Journal of
Theoretical and Applied Electronic Commerce Research

MDPI

Article

Integrating Blockchain for Health Insurance in Indonesia with Hash Authentication

Erwin Sutanto [1,*], Rahmat Mulyana [2], Franky Chandra Satria Arisgraha [3] and Guillermo Escrivá-Escrivá [4]

[1] Department of Physics, Universitas Airlangga, Kampus C Unair Mulyorejo, Surabaya 60115, Indonesia
[2] Department of Computer and System Sciences, Stockholm University, Borgarfjordsgatan 12, Kista, 16455 Stockholm, Sweden
[3] Biomedical Engineering, Universitas Airlangga, Kampus C Unair Mulyorejo, Surabaya 60115, Indonesia
[4] Institute for Energy Engineering, Universitat Politècnica de València, Camino de Vera, s/n, Edificio 8E, Escalera F, 2 °piso, 46022 Valencia, Spain
* Correspondence: erwin_sutanto@fst.unair.ac.id

Abstract: The use of blockchain has received great attention in its adoption as a financial instrument in cryptocurrencies. This phenomenon needs to be considered in the sense not only as a form of financial transactions but also in other fields such as health, which is also a challenge for modern society. In addition, several government policies have also supported the provision of health services as a form of improving people's living standards in the form of insurance. In this study, we try to design the system by using UML diagram and simulate the use of DApps offered by the Vexanium Ecosystem. For example, three basic activities between patients, doctors, and insurance will be simulated in the form of the transaction ledger. This method allows us to speed up the authentication process that previously needed to be performed for a long time with bureaucracy becoming the rule in smart contracts in a matter of minutes. The evaluation of this method will then be compared with eight existing blockchain projects. The result in healthcare processes is cost savings through increased automation, speed, standardization, and efficiency. All of this can be a preliminary analysis of its application in Indonesia, particularly related to the authentication and recording of medical records.

Keywords: blockchain; reduced inequalities; DApp; smart contract; health system access

check for updates

Citation: Sutanto, E.; Mulyana, R.; Arisgraha, F.C.S.; Escrivá-Escrivá, G. Integrating Blockchain for Health Insurance in Indonesia with Hash Authentication. *J. Theor. Appl. Electron. Commer. Res.* **2022**, *17*, 1602–1615. https://doi.org/10.3390/jtaer17040081

Academic Editor: Jemal Abawajy

Received: 12 September 2022
Accepted: 23 November 2022
Published: 29 November 2022

1. Introduction

Blockchain is a technology platform that is becoming a trend today. In recent years, it has also penetrated several different types of industries, including the healthcare industry. Blockchain itself offers privacy, security, and distributed databases that can operate without a central authority or administrator. Blockchain uses a distributed peer-to-peer network to create a continuous growth of ordered lists of records called blocks to form a digital ledger. Each transaction, represented in a cryptographically signed block, is then automatically validated by the network itself. This will make the data more trustworthy and the privacy of the user can be maintained compared to data that are equally accessible but without authentication.

Bitcoin and cryptocurrency are two things that are starting to be felt in the financial sector today and are predicted to become a digital currency system. First introduced in 2008, it is one of the most well-known blockchain implementations. The transfer of digital assets, such as bitcoin, in the blockchain begins when a seller or payer submits a transaction. By looking at the possibility of transactions, there is also the possibility of using blockchain to guarantee the use of health insurance in Indonesia. This use needs to be seen from several sides, both in terms of how to use it and its safety. In terms of how to use it, of course, is closely related to the blockchain itself [1]. Therefore, the idea of blockchain integration has emerged recently, following the massive increase in the use of blockchain and the opportunity to control and exploit it in terms of administration and standardization. The infrastructure of the blockchain runs on a peer-to-peer concept by utilizing both network users (both seller and payer). In addition, there is also a blockchain miner who will validate transactions in the ledger. Before then, it will be distributed to the network. By utilizing each node built by the miner, validation will be carried out with cryptographic. Furthermore, it should also be noted that the ledger is also created through the consensus method, and the hash chain ensure secure storage [2].

Service management in Indonesia is currently facing challenges mainly related to its quality and ability to balance and respond to community needs. Generally, this service is also provided in the form of insurance. Blockchain adoption has been carried out in various sectors, one of which is healthcare. However, this sector is quite slow in adopting digital transformation due to several things, such as trust in data handling and also security issues, as the two main causes [3]. This can be seen as a challenge to how blockchain technology can be used such as in the management, and exchange of medical records from patients where privacy needs to be taken into account. Tolerating privacy concerns by only prioritizing the digital revolution in the healthcare industry is not a priority [4]. Therefore, despite the potential impact of digital transformation on healthcare, it is not going to be easy. Further, it is as if progress has been limited simply because of a lack of confidence or concerns about data protection. Some things in the blockchain ecosystem that can be used include smart contract, DApp, and cloud server. However, research is still needed to verify the feasibility because blockchain technology has the potential to support programs in reduced inequalities.

The authentication process of health insurance in Indonesia should also be accelerated by using various features that already exist in the blockchain ecosystem. The adoption of cutting-edge technologies, such as DApp and smart contract, could be the answer to this problem. With the help of this technology, medical records and other information connected to healthcare services are able to be stored on a secure and opaque platform. Disclosure of sensitive patient information can have negative effects. The interest and momentum of blockchain can be seen from the previous use of IoT (Internet of Things). This kind of technology has extended to healthcare in its information technology field [5]. Therefore, this study answers at least two research questions regarding the adoption of blockchain technology, as follows:

1. How to adopt blockchain technology when patients want to claim health insurance?
2. What is the position of DApps and smart contracts in solving authentication problems in the insurance claim process?

Thus, the method is to test its possible usage with one of the ecosystems that have been adopted in Indonesia. It would be then compared with some existing projects in the healthcare sector. To test the hypothesis that blockchain can be easily integrated into many existing medical application start-ups, we simulated basic transactions to study DApps and smart contracts to realize the simple authentication model. However, because the data are spread across various medical facilities, handling EHR (electronic health records) or EMR (electronic medical records) securely becomes very difficult [6]. There are still certain issues with data integrity, ownership of user data, and security of medical information. Recognizing the potential relevance and importance of blockchain in healthcare, research is needed to update it and see its possible applications that will support many start-ups in the healthcare sector.

2. Methods

The user is part of a system that collects data from wearable devices that monitor user health data such as walking distance, sleep state, and heart rate [7]. A device that works to convert original health information into a human-readable format and then the data is synced by users to their online accounts. Healthcare providers such as doctors are appointed by certain users to carry out medical tests, provide some advice or provide medical care [8]. The last is the health insurance company. Users can request a health insurance quote from a health insurance company or agent to choose the right health insurance plan. Where, from a trusted party, it can be authenticated using a digital certificate [9]. On the other hand, patient data storage is still in the privacy area. The visualization of the proposed system will use the Unified Modeling Language (UML) to acquire standards in the explanation of this study.

Figure 1 illustrates the use case diagram of the entire general medical process between doctors and patients using blockchain technology. Of the three interactions represented by the lines between the roles above, some processes can take advantage of blockchain technology, including:

1. Between patients and doctors as users in the blockchain network, there are several stages; such as when a patient wants to send an EMR to the doctor. Then, from the doctor when they wanted to give the results of his health diagnosis. Further, how much it cost to pay for doctor's services. All these stages can be created in a new block. Blocks from the blockchain are used for all these stages, and these blocks are transmitted to all nodes connected to the network. Including payment transactions, which of course will be connected to the wallets of patients and doctors. In this process, a copy of the entire blockchain is made available to every node in the network for verification. In the verification process, the new block will be checked whether it has not been tampered with in any way after being distributed to all nodes. Next, nodes will add that block to their copy of the blockchain when successful.
2. Between the patient and insurance, here of course the patient will make sure whether they will use insurance. if yes, of course, it will provide access to the data to the doctor. As node verification is by consensus, the verification stage from the insurer can follow the verification results from the blockchain. Where will it be decided which blocks are valid to add to the blockchain and which are not? The node will perform validation to confirm the existing transaction and also make sure whether the sender is a legitimate member. Mining is the term for this transaction validation procedure.
3. Between insurance and a doctor, here, the doctor will charge the doctor's consultation fee and medicine, if any. The block is added to the blockchain after validation is complete. If a node successfully completes the validation, the transfer of cryptocurrency transactions between wallets can also be carried out.
4. Finally, the transaction is completed after the entire validation process is complete.

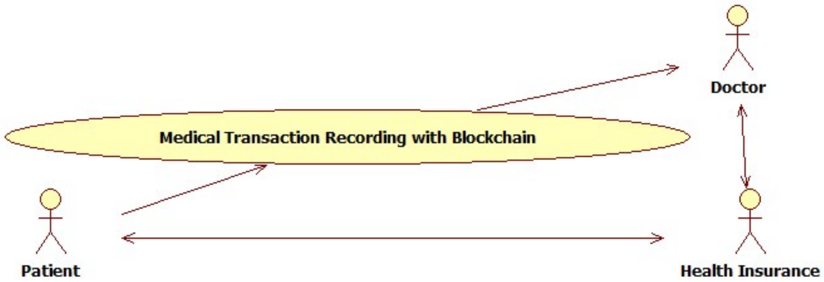

Figure 1. Use case diagram for data flow access.

The scenario of this stage can be one of the references in the process that describes transactions from doctors and insurance. This is, of course, not the only one and various other options need to be seen in this review.

2.1. Network Application

An internet-based application can be characterized by two architectural approaches, namely centralized and decentralized [10]. In a centralized system, nodes are located around the server and are connected to one server node, which functions as a coordination center, whereas decentralized, on the other hand, has several connected nodes without a central node where everything acts as a server.

Figure 2 illustrates the differences between the two architectures. There are several advantages of a distributed system, namely having greater computing power by combining the computing power of all connected nodes, increasing reliability because it has no single failure, and so on. However, some of the disadvantages of distributed systems include communication overhead and security issues associated with abuse of network access by untrusted nodes [11]. Centralized data are useful for quick collection. Meanwhile, decentralized systems are useful for the reliability of the system because each node can replace each other as a server [8] as summarized in Table 1.

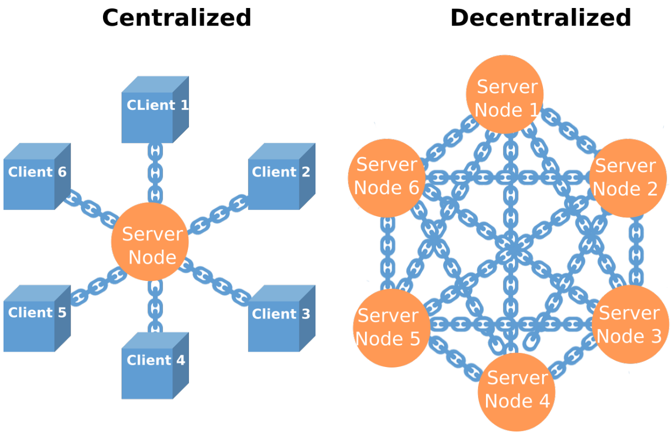

Figure 2. Centralized and decentralized network architecture.

Table 1. Comparison of centralized vs. decentralized.

No.	Name	Centralized	Decentralized	Ref.
1	Advantage	Fast Execution	Increase Reliability	[12]
2	Security	Depend on the Server's Administrator	Depend on the Algorithm	[13]
3	Problems	Can be attack with Denial of Service	Longer Validation Process	[14]

Table 1 provides a clear comparison of the two types of network architecture, by summarizing the advantages, security, and problems between them. In this study, we try to see the possibility to use blockchain as a decentralized system in the existing health care system, which is in centralized form. It will be possible to take advantage of those two system's characteristics.

2.2. Health Services in Indonesia

The Social Security Implementing Agency for Health, which is known as BPJS, is a revolutionary policy in the health sector in Indonesia. Although this policy aims to answer the basic needs of the community, this policy also bears serious problems. Problems both in terms of financing or late payments are often problems for several partner hospitals of insurance [15].

Provision of integrated technology, such as sending medical images in the form of radiology, electrocardiogram (ECG), ultrasonography (USG), and others that are currently more dependent on the patient. On the one hand, this is a matter of privacy or ethics where personal data cannot be shared and can only be owned by the patient; however, on the other hand, in reality, patients also do not really understand how to read the results and become less useful and are often scattered or lost [16]. This is where blockchain technology can have a role in bridging data storage either in an integrated manner or facilitating the granting of access permissions for doctors or medical parties who really need to access the data.

Digital applications in the health sector that are built up by start-ups are also widely used by the public. For example Halodoc in Table 2 for consultation with a doctor with more than 350,000 downloads from Google Playstore; other apps are similar. All of these applications still use the concept of centralized network architecture and do not yet use blockchain. These applications are only a few that have provided breakthroughs in providing information and services related to health [17]. It shows how big the e-health start-up opportunities are in simplifying the problems of health insurance for the community. Of course this breakthrough will provide an answer by bridging authentication between the security side and the speed of the service process. For example, in providing access to national medical record data with protocols that can be accepted by various parties.

Table 2. Medical application start-ups in Indonesia.

No.	Name	Function	Download
1	Alodokter	Platform to access the most complete health features	426,679
2	Halodoc	Chat with doctors, buy health products, visit hospitals, and check labs	375,019
3	YesDok	Ask Doctor Online in 24 h	15,766
4	PrimaKu	Check Child Growth	14,643
5	SehatQ	Healthcare application that offers a variety of services	10,847
6	KlikDokter	Online health solutions in one app	9982
7	Good Doctor	Applications that can be a choice and solution for health services	8069
8	HiDok	Online booking for patients who will seek outpatient treatment	4028
9	Speedoc	Treatment Comes to you for all your medical and health needs	1749
10	Aido Health	Health application with doctor consultation service	1048
11	ProSehat	Make it easier for modern families to obtain health services	910
12	Medi-Call	Health service provider liaison media	613
13	AlteaCare	Integrated and complete health application	575
14	Okadoc	Consult a doctor available from anywhere	127
15	Medical Tourism Indonesia	A platform that connects the tourism ecosystem and the medical industry	11

This can be imagined when a resident on the island of Java travels to the island of Sumatra and is suddenly critically ill and has to be admitted to a local hospital because of a heart attack. Doctors at the hospital can easily obtain patient medical records without having to contact the patient's personal doctor in Surabaya who may not always be ready. With the e-health system, access to patient medical records can be provided and proper treatment by doctors can be carried out quickly without complicated administration [18]. However, the danger of data theft from many parties who want to take advantage of integrated medical record data also needs to be taken into account. This is also no longer a rare thing either by hacking or through spyware that may be infiltrated by the responsible parties. For this reason, the blockchain protocol in this work will try to be a comparison for its implementation.

2.3. Blockchain Authentication

Figure 3 shows where each payment transaction from patient to doctor will be tested for validity. A transaction is considered valid if it has followed the rules and is in accordance with the structure, otherwise the transaction is considered invalid [5]. In addition to relaying these valid transactions, some nodes also provide computing power to the network by placing all valid transactions they receive into blocks. Where each block is arranged linearly and is referred to as a blockchain. This structure is hash-based and is one of the most promising candidates for use in this research because it can help data security, such as in the form of certificates [19]. Operational patterns and file behavior can be monitored based on time constraints so that they can be recorded in the ledger for each block transaction that is carried out [20].

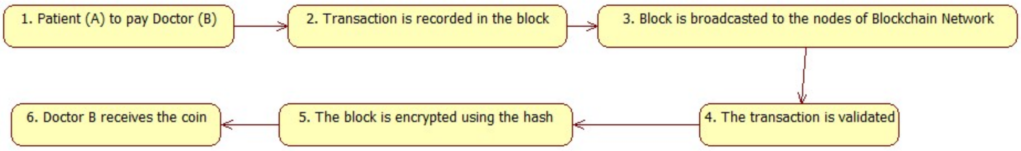
1. Patient (A) to pay Doctor (B)
2. Transaction is recorded in the block
3. Block is broadcasted to the nodes of Blockchain Network
4. The transaction is validated
5. The block is encrypted using the hash
6. Doctor B receives the coin

Figure 3. State machine diagram for patient transactions execution on a blockchain.

Generally, nonce is used for this authentication, where a random value will be generated that can be used for authentication [21]. This process more or less requires a verification table that will store the nonce for use in the next authentication session.

These transactions are broadcast to every peer connected to the blockchain network where clients, called miners, use cryptographic algorithms to validate transactions. This validation solves two main problems that previously existed with digital currency exchanges: ensuring that the digital asset exists and has not been used. A transaction is said to be valid if the miner considers the transaction to be well-formed (input and output contain only the fields specified in the protocol), and the output that is trying to be transferred exists. Miners are not certified and can be anyone who voluntarily invests their resources.

The incentive for miners comes in the form of bitcoins, which are generated and awarded to the miners for each validated block of transactions. Concepts and validations such as these should be validated in the form of simulations [22] before the real device's experiment [23], as is typical in research. If not, it will affect customer experience, which should be avoided as we want to maintain a good image from the very beginning of the application's usage. Next, the software required for mining is free to download and easy to run. Once a transaction is validated by a configurable number of clients, it is stored in a block, which contains details of the validated transaction, along with a timestamp and cryptographic hash (mathematically generated alphanumeric string) of the data. The block with transaction information is added to the end of the blockchain, which is followed by the transfer of the data block and created using the hash of the previous block as in Figure 4. By using the blockchain, each transaction will be unique and can be verified as the use of the address alias system in [24]. Because each block is securely linked to the previous block using a hash, malicious changes are prevented from being made to the blockchain ledger [5]. Immutability is the main property of blockchain.

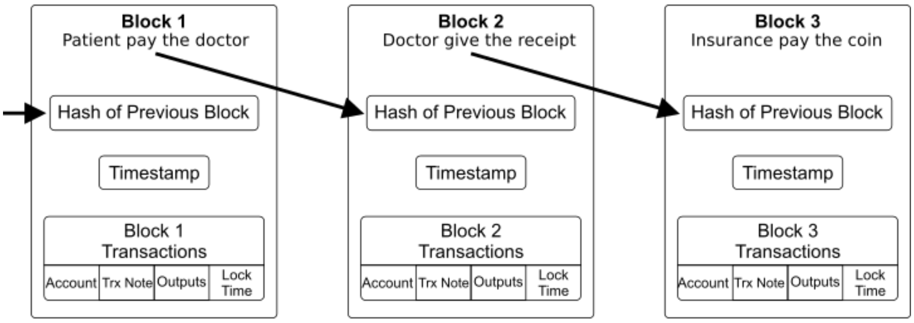

Figure 4. Patient's block representation and encryption cycle.

3. Results

As summarized before in Table 1, we could take advantage of two systems. Centralized servers could be utilized for fast data collection. Meanwhile, decentralization could be used for authentication. In this work, we are taking Vexanium (Vex) ecosystem for the test. This allows every transaction to be stored in every Vex user's wallet.

3.1. Data Flow

An overview of the blockchain application in health can be seen in Figure 5. Its use can be implemented with DApp creation as well as on Ethereum [25]. Authentication logic and activity traces can be embedded in smart contracts of the blockchain used as in remote patient monitoring [7,26]. Finally, every activity that has been confirmed can also be stored on the blockchain, such as a journal of patient medical records [11].

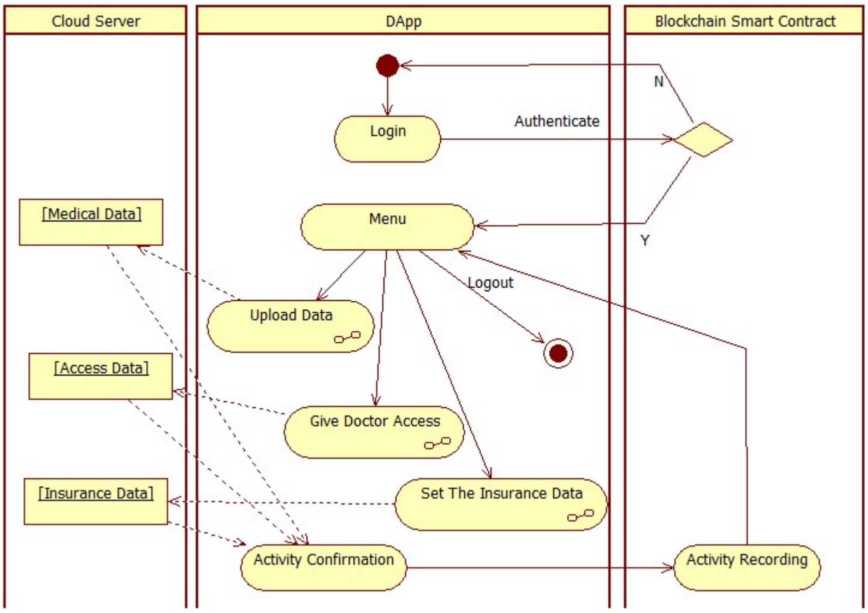

Figure 5. Activity diagram for the simple authentication process.

In general, this offered process resolves administrative problems between insurance and health service providers, whether it is doctors who open their practice or hospitals that organize many polyclinics. In terms of insurance, of course, it is necessary to ensure that the patient has fulfilled all the requirements for a health insurance claim for financing from insurance in the agreed program. Likewise, it is possible that private doctors or larger organizations such as hospitals also want to ensure that payments from the insurance company can run smoothly so that payments can be received directly, such as cash payments, especially in pandemic conditions such as the current COVID-19 pandemic [27]. This authentication process is a bit complicated when performed manually and generally has an impact on the provision of professional self-authentication parties from both insurance and hospital parties. In general, not much can be facilitated by doctors who open private practices except those who are willing to handle the administrative process; for example, in this case with BPJS [28]. By utilizing the existing blockchain platform, this process is no longer a scourge for doctors in general compared to the traditional process.

Figure 5 shows how patients can perform various activities that are connected with authentication and security from the blockchain and data storage with cloud servers. In this study, simulations were carried out using the Vexanium ecosystem, where transactions to be carried out can use direct authentication from the Vexanium ecosystem. Namely, with the private key that we obtain when registering at Vexanium. The first activity that will be carried out is logging in, as in general mobile applications; DApp also performs authentication, but here we use smart contracts, where various necessary rules can be programmed in the C++ language and compiled into a smart contract in the form of a file with the extension .wasm. before publishing it to our Vexanium account. The blockchain used in the smart contract will also use the Vexanium coin. After logging in, new patients can access the menu. Where there will be an option to upload data, provide access to doctor, and set insurance data. Data are stored on the cloud server in a centralized form, which already has security access features with blockchain, such as with CloudFlare [14]. The duration of process can last up to a few minutes depending on the internet connection between DAPP and the blockchain server and between DAPP and cloud server. Then, every activity carried out by the patient using the DApp needs to be verified also into the blockchain ledger. This verification is only in the form of recording activities and does not require large data storage.

For example, it could be recorded as text in the blockchain as shown in Table 3. The data only showed the account name, simple recorded text, and the hash value. The account name shows the credential properties to whom the transaction belong. Then, the simple recorded text describes what the transaction was about. The hash value is the encryption value where we could hold authentication in connection with the centralized server. All of them can be achieved with a smart contract. Following that authentication, uploaded medical data could be then stored in cloud server. This idea would help further possible improvement and development, which has already been in common applications as in Table 2.

Table 3. Recorded activities in transaction ledger.

No.	Acccount	Recorded Text	Hash
1	w4kff4ghz . . .	Patient pays the doctor	QmRTG5Wis . . .
2	s4bl3ng12 . . .	Doctor gives the receipt	QmPML76Mg . . .
3	v2fh1wxkn . . .	Insurance pays the coin	QmZ8SL52b . . .

3.2. Security and Reliability

As seen from Figure 3, three parties need to be hardware secure through access from the DApp, blockchain smart contract, and finally the cloud server; however, in terms of access, these three parties certainly follow the same encryption process from the public key scheme. The probability of a correct guess can be obtained by testing which one gives the decryption exponent d of the following equation:

$$(m^e)^d = m(modN) \tag{1}$$

where m is some random value and e is the public key and N is the modulus of the encryption algorithm. For example, with RSA encryption, with N = 9,449,868,410,449 and public key e = 6,792,605,526,025 and using Wiener attacks, we can calculate d = 569 for the probability of convergence with the private key value [29]. Furthermore, from the network analysis, the security side depends on how the three systems resist attacks such as denial of service (DoS) [30]. Blockchain, of course, as a decentralized system, as discussed above, will be maintained by having more than one server. Meanwhile, a cloud server as a centralized system is very dependent on the server service provider. Lastly, DApps are highly dependent on the blockchain platform being used.

In reality, the root node must first be accessible and trusted in DNS. In this case, the rules that apply will generally be in the jurisdiction of the particular country. In Indonesia, this will relate to the *.id domain. As for the blockchain, the root contract is under the control of the admin of the ecosystem. The security approach referred to here certainly does not depend only on administrators or other system controllers. Blockchain operates as a fully autonomous and decentralized system after publishing smart contracts that are open to every user. Alternatives built on blockchain are expected to withstand the drawbacks of DNS, such as DOS attacks. Blockchain nodes by default will be synchronized and will verify all data continuously [24].

In terms of security, various alliances also create hardware that can be used for mining. With sufficient resources and knowledge, these devices can also be realized with VGA Cards, FPGAs, and other custom devices to complete cryptographic calculations. In practice, only those with the necessary hardware will be able to validate in the majority. Although the algorithm is still decentralized in theory and everyone can try to compete, only a few nodes have a large hash rate. This condition needs to be considered to avoid only a small group being active and preventing the community from growing. This relates to the concept of decentralization at the beginning which prioritizes the number of nodes. Furthermore, security is also determined by the logic program embedded in the smart contract. This relates to whether a new transaction will be accepted into the general ledger or not. It relies on an if-then-else statement after all the validation calculations and complicated cryptographic calculations. With this argument, it is certainly not enough to fully believe in blockchain technology and cryptocurrencies [24]. Some security procedures can also take on a role in the layer as additional guarantees are provided, such as know your customer (KYC) policy.

Table 4 aims to compare the security parameters for the two types of network architecture and related solutions in directly and concisely. Everyone who wants to use blockchain in the validation process should also be aware of its limitations. The use of cryptography can reduce fraud and stop some direct attacks with more complex validation. Further, blockchain processes can help in facilitating the recording of transactions in the ledger; however, it cannot deliver the perfection that some claim. Here, we use Vexanium as blockchain for mass adoption in Indonesia [31]. The principle that transactions recorded on the blockchain will be recorded forever on the blockchain. Every transaction or change within the blockchain will be trackable or auditable, thus creating a transparent system, where the insurance and the patient can cross-check each other; however, not all records will be made on the blockchain. Only a few concise ones will be saved so that the process can run quickly, such as the authentication process and activity recording. Meanwhile, data such as patient medical records, permission access control to doctors, and insurance programs followed by patients will be stored on the cloud server.

Table 4. Security parameters.

No.	Parameter	Centralized	Decentralized
1	DDoS	Usage of Cloud Server [32]	Mitigating distributed DDoS [14]
2	Anonymity	Usage of temporary email [33]	Implementation of KYC [34]
3	Immutability	Usage of Digital Archiving System [35]	Challenge and Solutions [36]

3.3. Choices Limitation

This concept was also recommended for supply chains for ledger applications in the letter of credit processing at [37]; however, the choice of blockchain environments would be a crucial step in its integration into the existing insurance system in Indonesia. In addition, a synthesis will be carried out to compare the simulation with eight existing blockchain initiatives. Comparisons among them that are broken down into each project's profile, support, and implementation readiness for each category, can be observed in Tables 5–7, respectively.

Table 5 summarizes eight blockchain projects in the healthcare sector. All of these projects promote a unique approach to offering healthcare procedures. The scope of the project varies within areas: medical, dental, ecosystem, telemedicine, health charity, and radiology. With one ecosystem that has advantages in terms of adoption in Indonesia, we compare Vexanium among eight other projects that are specific to the healthcare sector. Slightly different from the previous comparison of Android applications from the health sector in Indonesia at Table 2, here it is seen that the popularity of this project is represented by a large market capitalization (market cap). The size of a blockchain project is determined by this value rather than the profit of the project in its user community. Market capitalization is used in acquisitions to assess whether a takeover candidate offers good value to the acquirer or not. In short, it can be said that the greater the value, the more acquisitions. Meanwhile, the rank of the project shows the opposite trend; the smaller the value, the better the project will be. From these two values, it can be seen that Medibloc (MED) is the best candidate for implementation in the healthcare sector with its value in terms of ranking and market capitalization. MED's ranking is below 250. Meanwhile, the value of other projects only ranked above 1500.

Table 5. Comparison of blockchain projects.

No.	Project (Code)	About	Rank	Market Cap
1	Medibloc (MED)	Built on blockchain technology, the MediBloc Health Information Platform offers a private data ecosystem for patients, providers, and researchers. Our goal is to simplify medicine for patients, healthcare professionals, and researchers.	243	96,020,302
2	Dentacoin (DCN)	Smart Contact manages a blockchain network called Dentacoin, which is based on Ethereum. This platform helps the dental industry by developing and producing solutions aimed at raising global dental care standards.	1643	1,691,984
3	Vexanium (VEX)	The next-generation blockchain, which is being developed by Vexanium, was created to facilitate the use of DApps (decentralized Apps) and retail penetration. The blockchain technology that can be used in many different businesses is called Vexanium.	1750	1,423,559
4	Doc.com (MTC)	Through Telemedicine, DOC.com has developed free primary healthcare and psychiatric services for the whole world. Doc.com places all epidemiological data on a state-of-the-art health blockchain.	1802	1,283,281
5	Medicalchain (MTN)	To securely store medical records and uphold one version of the truth, MedicalChain utilizes blockchain technology.	2304	505,563
6	MediShares (MDS)	An Ethereum-based, open-source, decentralized reciprocal marketplace called Medishares. Anyone who sends a variable number of MDS to a smart contract can participate in the mutual assistance system. chain	2479	373,546
7	Patientory (PTOY)	The top supplier of Blockchain Health Solutions is Patientory. Patientory's goal is to advance population health management by helping healthcare institutions transfer and securely store data using blockchain technology and smart contracts.	2861	190,786
8	Medi (MEDI)	Natural disasters and pandemics are just two of the problems plaguing today's rapidly changing planet.	3439	43,742
9	AI Doctor (AIDOC)	AIDOC provides you with sustainable health and wellness advice by combining medical data with artificial intelligence (AI) technology. We can create live 3D images of your health from vital sign readings using our blockchain and cutting-edge imaging technology, giving you access to 24-h health analysis from a digital medical professional who can spot problems and provide solutions.	3573	26,432

The implementation and solutions offered by blockchain projects in the medical field can be seen at a glance in the About column. It can be seen that the approach of each project is not uniform, although in general everything is still related to medics. For example, the MED project seems to have almost covered the entire ecosystem in the medical field, but Dentacoin (DCN) only wants to focus on the dental field. Table 2 gives a list of examples of a project that will dynamically have a changing rating and market cap. Similar to other blockchain projects, this project also has other parameters that can be used for further analysis. These parameters are in Table 6. This related to the consensus mechanism used wherein there was a protocol that would determine whether a particular transaction was valid or not in the network. With the right selection, the manufacture and maintenance process would run easily.

Table 6. Medical project parameters. (accessed on 1 November 2022).

No.	Code	Link	Ecosystem	Source Code
1	MED	https://medibloc.com/en/	Cosmos	https://github.com/medibloc
2	DCN	https://www.dentacoin.com	Ethereum	https://github.com/dentacoin
3	VEX	https://www.vexanium.com/	Vexanium	https://github.com/vexanium
4	MTC	https://doc.com/	Ethereum	https://github.com/Docademic
5	MTN	https://medicalchain.com/en/	Ethereum	https://github.com/medicalchain
6	MDS	https://www.mutualdao.org/en/	Ethereum	https://github.com/MediShares
7	PTOY	https://patientory.com/	Ethereum	https://github.com/Patientory
8	MEDI	https://meditoken.org/	Ethereum	-
9	AIDOC	http://www.aidoc.com/	Ethereum	-

Table 6 shows the ecosystem summary of each project. It can be seen that in the majority, Ethereum is used as an ecosystem. Furthermore, we can also see support from the open-source side. This will further provide a guarantee for further development with the participation of the community. Then, it would also link with the coin or token, which will be used and determine how it is exchanged with fiat currency. Eventually this should be associated with existing exchanges, such as in Indonesia, there were Indodax, TokoCrypto, Pluang, and other small exchanges [31]. Of the existing exchanges, only Indodax is the most active for the exchange from Vexanium to Indonesian's fiat currency.

Finally, a comparative analysis of several blockchain projects in the medical field is in Table 7. Three projects were analyzed to be classified specifically in the medical field, namely, MED, MTN, and PTOY. In general, it can be seen with the possibility of support for doctor's activities, service transactions, and the possibility of guarantees from the insurance but with different approaches. MED from its brief description in Table 5, tries to offer a private data ecosystem for patients, providers, and researchers. Providing access to personal healthcare data, from a research perspective, will be very helpful to advance medical science faster than ever before. Next up is MedicalChain (MTN), which will try to store medical records and provide access to patient files to speed up and simplify the patient management process. Here, it will involve many institutions that will directly need such access, such as doctors, hospitals, laboratories, pharmacies, and health insurance companies. Further, recording transactions in the distributed ledger as previously discussed. Lastly, specifically in the medical field, there is Patientory (PTOY), which is more or less the same as the previous two and also offers patient EMR storage, only more toward better health outcomes—in other words, it is more focused on coordinated care between doctor and patient.

The three projects above can be used directly because the projects have been created; however, in terms of adoption, Vexanium (VEX) is the only one that is included in the ecosystem category that has also tried to be compared with others. VEX from Table 5 is more to facilitate the use of DApps (decentralized applications) for retail penetration. Then, there is a different approach from the one with delegated proof of ownership (DPOS). A decentralized operating system with an autonomous enterprise architecture can better support decentralized applications. Thus, the option to build a project from scratch with reference to an existing project can also be seen as an option.

Table 7. Medical project readiness.

No.	Code	Field	Doctor	Medical Record	Insurance
1	MED	Medical	V	V	V
2	DCN	Dental	V	V	-
3	VEX	Ecosystem	-	-	-
4	MTC	Telemedicine	V	-	-
5	MTN	Medical	V	V	V
6	MDS	Medical Aid	V	-	-
7	PTOY	Medical	V	V	V
8	MEDI	Health Charity	V	-	-
9	AIDOC	Radiology	-	V	-

4. Discussion

By comparing VEX with other blockchain projects, we can see a comparison between the use of Ecosystem and Ready Project. Although it has been explained earlier that this technology can be used to provide verified and accurate patient information, we also need to remember several things, such as aspects of the jurisdiction of certain countries. Since the beginning, the biggest challenge is in the concept of decentralization, where no one claims to be the sole holder of the data, which is contrary to the legal aspects that generally only apply in certain countries.

However, the accessibility of Blockchain may be a significant trade-off for the above obstacles, such as the legal aspect. For example, there may be reduced costs associated with running and maintaining a provider's transactional system from a centralized system. Smart contracts are also seen to be dominant in the healthcare side, as shown by the large number of uses of Ethereum as an ecosystem in Table 6, where the popularity of using smart contracts from Ethereum is the most active and captivating [38]. This kind of smart contract will certainly be able to reduce the workload in the emergency room (ER) while reducing the cost of care and health administration processes that must be borne by the patient [39]. Blockchain, in general, can facilitate patient care plans in real time based on their medical records stored on the blockchain; however, integration with these various applications were very dependent on the available application programming interface (API) facilities from the application's provider, as listed in Table 2. In this work, the Vexanium ecosystem had been utilized for the testing and simulation for samples of transactions. A further tests would be about the connection with one of the available applications.

Blockchain technology has the ability to transcend patient administration barriers. However, from a security perspective, procedures, such as know your customer (KYC), still needs to be carried out for perpetual records, data security, and automatic validation [40]. The KYC procedure can also link to the jurisdictional aspects discussed earlier. If consumer data systems can be integrated into a global network powered with blockchain technology, legal procedures can be initiated with KYC.

5. Conclusions

Proofs and concepts from integrating Blockchain had been presented with data flow of its incorporating servers and samples of transactions using Vexanium coin. Blockchain with its smart contract could be used as replacement for the authentication needed by patients in making insurance claims. This was performed by leveraging the existing facilities of the chosen blockchain ecosystem; thus, the selection of blockchain was very crucial.

The blockchain network is decentralized, so it is difficult to predict its security when operating in real life. In this study, we tried to simulate the stages of the transaction process between patients, doctors, and insurance companies; however, due to different aspects of each country's rule of law (in this case, Indonesia), state-run insurance, and other attributes, more reviews are still needed.

With the right selection, the process of authenticating and verifying health service transactions can be carried out at the doctor's. It could be automatically approved by the insurance party without a complicated process by using hash encryption through the public key scheme. However, the only thread would come from the network side with the possibility of a DoS attack at the centralized server. Overall, this study could accelerate start-ups to implement this emerging technology, which has already begun in the world of finance.

The following are some guidelines and their practical implications: from these project studies, the biggest opportunity for blockchain adoption in healthcare processes is cost savings through increased automation, speed, standardization, and efficiency with the use of smart contracts. The immutable distributed blockchain data create digital and transparent trust, smart contracts via cryptography to encourage automation practices, and the use of KYC for possible jurisdictional issues. Therefore, for the use of blockchain technology, we also recommend looking at the ecosystem that is closest to the domain and rules of the country, and the most easily adopted regulatory framework.

Author Contributions: E.S. was the first author of this article. R.M. was responsible for the network security part. F.C.S.A. was responsible for the blockchain application. G.E.-E. assisted in editing and proofreading. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Universitas Airlangga with grant number is 1421/UN3.1.8/PT/2022.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This work has been funded by Universitas Airlangga, under scheme Penelitian Dosen Pemula (PDP 2022).

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

Abbreviations

The following abbreviations are used in this manuscript:

BPJS	Badan Penyelenggara Jaminan Sosial Kesehatan (Health Social Security Administering Agency)
DApp(s)	Decentralized Application(s)
DoS	Denial of Service
DNS	Domain Name System
ECG	Electrocardiogram
EHR	Electronic Health Records
EMR	Electronic Medical Records
ER	Emergency Room
FPGA	Field Programmable Gate Array
KYC	Know Your Customer
RSA	Rivest–Shamir–Adleman cryptosystem
USG	Ultrasonography
VGA	Video Graphics Array

References

1. McGhin, T.; Choo, K.K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [CrossRef]
2. Zhao, H.; Zhang, Y.; Peng, Y.; Xu, R. Lightweight backup and efficient recovery scheme for health blockchain keys. In Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), Bangkok, Thailand, 22–24 March 2017; pp. 229–234.
3. Kraus, S.; Schiavone, F.; Pluzhnikova, A.; Invernizzi, A.C. Digital transformation in healthcare: Analyzing the current state-of-research. *J. Bus. Res.* **2021**, *123*, 557–567. [CrossRef]
4. Tandon, A.; Dhir, A.; Islam, A.N.; Mäntymäki, M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Comput. Ind.* **2020**, *122*, 103290. [CrossRef]
5. Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain technology: applications in health care. *Circ. Cardiovasc. Qual. Outcomes* **2017**, *10*, e003800. [CrossRef] [PubMed]
6. Shahnaz, A.; Qamar, U.; Khalid, A. Using blockchain for electronic health records. *IEEE Access* **2019**, *7*, 147782–147795. [CrossRef]
7. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
8. Tama, B.A.; Kweka, B.J.; Park, Y.; Rhee, K.H. A critical review of blockchain and its current applications. In Proceedings of the 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), Palembang, Indonesia, 22–23 August 2017; pp. 109–113.
9. Rahardja, U.; Hidayanto, A.N.; Putra, P.O.H.; Hardini, M. Immutable Ubiquitous Digital Certificate Authentication Using Blockchain Protocol. *J. Appl. Res. Technol.* **2021**, *19*, 308–321. [CrossRef]
10. Van Steen, M.; Tanenbaum, A. Distributed systems principles and paradigms. *Network* **2002**, *2*, 28.
11. Li, P.; Nelson, S.D.; Malin, B.A.; Chen, Y. DMMS: A decentralized blockchain ledger for the management of medication histories. *Blockchain Healthc. Today* **2019**, *2*, 38.
12. Duan, J.; Zhang, C.; Gong, Y.; Brown, S.; Li, Z. A content-analysis based literature review in blockchain adoption within food supply chain. *Int. J. Environ. Res. Public Health* **2020**, *17*, 1784. [CrossRef]
13. Kim, B.G.; Cho, Y.S.; Kim, S.H.; Kim, H.; Woo, S.S. A security analysis of blockchain-based did services. *IEEE Access* **2021**, *9*, 22894–22913. [CrossRef]
14. Singh, R.; Tanwar, S.; Sharma, T.P. Utilization of blockchain for mitigating the distributed denial of service attacks. *Secur. Priv.* **2020**, *3*, e96. [CrossRef]
15. Nuraini, N.; Damayani, D.S.; Wijayanti, R.A. Factors Causing Delays in Submitting Inpatient BPJS Claims at RSU dr. H. Koesnadi Bondowoso. *J. Aisyah J. Ilmu Kesehat.* **2021**, *6*, 245–252. [CrossRef]
16. Matsumura, Y.; Kurabayashi, N.; Iwasaki, T.; Sugaya, S.; Ueda, K.; Mineno, T.; Takeda, H. A scheme for assuring lifelong readability in computer based medical records. In Proceedings of the 13th World Congress on Medical Informatics (MEDINFO), Cape Town, South Africa, 12-15 September 2010; pp. 91–95.
17. Rahardjo, D.; Sugiarto, M. Valuation model using a mixed real options method: A review on Singapore and Indonesia digital startups. In Proceedings of the 16th International Symposium on Management (INSYMA 2019), Manado, Indonesia, 4–6 March 2019; pp. 9–12.

18. Nugraha, D.C.A.; Aknuranda, I. An Overview of e-Health in Indonesia: Past and Present Applications. *Int. J. Electr. Comput. Eng.* **2017**, *7*, 2441–2450. [CrossRef]
19. Ma, Z.; Sha, E.H.M.; Zhuge, Q.; Jiang, W.; Zhang, R.; Gu, S. Towards the design of efficient hash-based indexing scheme for growing databases on non-volatile memory. *Future Gener. Comput. Syst.* **2020**, *105*, 1–12. [CrossRef]
20. Ho, S.M.; Kao, D.; Wu, W.Y. Following the breadcrumbs: Timestamp pattern identification for cloud forensics. *Digit. Investig.* **2018**, *24*, 79–94. [CrossRef]
21. Zainuddin, A.; Junaidi, J.; Putra, R.D. Design of E-Commerce Payment System at Tokopedia Online Shopping Site. *Aptisi Trans. Manag.* **2018**, *1*, 143–155. [CrossRef]
22. Sutanto, E.; Chandra, F.; Dinata, R. Simulation of leakage current measurement on medical devices using helmholtz coil configuration with different current flow. *J. Phys. Conf. Ser.* **2017**, *853*, 012004. [CrossRef]
23. Sutanto, E.; Chandra, F.; Gonnelli, E. Residual Current Measurement using Helmholtz Coil Configuration with different Current Flow. *Int. J. Electr. Comput. Eng.* **2018**, *8*, 1432. [CrossRef]
24. Bodziony, N.; Jemioło, P.; Kluza, K.; Ogiela, M.R. Blockchain-based address alias system. *J. Theor. Appl. Electron. Commer. Res.* **2021**, *16*, 1280–1296. [CrossRef]
25. Rupa, C.; Midhunchakkaravarthy, D.; Hasan, M.K.; Alhumyani, H.; Saeed, R.A. Industry 5.0: Ethereum blockchain technology based DApp smart contract. *Math. Biosci. Eng.* **2021**, *18*, 7010–7027. [CrossRef]
26. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **2018**, *42*, 1–7. [CrossRef] [PubMed]
27. Larson, W.D.; Sinclair, T.M. Nowcasting unemployment insurance claims in the time of COVID-19. *Int. J. Forecast.* **2022**, *38*, 635–647. [CrossRef] [PubMed]
28. Maryatmo, R.; Ellyawati, J. Moral Hazard on Public Health Insurance: Evidence from BPJS in Indonesia. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 479–482.
29. Smart, N.P. *Cryptography: An introduction*; McGraw-Hill: New York, NY, USA, 2003; Volume 3.
30. Deng, C.; Zhang, D.; Feng, G. Resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks. *Automatica* **2022**, *139*, 110172. [CrossRef]
31. Hartoyo, A.; Sukoharsono, E.G.; Prihatiningtyas, Y.W. Analysing the Potential of Blockchain for the Accounting Field in Indonesia. *J. Akunt. Dan Keuang.* **2021**, *23*, 51–61. [CrossRef]
32. Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Buyya, R. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Comput. Commun.* **2017**, *107*, 30–48. [CrossRef]
33. Vishwanath, A.; Herath, T.; Chen, R.; Wang, J.; Rao, H.R. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decis. Support Syst.* **2011**, *51*, 576–586. [CrossRef]
34. Malhotra, D.; Saini, P.; Singh, A.K. How blockchain can automate KYC: systematic review. *Wirel. Pers. Commun.* **2021**, *122*, 1–35. [CrossRef]
35. Senthilkumar, T.; Rajasekaran, S. Data Immutability Challenges: A Security Analysis of Digital Archiving Systems. *Planning* **2022**, *5*, 6. [CrossRef]
36. Politou, E.; Casino, F.; Alepis, E.; Patsakis, C. Blockchain mutability: Challenges and proposed solutions. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 1972–1986. [CrossRef]
37. Rijanto, A. Blockchain technology adoption in supply chain finance. *J. Theor. Appl. Electron. Commer. Res.* **2021**, *16*, 3078–3098. [CrossRef]
38. Wang, Z.; Jin, H.; Dai, W.; Choo, K.K.R.; Zou, D. Ethereum smart contract security research: survey and future research opportunities. *Front. Comput. Sci.* **2021**, *15*, 152802. [CrossRef]
39. Gökalp, E.; Gökalp, M.O.; Çoban, S.; Eren, P.E. Analysing opportunities and challenges of integrated blockchain technologies in healthcare. In Proceedings of the 11th SIGSAND/PLAIS Eurosymposium on Systems Analysis and Design (Eurosymposium), Gdansk, Poland, 20 September 2018; pp. 174–183.
40. Lee, C.C.; Kriscenski, J.C.; Lim, H.S. An empirical study of behavioral intention to use blockchain technology. *J. Int. Bus. Discip.* **2019**, *14*, 1–21.