Journal of Korea Multimedia Society Vol. 22, No. 5, May 2019(pp. 613-625)
https://doi.org/10.9717/kmms.2019.22.5.613

Healthcare System using Pegged Blockchain considering Scalability and Data Privacy

Akmal Azizan[†], Quoc-Viet Pham[††], Han Suk Young[†††], Kim Jung Eon[††††], Kim Hoon[†††††], Park Junseok[††††††], Hwang Won-Joo[†††††††]

ABSTRACT

The rise of the Internet of Things (IoT) devices have greatly influenced many industries and one of them is healthcare where wearable devices started to track all your daily activities for better health monitoring accuracy and even down to tracking daily food intake in some cases. With the amounts of data that are being tracked and shared between from these devices, questions were raised on how to uphold user's data privacy when data is shared between these IoT devices and third party. With the blockchain platforms started to mature since its inception, the technology can be implemented according to a variety of use case scenarios. In this paper, we present a system architecture based on the healthcare system and IoT network by leveraging on multiple blockchain networks as the medium in between that should enable users to have direct authority on data accessibility of their shared data. We provide proof of concept implementation and highlight the results from our testing to show how the efficiency and scalability of the healthcare system improved without having a significant impact on the performance of the Electronic Medical Record (EMR) that mostly affected by the previous solution since these solutions directly connected to a public blockchain network and which resulted in significant delays and high cost of operation when a large amount of data or complicated functions are involved.

Key words: Healthcare, Privacy, Blockchain, Scalability, Wearable Devices, Smart Contract, Pegged Blockchain, Sidechain, IoT, Electronic Medical Record

1. INTRODUCTION

With many industries are conforming to the use of blockchain, a lot of new implementation methods have been developed to extend its original functionality. One of them is a smart contract where users can implement the traditional contract without having intermediaries to authenticate the contract, thus making it more secure. Blockchain also has been adopted by IBM with Hyperledger [1], which started as intermediaries for international businesses contracts between different business especially with a lot of layer of communication and then have been extended to other types of data exchange and even more complicated operations.

Wearable devices or henceforward we generalize as IoT devices have started to be significantly important in our daily life since it started to in-

※ Corresponding Author : Won-Joo Hwang, Address: 197 Injero, Gimhae, Gyeongnam 50834, South Korea,, TEL : +82-55-320-3847, FAX : +82-55-322-6275, E-mail : ichwang@inje.ac.kr

Receipt date : Jan. 10, 2019, Revision date : Apr. 2, 2019
Approval date : May 8, 2019

[†] Dept. of Information and Communication Systems, Inje University (E-mail: maxburnz@gmail.com)
[††] ICT Convergence Center, Changwon National
[†††] Institute of Digital Anti-Aging Healthcare (IDA), Inje University (E-mail: thewayceo@inje.ac.kr)
[††††] Dept. of Emergency Medicine, Inje University, Ilsan Paik Hospital (E-mail: jekim1229@naver.com)
[†††††] Dept. of Emergency Medicine, Inje University, Ilsan Paik Hospital (E-mail: megali@hanmail.net)
[††††††] Dept. of Emergency Medecine, Inje University, Ilsan Paik Hospital (E-mail : edpjs@inje.ac.kr)
[†††††††] Dept. of Electronics, Telecommunications, Mechanical & Automotive Engineering, Inje University (Email: ichwang@inje.ac.kr)

tegrate with many of our life aspects such as security system and health monitoring [2]. This integration means that IoT devices are collecting sensitive data that is stored in less secured storage especially if we are sending the data directly to another party from the device itself. With the introduction of the wearable health tracking devices, e.g. Apple Watch or Mi Band 3, people are more open to the concept of sharing their medical data over the air to another third party [3]. Despite the fact of security concern from these devices, it did not stop the government or healthcare providers from wanting to have their hand on these valuable sensitive data thus it is a major concern for users considering these devices are not secured enough as they are low powered devices and the recent development of data leakage from major websites where user's passwords are stored in plaintext and are not even encrypted properly.

Inefficient power usage typically involved due to the 'mining' operation needed in the blockchain network to run it is the biggest concern for any kind of industries when trying to adopt blockchain with their system. This is due to the consensus algorithm used by the first blockchain network aka Bitcoin [4] which is based on Proof of Work (PoW) algorithm that required high computing power to solve increasing complexity mathematical problems over time which resulted in the familiarity of blockchain is equal to a very secure network. However, as time goes, maintaining the blockchain network will be too costly for the benefits it provided. Due to this, a different type of consensus algorithms was developed and able to compensate these drawbacks such as Proof of Authority (PoA) [5] that overcomes this problem by having a set of validators to validate every transaction in the blockchain instead of all the nodes in the network mining for the correct answer for each transaction which resulted in a quicker transaction and more energy efficient network. With several other algorithms getting more popular, this opens up more opportunity for industries to adopt blockchain according to their requirements with each algorithm have their own advantages and drawbacks.

In this paper, we proposed using pegged blockchain concept where we connect the EMR system to a private blockchain or sidechain before connecting it to a public blockchain henceforward mainchain to create a trusted data-sharing platform for patients to exchange data with specific physicians or other parties from specific hospitals. Different from other solutions, we did not directly connect the EMR system to the mainchain in order to maintain the performance when transferring a big chunk of data or handling multiple operations. We explored the scalability and efficiency of our solutions compared to the system that connects directly to the mainchain. The scientific contribution for this paper is the new architecture model for the healthcare system based on pegged blockchain so that it can provide patients with data authentication through smart contract and allows any third parties to join the system without having the patients to lose their data ownership after their data have been sent to the hospital.

The structure of the paper will be as follows. The next section, we discuss the motivation for this paper. Related works section discusses the previous researches that have a significant contribution to the field. Background section explains the backbone of our proposed solution. The methodology is presented in the system architecture section with system implementation follows through with our experimental results i.e. throughput performance, scalability, efficiency, etc. Finally, the conclusion section summarizes our current progress and limitation.

2. MOTIVATION

EMR in Healthcare System in some hospitals is accessible by all the physicians in the hospital, which can lead to a big problem considering that wearable devices might be sharing sensitive health data on a daily basis. We can see recently from Facebook Analytica scandal where data leakage and mishandling are not only users concern but also is considered as an operational cost that amounted to millions of dollars lost in revenue which should be considered by the healthcare provider too. Introduction of smart contract on Ethereum enable patients to permit only the requestor to access the data they shared and by implementing the same concept on Healthcare system, we will be able to protect user data privacy from the third party that handles their data, in this case, the hospital.

Sending sensitive data directly from IoT devices concern us with attacks such as Eavesdropping or Man in the middle which is typically solved by having data encrypted or signage algorithm. Furthermore, even though encrypted, the medium to transfer the data can still be vulnerable. By having data encrypted and sending it through the blockchain network, it enables an additional layer of security since blockchain can assure that data integrity can be achieved. We solve the IoT devices lack of power and security issues by shifting the responsibility of sending the data to a blockchain node instead. The node processing power and storage capability enable the sent data to be hash before sending it and the node is more secure to store all the data compared to IoT devices [6].

Furthermore, the third parties that usually connected to healthcare systems such as insurance companies or researchers may have access to patient's data sometimes bypassing the user acknowledgment. In other cases, patients did not know what they are agreeing to when signing some forms in the hospital which led to confusion of data usage by third parties. Our solution helps the user to review the accessibility of the data since the data flow is clearer and more transparent for them to give permission easier compared to traditional contractual form that can be long and messy [7].

3. RELATED WORKS

Blockchain application in the healthcare system has started since 2016 where Medrec [8] uses blockchain on medical data accessibility and permission management with a fully functional prototype. Medrec applies blockchain directly to the EMR system where permission is handles based on patient-provider relationships as a reference. The research has led to several others blockchain implementation on the healthcare system such as FHIRChain [7] where blockchain is used to share scalable data securely using the decentralized app (DApp) based on access token using HL7 standard for interoperability with any blockchain that able to execute a smart contract. R. Guo et al. [9] proposed a secure MA-ABS scheme for better security of the blockchain by having multiple authorities signing key to be embedded to the private key of the patients. HealthSense [10] then dive into IoT protocol where application binary interface (ABI) is used to connect device program directly to the blockchain so it can interact directly with the contract and MQTT protocol uses device ID to generate a hash that is mapped to the chaincode of the blockchain without needing blockchain node to connect to the blockchain network.

All of these researches have concentrated on the different type of improvement in the healthcare system. We can see that for examples security, connectivity, interoperability and permission management [11-13] [15-17] [19-21] are some of the aspects that have been concentrated on by using blockchain. However, none of these researches touch on the performance of the system when using blockchain or specifically dive into the details of the chosen blockchain as they all assume to be connected to one of the public blockchains like Bitcoin or Ethereum. Blockchain now has evolved in term of using another type of consensus algorithm and also Turing complete where blockchain system now able to run complicated functions such as a database (DB) queries or even simple games. By taking advantage of current development, we touch on the issues of the blockchain performance which have not been touched previously in order to improve the system scalability and efficiency especially if all healthcare systems are to agree on implementing our proposed solution.

Based on the recent movement and demand of pegged blockchain for interoperability, our researches are based on the same concept as Medrec [8] by utilizing both private and public blockchain. We compare our solution with the current solution to see the improvement which we expect in term of performance, efficiency and scalability. We only dive into improving the architecture of the connected network without going deeper into topics like security where which protocol to be used by the IoT devices or the hashing algorithm and also the filing system on how data is stored in Merkel Tree in the block which has been researched on the aforementioned papers [7-10].

4. SYSTEM OVERVIEW

4.1 CONSENSUS ALGORITHM

In order to authorize any transaction or new creation of blocks, consensus algorithm [11] determined how the blockchain network agreed to the latest block addition. The consensus, in other words, is the way for all the miners in the blockchain to agree with the next valid blocks. PoW is the de facto consensus algorithm now because of the “hard work” needed for any block validation thus making the whole blockchain system extremely secure from tampering from another third party. Even changing any simple data on the blockchain require processing power bigger than 51% of the whole blockchain network processing power. Due to the lack of power efficiency, different consensus algorithms are proposed to overcome some of the weaknesses of PoW in exchange for lesser security and faster transaction. Currently, there are many consensus algorithms such as Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) [5] that has been proposed which works by having the next block creator will be chosen based on certain criteria like age of the miners or accountability which is useful for certain kind of scenarios.

4.2 PROOF OF AUTHORITY

Proof of Authority was introduced as an alternative to enable faster block validation at a cost of centralization compared to the traditional decentralization method. PoA works by having a set of validators i.e. Miners, Sealers to validate the next valid blocks instead of solving the complex problem over time. These validators are pre-chosen at the start of the blockchain creation typically as low as three nodes will be needed as any matters concerning the blockchain network will require (N/2)+1, N number of validators to agree on things such as the addition of new validators or nodes. Only validators are the miner when using this algorithm and the only one able to seal approval for any transaction thus making it one of the most efficient blockchain consensuses out there albeit at the cost of centralization. This makes it suitable for the private use case when validators are trusted to be secure enough for the whole blockchain network. However, there is a few public PoA based blockchain network such as POA or Rinkeby which are using this concept as public blockchain instead [2]. Because of this, each validator is limited to validating floor (N/2)+1 number of next valid block in order to preserve trustability of the network.

4.3 PEGGED BLOCKCHAIN

There are two types of token exchange in pegged blockchains [12] setup, which is called 1-way peg (1WP) or 2-way peg (2WP). 1WP is one-way traffic for token transfer where the token from the sender blockchain will be locked forever after transferring to another blockchain. 2WP however, works by having the same ratio of token exchange where the sent token is temporarily locked according to the amount of the received token that will be unlocked in the other blockchain. Both methods are considered as only the illusion of tokens transfer from one network to another but in reality, the token is temporarily or permanently lock in the first blockchain and the receiving one will just unlock the same number of tokens since normally both blockchains is using a different consensus algorithm thus making the token not compatible with each other. The drawbacks of this method are the inclusion of the third party to hold the tokens involved in the transaction and complexity issues such as forking especially when involving a different type of consensus blockchain together.

4.4 SIDECHAIN

Sidechain [13] is one of the methods when pegging multiple blockchains together which works having a lighter version of the mainchain that it is connected to. Sidechain is able to provide with a lower cost of operation by allowing the tradeoff of decentralization for scalability and security. Sidechain can extend the functionality of mainchain because it does not use the same script as the mainchain. Some of the example for its use case, sidechain uses another type of cryptocurrency for the cheaper transaction or administering the token exchange to maintain the value of the cryptocurrency. Sidechain also enables merge mining; in this case, miners mine concurrently for both mainchain and sidechain to lessen the chance of block rejection typically involved when mining in current blockchain solution thus increasing efficiency. Drawbacks of sidechain are that both blockchains need to understand each other consensus algorithm to make sure the proof of a locked transaction can be achieved while maintaining the number of tokens being an exchange between them. Our main research here considers sidechain method as database administration backend for the EMR system by allowing access only through the validators in the sidechain network. Amongst other pegged blockchain method, sidechain is the only method that does not involve other third party or federation for token exchanging between the pegged blockchain.

5. SYSTEM ARCHITECTURE

As shown in Fig. 1, our proposed solution consists of two main components that are the Block Manager (BM) for both patients and hospital which is the node in the blockchain and the pegged blockchain between mainchain, which is the public blockchain network where patients will directly be connected to, and a sidechain which is the hospital private blockchain network. The IoT devices use BM as a gateway for dumping and sending data to another party. We propose using a BM instead of directly from the IoT devices to overcome IoT devices weaknesses that we have mentioned previously. Furthermore, the current processing power of IoT devices is too low and not efficient enough to join a public blockchain network even as a light client.

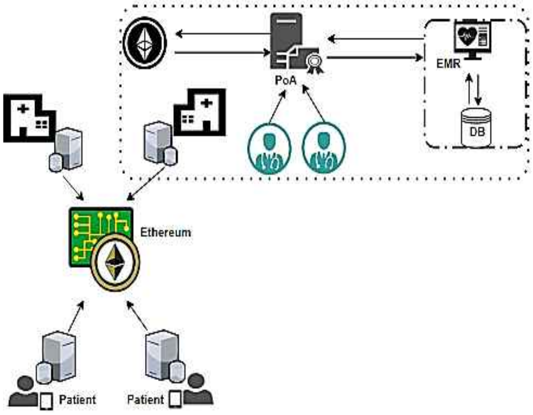


Fig. 1. Simplified Architecture of Our Proposed Solution.

The BM is able to overcome this drawback with a device that has storage capability to store data securely and powerful enough to run either a full or light client of mainchain. Patients BM only need to run the light client and the hospital BM run the full client since they will have their own EMR server which is powerful enough to run the full client concurrently. Both BMs will need to run an interface to interact with the smart contract using JSON-RPC message that directly connects the database to run the typical DB queries from the node to the blockchain network. We can use web3 API to connect our DApp containing the DB to both the mainchain and the sidechain. DApp is an application that has a blockchain as its backbone where normally blockchain token will be involve when running the application. In our case, we need to run a DApp on reading the EMR for the physicians and requesting data from patients. Patients DApp meanwhile is on seeing the requestor ID and to attach their health data by allowing certain ID to be able to access it.

The mainchain in the system in our case, we use Ethereum where the smart contract is executable since the system will be using DApp to connect between patients and physicians. Meanwhile, the sidechain is set up with specific nodes in mind from the start of the blockchain lifetime as validators and the new addition of validators will not be considered if the system is able to securely maintain the system. The EMR system connects directly to the sidechain to allow authorization management through the validators. Any interaction with the EMR system requires physicians to communicate directly with one of the nodes in the sidechain instead of connecting as one of the nodes in the case of the current public blockchain. Using the PoA algorithm, transactions can be sealed faster as the authentication process is as short as 5 seconds [15]. Sidechain also enables other third parties to interact with the EMR directly for patient's data by running through the same process on how physicians request the patient's data. Using this way, it is more efficient compared to the traditional method of going through both the patients and the hospital.

Fig. 2 shows the process model of our proposed application on how patients authenticate their data

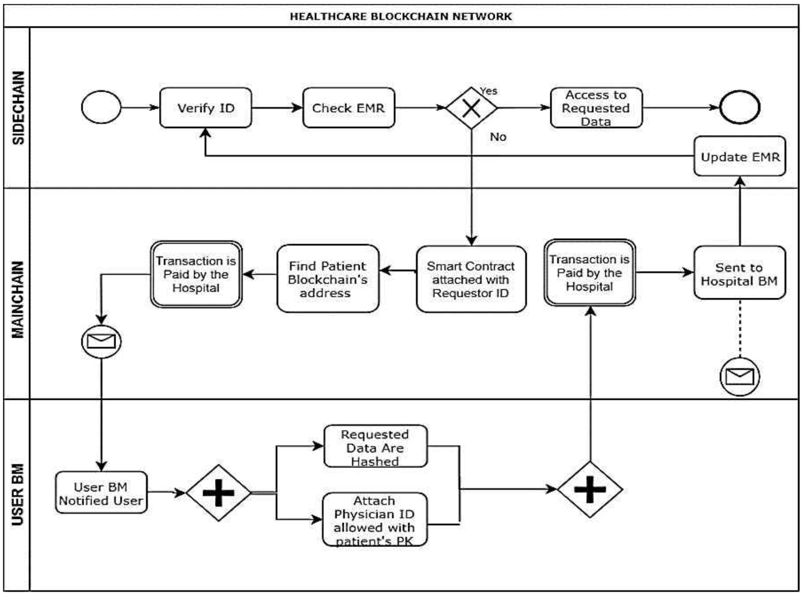

HEALTHCARE BLOCKCHAIN NETWORK
SIDECHAIN
Verify ID
Check EMR
Yes
No
Access to Requested Data
Update EMR
MAINCHAIN
Transaction is Paid by the Hospital
Find Patient Blockchain's address
Smart Contract attached with Requestor ID
Transaction is Paid by the Hospital
Sent to Hospital BM
USER BM
User BM Notified User
Requested Data Are Hashed
Attach Physician ID allowed with patient's PK

Fig. 2. Process Model of Physicians Requesting Data Using Our Proposed Solution.

when being requested by a physician. The application works when physicians or other third party requests the user data through the sidechain. When data is unavailable in the EMR system, the hospital BM will then execute a contract requesting the patient's data through the mainchain by attaching the ID of the requestor. We generate the Private Key (SK) for each user by using Web3Py library which then will be bind to the address of the users' node. Patients can deny the permission or granted access through the contract and attach their hashed data using Inter Planetary File System (IPFS). Only the hospital that the patients attend will have the patient's public key to read the hashed data. We expect the patient to set up their account with their respective hospital in advance.

We replicate the overall system process flow by using contract consist of both patient and requestor ID in our case node address and DB queries through the contract to get the hashed data from the patients. More details on this implementation can be seen in FHIRChain [7] implementation. In our experiment, we concentrate on requesting and reading data from the DB that we built with our own made data to get the performance evaluation that we wanted to improve instead of the security analysis of our proposed solution. Some papers [20-21] also did not justify properly and choose between their performance or their security analysis based on the objective that they are trying to prove.

6. SYSTEM IMPLEMENTATION

We performed a proof of concept (PoC) implementation in order to evaluate the performance of our proposed solution. We first try to find the lowest number of Sealers or miners needed to maintain the BlockTime we expected from the sidechain. We build two private blockchain network based on PoA and PoW consensus consisting of one up to six miners to simulate a typical use case from a small hospital up to a well-connected network of hospitals. Our setup after numbers of testing is running on Ubuntu 18.04 LTS using Core i7 6700 with 3 cores and 3GB RAM at least. We use GO language based Ethereum (GETH) to create both of the private networks. Virtualization here is important in the case of opening the wrong socket to the public when connecting to the public blockchain. We set our block with a very large GasLimit since we needed to maximize the number of transactions per block. However, BlockTime is not equalled to transaction rate as it depends on the length of the data and the GasLimit. For examples, if a contract uses 94000 of Gas and the GasLimit is 94000000, the transaction rate calculated as 1000 transaction per BlockTime or 5 seconds in this case which is better compared to average Bitcoin transaction rate and even average rate of payment processing system like Visa [17].

Results. Table 1 shows the amounts of miners needed to maintain BlockTime under target between PoA compared to PoW based blockchain. PoA able to maintain close to 5 seconds BlockTime by having at least four miners but PoW consensus could not reach the expected 15 seconds Block Time. We also attached the CPU usage from Ubuntu of both algorithms after 1000 blocks validation to stabilize the network first. The typical energy efficiency concern from PoW consensus can be seen in this result. Expected BlockTime of PoA gradually reach 5 seconds after more than 10000 blocks validated but in the case for PoW based blockchain, it will need more processing power to achieve the BlockTime of 15 seconds. This confirms our cost-efficiency of PoA based private blockchain for cost efficiency when compared to using PoW as private blockchain.

We then execute a contract based on a Read queries on our private blockchain from 1 up to 1000 of our replicated patients' data that we have created. We used four miners for our PoA blockchain in this setup. We take the average times tak-

Table 1. Power Usage Evaluation

No. of Miner	Proof of Authority		Proof of Work	
	Block Time(s)	*CPU Usage (%)*	*Block Time(s)*	*CPU Usage (%)*
1	5.7	28	19.45	44
2	5.45	35	19.1	57
3	5.25	44	18.7	64
4	5.1	53	18.25	71
5	5.05	58	17.8	88
6	4.95	62	17.1	91

en for block validations between our private PoA blockchain and a public testbed. We use Rospten testbed because it is the only testbed using PoW to replicate the true performance of Ethereum. Other Ethereum testbed has moved to PoA consensus to avoid Spam attack and better efficiency as a public testbed. We use Remix IDE for both blockchains to run our contract based on reading the patient database. We connect using Web3 socket for our private blockchain and set to the auto-configuration for our contract deployment for both blockchains to deploy our code and using Metamask as our wallet provider since we will be needing token when using public blockchain. We are limited to a request for 100 tokens when using public testbed thus are limited in term of running a more complicated contract or a bigger size contract.

Results. Fig. 3 shows that the EMR system with PoA can handle more than reading 1000 patients data though we can expect some delay in Ropsten since we are executing it on the public testbed. The result shows the shortcoming of connecting EMR directly to the public blockchain when comparing to our own private blockchain. When comparing to traditional DB I/O performance, public blockchain is not acceptable enough especially when dealing with a bigger amount of data. Besides that, we confirm that scalability is not an issue as four miners are capable of handling the vast amount of data and in addition able to maintain the security of the EMR by needing at least three nodes out of the four nodes that were setup to authorize any actions taken on the EMR including adding or removing the nodes on the network.

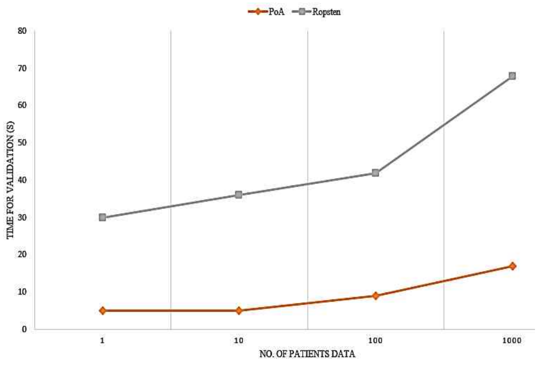


Fig. 3. The average time of Block Validation Comparison.

Next, we tested a contract for requesting data between 1 to 20 different patients on Ropsten and Sokol Network testbed, which is a PoA based Ethereum sidechain network for a real-world performance comparison. We take the time taken to get users data for our comparison by combining the time of a real sidechain network in addition to time taken with Ropsten to see the delay introduced when any transaction is going through the both the mainchain and the sidechain network. We use the most minimum number of tokens required to run the contract instead of raising the amount of Gas to fasten the process to emulate the cost effectiveness when using blockchain in real world usage.

Results. Fig. 4 shows that the total times for requesting patients' data using sidechain in combination with public blockchain in comparison to directly from a public blockchain. We chose this method as our experiment since connecting private blockchain to Ethereum is still limited in term of simulating it ourselves and we wanted to prove the concept before moving on to the deeper task of trying to connect our private blockchain to a public testbed which requires a significant amount of times. We can see from the result that both testbeds do not have a big difference between each other since both are having a different expected BlockTime. We can see here the delay introduced by using sidechain when requesting patients' data. Combining the time taken for requesting patients' data through mainchain and the time taken for DB queries through a sidechain, we can see the expected real-world results on using a sidechain which is the added delay when requesting for user's data. This result is expected since we are using two blockchains to do our operation with the time's delay is significant compared to our expectation. We needed to improvise our solution in term of this use case in order for it to be a viable option in real-world usage. We will see further on the advantages of our solution and methods to improve the performance of this scenario in the next experiment.

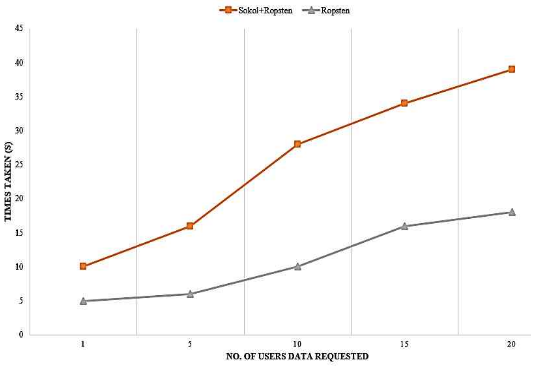


Fig. 4. Times needed to get user data.

The results from the previous test seem to show that delays will be introduced when dealing with requesting data from patient's operation. However, the time taken is considered only through both the mainchain and the sidechain when physicians are requesting for patients' data but most of EMR system operations will only be dealt in the sidechain network only. In addition, what we have not consider is that Sokol is a public sidechain network and is not owned by us. The test is meant to show the expected real-world performance for comparison. Optimization of the blockchain is the advantage here when it comes to having our own private blockchain network which can be tailored to our own use case. If we use our own PoA based sidechain times taken to read data on EMR against Ropsten, we can take a look at a well-optimized sidechain performance where improvement on the EMR system performance can be seen.

Results. To conclude our research, Fig. 5 shows that our proposed solution may cause delay in term of when requesting patients' data as it will always add some delay in addition to the mainchain times taken but we can see a bigger improvement when involving the EMR system only as only our own sidechain is involved. This is because when having our own private blockchain, we can maximize the transfer speed by raising the Gas needed for the operation whenever possible. However, in main-

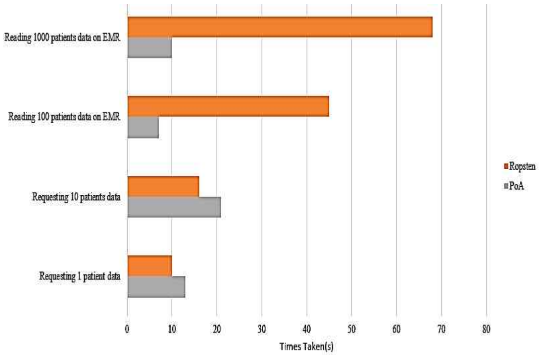


Fig. 5. Times taken comparison between requesting patients' data and EMR system only.

chain, Gas is equalled to the token which is real money or in other word, cryptocurrency which will cost money to us if we want to speed up any transaction. In our case, we just set the maximum gas limit as the processor usage of our virtual PC is still well under 70%. In real life, the GasLimit need to be setup with the processing power in mind as we do not want the unnecessary operation to hinder the processing power for a more important operation. Furthermore, with a more powerful node or BM, the sidechain performance can be better that what we expected from these results.

We added another real-world result using the same configuration as Fig. 4 but by raising the token for all the request through Sokol network to emulate our sidechain ability where we can just raise the tokens usage for faster transaction. We wanted to see the result if the improvement made is worth the cost of the paid transaction. We added 25 more tokens per transaction on top of the calculated token payment needed to run our contract as we are limited to 100 tokens per day when requesting for tokens for testing our contract. We used a smaller amount of token before running the experiment but without a significant value of improvement when reaching 15 patients' data and settle down with 25 tokens added per transaction where we can see some relationship between the cost efficiency of adding more tokens that the pre-calculated value done in the Remix IDE.

Results. With simpler operation or smaller sized data, Fig. 9 shows that increasing the token payment for the transaction will not add enough value for the time's improvement it made since it shaved around 1 to 2 second in times. As data get bigger or operation get complicated, it makes more sense to pay more for each of the transaction as the time improvement made will be significant as the time saved in this case will be near to 10 seconds per transaction. We solved this problem with our solution since we can just spend any number of tokens needed whenever faster throughput is required since all the nodes in blockchain are run by our own server thus also keeping the cost of operation minimal. Keeping in mind also that the transaction speed is still limited by few factors not just by the sheer processing power of the blockchain nodes but also how the blockchain is set up such as block size, GasLimit per block or BlockTime. Finding the right configuration depending on the hardware availability and type of operation usage will be an important part in making sure that pegged blockchain will be more advantageous than directly connecting to a public blockchain network. This results also show that we can solve the delay introduced for the scenario in Fig. 6 by minimizing the delay as much as possible by running a really fast private blockchain when the situation needed.

7. CONCLUSIONS

The big question on this proposed solution is currently the hot in discussion between relational DB versus blockchain based DB. Blockchain although is praised for its immutability, security and transparency, is debatable to deploy in real world, especially when comparing to traditional DB. Traditional DB has always the advantage over blockchain in term of speed and costs in some use case for example, an operation that needed con-

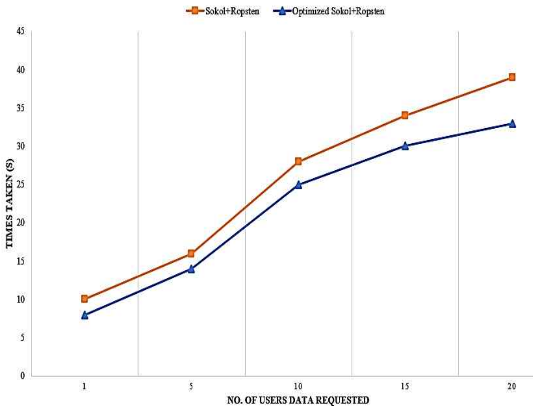


Fig. 6. Times taken improvement when increasing the token for each transaction in Sokol.

tinuous updating or fast online transaction, using a blockchain will defeat the purpose as blockchain speed will not be as close to as the speed of traditional DB even for the advantages it comes with [26]. Another example is simple data storing application where using blockchain will just add delay to the operation time and cost of running the operation without significant advantage that might be able to overtake the function of a traditional DB. Our proposed solution highlights one of the advantages of blockchain when used in proper use case scenario.

As health tracking devices will be widely adopted, the healthcare system can be improved in terms of data privacy and usage transparency since the vast amount of sensitive data will be exchanged between the patients and the hospital publicly. This paper highlights that pegged blockchain implementation did not sacrifice the performance of the healthcare system while achieving the objectives we wanted where scalability is not an issues and efficiency is better than connecting directly with public blockchain. We used public testbed to simulate our concept performance and tested our contract based on reading and requesting from patients for their hashed data. Our works done so far is to review the performance when using a connected private blockchain to a public blockchain to overcome the drawback from connecting directly to a public blockchain. We did not touch on deeper issues such as security analysis of the system or the protocol on IoT devices when sharing hashed data as mentioned in [17] and the method to peg blockchains together [18]. In the future, we will try to test the different methods of combining multiple blockchains where introduction of governance is needed for interoperability from each blockchain tokens, IPLD as our hashed data management system [19] which is a more efficient method of storing data in the contract and running a real DApp directly from user IoT or mobile devices.

REFERENCE

[1] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications," *Proceeding of 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications*, pp. 1-5, 2017.

[2] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based Data Sharing for Electronic Medical Records in Cloud Environments," *Information*, Vol. 8, No. 2, pp. 44, 2017.

[3] M.I. Joo, D.H. Ko, and H.C. Kim, "Development of Smart Healthcare Wear System for Acquiring Vital Signs and Monitoring Personal Health," *Journal of Korea Multimedia Society*, Vol. 19, No. 5, pp. 808-817, 2016.

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," pp.1-9, 2018.

[5] Hacker Noon, 11 Sidechain Projects Every Blockchain Developer Should Know About, https://hackernoon.com/13-sidechain-projects-every-blockchain-developer-should-know- about-804b 65364107 (accessed Sept., 29, 2018).

[6] R. Neisse, G. Steri, and I. Nai-Fovino, "A Blockchain-based Approach for Data Accountability and Provenance Tracking," *Computer Science*, arXiv:1706.04507[cs], 2017.

[7] P. Zhang, J. White, D.C. Schmidt, G. Lenz, and S.T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," *Computational and Structural Biotechnology Journal*, Vol. 16, pp. 267-278, 2018.

[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," *Proceeding of 2016 2nd International Conference on Open and Big Data*, pp. 25-30, 2016.

[9] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure Attribute-based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," *IEEE Access*, Vol. 6, pp. 11676-11686, 2018.

[10] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, "HealthSense: A Medical Use Case of Internet of Things and Blockchain," *Proceeding of 2017 International Conference on Intelligent Sustainable Systems*, pp. 486-491, 2017.

[11] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment," *Proceeding of 2018 IEEE International Conference on Information Reuse and Integration*, pp. 15-22, 2018.

[12] P. Zhang, M.A. Walker, J. White, D.C. Schmidt, and G. Lenz, "Metrics for Assessing Blockchain-based Healthcare Decentralized Apps," *Proceeding of 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services*, pp. 1-4, 2017.

[13] S. De Angelis, "Assessing Security and Performances of Consensus Algorithms for Permissioned Blockchains," *Computer Science*, arXiv:1805.03490[cs], 2018.

[14] Medium, RSK and Sidechains-The Litecoin School of Crypto-Medium, https: //medium.com/the-litecoin-school-of-crypto/rsk-and-sidechains-44d2ec88b896 (accessed Oct., 29, 2018).

[15] Enabling Blockchain Innovations with Pegged Sidechains, http://kevinriggen.com/files/sidechains.pdf (accessed Oct., 29, 2018).

[16] W. Xin, T. Zhang, C. Hu, C. Tang, C. Liu, and Z. Chen, "On Scaling and Accelerating Decentralized Private Blockchains," *Proceeding of 2017 IEEE 3rd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, and IEEE International Conference on Intelligent Data and Security*, pp. 267-271, 2017.

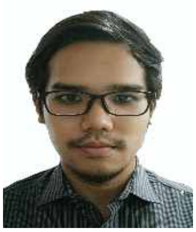
[17] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet of Things Journal*, Vol. 5, No. 2, pp. 1184-1195, 2018.

[18] Sidechains, Drivechains, and RSK 2-Way Peg Design, https://www.rsk.co/blog/sidechains-drivechains-and-rsk-2-way-peg-design (accessed Oct., 30, 2018).

[19] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards Data Assurance and Resilience in IoT Using Blockchain," *Proceeding of 2017 IEEE Military Communications Conference*, pp. 261-266, 2017.

[20] V. Patel, "A Framework for Secure and Decentralized Sharing of Medical Imaging Data Via Blockchain Consensus," *Health Informatics Journal*, pp. 1-14 2018.

[21] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, "Secure and Efficient Data Accessibility in Blockchain Based Healthcare Systems," *Proceeding of 2018 IEEE Global Communications Conference*, pp. 206-212, 2018.



Akmal Azizan Md Zin

2016 Data Communications and Networking, Multimedia University, Malaysia (B.S)
2019~Current Department of Information and Communication Systems, Inje University, (M.S)

Quoc-Viet Pham

2013 Electronics and Telecommunications Engineering, Hanoi University of Science and Technology, Vietnam (B.S.)
2015 Information and Communications Engineering, Inje University, Korea (M.S.)
2017 Information and Communications Engineering, Inje University, Korea (Ph.D.)
2018~Current ICT Convergence Center, Changwon National University, Research Professor

Han Suk Young

1999 Busan National University Computer Engineering Department (Bachelor)
2003 USC, Software Engineering (Master)
2004~2014 Product Planning for Mobile Phone in Samsung Electronics" Wireless Business Department 2012~2017 The Way Consulting CEO 2017˜ Currently Professor of Institute or Digital Anti-aging Healthcare at Inje University

Kim Jung Eon

2006 Gyeongsang National University, School of Medicine (M.D.)
2018~Current Inje University Ilsan Paik Hospital, Department of Emergency Medicine, Clinical Professor

Kim Hoon

2002 Inha University, College of Medicine (M.D.)
2007 Inha University, College of Medicine, Graduate school, (M.S.)
2017 Inha University, College of Medicine, Graduate school (Ph.D.)
2010~Current Inje University Ilsan Paik Hospital, Department of Emergency Medicine, Professor

Park Junseok

1997 Yonsei Wonju Medical School (M.D.)
2008 Yonsei University College of Medicine, Graduate School (M.S.)
2014 Chungnam Univeristy College of Medicine, Graduate School (Ph.D.)
2005~Current Inje University Ilsan Paik Hospital, Department of Emergency Medicine, Professor

Hwang Won-Joo

1998 Pusan National University Dept. of Computer Engineering (B.E.)
2000 Pusan National University Dept. of Computer Engineering (M.E.)
2002 (Japan) Osaka University Dept. of Information Systems Engineering (Ph.D.)
2002~Current Inje University Dept. Of Electronic, Telecommunications, Mechanical & Automotive Engineering, Professor