Article

BloodChain: A Blood Donation Network Managed by Blockchain Technologies

Hai Trieu Le [1], Tran Thanh Lam Nguyen [2], Tuan Anh Nguyen [3], Xuan Son Ha [4] and Nghia Duong-Trung [5],*

1   Department of Information Technology, Can Tho University of Technology, Can Tho City 900000, Vietnam;
    lhtrieu.0127@gmail.com
2   VNPT Information Technology Company, Ho Chi Minh City 700000, Vietnam; thanhlam.bk.2110@gmail.com
3   School of Information and Communication Technology, Hanoi University of Science and Technology,
    Ha Noi 100000, Vietnam; anh.nt176680@sis.hust.edu.vn
4   Department of Theoretical and Applied Sciences, University of Insubria, Via Ravasi 2, 21100 Varese, Italy;
    sha@uninsubria.it
5   Institut für Biotechnologie, Technische Universität Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany
*   Correspondence: nghia.duong-trung@tu-berlin.de

Abstract: Due to the rapid change of population structure, leading to lower birth rates and quick aging rates, the demand for blood supply is increasing significantly. In most countries, blood quality and origin are managed by blood management information systems, such as national authorities. Nevertheless, the traditional system has limitations in this field, such as a lack of detailed blood information, making it challenging to manage blood quality, supply, and demand. Hence, to solve these issues, this paper proposes a blockchain-based system called BloodChain, an improved system to support blood information management, providing more detailed information about blood, such as blood consumption and disposal. BloodChain exploits private blockchain techniques with a limited number of relatively fast and reliable participants, making them suitable for B2B (Business to Business) transactions. In this paper, we also develop a proposed system based on the architecture of Hyperledger Fabric. The evaluation of BloodChain is performed in several scenarios to prove our proposed model's effectiveness.

Keywords: blood donation network; blockchain; Hyperledger Fabric; blood quality; information visibility

1. Introduction

Since Satoshi Nakamoto announced to the world the concept of bitcoin and its applications through the article [1], related blockchain applications began to develop strongly in various fields, such as delivery [2,3], transportation [4–6], healthcare [7,8], Internet of Things [9,10], energy [11] and healthcare [12,13].

Thanks to blockchain, the traceability and trackability of data to ensure compliance with reliability requirements is exploited in several fields, i.e., not only in healthcare systems [14] but also in aeronautical ones [15]. This claim proves that the blockchain-based system is increasingly applied to define the trusted architecture where the requirement of transparency and security is ensured.

Blood is considered the flow of life for every human being. Hence, blood is regarded as an essential resource in medical treatment. However, blood is banned from commercialization globally, and the primary source is blood donation within a particular nation. Despite the great demand for blood, there is a lack of efficient supply chains within borders. In addition, blood recipients do not know anything about the quality and origin of the blood they are receiving for medical treatment.

Therefore, the issue of clarifying all the details of blood donation in a supply chain system becomes an important topic. A WHO report stated that the body responsible

for managing health problems had defined a blood clot management system. The blood temperature and storage conditions must be accurate. Blood is donated until distribution to the patient [16]. The WHO report also guides the location of blood donations, storage, and distribution of blood. However, no documents show the ability to trace the origin and quality of blood. In Korea, the Blood Service Headquarters of the Korean Red Cross, which has fifteen blood banks and three blood tests, was established in 1958 [17]. The system is operated only to collect, store, and distribute blood and check the blood's quality and origin.

The information of blood donors, blood types, and blood quality is sensitive, and it requires transparency and good confidentiality. In addition, the process from blood donation to blood transfusion to the patient goes through many stages, such as storage and transportation; hence, the ability to store transaction information quickly is needed, and the information cannot be unaccountably modified. From the above requirements, blockchain technology is considered the right solution today to provide helpful information for blood ownership, hospitals, and blood recipients. The current blood management system only reports information about the amount of blood taken and lacks information about the patient's needs [18].

Therefore, this paper proposed a blockchain-based blood supply chain system called BloodChain. This system designs and provides an essential understanding to the reader of how the process works. In the process of blood provision with ambiguous information about blood origin and quality, complex storage, and transportation conditions, blockchain technology can create traceability.The patients can access the system and view necessary information on this platform without any privacy violation. Blockchain implements the transparency and privacy of each stakeholder along the blood donation supply chain. Blockchain technology promises to address essential aspects of the healthcare industry that have not been studied before, representing the transition from trusting people to trusting mathematics, playing a critical role in developing the blood donation system. Using a blockchain-based healthcare system, stakeholders receive beneficiaries to improve their health and stabilize blood supply and demand even in unusual situations.

In this paper, the structure is organized as follows: the next section of the paper presents the background of the research; Section 3 offers a literature review of relevant issues; the BloodChain overall architecture and implementation are shown in the following two sections; Section 6 describes the framework and benefits of the proposed system via evaluation; finally, Section 7 presents the conclusions and future research opportunities.

2. Background

An itemized depiction of blockchain is outside the extent of this article. Nonetheless, to explain the concepts utilized in the article, we will feature some significant ideas introduced below.

2.1. Blockchain Technology

Blockchain uses distributed ledger technology and is famous for the Bitcoin cryptocurrency. The Financial Times defined blockchain as a network of computers, all of which must approve a transaction that has taken place before it is recorded in a chain of computer code. The transfer's details are recorded on a public ledger that can be seen by anyone on the network [19].

Alongside the improvement of technology, blockchain is applied in digital currencies and has, likewise, become well known in numerous different fields. The current blockchain is a technology that maintains a peer-to-peer digital ledger that stores all transactions distributed freely or secretly to all clients. Blockchain works on the consensus mechanisms of part or all of the participants, thus eliminating the role of an administrator [20]. In addition, the blockchain provides smart contracts used for generating transactions which are then distributed to every peer in the network, where they are immutably recorded on their copy of the ledger.

The model is based on one smart contract that has the function of storing and querying data. The data is stored in the distributed ledger through the functions defined inside the smart contract, similar to function query data. Depending on the system's requirements and different operations, the development of more smart contracts is also considered to ensure the feasibility of the entire system.

Moreover, a blockchain network is defined when numerous associations meet up and characterize a series of arrangements after going along with them. Furthermore, these strategies might occasionally change, relying upon the structure of the participating associations.

2.2. Permission and Permissionless Blockchain Network

In a permissionless blockchain, almost anyone can join, and every participant is anonymous. In such context, there is no trust other than the state of the blockchain, which is immutable. To eliminate the lack of trust, permissionless blockchains typically use mined cryptocurrencies or transaction fees to provide an economic incentive to offset the extraordinary costs of engaging in a fault-tolerant byzantine. Consensus is based on proof of work (PoW) [21,22].

On the other hand, a permission blockchain operates a blockchain that is a collection of known, defined, and often audited participants that operate under a governance model that provides a certain amount of trust. By relying on the participants' identities, the permission blockchain can use the crash fault-tolerant (CFT) or byzantine fault-tolerant (BFT) consensus protocol without requiring expensive mining [23,24].

In addition, in the context of permission Blockchain, the risk of participants who intentionally introduce malicious code through smart contracts will be reduced. First, the participants will know each other. All actions, whether submitting application transactions, modifying network configurations, or deploying smart contracts, are recorded on the blockchain according to the network's endorsement policy settings and the transaction type involved. Instead of being completely anonymous, the offending party can be easily identified, and the incident is easily recognized and handled in terms of the governance model.

2.3. Hyperledger Fabric

Hyperledger Fabric [25] is an open-source enterprise-grade permission distributed ledger technology (DLT) platform intended for significant business utilization that offers a few essential capacities that separate it from other distributed ledger or blockchain platforms. The Fabric has a modular, configurable architecture, allowing for innovation, is adaptable, and advanced for some utilizing cases, including banking, finance, insurance, healthcare, human resource, and supply chain. The simple architecture of a Hyperledger Fabric (Figure 1) network includes:

- **N**: Network.
- **NC**: Network Configuration.
- **C**: Channel. A collection of organizations with a certain role in the same business process. For example, two organizations, such as car manufacturers and car distributors, will be in a channel about buying and selling cars.
- **CC**: Channel Configuration.
- **R**: Organization.
- **O**: Orderer Node. In public blockchain, all network nodes participate in the consensus process; in Hyperledger Fabric, only the orderer participates in that process.
- **P**: Peer is the point of interaction between members of the organization corresponding to the channel. All user actions must go through the peer.
- **S**: Smart Contract (Chaincode) is installed on the channel, clearly defining structs, actions that users can perform to interact with the state of the struct stored in the ledger.
- **CA**: Certificate Authority. Issue identity assigned to user or node of the respective organization. For example, user A is a member of Organization R1. When he wants to join the network, he will request CA1. Then, CA1 will generate an identity consisting

of a private key, a public key, and associated properties. Then, CA1 returns it to user A. From then on, A uses the identity to perform interactions with the network. The network automatically knows that it is user A from organization R1.

- **A**: Application. An application or an interface (web, mobile app) helps users interact with the system more easily.
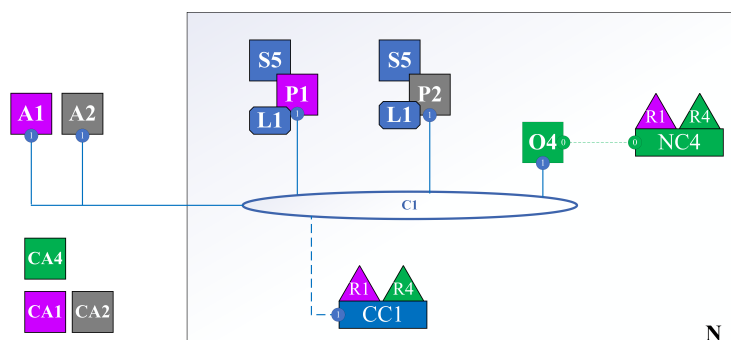

Figure 1. Hyperledger Fabric Network.

This paper applies Hyperledger Fabric to implement our proof-of-concept for three main reasons. The first reason is the Hyperledger Fabric architecture is based on a modular architecture separating the transaction processing into three phases: distributed logic processing and agreement called chaincode (i.e., smart contract), transaction ordering, and and validating and committing a transaction. This separation offers several advantages, such as less trust and verification levels required across node types and optimized performance and network scalability. The second reason is the data structure, which requires a need-to-know basis. In particular, personal data security, which considers the necessity of specific data elements' privacy, can be achieved through data partitioning on the blockchain. Channels, supported in Hyperledger Fabric, allow data to reach only those parties that need to know. Finally, Hyperledger Fabric supports massive queries based on an immutable distributed ledger where the ledger is a sequenced record of state transitions for a blockchain application. Each transaction results in a set of asset key-value pairs committed to the ledger upon creation, update, or deletion.

2.4. Hyperledger Caliper

Hyperledger Caliper [26] is a standard blockchain apparatus, a Hyperledger project facilitated by the Linux Foundation. It is utilized to gauge the productivity of the particular blockchain execution with a predefined set of use cases. The performance reports, transaction latency, and resource usage are produced by the Hyperledger Caliper so that the other projects of Hyperledger might leverage these resources. Hyperledger Caliper is an open-source project contributed by Huawei, Hyperchain, Oracle, Bitwise, IBM, and the Budapest University of Technology and Economics.

3. Related Work

3.1. Blockchain-Based Medical System

Blockchain as a decentralized and distributed technology can be utilized and powered for many daily life applications. Healthcare is one of the prominent fields where blockchain is supposed to make a substantial impact. It generates a wide range of opportunities and possibilities in current healthcare systems. Specifically, in 2018, Kumar et al. [27] exploited the potential apps of blockchain technology in current healthcare systems to positively address the trustless and transparent aspects of such system. A year later, Marcela et al. [28] introduced a blockchain-based peer-to-peer medical platform to manage the electronic medical records (EMRs). Their proposal kept the encrypted data in the blockchain and allowed the patients to share the decryption key only with healthcare professionals in which he/she trusts. Similarly, Wilber et al. [29] surveyed the blockchain-based medical

system to highlight the most important requirements to fulfill the need of sensitive data protection. Moreover, some papers applied the blockchain architecture to define the healthcare system for specific diseases such as diabetes [30] and COVID-19 [31]. However, the above approaches did not define the blockchain-based healthcare system to address blood donation management.

3.2. Blood Supply Chain Management System

Supply chain management integrates core business processes and information. The process goes through many steps, including customers, retailers, wholesalers, manufacturers, and suppliers, which add value to customers and other stakeholders [32]. The system incorporates a highly complex process that requires synchronization of various activities, resulting in randomness and supply chain risk [33,34]. Regarding the blood supply chain system, Nagurney et al. [35] proposed a model to minimize cost and risk by representing the decay characteristics of blood as an arc multiplier. Armaghan and Pazani [36] suggested a blood supply chain to handle urgent requests for blood units in the earthquake. It is a multi-level, multi-objective model to minimize the cost of blood supply chain networks and maximize the reliability of the selected routes for blood transportation. Eskandari-Khanghahi et al. [37] developed a supply model incorporating mixed-integer linear programming that simultaneously considers location, allocation, inventory, and delivery. Delen et al. [38] sought to support the decision-making process in the blood supply chain using both a geographic information system and data mining techniques. Not only can the blood supply chain store and distribute blood, but it is also a vital issue that is necessary to pay attention to in the medical field, especially to save a patient's life. Thus, designing a system to improve information sharing in a blood supply chain is mandatory and vital. A better method can be found by using blockchain technology to cope with urgent demand, track blood origin, and access blood quality.

3.3. Application of Blockchain Technologies Supply Chain Management

Blockchain is a state sharing and consensus-building technique that fulfills transaction record retention and synchronization of distributed network participant systems [39]. Without having a centralized server, transaction records are recorded, shared on the distributed ledger, and organized into blocks when a new transaction is generated. According to blockchain structure, it is classified into three main types: public, private, and consortium with base technologies, including Bitcoin Core, Ethereum, Hyperledger Fabric, etc. Hyperledger Fabric is an open-source distributed ledger platform designed for developing enterprise-grade permission applications. Fabric provides a platform to build fast, efficient, and secure enterprise blockchain applications. It is characterized as being suitable with B2B transactions, and its membership services have limitations to the entry of unauthorized participants. Because of having a node for verifying the transactions during transaction processing, it is possible to remove uncertain transactions early and fast. Due to these benefits, we intend to design a Hyperledger Fabric architecture-based system for managing blood quality.

The benefits of using Blockchain are it improves the visibility of the product supply chain and streamlines work among participants through real-time tracking capability and smart contract-based characteristics. Blockchain can be used in many industries to track the origin and quality of other products. One of the blockchain-based supply chain projects is the case of China's Walmart and IBM affiliation in 2016, aiming at guaranteeing consumers' confidence in food safety [40]. Using this blockchain technology, consumers can track the food's origin, freshness, and the authenticity of its certifications, such as whether the information of the source, production sites, and distribution process is transparent or not. Another project, the Counterfeit Medicines Projects, is one of the projects in the Hyperledger Research Network, which displays the timestamp for each drug to prevent the production of counterfeit medicines [41]. Blockchain technology can be applied in various fields, such as tracking and classifying forgery, quality degradation, and theft by following

drug production time and location and clarifying its origin. It can also help to improve safety and reduce costs relating to medical sectors. In addition, Nga et al. [42] applied blockchain to store and deliver the volunteer blood donations.

On the other hand, research on blood supply chain management have been conducted by several approaches. Blockchain application in the healthcare supply chain is not as common as others; they are considered "vital". Blockchain solutions are more suitable for healthcare supply chains; however, there are not yet using blockchain solutions for healthcare. Although research investigating applying Blockchain in this sector is increasing, it is mainly used for data sharing and recording data, while using it for supply chain management is rare [43]. Some companies, like Imperial Logistics and FarmaTrust available online: https://www.farmatrust.com/ (accessed on 1 December 2021), use blockchain to manage pharmaceutical supply chains. Other experimental projects such as OrganTree and Dhonor Blockchain also use this technology to connect organ donors available online: https://.organ-tree.com (accessed on 1 December 2021), recipients, and practitioners by using incentives such as paying for funeral costs. Several articles have investigated blood donation tracking. BloodChain and SmartBag focus on preventing contamination in the supply chain and reducing the spread of HIV in developing countries [44]. Another project, called BLOODCHAIN, focuses on motivating blood donors by giving monetary returns. Wust and Gervais (2018) have proposed a flow chart to emphasize the importance of blockchain application in blood origin tracking [45]. The model is presented and discussed in the paper to see whether blockchain should solve the problem; however, the situation has not been solved well.

3.4. Limitation of Existing Research

This study overcomes the restriction of the prevailing research and methods regarding blood information systems and blood supply chain management. The proposed approach can secure the transparency of blood information management by using real-time information recording. When focusing on this point, the system has the advantage of clarifying blood types, such as origin and quality. In terms of blood supply and demand, this system can cope with emergencies when a sudden increase in blood demand in a specific region occurs. Moreover, the blockchain is actively investigated in the supply chain and healthcare sectors. This research contributes further to the scope of investigations in the healthcare system, especially in the blood supply chain, which blockchain technologies have not yet recovered.

4. BloodChain Architecture

This paper designs and develops a blood donation network based on Hyperledger Fabric architecture. This system can detect various supply chains' problems regarding blood donation, such as blood origin or quality, especially for emergency blood requests. The most crucial issue to deal with in this system is blood quality, and it tries to manage the supply and demand of the blood by transactions recorded in the blockchain technology. The procedure below shows the process of how our proposed system works.

The BloodChain model includes five main components in Figure 2, where the four actors (i.e., patient, donor, medical staff, and transportation) send/receive the data to the ledger component, defined by the Hyperledger Fabric.

Based on the role of stakeholders in the system, they (e.g., donors) can track their information from the ledger, which might be hidden from the other parties. Moreover, the coordination among the parties is controlled by the smart contract of the system. In particular, the authorized user obtains the release information and ignores the sensitive data. The primary purpose of this design is that BloodChain minimizes unnecessary data release that may violate privacy. In addition, all the queries of the stakeholders are logged in the ledger. Therefore, the stakeholders can detect who accesses their data, where, and when.
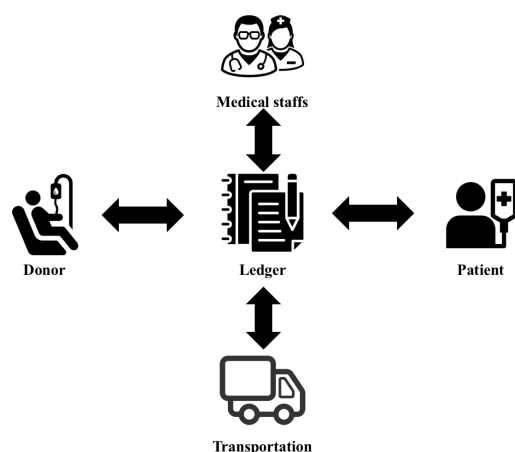
Figure 2. The overall architecture of the BloodChain model.

Figure 3 shows seven steps in the workflow of the BloodChain model. In the first step, after donations from the volunteers, blood will be stored at the healthcare center and delivered to the medical center in step 2; these blood samples are determined based on the ID_Vol of each volunteer. All the metadata, including the information of volunteers, type of blood, time, and place, is stored on the ledger in the third step. These blood data are only accessible by the facility's medical staff (step 3.1) to prevent unauthorized exploitation of information from external individuals. The blood samples will be shipped to other medical facilities or hospitals after the test is completed (steps 4 and 5).

These steps are performed based on the actual requirements of the system, where the blood bank has collected all the donated blood from the donors and shares these amounts with another hospital, if needed [46].

After changing the storage location, data for each blood sample will be updated with the respective medical facility. The staff's inquiry at the new medical facility is also recorded in the system to help monitor and manage better (steps 6 and 7); certainly, the querying of information is only done by the staff of the new medical facility.
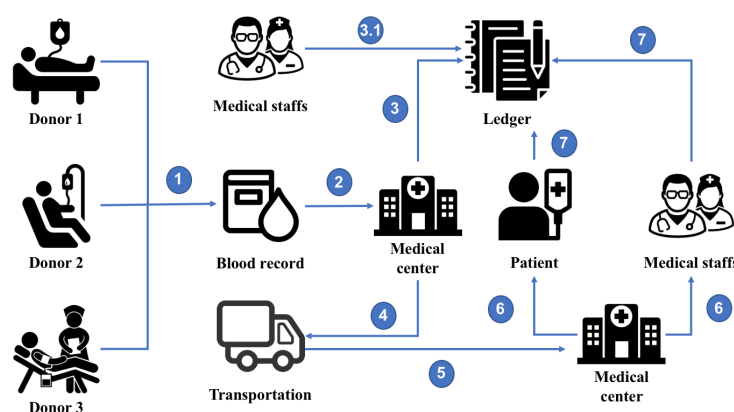

Figure 3. BloodChain overall architecture.

In addition, blood-using data, such as emergency care and blood transfusion, are also recorded to determine which patients have used blood samples donated by volunteers. In many cases, when the donated blood samples have problems or are of poor quality, recording the data also helps improve blood traceability so that health facilities can know which volunteers are in poor health and how much blood they donated to health facilities.

One of the important reasons to implement our proposed system in blockchain is information visibility. Many medical institutions, wherein blood transfusions data are made, record when the final blood is used or disposed of, improving blood inventorying and blood-demand predictability. The participant consensus algorithm of Hyperledger

Fabric sequentially records transactions over time and manages information transparently to prevent forgery or alteration.

5. Implementation

5.1. Data Structure

The participants in the blood management system are defined in the code below. There are five main participants in this system: staff, volunteer, transporter, medical center, and patient. Each actor of BloodChain, during processing, is identified by the corresponding ID in the process. In addition, the participants' metadata is also stored to support data query and tracking.

The volunteers performing the blood donation are the first participants of the process, their data collected after the blood donation procedure is completed. It is stored together with the metadata of their blood sample. The code below describes volunteers' reports in detail with their metadata, such as name, age, gender, address, nationality, career, and health condition. This information is essential to evaluate blood quality.

```
{ "ID_Vol":"dn001",
"name":"Nguyen Van A",
"age":"32",
"gender":"female",
"address":"Ho Chi Minh",
"nationality":"Viet Nam",
"career":"student",
"healthcondition:"good"}
```

Blood has a specific shelf life depending on its ingredient formulation. Therefore, storing and preserving the quality of the blood is critical in the whole process, which is done after completing the blood collection and keeping the volunteer's information. Blood sample data is identified by a separate ID_Blood and ID_Vol, making blood quality and origin management easier. In addition, it allows the user to view the number of blood assets based on the volunteer's information. If the quality of blood has a disease that is unknown when donating, medical facilities will quickly notify the volunteer of their health status. Due to the specific ingredient-dependent shelf life of blood, it is necessary to check the shelf life and dispose of it afterward regularly. That is why we record the date and time information in the transaction. After a day in the system, the retention time of all blood assets is reduced by one day. The blood group's unique ID_Blood includes its date and time metadata. This information allows the medical staff to see how long the blood donation is kept. Blood moves according to the blood supply for blood transfusion. The procedure for storing blood sample data is presented in the structure below.

```
{ "ID_Blood":"bs001",
"ID_Vol":"dn001",
"type":"O",
"date":"09/20/2021",
"time":"11:45",
"location":"Ho Chi Minh",
"medicalcenter":"Cho Ray"}
```

The state of motion is determined to indicate whether the blood is currently moving or within the organ. In addition, blood possession information is determined. Management of the blood collection process, including transportation, has been identified as a critical step in the entire process. Therefore, information related to the shipping company also needs to be stored in the system.

As can be seen from the structure of the process to record blood sample information, the information of the delivery company is also registered to serve the purpose of verification during the transport of blood samples. The information recorded in the system includes

ID_Company (name of delivery company), ID_Delivery (name of delivery worker), name of delivery person, age, phone number, address of the delivery person. This information is structured in the process of recording transportation.

```
{ "ID_Company":"company001",
"ID_Delivery":"delivery001",
"name":"deliverer001",
"age":"30",
"number":"12345678",
"address":"Ho Chi Minh"}
```

The patient's information who receives donation blood is recorded in the system under the structure below.

```
{ "ID_Pat":"volunteers001",
"ID_Blodd":"bs001",
"name":"Le Thi B",
"age":"20",
"address":"Binh Duong",
"medicalstatus":"status record 001"}
```

Patient and medical personnel information is also created and stored to determine which patients have received which units of blood and whether healthcare staff has access to blood data. The information recorded in the system consists of six components: ID_Pat, blood sample, name, age, address, and medical status. The sample information can be seen clearly in the structure below.

```
{ "ID_Staff":"staff001",
"name":"Jenny",
"age":"25",
"number":"+84 22334455",
"gender":"female",
"address":"Long An",
"workingStatus":"active"}
```

5.2. Algorithms

In the proposed system, we have several algorithms to operate the system. The proposed method in this paper uses Hyperledger Fabric to conduct transactions. BloodChain exploits JavaScript structure for the data structure and the blockchain network for the process structure since it is suitable for a private business environment.

BloodChain consists of two main algorithms, including Algorithm 1 (to describe the mechanism to store volunteer blood samples) and Algorithm 2 (which summarizes delivering blood samples from the donation place to the medical center).

Algorithm 1 consists of five main steps. It describes the mechanism to gather volunteers' blood samples (i.e., blood metadata). Blood samples, once collected, will be identified with the ID_Vol of the respective volunteer. Each blood sample will have a separate ID_Blood to avoid duplicating data inside the ledger; the blood will be stored at the medical facility after being donated. The blood samples will also be stored in the ledger.

Algorithm 1 storing blood samples of Volunteer.

1: Input: Volunteer ID, name, age, date of birth, blood type, amount of blood unit
2: Output: data of Volunteer and their blood is stored into ledger
3: **for** unit of blood **do**
4:     storing data of Volunteer and blood to ledger
5: **end for**

Algorithm 2 summarizes delivering blood samples from the donation place to the medical center; this process can be repeated based on the context. After storage, the blood samples will be transported to different medical facilities in the donation place. To this end, the shipper information will be stored in the ledger to determine which company transports the blood and how many units of blood have been transported, i.e., updates the metadata. The process's input is the data of the delivery unit, and the output of the algorithm is the data of delivery and the new medical center, which receives the blood from the volunteer. Its corresponding ID_Center further identifies each step.

Algorithm 2 transportation of blood samples from donation places to medical center.

1: Input: data of delivery unit
2: Output: data of delivery is stored to ledger, new medical center also updated
3: **for** delivery unit **do**
4:   **for** blood samples **do**
5:     storing ID of blood unit with correspondence ID of delivery unit
6:   **end for**
7:   **for** blood samples **do**
8:     update location of new medical center of blood samples
9:   **end for**
10: **end for**
11: **return** Encrypted hash

Moreover, the authors provide the source code for the proof of concept and instruction of installation. Interested readers might refer to our GitHub repository : https://github.com/Masquerade0127/bloody-blockchain (accessed on 1 December 2021).

6. Evaluation Scenarios

6.1. Environment Setting

Our paradigm is deployed on the Hyperledger Fabric network maintained inside docker containers. The evaluated result is developed on a personal workstation equipped with 8 GB RAM and Intel Core i5 2.7GHz x 4 .

To prove the effectiveness of BloodChain, we also define several experiments by exploiting the Hyperledger Caliper that is used to design the test scenarios and collect all the information regarding the BloodChain performance.

6.2. First Scenario

In the first scenario, we measure the results of the requests sent to the create data function; with one worker being initialized in the network, the initial number of requests is 1000 per second. The number of requests is continuously sent to the system within 2 min and gradually increases to 10,000 requests per second. The measurement results are shown in Figure 4. We observe that the number of successfully executed requests is relatively high compared to the failed requests; most of the successful requests are above 12,000 requests per second, while the number of failed requests only ranges from 2–3 requests.
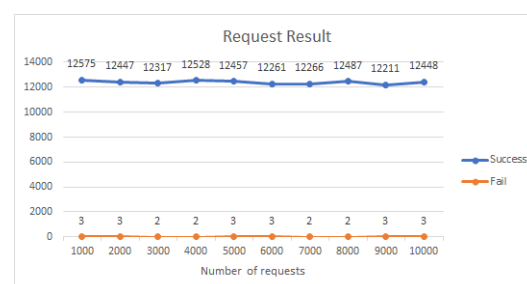

Figure 4. The results of the create data functions.

Figure 5 depicts the results and number of requests to query the data of blood records in the database. In this scenario, the number of workers increases to 10; each worker, in turn, sends 1000 requests to create 10,000 requests per second in the system. The system's data query results are still stable, in which the number of successful requests ranges from the lowest level of 37,204 to the highest 42,169 requests, while the number of failed data query requests is only from 0 to 1 request.
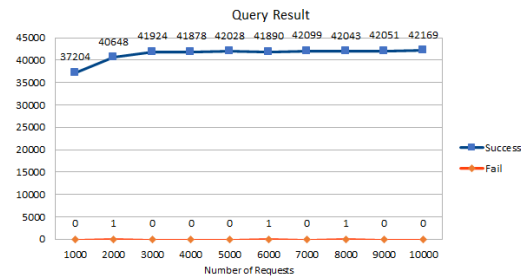

Figure 5. The results of the request data functions.

Figure 6 depicts the measurement results of requests that perform the data update function for blood samples. In this feature, the number of workers increased by two compared to the initial data initialization request; the number of requests is also increased from 1000 requests to 10,000 requests per second per worker. The number of successful requests increased slightly from the lowest level of 15,235 to the highest of 16,206 requests per second. However, the number of failed requests is higher than that in scenario number one because the number of workers has increased. This means that the system takes longer when the number of users increases. It takes more time to process the received requests, and the number of failed requests increases.
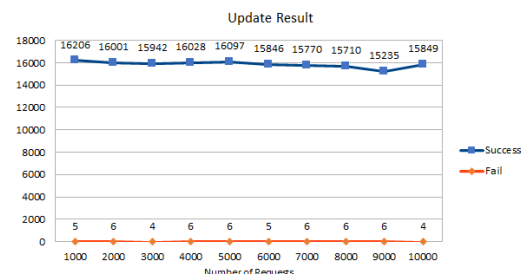

Figure 6. The results of the update data functions.

6.3. Second Scenario

In this second scenario, the article measures and evaluates the latency corresponding to three functions of data initialization, query, and update.

Figure 7 shows the latency of the data initialization function of the blood samples, in which most of the three latency levels are stable. Specifically, the maximum latency index fluctuates in the range of 500 s when the number of requests increases from 1000 to 10,000 requests. However, a particular case occurs in case 6 with 6000 requests per second; the latency increases quite a lot at 2240.21 s, which may occur when the system has a bottleneck in processing transactions, so incoming transactions take longer to complete processing. Nevertheless, at the two indicators Min and Avg latency, the processing time for requests is still kept at a stable level of 363.16 s/request and 0.64 s/request, respectively.
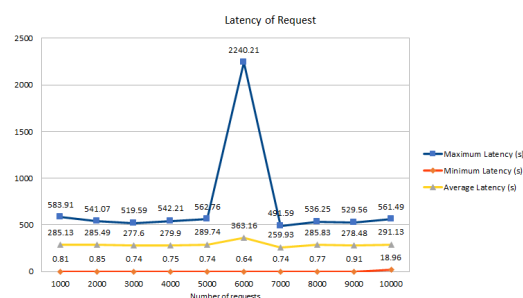
Figure 7. The latency of the data initialization functions.

The latency of data query requests is shown in Figure 8. The maximum latency index fluctuates quite strongly from 1.41 s/request to 4.64 s/request. However, the system's processing time gradually decreased and remained stable when the number of requests increased from 1000 to 10,000. The highest value is 4.65 s for a total of 2000 requests.
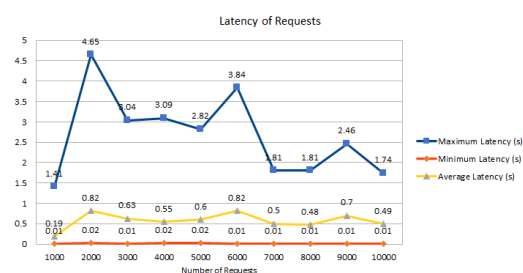

Figure 8. The latency of the request data functions.

Figure 8 describes the latency of requests to query data of all users in the system. Minimum latency 0.01–0.02 and average latency 0.19–0.82 are minimal even when the number of requests increases to 10,000 requests simultaneously. The maximum value of Max latency is 4.65 s, corresponding to the situation of 10 users sending 2000 requests to the system at the same time.

Finally, the latency of the data update function of the blood samples is also shown in Figure 9. The latency of the requests is kept stable when the number of requests increases from 1000 to 10,000 requests. However, the processing time is at the highest level compared to 2 requests to initiate and query data; this happens when the system starts querying the data and then updates the data fields that requested data and stores new ones. The maximum value of Max Latency is 795.4 s for 1000 requests; in addition, the rest of the cases are stable with a delay of over 700 s.
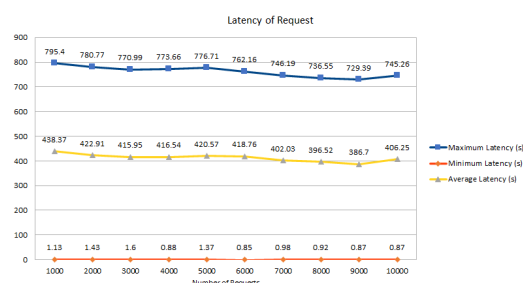

Figure 9. The latency of the update data functions.

6.4. Security and Privacy Discussion

The blockchain plays a vital role in the modern system; this model meets the transparency and availability requirements for the supply chain [6,47,48]. However, the blockchain-based system still has some problems that are listed in [49], especially in the security and

privacy aspect. To improve the security and privacy issues in the blockchain-based blood donation system, we consider the authorization for the parties in the same transaction and the flexibility in the medical environment.

For the authorization aspect, we will exploit attribute-based access control (ABAC) [50,51] to manage the access control process. The main benefit of this model is that only authorized users can access the release data. In addition, the query rewriting can apply for the complex context where the released data is shared to multiple users [52,53]. Finally, some approaches split the original policy into sub-policy [54,55] (i.e., public and private policy) to ensure the data is only accessed via permission, even by parties in the same transaction.

Finally, compared to the prior work, this is the first approach providing the proof-of-concept to target blood donation management. In the state of the art, some papers consider the general issues in the healthcare system rather than focus on the specific problem, i.e., blood management. This paper highlighted BloodChain by applying blockchain technology to exploit the benefits of this system. We also present the result of our proposed model based on several experiments.

7. Conclusions

This paper designed, developed, and evaluated the BloodChain system, which manages a blood donation network based on private blockchain technology to obtain several goals: secure blood information visibility and guarantee the blood quality for both receivers and donors. Thanks to the real-time recording and sharing of information, blood is donated, classified, and recorded in distributed ledgers, enabling the efficient management of blood. The information of the actors is transparent with the other parties in the same transaction. This protocol helps participants track the source of blood quality easily via the corresponding metadata. In addition, BloodChain prevents forgery and information tampering, making the blood management operation more transparent by solving problems in traditional medical institutions, such as missing entry inputs, exit, and band errors. Moreover, the BloodChain system supports blood transactions among medical institutions and can easily manage blood quality. This function benefits both receivers and donors: (i) receivers feel safe when the blood quality is ensured, and (ii) donors know their health situation. A thorough evaluation of BloodChain is performed to prove the effectiveness of the proposed scheme. However, to realize the blockchain network proposed by this paper, consideration should be given to the coordination of interests among participants in the blood chain system and the infrastructural, legal, institutional, and technical aspects.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. Disponible. 2009. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 25 November 2021).
2. Le, N.T.T.; Nguyen, Q.N.; Phien, N.N.; Duong-Trung, N.; Huynh, T.T.; Nguyen, T.P.; Son, H.X. Assuring Non-fraudulent Transactions in Cash on Delivery by Introducing Double Smart Contracts. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 677–684. [CrossRef]
3. Le, H.T.; Le, N.T.T.; Phien, N.N.; Duong-Trung, N. Introducing multi shippers mechanism for decentralized cash on delivery system. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 590–597. [CrossRef]
4. Ha, X.S.; Le, H.T.; Metoui, N.; Duong-Trung, N. Dem-cod: Novel access-control-based cash on delivery mechanism for decentralized marketplace. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 10–13 November 2020; pp. 71–78.

5. Ha, X.S.; Le, T.H.; Phan, T.T.; Nguyen, H.H.D.; Vo, H.K.; Duong-Trung, N. Scrutinizing trust and transparency in cash on delivery systems. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Nanjing, China, 18–20 December 2020; pp. 214–227.

6. Son, H.X.; Le, T.H.; Quynh, N.T.T.; Huy, H.N.D.; Duong-Trung, N.; Luong, H.H. Toward a Blockchain-Based Technology in Dealing with Emergencies in Patient-Centered Healthcare Systems. In Proceedings of the International Conference on Mobile, Secure, and Programmable Networking, Paris, France, 28–29 October 2020; pp. 44–56.

7. Duong-Trung, N.; Son, H.X.; Le, H.T.; Phan, T.T. On Components of a Patient-Centered Healthcare System Using Smart Contract. In Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, Nanjing China, 10–12 January 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 31–35. [CrossRef]

8. Duong-Trung, N.; Son, H.X.; Le, H.T.; Phan, T.T. Smart Care: Integrating Blockchain Technology into the Design of Patient-Centered Healthcare Systems. In Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, ICCSP 2020, Nanjing, China, 10–12 January 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 105–109. [CrossRef]

9. Thanh, L.N.T.; Nguyen, T.A.; Vo, H.K.; Luong, H.H.; Nguyen, H.T.K.; Dao, A.T.; Ha, X.S. Toward a Unique IoT Network via Single Sign-On Protocol and Message Queue. In Proceedings of the International Conference on Computer Information Systems and Industrial Management, Ełk, Poland, 24–26 September 2021.

10. Thanh, L.N.T.; Phien, N.N.; Vo, H.K.; Luong, H.H.; Anh, T.D.; Tuan, K.N.H.; Son, H.X. UIP2SOP: A Unique IoT Network applying Single Sign-On and Message Queue Protocol. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 19–30. [CrossRef]

11. Thanh, L.N.T.; Nguyen, T.A.; Vo, H.K.; Luong, H.H.; Tuan, K.N.H.; Dao, A.T.; Son, H.X. Toward a Security IoT Platform with High Rate Transmission and Low Energy Consumption. In Proceedings of the International Conference on Computational Science and its Applications, Cagliari, Italy, 13–16 September 2021.

12. Son, H.X.; Nguyen, M.H.; Vo, H.K. Toward an privacy protection based on access control model in hybrid cloud for healthcare systems. In *Advances in Intelligent Systems and Computing, Proceedings of the International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019), Seville, Spain, 13–15 May 2019*; Springer: Cham, Switzerland, 2019; pp. 77–86.

13. Thanh, L.N.T.; Phien, N.N.; Nguyen, T.A.; Vo, H.K.; Luong, H.H.; Anh, T.D.; Tuan, K.N.H.; Son, H.X. IoHT-MBA: An Internet of Healthcare Things (IoHT) Platform based on Microservice and Brokerless Architecture. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*. [CrossRef]

14. Hajipour, V.; Niaki, S.T.A.; Akhgar, M.; Ansari, M. The healthcare supply chain network design with traceability: A novel algorithm. *Comput. Ind. Eng.* **2021**, *161*, 107661. [CrossRef]

15. Ho, G.; Tang, Y.M.; Tsang, K.Y.; Tang, V.; Chau, K.Y. A blockchain-based system to enhance aircraft parts traceability and trackability for inventory management. *Expert Syst. Appl.* **2021**, *179*, 115101. [CrossRef]

16. Emmanuel, J.C. *The Blood Cold Chain*; WHO Report: Geneva, Switzerland, 2017.

17. Baek, E.J.; Kim, H.O.; Kim, S.; Park, Q.E.; Oh, D.J. The trends for nationwide blood collection and the supply of blood in Korea during 2002–2006. *Korean J. Blood Transfus.* **2008**, *19*, 83–90.

18. Delaforce, A.; Duff, J.; Munday, J.; Hardy, J. Overcoming barriers to evidence-based patient blood management: A restricted review. *Implement. Sci.* **2020**, *15*, 1–13. [CrossRef]

19. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.

20. Michael, J.; Cohn, A.; Butcher, J.R. Blockchain Technology. Available online: https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-Feature-Blockchain.pdf (accessed on 1 December 2021).

21. Shahriar Hazari, S.; Mahmoud, Q.H. Improving Transaction Speed and Scalability of Blockchain Systems via Parallel Proof of Work. *Future Internet* **2020**, *12*, 125. [CrossRef]

22. Qu, Q.; Xu, R.; Chen, Y.; Blasch, E.; Aved, A. Enable Fair Proof-of-Work (PoW) Consensus for Blockchains in IoT by Miner Twins (MinT). *Future Internet* **2021**, *13*, 291. [CrossRef]

23. Feng, L.; Zhang, H.; Chen, Y.; Lou, L. Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain. *Appl. Sci.* **2018**, *8*, 1919. [CrossRef]

24. Nijsse, J.; Litchfield, A. A Taxonomy of Blockchain Consensus Methods. *Cryptography* **2020**, *4*, 32. [CrossRef]

25. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.

26. Díaz-Santiso, J.; Fraga-Lamas, P. E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts. *Eng. Proc.* **2021**, *7*, 11. [CrossRef]

27. Kumar, T.; Ramani, V.; Ahmad, I.; Braeken, A.; Harjula, E.; Ylianttila, M. Blockchain utilization in healthcare: Key requirements and challenges. In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018; pp. 1–7.

28. de Oliveira, M.T.; Reis, L.H.; Carrano, R.C.; Seixas, F.L.; Saade, D.C.; Albuquerque, C.V.; Fernandes, N.C.; Olabarriaga, S.D.; Medeiros, D.S.; Mattos, D.M. Towards a blockchain-based secure electronic medical record for healthcare applications. In Proceedings of the ICC 2019-2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.

29. Wilber, K.; Vayansky, S.; Costello, N.; Berdik, D.; Jararweh, Y. A Survey on Blockchain for Healthcare Informatics and Applications. In Proceedings of the 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Paris, France, 14–16 December 2020; pp. 1–9.

30. Shynu, P.; Menon, V.G.; Kumar, R.L.; Kadry, S.; Nam, Y. Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing. *IEEE Access* **2021**, *9*, 45706–45720. [CrossRef]

31. Torky, M.; Hassanien, A.E. COVID-19 blockchain framework: Innovative approach. *arXiv* **2020**, arXiv:2004.06081.

32. Kim, D. An integrated supply chain management system: A case study in healthcare sector. In Proceedings of the International Conference on Electronic Commerce and Web Technologies, Copenhagen, Denmark, 23–26 August 2005; pp. 218–227.

33. Shahbaz, M.S.; RM, R.Z.; Bin, M.F.; Rehman, F. What is supply chain risk management? A review. *Adv. Sci. Lett.* **2017**, *23*, 9233–9238. [CrossRef]

34. Lavastre, O.; Gunasekaran, A.; Spalanzani, A. Effect of firm characteristics, supplier relationships and techniques used on supply chain risk management (SCRM): An empirical investigation on French industrial firms. *Int. J. Prod. Res.* **2014**, *52*, 3381–3403. [CrossRef]

35. Nagurney, A.; Masoumi, A.H.; Yu, M. Supply chain network operations management of a blood banking system with cost and risk minimization. *Comput. Manag. Sci.* **2012**, *9*, 205–231. [CrossRef]

36. Armaghan, N.; Pazani, N. A Model For Designing A Blood Supply Chain Network To Earthquake Disasters (Case Study: Tehran City). *Int. J. Qual. Res.* **2019**, *13*, 605–624. [CrossRef]

37. Eskandari-Khanghahi, M.; Tavakkoli-Moghaddam, R.; Taleizadeh, A.A.; Amin, S.H. Designing and optimizing a sustainable supply chain network for a blood platelet bank under uncertainty. *Eng. Appl. Artif. Intell.* **2018**, *71*, 236–250. [CrossRef]

38. Delen, D.; Erraguntla, M.; Mayer, R.J.; Wu, C.N. Better management of blood supply-chain with GIS-based analytics. *Ann. Oper. Res.* **2011**, *185*, 181–193. [CrossRef]

39. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov.* **2016**, *2*, 71.

40. Hackius, N.; Petersen, M. Blockchain in logistics and supply chain: Trick or treat? In *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment, Proceedings of the Hamburg International Conference of Logistics (HICL), Hamburg, Germany, 12–13 October 2017*; Epubli GmbH: Berlin, Germany, 2017; Volume 23, pp. 3–18.

41. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 1–3.

42. Quynh, N.T.T.; Son, H.X.; Le, T.H.; Huy, H.N.D.; Vo, K.H.; Luong, H.H.; Tuan, K.N.H.; Anh, T.D.; Duong-Trung, N. Toward a Design of Blood Donation Management by Blockchain Technologies. In Proceedings of the International Conference on Computational Science and Its Applications, Cagliari, Italy, 13–16 September 2021; pp. 78–90.

43. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A systematic review of the use of blockchain in healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]

44. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.

45. Wüst, K.; Gervais, A. Do you need a blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; pp. 45–54.

46. Pradhan, N.R.; Singh, A.P.; Kumar, V. Blockchain-enabled traceable, transparent transportation system for blood bank. In *Advances in VLSI, Communication, and Signal Processing*; Springer: Cham, Switzerland, 2021; pp. 313–324.

47. Campanile, L.; Iacono, M.; Levis, A.H.; Marulli, F.; Mastroianni, M. Privacy Regulations, Smart Roads, Blockchain, and Liability Insurance: Putting Technologies to Work. *IEEE Secur. Priv.* **2020**, *19*, 34–43. [CrossRef]

48. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* **2017**, *41*, 1027–1038. [CrossRef]

49. Joshi, A.P.; Han, M.; Wang, Y. A survey on security and privacy issues of blockchain technology. *Math. Found. Comput.* **2018**, *1*, 121. [CrossRef]

50. Hoang, N.M.; Son, H.X. A dynamic solution for fine-grained policy conflict resolution. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lumpur, Malaysia, 19–21 January 2019; pp. 116–120.

51. Son, H.X.; Hoang, N.M. A novel attribute-based access control system for fine-grained privacy protection. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lumpur, Malaysia, 19–21 January 2019; pp. 76–80.

52. Son, H.X.; Dang, T.K.; Massacci, F. REW-SMT: A new approach for rewriting xacml request with dynamic big data security policies. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Guangzhou, China, 12–15 December 2017; pp. 501–515.

53. Xuan, S.H.; Tran, L.K.; Dang, T.K.; Pham, Y.N. Rew-xac: An approach to rewriting request for elastic abac enforcement with dynamic policies. In Proceedings of the 2016 International Conference on Advanced Computing and Applications (ACOMP), Tho City, Vietnam, 23–25 November 2016; pp. 25–31.

54. Son, H.X.; Chen, E. Towards a fine-grained access control mechanism for privacy protection and policy conflict resolution. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 507–516. [CrossRef]

55. Thi, Q.N.T.; Dang, T.K.; Van, H.L.; Son, H.X. Using json to specify privacy preserving-enabled attribute-based access control policies. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Guangzhou, China, 12–25 December 2017; pp. 561–570.