Techno-Science Research Journal V13 (3) (2025) P 19-26

Content list available at ITC

Techno-Science Research Journal

Journal Homepage: http://techno-srj.itc.edu.kh/

Techno-Science Research Journal

Security Management of Reputation Records in the Self-Sovereign Identity Network for the Trust Enhancement

Selasak Song [1*], Dara Tith [1, 2], Dona Valy [1]

[1] *Department of Information and Communication Engineering, Institute of Technology of Cambodia, Russian Federation Blvd., P.O. Box 86, Phnom Penh, Cambodia*

[2] *Faculty of Computer Science, University of Namur, Rue Grandgagnage 21, 5000 Namur, Belgium*

Received: 01 August 2024; Revised: 16 September 2024; Accepted: 14 November 2024; Available online: December 2025

Abstract: *In many companies and organizations around the world, user's identity data is stored and handled in centralized systems rather than decentralized ones. A centralized system comes with many risks, such as data leaks or users not being in control of their data. These problems can be fixed by using a decentralized system known as the Self-Sovereign Identity (SSI) system. SSI system is a user-centric system that lets users manage and control their own identity data. In an SSI system, there are three main actors, which are the user called the holder, the issuer who issues credentials to the user, and the verifier who checks the credentials presented by the user. However, SSI system is not perfect since it has the problem of not knowing whether the credential information that the user provides is authentic or not. Since credentials can be issued by any issuers in the SSI system, there needs to be an established trust between the verifier and the issuer. Therefore, the solution to improving trust within the SSI system is to implement a model called the reputation system. This proposed reputation system will determine if an issuer can be trustworthy. To establish robust security protocols within the system, it also needs to have a secured storage system. This can be achieved by leveraging blockchain technology for storing reputation data. The framework that is used to build the blockchain network in this reputation system is called Hyperledger Fabric. Using this proposed reputation system can ensure data authenticity and transparency.*

Keywords: Self-Sovereign Identity, Reputation System, Trust, Blockchain, Hyperledger Fabric

1. INTRODUCTION

1.1 Introduction

Identity management systems are essential in modern society as most medium and large organizations provide information and services through the use of technology, which requires users to have a digital identity [1]. It is important for this system to be secured and be able to protect user data. However, most of the current identity management systems are not up to standard to handle and protect those digital identities, as they are often vulnerable to data leakages, which occur because of the centralized storage system [2]. One system that can solve this problem is the Self-Sovereign Identity (SSI) system. Self-Sovereign Identity system or SSI system, is a decentralized identity management system that allows individuals to fully own and manage their own digital identity and credentials [2]. Not only is the SSI system more secure than centralized identity management systems, but it also prevents third parties from benefiting from users' data. Trust plays an important role within an SSI system. However, it is hard to establish trust in the system because issuers can act in bad faith and issue wrong credentials for holders, making it challenging for a verifier to trust a Verifiable Credentials (VC) issued by a malicious issuer [3]. In SSI, honest and malicious issuers have no distinguishing features that separate them from each other. The decision to trust which organization is honest or not is placed on the verifiers, which will give them a burden because of the serious decision that they need to make. If the verifiers want to check the authenticity of the credentials that they receive, they would have to look up the information about the organization by themselves.

In a previous research project of SSI, one researcher has addressed this challenge by evaluating the VC and collecting reputation records of a VC issuer based on the accuracy of the VCs when compared to those issued by different entities [4]. Reputation is an assessment or evaluation of an entity's

* Corresponding author: Selasak Song
E-mail: song.selasak@gmail.com; Tel: +855-70 751 165

trustworthiness, reliability, and overall behavior within the network. To verify the correctness of a VC, he adopted the Byzantine Fault Tolerance (BFT) concept, collecting multiple VCs and evaluating their contents to identify any with incorrect information.

Thanks to the previous research of this researcher [4], he has provided a method to solve a problem and enhance trust in a VC. However, that research does not yet address the security aspects of storing reputation data for a verifier or other stakeholders who wish to check and validate the reputation records of an issuer.

The main objective of this project is to design a system architecture using existing security mechanisms to enhance the management of reputation records in the reputation system of SSI. Within this system, users can check the credibility of the credentials by checking the reputation of the person who issues them. The system needs to employ a strong security architecture that can prevent unwanted data manipulation. The main tool that can be used to handle this task is a decentralized system called a Blockchain network.

1.2 Background

In a reputation system, trust and privacy have a connection with each other [5]. If we want to facilitate trust-based relationships, there will be some shortcoming for the privacy of users. If we hide our reputation, we would have privacy, but others would not know if we could be trusted or not. Privacy prevents trust because it makes it hard to know the reputation of others. Privacy is needed for only data that shows personal information. Since reputation data allows the public to make judgments, the justification for collecting and showing reputation data is to have informed evaluations and have a reputation emerge. However, some privacy will still need to be preserved to enable better security. According to research conducted by Hasan et al [6], privacy enables users to feel safe when using a reputation system.

Blockchain is a decentralized system that keeps data across multiple parties to keep the contents secure [7]. Blockchain does not need any third-party organization to manage the system, and it could ensure that data cannot be tampered with by unauthorized access. There has been an increase in interest in implementing Blockchain in various sectors, such as financial, educational, medical, industrial, Internet of Things, and many more. Similarly, reputation systems have been utilizing Blockchain to a great extent. Using blockchain in reputation systems not only protects privacy but also introduces unique features like trustlessness, transparency, and immutability [6].

Blockchain can be categorized into two main groups, permissionless Blockchain and permissioned Blockchain [8]. Each type of Blockchain is used to handle different kind of tasks. Permissionless Blockchain is a type of Blockchain where anyone can join the Blockchain network [9]. Permissionless Blockchain has the characteristics of being openness and transparency, where data stored in permissionless Blockchain is visible to anyone to see. As for permissioned Blockchain, it is a type of Blockchain system where the participant of this system is known, and the user must register onto this system in order to use it [10]. This kind of Blockchain is intended for organizations or consortiums to use, rather than the general public.

2. RELATED WORKS

Based on the research conducted by Khun [4], the architecture of reputation modem contains two main components that aim to improve trust within an SSI system, which is shown in Fig. 1. The first component is a reputation system, which evaluates and assigns reputation scores to issuers. The reputation system determines if an issuer is trustworthy based on the reputation score, which is calculated based on the issuer's ability to provide authentic information. The second component is a feedback system, which allows the verifier to submit feedback to the issuers. The feedback system collects feedback from verifiers and analyzes that feedback to assess the issuer's service. The reputation system and the feedback system exchange data with each other to improve trust within the overall SSI system. In this system, the reputation records are stored in a centralized file storage and does not have any security mechanisms to protect those data.

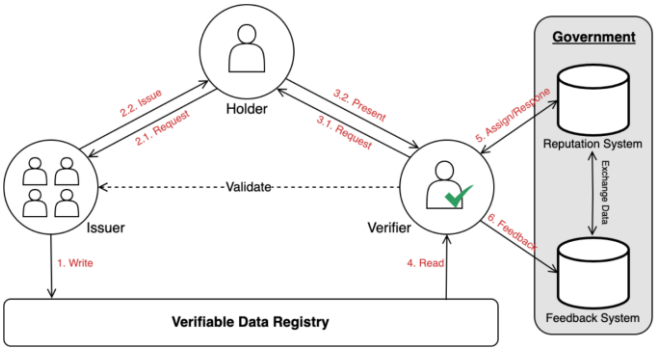

Fig. 1. Khun Reputation Model [4]

Another paper by Zhao et al [11] has demonstrated the implementation of a reputation management system with a Blockchain network. The Blockchain network allows for the prevention of malicious users from committing nefarious

act, and also preserve the privacy of the user in the system. The reputation system implemented in this research uses Hyperledger Sawtooth framework. In the research presented by Schaub et al [12], they have proposed a reputation system for e-commerce domain that is built with using blockchain technology. Traditional centralized reputation system has some shortcoming related to potential abuse by the central authority and needing to place trust on a third-party organization. Blockchain allows the reputation system to be decentralized, while also provide integrity by allowing the history of the reputation to be verified, and also preserve the privacy of the reputations within the system.

Tamang [13] has implement the use of blockchain technology to model a trust framework and implement a reputation system, which allow the participating entities to endorse or rate each other. The proposed reputation/endorsement system is implemented with a browser (client side) and blockchain network (endorsement system). The client application is a front-end software that allows the users to send endorsement to the blockchain network to be executed by the smart contracts. As for the proposed blockchain platform, it uses Ethereum, which is a public blockchain setup with Proof of Work (PoW) as the consensus algorithm.

3. METHODOLOGY

3.1 Technologies uses

3.1.1 Self-Sovereign Identity System

Within an SSI system, there are three main actors that are related to each other [14]. These three actors include the issuer, the holder, and the verifier, which is shown in Fig. 2 [2]. The issuer is an entity that issues credentials within the SSI system. When issuers issue credentials, they will also store cryptographic proof that they are the one who issued those credentials in Verifiable Data Registry [2]. This cryptographic proof is in the form of Decentralized Identifier Documents (DID Document), which contains information related to the Decentralized Identifier and also verify if the issuer really signs the credentials. An example of an issuer is a bank or government official. They issue credentials for their users to use. The user who uses those credentials is called the holder. The holder is an entity that stores and manages the credentials issued by the issuer. When the holder wants to use a service that requires authentication, the holder will present their credentials to the verifier. A verifier is an entity that verifies the holder's credentials to see if they are issued by a trustworthy issuer. When the verifier receives the Verifiable Presentation, they will verify the signature of the issuer of the credentials with the DID document in the Verifiable Data Registry. The reason why trust in an issuer is important is because anyone can be an issuer and issue credentials in an SSI system. In order to accept the credentials, the verifiers need to have trust in the issuer. If the issuer is a government official, the verifier will trust them to always issue trustworthy credentials. However, if the issuer is from an unknown organization, then it is hard for the verifiers to trust them. This is where the reputation model can help verifiers make decisions about whether to trust issuers or not.

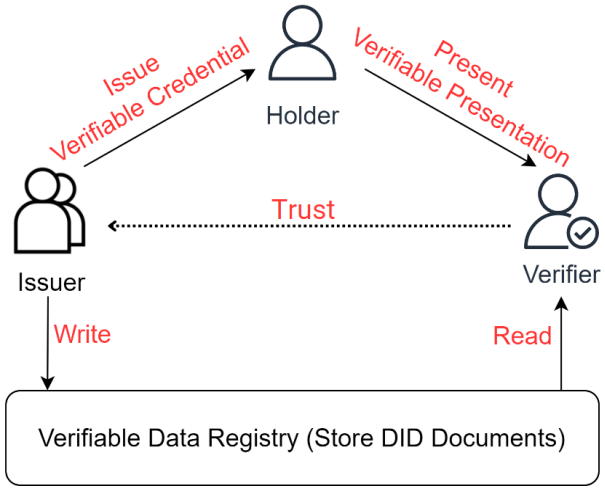

Fig. 2. Self-Sovereignty System Model

3.1.2 Hyperledger Fabric

The implementation of the Blockchain network is done on a framework called Hyperledger Fabric. The implementation was not done in Ethereum like in Tamang [13] research is because it is a public blockchain, while Hyperledger Fabric is a private blockchain. While Ethereum can also operate as a private blockchain similar to Hyperledger Fabric, Hyperledger Fabric offers several additional advantages over Ethereum [15]. First of all, Ethereum uses Proof-of-Work (PoW) and Proof-of-Stake (PoS) as its consensus algorithm, which uses more resources than the consensus algorithm in Hyperledger Fabric, which can use many consensus algorithms. Not only that, the speed of transactions in Hyperledger Fabric is faster than Ethereum, and Hyperledger Fabric scale better as well. The last reason is that smart contracts in Ethereum can be developed with one programming language, while smart contracts in Hyperledger Fabric can be developed with a wide range of languages such as Java, Node.js, Go, and JavaScript. A private blockchain is utilized because the reputation system is intended for users within the SSI system to use, rather than for the general public. Hyperledger

Fabric utilizes concepts such as Membership Service Provider (MSP), nodes, chaincodes, also known as Smart Contract, ledgers, and consensus algorithms [16]. The MSP contains a list of identity that is used to identity who are the user and the peers or nodes within the system. The node in the Hyperledger Fabric can be a peer that keeps a copy of the ledger. The peer can also be an endorser who will approve the addition of new data to the ledger, and also be the orderer peer which act as a middleman that collect the transactions and order them into block to be added into the ledger. Within this platform, the ledger is used to store the reputation records of the issuer. Within the Blockchain, there are two main chaincodes, which are creating and retrieving reputation records. As for the consensus algorithm, it will use Practical Byzantine Fault Tolerance (PBFT) to come to an agreement between multiple nodes within the system. PBFT is used as a consensus algorithm because it allows different nodes to keep the same records by communicating with each other and coming to an agreement about what the data should look like. This consensus algorithm is cost-efficient as it does not require a lot of computational power, when comparing to other consensus algorithms such as Proof of Work (PoW) [17].

3.2 Proposed System Architecture

The proposed system architecture is a trust model called reputation system. It is a system that run outside the SSI system, which can be connected to SSI system to improve trust within the system.

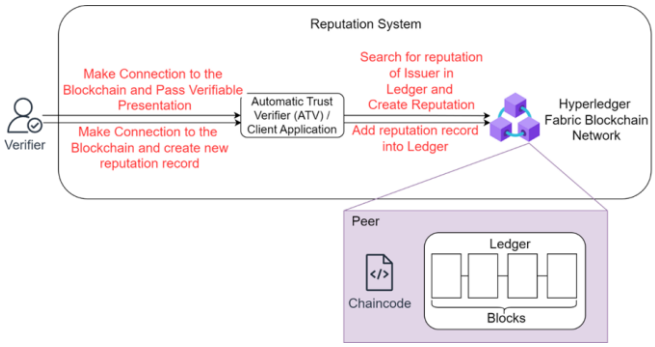

Fig. 3. Proposed System Architecture

This proposed architecture in Fig. 3 is connected to the SSI system. When the verifier receives Verifiable Presentation (VP) from the holder, the verifier uses the proposed architecture above to evaluate the credibility of the VP. The verifier will pass the VP into the Automatic Trust Verifier (ATV). The ATV is an application that allow the user to connect to the blockchain network and provide Application Programming Interface (API) for the users to make request to run functions within the blockchain, which is similar to the client application implemented by Tamang [13]. After the ATV receives the VP, it will search for the issuer who issued the VP in the reputation storage. The reputation storage uses a blockchain to store reputation records because it is harder to tamper with the data. The reputation record in the reputation storage contains information related to the issuer, such as the reputation ID, issuer ID, record owner name, time record created and trust score which tells it whether the issuer is trustable or not. This is because the trust score can help determine the trust status. The scoring of the reputation record follows the FICO scoring model, ranging from 300 to 850, as this scoring model is used by banking to determine the trustworthiness of customers [18]. When the ATV gets the reputation record of the issuer, it will return this record back to the verifiers, which included the trust score of the issuer. This proposed architecture will only help the verifier make decisions related to trust, and the final decision is still up to the verifier to make.

3.3 Chaincode process

To develop the reputation system, it needs to have functions to run the basic tasks of creating reputation records and retrieving reputation records. Therefore, four main functions will be implemented, which include creating reputation records, retrieving specific reputation records, retrieving reputation records between specific dates, and retrieving the latest reputation records. These functions are implemented based on the use cases for the reputation system. The chaincode functions listed above can be grouped into two main processes, one for creating reputation records and the other for retrieving reputation records. Since the multiple chaincode functions for retrieving reputation records are similar to each other, they can be viewed as one process of retrieving reputation records.

3.3.1 Creating Reputation Records

In order to create a reputation record for the issuer, the reputation system utilizes chaincodes to run code on the blockchain network. This process begins when the verifier receives the credentials from the holder, which are issued by the issuer. First, the verifier sends the request to give rating along with the verifiable presentation that he had received from the holder to the Automatic Trust Verifier (ATV). Then, the application sends those data to the endorser peer and propose request to run the chaincode within the network. The endorer peer first verify the request to make sure it from a valid user who make this request, and also to make sure that the requested user has proper permission to make this request. When the endorser peers successfully verify the

request, they will run the chaincode function. The chaincode first query data from the ledger to see the state of the ledger and write data into it. Since it writes data into the ledger, it will need to broadcast the transaction proposal to the orderer peers. The orderer peers will package the transactions into block and broadcast it to all peer within the network. When all peers receive the new block, they will add it into their ledger and notify the client application and the user that their rating have been given successfully.

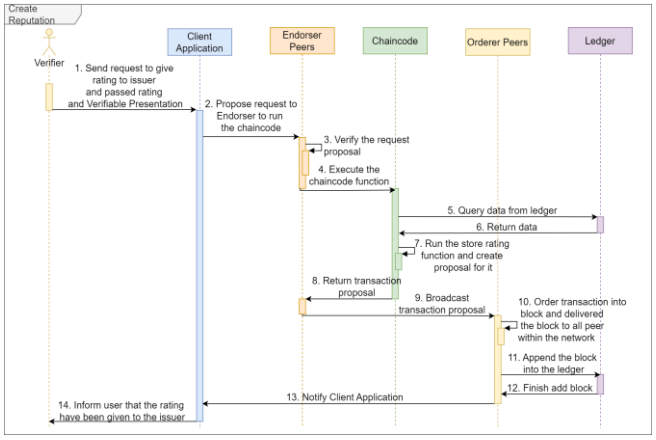

Fig. 4. Creating Reputation Record Process

3.3.2 Retrieving Reputation Records

When verifiers or other stakeholders want to see the reputation of an issuer, they will have to make a request to the blockchain network in order to retrieve the reputation record. First of all, the holder will request a service from the verifier and the verifier will request credential from the holder. When the holder provides their verifiable presentation, the verifier will pass that information to the client application. Then, the application sends those data to the endorser peer and propose request to run the chaincode or smart contract within the network. The endorer peer first verify the request to make sure it is valid, and then it run the chaincode. The chaincode will then query data from the ledger and return it to the endorser peer. Finally, the endorser peer will broadcast the result to the client application and inform the user about the trust score of the issuer.

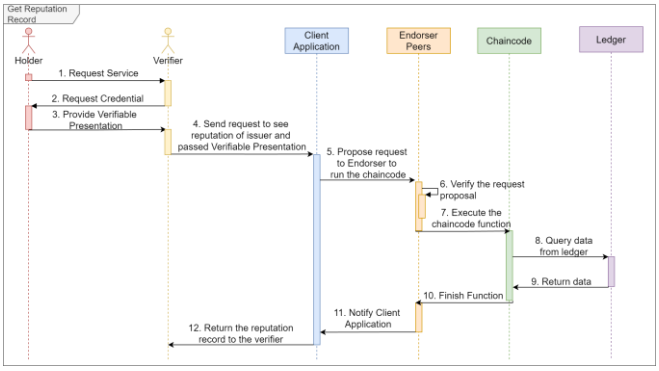

Fig. 5. Retrieving Reputation Record Process

4. RESULTS AND DISCUSSION

4.1 Result

After the reputation system successfully implemented, the system needs to do performance testing to ensure that it work for real world scenario. The testing of this system is conducted in an Ubuntu Operating System running version 20.04 using the Windows Subsystem for Linux 2 (WSL2), and the Hyperledger Fabric Network version is running on version 2.5.4. As for the hardware of the machine that is used to run this system, it has a Ryzen 7 5800H central processing unit (CPU) as well as 16 gigabytes of random-access memory (RAM). For the testing of the system, there are three tests that was conducted, the first one is for one thousand records, the second one is for ten thousand records, and the last one is for a hundred thousand records. This test is performed to determine how long it take for each chaincode to finish its functions, and to also see if this system can handle large amount of reputation records. To get the result of these chaincode functions, the chaincode is run from Postman to get accuracy time. Each test of chaincode is run five times to get an average result.

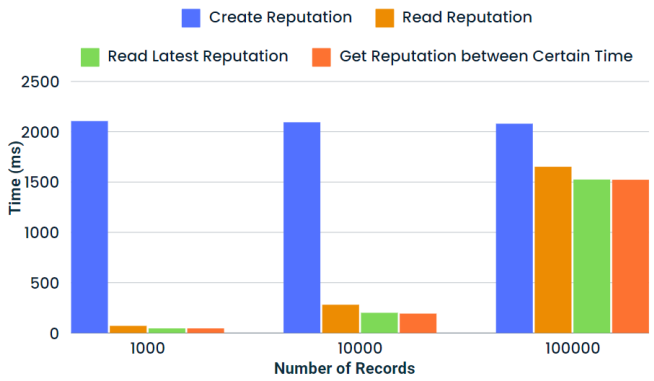

Fig. 6. Performance Graph of Chaincode Functions within the Blockchain Network

The assessment of the performance of the chaincode functions above only consists of two peers within the blockchain network. Therefore, to get a more robust and accurate result for the real-world performance, more peers need to be added to the blockchain system. So, three tests were performance, the first one for two peers, the second test for ten peers, and the last test for twenty peers. However, when running the chaincode function for query data from the ledger, only the peer that is connected through the Automatic Trust Verifier runs the chaincode functions. As for the chaincode function that writes data onto the ledger, all the peers on the blockchain network run to evaluate the transaction and to add the data onto the ledger. Therefore, the test will be conducted only on the create reputation chaincode function. After performing the test for ten peers and twenty peers, the result is shown in Fig. 7, with the result for testing of two peers from the first test. With the first test, the average time it takes for the create reputation chaincode function to finish is 2106 milliseconds, while the average time for ten peers is 2194 milliseconds, and the average time for twenty peers is 2262 milliseconds.

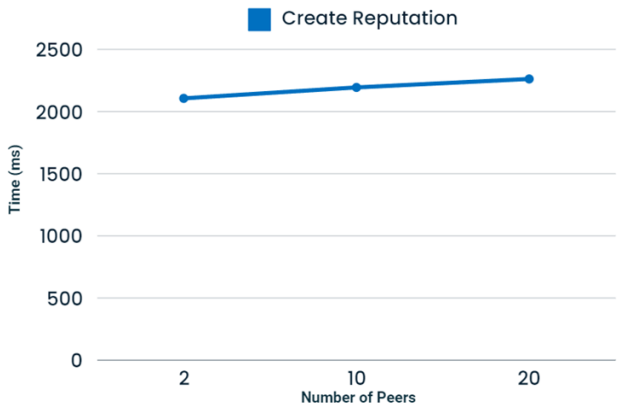

Fig. 7. Performance Graph of Create Reputation functions in Multiple Peers

4.2 Discussion

4.2.1 Results Analysis

Based on the graph in Fig. 6, the chaincode for create reputation record does not get affected by the number of reputation records in the ledger, and it has a constant executing duration. As for the chaincode function to retrieve reputation record, the duration for the chaincode to finish executed grow along with the amount of reputation records. Even though there are three different chaincode to get reputation record for different purposes, the duration each chaincode take to finish running does not differ from each other.

Judging by the result from the graph in Fig. 7, the duration for the create reputation function to increase from 2 peers to 10 peers is about 88 milliseconds, and from 10 peers to 20 peers is about 68 milliseconds. The reason for why this duration increases is because of how the Hyperledger Fabric architecture operates [16]. In order for a chaincode function to write data onto the ledger, all peers within the network need to run the chaincode function to get a result. Before the result of the chaincode function is submitted to the ledger, they need to verify to make sure that the majority of peers had the same result through a consensus algorithm. As more peers increase, more peers would need to run the chaincode function, and more results would need to be verified, so the duration would also increase. The increase of peers increases the duration for a chaincode function to run, but since the duration increase is minuscule, it has little impact on the performance of the proposed system. Therefore, it can be concluded that the proposed system can easily scale to multiple peers without any affect to the performance of the system. However, since these tests are performed on a single machine, they do not account for the network latency when the peer is deployed on another machine on the same network or on a different network.

4.2.2 Proof of Security

In order to determine if the proposed system is adequate at protecting reputation records against threats, the proposed system needs to follow the framework of the CIA (Confidentiality, Integrity, and Availability) Triad. To see if each component of CIA is followed, the proposed system needs to be tested. The first component to compare with is confidentiality. Confidentiality means that only users with proper permission can view specific data. To test the system's confidentiality, the chaincode functions need to be called from a user who does not have an identity in the Member Service Provider list. In the Automatic Trust Verifier, it makes connections to the blockchain network by providing the user identity, signature, and the peer on the network. When the user does not have the private key to prove they are users of the blockchain network, that users cannot make a connection to the blockchain network. Therefore, only users within the system have access to these reputation records.

For the second component of integrity, a system that is said to have integrity is any system that prevents unwanted altering or tampering of data. To see if the proposed system can prevent the tampering of data, then the stored data needed to be retrieved to see how it is stored on the blockchain. After retrieving the latest block on the ledger, it shows the latest block hash and the previous block hash. The block hash is the hash of the data store on the block. If an

attacker wants to change the data store on the blockchain, they would have to change the hash of the current block and the block after that. This is because a single block stores both the hash of the data and the hash of the previous block. Therefore, changing one data in a single block would mean changing data for all the following blocks, which is mathematically impossible. So, the proposed reputation system follows the integrity guideline.

As for availability, this means that the system would have to be available for the users to use and not be out of service. To see if the proposed system can follow this guideline, a test is conducted where some peers within the network are not running. Based on the test that was conducted, a chaincode function that writes data onto the blockchain network is run while four out of twenty peers are stopped running. After the chaincode function finishes running, the data is stored on the ledger, and it can retrieve those data. Therefore, if one node is down or got attacked, then the reputation system is still running on other nodes.

4.2.3 Comparison to other researches

Based on the implementation of the proposed model, the reputation system will yield desirable results when comparing to past reputation system that uses centralized system such as in Khun's system [4]. In this centralized reputation system, there is no proper security mechanisms to protect against the altering of data. By using blockchain as a storage for reputation records, it will prevent the tampering of data, which will increase the trust of the verifier on the reputation record.

When comparing the implemented reputation system against other blockchain-based reputation systems [11], [12], there is some similarity as well as some differences. The reputation systems proposed by those researches both focus on preserving privacy for reputation records to resist malicious users and to protect users' identities. As for the proposed reputation system, it also provides privacy for the reputation records by encrypting the records for only verifiers with proper permission to decrypt and view the data of the reputation records. As for the differences, the first research was implemented with Hyperledger Sawtooth framework, while this research uses Hyperledger Fabric. With Hyperledger Sawtooth, the blockchain could be implemented using permissioned and permissionless blockchain, while Hyperledger Fabric could be implemented with permissioned blockchain. Since the use case of the proposed reputation system is for verifiers within the SSI system, the framework implemented only needs to support permissioned blockchain. As for the second research, it focuses on e-commerce applications, while the proposed system focuses on SSI applications.

As for comparison against research conducted by Tamang [13], there is some similarity as well as some differences. Since both systems use Blockchain network as the storage system, both systems have the benefits that Blockchain provided such as data integrity and less prone to attack when compare to centralized storage system. As for the differences, Tamang's reputation system uses public Blockchain while the proposed system uses a private one. The key different between these two systems is that Tamang's system is for the public to use, while the proposed system is built for a consortium such as for a specific country or an organization to use. Therefore, my reputation system tackle one area that not many other researchers had tackled yet.

Even though the proposed system can ensure security against certain threats, it does not provide protection against all kinds of attacks. One kind of attack that attackers could use is to compromise user accounts through social engineering, supply-chain attacks, hardware compromises, or other attack methods. With this attack, the attacker would have free access to the system and be able to exploit the system. Moreover, the availability of the proposed system only checks with multiple peers within the network and not multiple users using the system. Therefore, if the number of users reaches a certain amount, there might be a delay to the responding time of chaincode functions, or the system would stop running.

5. CONCLUSIONS

This paper highlights the advantages of using blockchain technology in a reputation system connected to an SSI system. The reputation record will be tamper-proof against unwanted attacks. Not only that, this paper highlights one areas that rarely explore by other researcher, which is private Blockchain-based reputation system. Implementing reputation system using Hyperledger Fabric as its framework have both benefits and disadvantages. The benefit of using Hyperledger Fabric is that there are many documentations related to this framework, and it has a large community that help others when they have problem with using Hyperledger Fabric. As for the disadvantages, it is hard to setup Hyperledger Fabric for the first time since there are many dependencies that are needed for it to work. Not only that, each dependency required specific version for it to work. Therefore, the setup of this project took most of time during the implementation phase.

For future work, researchers can focus on implementing access control related to the reputation system to ensure that

only users with proper permission can access the reputation records and make changes to the ledger. Researchers can also further expand this area of research by conducting research on the transfer of reputation records from a Blockchain network to the Automatic Trust Verifier. Research can use tools such as cryptography to ensure there is proper security when user try to connect to the reputation system. Moreover, analyzing the performance of the reputation system with multiple users and ensuring protection against different kinds of attacks, such as compromising hardware or user accounts are research areas that could be further studied.

ACKNOWLEDGMENTS

This research was possible thanks to the funds provided by the ERASMUS+ Program and the University of Namur for providing a research internship. The authors would also like to give their sincere thanks to Pr. Jean-Noël COLIN who is always there to help guide the authors throughout the research period, provide the authors with valuable insights, and also provide helpful comments for this research.

REFERENCES

[1] D. Pöhn and W. Hommel, "An overview of limitations and approaches in identity management," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, in ARES '20. New York, NY, USA: Association for Computing Machinery, Aug. 2020, pp. 1–10. doi: 10.1145/3407023.3407026.

[2] M. A. López, "Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain," Sep. 2020, doi: 10.18235/0002635.

[3] M. Kubach and H. Roßnagel, "A lightweight trust management infrastructure for selfsovereign identity," 2021, Accessed: Dec. 04, 2023. [Online]. Available: https://publica.fraunhofer.de/handle/publica/413107

[4] D. Khun, "Reputation Model For Trust-Based Policy In Self-Sovereign Identity Systems For Healthcare," 2023.

[5] G. Sartor, "Privacy, Reputation, and Trust: Some Implications for Data Protection," in *Trust Management*, K. Stølen, W. H. Winsborough, F. Martinelli, and F. Massacci, Eds., Berlin, Heidelberg: Springer, 2006, pp. 354–366. doi: 10.1007/11755593_26.

[6] O. Hasan, L. Brunie, and E. Bertino, "Privacy-Preserving Reputation Systems Based on Blockchain and Other Cryptographic Building Blocks: A Survey," *ACM Comput. Surv.*, vol. 55, no. 2, p. 32:1-32:37, Jan. 2022, doi: 10.1145/3490236.

[7] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalimeh, "A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities," *IEEE Access*, vol. 9, pp. 12730–12749, 2021, doi: 10.1109/ACCESS.2021.3050241.

[8] A. Miller, "Permissioned and permissionless blockchains," *Blockchain Distrib. Syst. Secur.*, pp. 193–204, 2019.

[9] "Privacy preservation in permissionless blockchain: A survey," *Digit. Commun. Netw.*, vol. 7, no. 3, pp. 295–307, Aug. 2021, doi: 10.1016/j.dcan.2020.05.008.

[10] S. Solat, P. Calvez, and F. Naït-Abdesselam, "Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice," *J. Softw.*, vol. 16, pp. 95–106, Dec. 2020, doi: 10.17706/jsw.16.3.95-106.

[11] K. Zhao, S. Tang, B. Zhao, and Y. Wu, "Dynamic and Privacy-Preserving Reputation Management for Blockchain-Based Mobile Crowdsensing," *IEEE Access*, vol. 7, pp. 74694–74710, 2019, doi: 10.1109/ACCESS.2019.2920922.

[12] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A Trustless Privacy-Preserving Reputation System," in *ICT Systems Security and Privacy Protection*, J.-H. Hoepman and S. Katzenbeisser, Eds., Cham: Springer International Publishing, 2016, pp. 398–411. doi: 10.1007/978-3-319-33630-5_27.

[13] S. Tamang, *Decentralized Reputation Model and Trust Framework Blockchain and Smart contracts*. 2018. Accessed: Jan. 29, 2024. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-393203

[14] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Comput. Sci. Rev.*, vol. 30, pp. 80–86, Nov. 2018, doi: 10.1016/j.cosrev.2018.10.002.

[15] K. Jyothilakshmi, V. Robins, and A. Mahesh, "A comparative analysis between hyperledger fabric and ethereum in medical sector: A systematic review," *Sustain. Commun. Netw. Appl. Proc. ICSCN 2021*, pp. 67–86, 2022.

[16] "Hyperledger Fabric Docs." Accessed: Apr. 29, 2024. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html

[17] D. A. Sharma, "Consensus Mechanisms in Blockchain Networks: Analyzing Various Consensus Mechanisms Such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT)," Jan. 2021, Accessed: Jul. 17, 2024. [Online]. Available: https://thesciencebrigade.com/btds/article/view/148

[18] M. Renzi, M. Canale, B. Witherell, and A. Nolan, "Underwriting the American Dream," 2021.