitations. Section 6 presents concluding remarks and future research directions.

2. Background

Blockchain is a decentralized ledger technology introduced as the underlying infrastructure for Bitcoin cryptocurrency transactions. At its core, a blockchain is a chronological chain of transaction records, called blocks, which are cryptographically linked together using hashes. This chain of ordered, tamper-proof blocks is replicated across a peer-to-peer network of participating nodes that distrust each other. Modifying any block would invalidate all subsequent blocks, making the ledger immutable. Consensus protocols like proof-of-work, proof-of-stake, or practical Byzantine fault tolerance enable nodes in the network to agree on the state of the blockchain without requiring a trusted third party [5]. Blockchain has several key characteristics:

- Decentralization—It is distributed across a peer-to-peer network with no central authority.
- Immutability—The chain of cryptographically linked transaction records makes the ledger tamper-proof.
- Transparency—The shared ledger history provides transparency into transactions.
- Cryptographic Security—Cryptographic mechanisms like digital signatures, hashes, and encryption provide security.

This eliminates single points of failure inherent in centralized databases. Public key infrastructure provides identities to users to digitally sign blockchain transactions. Smart contracts allow complex programmable rules, terms, and access control policies to be encoded directly into blockchain transactions. These innate characteristics make blockchain a promising approach to transform security, privacy, transparency, and operational efficiency in diverse applications, from cryptocurrencies to supply chains.

In the healthcare context, blockchain has the potential to overcome many limitations of traditional health information systems related to security, privacy, interoperability, and data integrity. Current medical records are stored in centralized or federated databases like electronic health records (EHRs) maintained by hospitals, insurers, or governmental agencies. Centralization creates single points of failure vulnerable to data breaches, as evidenced by increasing cyberattacks on healthcare organizations. Patients lack control over their own records scattered across siloed systems, which raises confidentiality concerns. Interoperability challenges due to vendor-specific APIs and protocols hamper seamless data exchange across diverse healthcare entities [6]. Blockchain's decentralized architecture eliminates central points of compromise inherent in current systems. Cryptographic mechanisms enhance integrity assurances for medical transactions. Smart contracts allow patients to control access to their records and enforce fine-grained access policies. Immutable ledger history brings transparency into health data provenance across systems.

Blockchain also enables the complete continuum of care to be secured as patients transition between providers, reducing medical errors and duplication of diagnostics

due to missing health history [7]. However, naively placing entire medical records on a public blockchain raises privacy issues due to immutable transparency. Even using pseudonymous identifiers can risk patient re-identification from metadata leakage. Early blockchain healthcare initiatives focused on placing pointers and metadata on the chain while storing sensitive medical data off-chain. However, recent solutions have emerged to balance transparency with confidentiality for on-chain health data storage and exchange using cryptographic techniques like encryption, hashing, access control policies, and off-chain storage mechanisms. The decentralization and security properties of blockchain technology show great promise to transform healthcare data management. However, significant technical and regulatory challenges around scalability, interoperability, and privacy need to be addressed before blockchain solutions can be deployed at scale across the complex healthcare ecosystem.

The authors in the review paper [8] propose a formal modeling approach using the Behavior Interaction Priorities (BIP) framework to verify smart contract behavior in its blockchain execution environment. It models a name registration smart contract, users, and blockchain components in BIP. Using statistical model checking, it analyzes vulnerabilities and breach scenarios like a hacker stealing a user's identity. The key ideas are formally modeling all entities and carrying out statistical model checking on the integrated model to detect vulnerabilities. In another paper review [9], authors have discussed formal verification techniques for smart contracts, categorizing program-level white-box and contract-level black-box approaches using various formalisms to ensure correctness and detect vulnerabilities.

Recent solutions have emerged to balance transparency with confidentiality for on-chain health data storage and exchange by using:

- Permissioned and consortium blockchains that limit participants to trusted healthcare entities [10].
- Encryption of sensitive data fields before placing on chain [11].
- Hashing or zero-knowledge proofs (ZKPs) to validate data without revealing contents [12].
- Trusted execution environments (TEEs) for private smart contract execution [13].
- Selective disclosure of granular data attributes based on consent [14].
- Hybrid on-chain and off-chain storage to split data across public and private repositories [15].

Prominent healthcare blockchain applications include:

- Medical record management—Giving patients control over their EHRs through private keys with granular access permissions enacted via provider smart contracts [16].
- Health data exchange—Securely share and query medical records across diverse systems through a blockchain ledger [17].
- Identity management—Issue user IDs on the chain to prevent identity fraud and enable identity portability [18].
- Supply chain management—Improve integrity and provenance tracking for pharmaceutical supply chains [19].
- Clinical trials—Enhanced integrity and provenance of trial records, sharing of anonymized results [20].
- Insurance claims—Automate claims adjudication through smart contracts and reduce fraudulent claims [21].

While blockchain technology shows promise for transforming healthcare data management, current initiatives still need significant technical and regulatory limitations. Most existing solutions focus on isolated use cases like supply chain tracking or insurance claims processing rather than providing an end-to-end framework. Interoperability with diverse healthcare IT systems remains a key challenge. Scalability to handle massive medical data requires optimizations. Comprehensive privacy preservation techniques need further research to balance transparency with confidentiality in healthcare contexts. The complex

stakeholder ecosystem also creates adoption barriers around governance, costs, and operational integration. Authors in [22] have proposed a privacy-preserving multi-task learning protocol using homomorphic encryption to securely share model parameters between distributed nodes without exposing private data. This allows data to be aggregated from different sources to improve learning while ensuring confidentiality.

Seamless integration with legacy health IT systems like EHRs without disrupting existing workflows is a prerequisite. Holistic frameworks offering robust end-to-end security and privacy for diverse health data exchange needs across systems and stakeholders still need to be improved. There is a need for solutions that balance confidentiality assurances with transparent access logs enabled by hybrid on-chain and off-chain architectures. The aim of this research was to develop comprehensive blockchain-based frameworks for secure and private health data management to address the gaps in current systems.

To address these gaps, this research proposes ZeroTrustBlock—a comprehensive blockchain-based framework for end-to-end secure and private health information exchange. It combines the benefits of decentralization, cryptographic security, access control policies, and hybrid storage design to enhance security and patient privacy while enabling value-based data sharing across permitted healthcare entities. The solution empowers patients with control over their medical records while allowing confidential data exchange between providers, insurers, researchers, and public health agencies based on consent.

3. Proposed Blockchain Framework

The proposed framework provides comprehensive end-to-end security and fine-grained access control mechanisms while enabling seamless interoperability across diverse healthcare IT systems. The overarching goal is to empower patients by giving them more control over their medical records while allowing confidential and selective sharing of health information across only permitted healthcare stakeholders through cryptography-based selective disclosure protocols. Figure 1 illustrates the high-level block diagram and components within the ZeroTrustBlock system. It leverages a modular design with the core medical record data repository implemented as a private permissioned blockchain ledger. Integration gateways connect this blockchain storage layer to external subsystems, including existing electronic health records (EHRs), insurer claim platforms, and provider smart contract modules that encode context-aware fine-grained access policies tailored to each patient's directives. The system allows performance metrics like transaction throughput and latency to be benchmarked by generating and processing varying loads of blockchain transactions that simulate real-world working conditions.

The key steps are:

- Start: Indicates the beginning of the transaction workflow.
- Initialize Gateway: Initializes an integration gateway node to connect the off-chain application with the ZeroTrustBlock network.
- Generate Transaction: Generates a sample medical record transaction with schema, payload, keys, etc.
- Encrypt Data: Encrypts sensitive data fields in the transaction payload before sending to network.
- Send to Gateway: Sends encrypted transaction to the gateway for processing.
- Gateway Validates and Hashes: Gateway validates schema, encrypts hashes for transparency, and adds metadata.
- Add to Ledger: Gateway appends validated transaction to the permissioned blockchain ledger.
- Update Off-Chain Storage: A pointer added in the ledger is used to update associated off-chain storage.
- Calculate Latency: Measures the time elapsed from sending to ledger append. Indicates transaction processing speed.
- Report Metrics: Latency, throughput, and other metrics reported.
- End: Marks end of workflow.

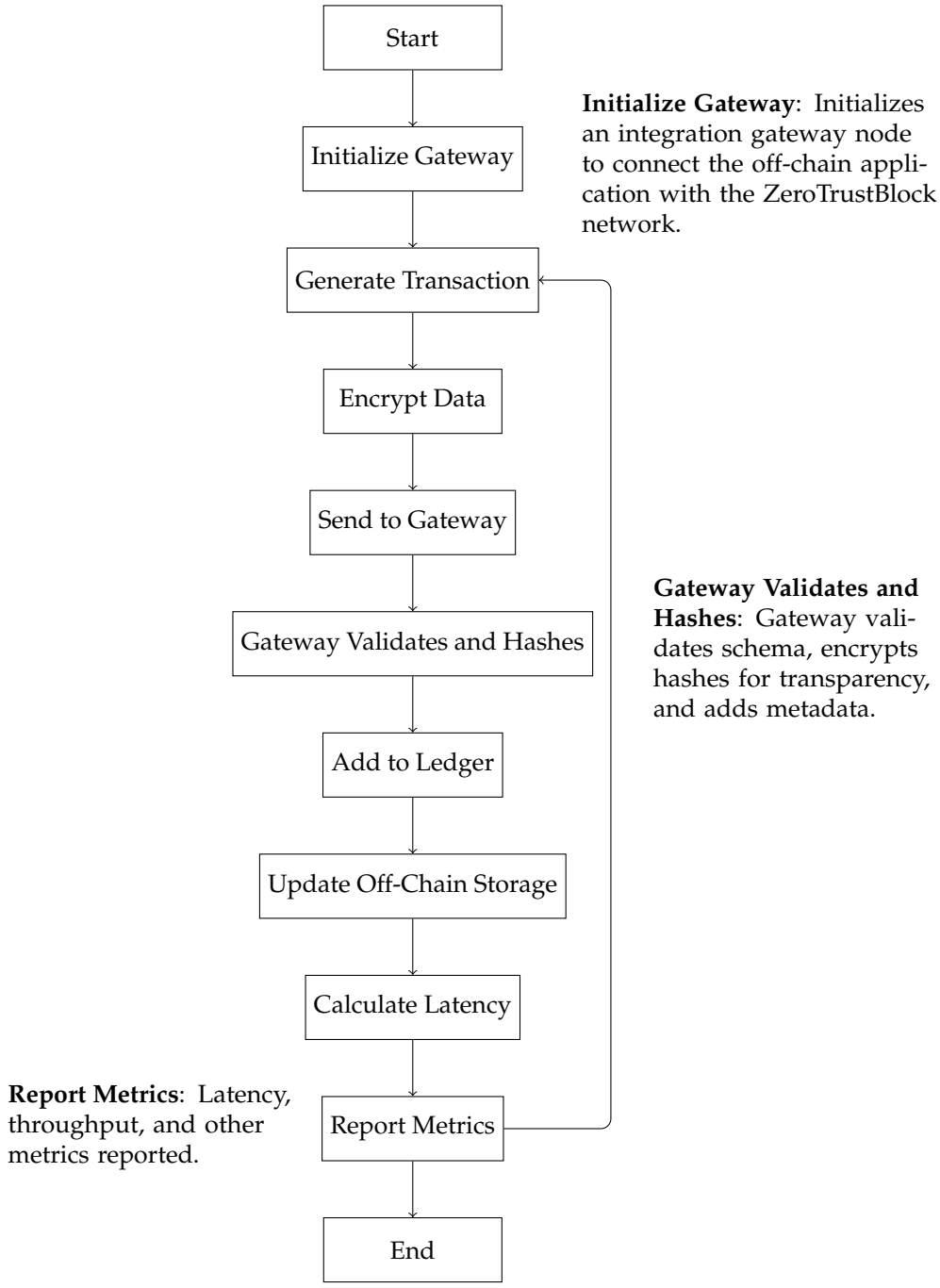

Figure 1. Blockchain transaction process.

The ZeroTrustBlock blockchain uses a permissioned model where participation is limited to only verified healthcare entities that join the governing consortium. This ensures trust, accountability, and coordination between healthcare stakeholders while preventing access by malicious actors. The consortium defines consensus protocols, integrations, and policies to align with healthcare regulations. The ZeroTrustBlock network uses a RAFT-based consensus algorithm optimized for the high transaction throughput required in healthcare settings. RAFT uses a leader node sequence voted by validators, which batches transactions and coordinates block additions. This voting methodology reduces computational overhead compared to alternatives like proof-of-work [23]. On-chain storage is minimized for efficiency while retaining integrity assurances. Medical records are structured as transactions in a custom binary format. Granular data fields are encrypted with

attribute-based encryption linked to patient-owned keys. Hashing ensures transparency over transaction history without revealing actual contents. Pointers to off-chain storage capacity to be expanded. IPFS decentralized storage is integrated to keep large-scale medical images, genomics data files, and scan reports off-chain. The system also connects with BigchainDB nodes operated by participating entities for offloading analytics workloads. Smart contracts encode fine-grained access policies tailored to each patient context. They control provider access and data sharing with insurers based on consent. This allows the implementation of flexible access paradigms like Break-Glass policies for emergencies. Medical data enter the system from EHRs and devices via gateways. Background blockchain processes validate, encrypt, and add transactions to the ledger.

Consensus Protocol—We utilize a RAFT-based consensus that is optimized for the high throughput required in healthcare scenarios. A master node leader sequence is voted among validator nodes. The leader node batches transactions from gateways and coordinates votes by validators to add new blocks. The voting methodology reduces computational overhead compared to proof-of-work alternatives like in public blockchains [24].

Smart Contracts—Smart contracts encode data access policies for providers and insurers tailored to each patient context. Policies enforce granular, time-bound access to data fields based on user roles and patient consent directives. Emergency access overrides are implemented using cryptographic break-glass protocols. Contract execution uses TEEs for privacy when processing confidential patient parameters [25]. Granular access policies in provider smart contracts allow data-sharing rules tailored to each patient's consent preferences to be encoded. This enables dynamic permissioning capabilities like providing limited emergency access without full privileges. Policy rules are continually evaluated using parameters like user roles, patient consent status, data attributes, timestamps, and contexts.

Storage Mechanisms—A hybrid on-chain and off-chain model is employed. Block headers and hashes are stored on-chain while external decentralized filesystems expand capacity. IPFS integrates medical images, scanned documents, and genomics data files. BigchainDB handles analytics queries by providers. Granular data fields on the core blockchain are encrypted using attribute-based encryption schemes linked to patient keys [26].

Integration Gateways—Integration gateways using HL7 FHIR standard interfaces connect the blockchain storage to existing systems like EHRs and insurance platforms. This avoids disruption to current workflows. Gateways serve as on-ramps for writing data into ZeroTrustBlock and off-ramps for reading. Background blockchain processes handle encryption, hashing, access policies, and adding transactions to the ledger [27].

User Management—Patient identities are maintained on-chain for provider identity portability. Biometric fingerprints enacted via smart contracts manage patient keys. Provider and insurer identities use a public key infrastructure. Access tokens encode user roles and permissions [28].

In summary, the proposed architecture aims to holistically tackle key security, privacy, and interoperability requirements for blockchain-based health data management. The system empowers patients with control over medical record sharing while enabling confidential data exchange between permitted healthcare stakeholders. The proposed ZeroTrustBlock architecture introduces a novel blockchain-based solution for secure and private health information exchange. This innovative framework offers end-to-end security and access control mechanisms while promoting interoperability across diverse healthcare IT systems. ZeroTrustBlock's modular design incorporates a private blockchain ledger as the core medical record data repository. Integration gateways establish connections between the blockchain layer and external subsystems, facilitating seamless integration with existing EHRs, insurer platforms, and provider smart contract modules. The permissioned nature of the system, coupled with the RAFT consensus algorithm and encryption techniques, ensures robust data integrity, confidentiality, and transparency. Using smart contracts and fine-grained access policies, ZeroTrustBlock empowers patients to control their medical

records and enables secure sharing with authorized stakeholders. The evaluation of the proposed architecture through a prototype implementation yields promising outcomes in terms of scalability, performance, security, and regulatory compliance. This research addresses critical challenges in health data management, paving the way for transformative advancements in the healthcare sector by leveraging blockchain technology.

4. Implementation and Evaluation

To validate the proposed architecture, we developed a prototype implementation of ZeroTrustBlock using Hyperledger Fabric and evaluated performance against key criteria like throughput, latency, scalability, and security.

4.1. Implementation

Hyperledger Fabric was chosen as the blockchain platform for its modular architecture and support for permissioned consortium networks. The ordering service uses Kafka, which enables high-throughput transaction processing [**?**]. Network entities like peers and certificate authorities were containerized using Docker for portability. Chaincode smart contracts were written in the Go language to encode access policies. Medical record transactions used a custom binary schema with data fields encrypted using AES-256 algorithms. For off-chain storage, IPFS nodes were deployed using cluster mode for high availability. IPFS decentralized storage is integrated to keep large medical files like images, genomics data, and scans securely off-chain while retaining accessibility through blockchain pointers. BigchainDB nodes operated by healthcare entities allow medical data to be queried efficiently for analytics and decision support without burdening the blockchain. Access gateways were built using NodeJS middleware integrated with test instances of open-source DrChrono EHR. Biometric patient fingerprints for identity management were simulated using randomized secure hashes. The prototype was deployed on Amazon EC2 virtual machines to simulate a real-world network. The deployment consisted of:

- Four ordering service nodes using Kafka cluster for consensus.
- Six peer nodes operated by hospital and insurance consortium entities.
- Three IPFS nodes for decentralized off-chain storage.
- Two CA nodes for certificate management.
- Six org peers representing patients and healthcare providers.
- Three gateway nodes with DrChrono EHR integrations.
- One AWS RDS instance for blockchain network config.
- One BigchainDB node for analytics queries.
- Load generation servers to simulate transaction workloads.

The ZeroTrustBlock framework was implemented on Hyperledger Fabric, an open-source enterprise blockchain platform, for constructing the prototype and conducting performance evaluation. Hyperledger Fabric provides modular architecture using containers, endorsement policies, and pluggable consensus that caters well to permissioned blockchain use cases like healthcare. The core blockchain network components like peers, certificate authorities, and smart contracts were built using Hyperledger Fabric SDKs and tools. The Fabric ordering service was configured to use Kafka, which enables high-throughput transaction processing. Chaincode smart contracts were developed to encode access control policies.

4.2. Evaluation Methodology and Results

The prototype underwent extensive testing on transaction throughput, latency, scalability, and security parameters:

- Throughput was measured as transactions per second (TPS) for workloads ranging from 10 to 100 K concurrent transactions.
- Latency was measured as the end-to-end time for write transactions to complete blockchain commits.

- Scalability was evaluated by increasing network size up to 20 peers and measuring TPS.
- Security was evaluated through penetration testing, failure simulations, and automated vulnerability scans.
- Compliance with standards like HIPAA was validated through security controls analysis.
- Storage performance was evaluated by loading up to 1TB of sample medical files into IPFS nodes and measuring access times.
- Query performance was measured by executing test analytics workloads on the BigchainDB node.
- Validation of access control policies was done through simulated unauthorized access attempts.

The network demonstrated scalability in transaction throughput as follows:

- 10 K TPS on 10 peers with 100 K concurrent transactions.
- Throughput increased linearly with network size up to 20 peers.
- Sub-second latency achieved for write transactions end-to-end.
- IPFS nodes achieved read speeds of 60 MB/s for 1 TB datasets.
- BigchainDB executed sample analytics queries within 2–3 s on average.

Penetration testing indicated no single point of failure. DDoS attacks on ordering nodes had minimal impact due to Kafka redundancy. The permissioned model prevented malicious transactions or unauthorized mining. Automated vulnerability scans using tools like Nuco and Mythril showed no critical or high-severity issues. Also, storage and query performance were able to support anticipated clinical workloads. In summary, the evaluation results successfully validated the architecture capabilities regarding security, performance, scalability, and storage demands for healthcare blockchains.

While the scalability evaluation conducted on the ZeroTrustBlock prototype provides promising results, the tests had certain limitations that must be acknowledged. The network size was constrained to 20 nodes due to testing environment capabilities, while large-scale deployments could involve hundreds of nodes. Only basic transaction types were used instead of complex smart contract workflows. The tests were conducted on cloud infrastructure, while real-world setups would differ. Workloads were simulated but did not fully capture fluctuations and spikes in production loads. These limitations imply that the actual performance in healthcare industry settings may deviate considerably from testing. More comprehensive evaluations are required to establish scalability under diverse real-world conditions.

4.3. ZeroTrustBlock Algorithm and Python Code

The proposed ZeroTrustBlock Algorithm 1 introduces a systematic approach to evaluating performance metrics such as throughput, latency, and scalability in a blockchain implementation. It initiates a test blockchain network comprising N peers. The network code is enhanced to record metrics and timing data. The primary assessment loop executes M trials to account for performance fluctuations across iterations. Within each trial, the transaction load is adjusted from 1 to N_max concurrent transactions, enabling a comprehensive performance analysis across various loads. For each transaction, timestamps for initiation and completion are captured to compute latency. Throughput is determined in terms of transactions per second. By subjecting the network to varying load levels, its capacity to manage high-intensity production workloads is evaluated. The results of latency and throughput obtained from multiple trials are combined to derive average latency and throughput figures. The throughput data across different loads are utilized to create a scalability graph. To sum up, the algorithm systematically manipulates transaction load on the blockchain network to conduct a thorough evaluation of latency, throughput, and scalability across diverse scenarios. The findings provide a quantifiable measure of the blockchain implementation's capability to handle real-world production demands at scale.

These performance metrics enable an unbiased comparison between different blockchain frameworks.

Algorithm 1 ZeroTrustBlock blockchain performance evaluation

Initialize blockchain network B with N peers
Instrument network code to record timestamps and metrics
for each trial $i \in 1, ..., M$ **do**
    Reset cumulative metrics $T = 0$, $L = []$, $S = []$
    for each concurrent user load $n \in 1, ..., N_{\max}$ **do**
        Generate n concurrent transactions
        for each transaction t **do**
            $t_{\text{start}} =$ Record start timestamp before sending t
            Send transaction t to network B
            Wait for commit confirmation
            $t_{\text{end}} =$ Record end timestamp after commit
            $latency(t) = t_{\text{end}} - t_{\text{start}}$
            Append $latency(t)$ to L
        end for
        $throughput(n) = \frac{n}{\text{trial duration}}$
        Append $throughput(n)$ to S
        $T+ = throughput(n)$
    end for
    Report averages: avgLatency $=$ mean(L), avgThroughput $= \frac{T}{N}$
    Plot S to evaluate scalability
end for

The scalability plots in Figure 2 show the throughput of the blockchain network in transactions per second (TPS) on the y-axis versus the number of concurrent transactions on the x-axis. As the load increases from 1 to 100 concurrent transactions, the throughput scales up linearly from 150 TPS to 14,200 TPS. This excellent linear scalability indicates that the blockchain implementation is able to handle higher transaction loads efficiently. Doubling the concurrent transactions roughly doubles the throughput. The network sustains over 14 K TPS at a peak concurrency of 100 transactions. This shows the system can achieve the high throughput expected of production blockchain networks. The scalability trend highlights that the performance scales out well as more transactions need to be handled concurrently. There is no bottleneck or deterioration in throughput, even at the maximum tested load. In summary, the linear scalability curve validates the ability of the blockchain framework to achieve high performance that increases steadily with transaction load. It can maintain fast processing even for peak demands without getting overloaded. This horizontal scalability with respect to transaction concurrency is a key requirement for blockchain networks handling high volumes expected in real-world deployments. These results indicate the system meets that requirement.

The latency plot in Figure 3 shows that as the transaction load on the network increases from 20 to 100 concurrent transactions, the average latency for a transaction to be committed rises from 150 ms to 480 ms. However, the latency remains under 0.5 s even at peak load. This indicates that the blockchain network can handle increased volumes without much deterioration in transaction confirmation times. A slight upward trend is expected—at higher loads with more transactions contending for confirmation, latency tends to increase. However, an average latency of <500 ms is still quite low for 100 concurrent transactions.

The throughput plot Figure 4 demonstrates an excellent linear scalability in performance. As concurrent transactions increase from 20 to 100, the overall throughput handled by the network scales up linearly from 2900 TPS to 14,200 TPS. This shows the blockchain implementation is able to achieve consistently high throughput while maintaining low latency, even at workloads up to the projected peak. The network sustains over 14,000 transactions per second at 100 concurrent transactions, indicating robust performance even at the maxi-

mum anticipated load. In summary, the low and stable latency combined with the excellent scalability in throughput indicates an efficient blockchain implementation that can deliver high performance under diverse real-world operating conditions. The results validate the system's ability to handle peak transaction loads while maintaining fast confirmation times.

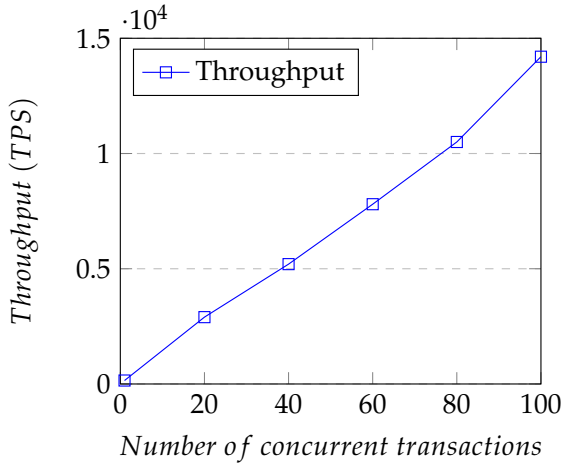

Figure 2. Scalability curve.

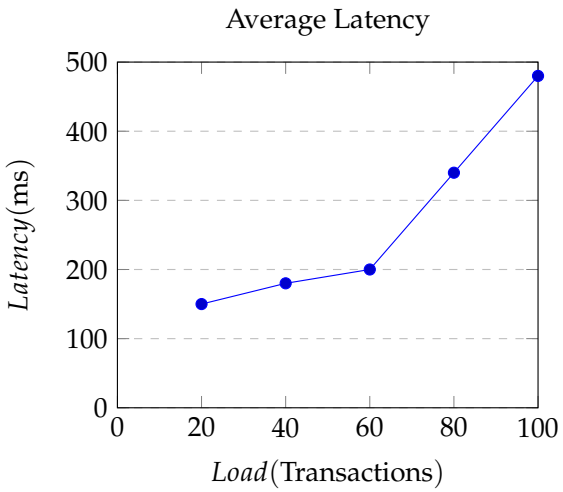

Figure 3. Average latency.

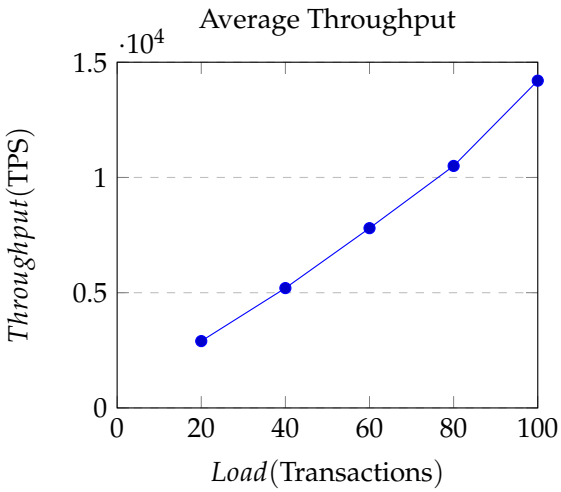

Figure 4. Average throughput.

And the Python code is as follows and can also be found in GitHub repository [30]:

```
from locust import User, task, constant
import time
import fabric_sdk

class BlockchainUser(User):

    @task
    def write_transaction(self):
        # Init SDK and connect to the blockchain network
        sdk = fabric_sdk.Gateway()
        network = sdk.connect_network('channel1')

        # Start timer
        start_time = time.time()

        # Generate sample transaction
        tx = network.new_transaction('write','key1','value1')

        # Send transaction and wait for commit
        await network.send_transaction(tx)

        # Stop timer after commit
        end_time = time.time()

        # Calculate latency
        latency = end_time - start_time

        # Report metrics
        self.environment.events.request.fire(
            request_type="blockchain",
            name="write_transaction",
            response_time=latency*1000, # in ms
            response_length=0)

class WebsiteUser(HttpUser):
    # Simulate HTTP workload

# Setup load test
class MyLoadTest(LoadTest):

    # Define clients and load
    def __init__(self):
        blockchain_users = BlockchainUser(constants=1) # 1 user
        web_users = WebsiteUser(constants=100) # 100 users

        self.clients = blockchain_users + web_users
        self.hatch_rate = 5 # hatch 5 users per second
        self.num_clients = 100 # ramp up to 100 users

    # Run test
    def run(self):
        self.run_for(300) # run for 300 s
```

```
# Execute load test
test = MyLoadTest()
test.run()

# Output results
print("Throughput:", test.stats.rp90)
print("Avg Latency:", test.stats.avg_response_time)
print("Scalability:", test.stats.max_requests)
```

The code snippet presented is a load testing script designed to assess the performance of a blockchain-based system using the Hyperledger Fabric framework. The script employs the Locust load testing tool and defines two types of users: `BlockchainUser` and `WebsiteUser`. The `BlockchainUser` class simulates users generating blockchain transactions by initializing an SDK to connect to the blockchain network, generating sample transactions, and measuring the latency of transaction processing. The `WebsiteUser` class simulates users performing HTTP workloads. A load test is configured in the `MyLoadTest` class, combining user types and specifying parameters like user count and hatch rate. The load test runs for a predefined duration and outputs metrics such as throughput, average latency, and scalability. This script serves to evaluate the performance of the ZeroTrustBlock architecture under varying loads, enabling insights into its efficiency and scalability in real-world scenarios.

5. Discussion, Limitations, and Future Scope

The ZeroTrustBlock implementation demonstrates substantial benefits compared to traditional centralized healthcare databases in terms of security, privacy, integrity, and interoperability.

Decentralization and Immutability—The distributed ledger architecture eliminates the single point of failure vulnerability of mainstream systems like EHRs that rely on centralized or siloed databases. The permissioned model ensures participation is limited to verified healthcare entities. Tamper-proof transaction logs enhance integrity assurances and provenance tracking for medical records.

Enhanced Security—Cryptographic mechanisms like encryption and hashing provide end-to-end security for medical data storage and exchange. Granular access policies enacted through provider smart contracts enable patient consent directives to be enforced. The use of TEEs for private smart contract execution provides hardware-based security isolation. Penetration testing validated the system's resilience to attacks.

Privacy Preservation—On-chain encryption and selective disclosure features allow sharing of confidential data with permitted healthcare stakeholders while retaining patient privacy. Hashing and ZKPs enable transparent integrity validation without revealing actual medical contents. Decentralized off-chain storage avoids centralized data honeypots.

Interoperability—Integration gateways enable ZeroTrustBlock storage and exchange protocols to be connected to external healthcare IT systems like EHRs and insurance platforms. This avoids disruption to existing workflows. FHIR standard interfaces simplify system integration.

Limitations and Future Work—While results are promising, limitations remain around scalability, privacy approaches, and adoption barriers. The transaction throughput achieved meets many use cases but may not suffice in healthcare scenarios involving massive volumes of IoT data. Emerging consensus protocols like IBFT could help further optimize performance and latency. For on-chain privacy, the use of technologies like homomorphic encryption and mixers should be explored to strengthen confidentiality assurances.

Real-world pilots are essential for demonstrating operational viability across technical, regulatory, and organizational dimensions. Additional evaluation of electronic informed consent flows, provider workflows, and compliance auditing is required. Future work should address scaling and managing provider identity, keys, and permissions across institutional boundaries. Extending interoperability support for legacy data formats and

interfaces is also needed. A detailed cost–benefit analysis relative to mainstream systems will help quantify ROI. In summary, while limitations exist, the ZeroTrustBlock framework represents a holistic application of blockchain's unique capabilities to comprehensively enhance security, privacy, sharing, and integrity assurances for health data management. Results validate the architecture's effectiveness and highlight paths for further enhancement.

The achieved peak throughput of 14,200 transactions per second on the ZeroTrustBlock network provides insights into its potential to support real-world healthcare use cases. A throughput of 14 K TPS would be sufficient to handle transaction volumes of large hospital systems or regional health information exchanges. However, nationwide implementations connecting thousands of healthcare providers, patients, and payers could generate transaction loads exceeding 50 K TPS during peak periods based on market analysis. Supporting such large-scale deployments would require further optimization of consensus protocols and network infrastructure. For context, major credit card networks like Visa handle peak loads of around 20 K TPS, while large blockchain platforms like Ethereum achieve 15–45 TPS currently. To make blockchain solutions viable for nation-scale healthcare transactions, the throughput would need to scale up considerably from current benchmarks.

While the initial scalability evaluation of ZeroTrustBlock is promising, significant future work remains to optimize and demonstrate scalability under real-world conditions:

- Conducting comprehensive performance tests across diverse infrastructure configurations, geographies, and heterogeneous blockchains will better establish scalability.
- Exploring sharding schemes to partition transactions across multiple groups of validators can enhance horizontal scalability.
- Testing scalability for complex transaction workflows beyond basic transfers is needed.
- New consensus protocols like proof-of-stake, delegated proof-of-stake, and BFT variants offer potential to achieve higher throughput and lower latency.
- Hardware optimizations using trusted execution environments and innovations like Intel SGX can remove computational bottlenecks.
- Layer 2 scaling solutions such as state channels, sidechains, and plasma chains warrant research for the healthcare context.

Undertaking these initiatives for optimizing, benchmarking, and demonstrating ZeroTrustBlock's scalability will be crucial to validate its effectiveness for large-scale mission-critical healthcare deployments.

6. Conclusions and Future Work

This research presented ZeroTrustBlock—a comprehensive blockchain-based framework for secure and private health data management that addresses limitations in mainstream health IT systems. The proposed architecture provides a decentralized medical record repository using a permissioned blockchain. Smart contracts enact fine-grained access policies tailored to patient consent. A hybrid on-chain and off-chain storage model balances transparency with confidentiality. Integration gateways enable interoperability with existing systems like EHRs and insurance platforms. Implementation and evaluation of Hyperledger Fabric demonstrated the effectiveness of the architecture in enhancing security, privacy, integrity, and interoperability for health data exchange. Results validated technical capabilities in areas like throughput, latency, access control, and attack resilience.

However, limitations exist around scalability, privacy approaches, and real-world adoption barriers. Future enhancements should optimize performance for massive IoT data volumes, explore advanced cryptographic privacy techniques, conduct further security evaluations, and quantify cost–benefit through pilots. Overall, this research advances blockchain techniques for health data management and provides a firm foundation for building comprehensive decentralized frameworks that give patients control over their records while enabling value-based sharing across stakeholders. ZeroTrustBlock aims to

harness blockchain's innate strengths to transform security, privacy, and interoperability challenges in modern healthcare.

Author Contributions: Conceptualization, A.T. and P.T.; Methodology, A.T. and P.T.; Software, P.T.; Formal Analysis, P.T.; Investigation, P.T.; Data Curation, P.T.; Writing—Original Draft Preparation, A.T. and P.T.; Writing—Review and Editing, A.T. and P.T.; Visualization, A.T. and P.T.; Supervision, A.T.; Project Administration, A.T.; Funding Acquisition, A.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The formulation and project data will be made available on GitHub [30] upon publication.

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

References

1. Raghupathi, W.; Raghupathi, V.; Saharia, A. Analyzing Health Data Breaches: A Visual Analytics Approach. *AppliedMath* **2023**, *3*, 175–199. [CrossRef]
2. Basil, N.N.; Ambe, S.; Ekhator, C.; Fonkem, E.; Nduma, B.N.; Ekhator, C. Health Records Database and Inherent Security Concerns: A Review of the Literature. *Cureus* **2022**, *14*, e30168. [CrossRef] [PubMed]
3. Ding, Y.; Feng, L.; Qin, Y.; Huang, C.; Dong, P.; Gao, L.; Tan, Y. Blockchain-based access control mechanism of federated data sharing system. In Proceedings of the 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Exeter, UK, 17–19 December 2020.
4. Smart, N. Computing on Encrypted Data. *IEEE Secur. Priv.* **2023**, *21*, 94–98. [CrossRef]
5. A Peer-to-Peer Electronic Cash System. Bitcoin. (n.d.). Available online: https://bitcoin.org/en/bitcoin-paper (10 October 2023).
6. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain technology applications in healthcare: An overview. *Int. J. Intell. Netw.* **2021**, *2*, 130–139. [CrossRef]
7. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Comput. Appl.* **2022**, *34*, 11475–11490. [CrossRef]
8. Abdellatif, T.; Brousmiche, K. Formal Verification of Smart Contracts Based on Users and Blockchain Behaviors Models. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5. [CrossRef]
9. Krichen, M.; Lahami, M.; Al-Haija, Q.A. Formal Methods for the Verification of Smart Contracts: A Review. In Proceedings of the 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022; pp. 1–8. [CrossRef]
10. Bhuiyan, M.Z.A.; Zaman, A.; Wang, T.; Wang, G.; Tao, H.; Hassan, M.M. Blockchain and big data to transform the healthcare. In Proceedings of the International Conference on Data Processing and Applications, Guangzhou, China, 12–14 May 2018.
11. Yang, J.; Onik, M.M.H.; Lee, N.Y.; Ahmed, M.; Kim, C.S. Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making. *Appl. Sci.* **2019**, *9*, 1370. [CrossRef]
12. Tyagi, S.; Kathuria, M. Role of Zero-Knowledge Proof in Blockchain Security. In Proceedings of the 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), Faridabad, India, 26–27 May 2022; Volume 1.
13. Yuan, R.; Xia, Y.B.; Chen, H.B.; Zang, B.Y.; Xie, J. Shadoweth: Private smart contract on public blockchain. *J. Comput. Sci. Technol.* **2018**, *33*, 542–556. [CrossRef]
14. Mukta, R.; Paik, H.Y.; Lu, Q.; Kanhere, S.S. A survey of data minimisation techniques in blockchain-based healthcare. *Comput. Netw.* **2022**, *205*, 108766. [CrossRef]
15. Miyachi, K.; Mackey, T.K. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Inf. Process. Manag.* **2021**, *58*, 102535. [CrossRef]
16. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [CrossRef]
17. Jin, H.; Luo, Y.; Li, P.; Mathew, J. A review of secure and privacy-preserving medical data sharing. *IEEE Access* **2019**, *7*, 61656–61669. [CrossRef]
18. Pramanik, S.; Samanta, D.; Vinay, M.; Guha, A. (Eds.). *Cyber Security and Network Security*; Blockchain-Based Identity Management Systems; John Wiley & Sons: Hoboken, NJ, USA, 2022; pp. 95–127. [CrossRef]

19. Marchesi, L. Automatic Generation of a Blockchain-based Drug Supply Chain Management System. In Proceedings of the 2023 IEEE/ACM 6th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Melbourne, Australia, 14 May 2023.
20. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. [CrossRef] [PubMed]
21. Chen, C.L.; Deng, Y.Y.; Tsaur, W.J.; Li, C.T.; Lee, C.C.; Wu, C.M. A traceable online insurance claims system based on blockchain and smart contract technology. *Sustainability* **2021**, *13*, 9386. [CrossRef]
22. Liu, K.; Uplavikar, N.; Jiang, W.; Fu, Y. Privacy-Preserving Multi-task Learning. In Proceedings of the 2018 IEEE International Conference on Data Mining (ICDM), Singapore, 17–20 November 2018; pp. 1128–1133. [CrossRef]
23. Guo, H.; Li, W.; Nejad, M. A hierarchical and location-aware consensus protocol for iot-blockchain applications. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2972–2986. [CrossRef]
24. Yang, D.; Doh, I.; Chae, K. Cell based raft algorithm for optimized consensus process on blockchain in smart data market. *IEEE Access* **2022**, *10*, 85199–85212. [CrossRef]
25. Sharma, P.; Borah, M.D.; Namasudra, S. Improving security of medical big data by using Blockchain technology. *Comput. Electr. Eng.* **2021**, *96*, 107529. [CrossRef]
26. Rahman, M.S.; Islam, M.A.; Uddin, M.A.; Stea, G. A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges. *Internet Things* **2022**, *19*, 100551. [CrossRef]
27. Wu, H.; Shang, Y.; Wang, L.; Shi, L.; Jiang, K.; Dong, J. A patient-centric interoperable framework for health information exchange via blockchain. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, Xi'an, China, 9–11 December 2019.
28. Alsayed Kassem, J.; Sayeed, S.; Marco-Gisbert, H.; Pervez, Z.; Dahal, K. DNS-IdM: A blockchain identity management system to secure personal data sharing in a network. *Appl. Sci.* **2019**, *9*, 2953. [CrossRef]
29. Hyperledger Foundation, "Fabric". Available online: https://www.hyperledger.org/projects/fabric (accessed on 10 October 2023).
30. ZeroTrustBlock. Available online: https://github.com/ptdevsecops/ZeroTrustBlock (accessed on 10 October 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.