A Blockchain and Self-Sovereign Identity Empowered Digital Identity Platform

Eranga Bandara*, Xueping Liang†, Peter Foytik*, Sachin Shetty*, Kasun De Zoysa‡
* {cmedawer, PFoytik, sshetty}@odu.edu
Old Dominion University, Norfolk, VA, USA
† {x_liang}@uncg.edu
University of North Carolina at Greensboro, NC, USA
‡ {kasun}@ucsc.cmb.ac.lk
University of Colombo School of Computing, Sri Lanka

***Abstract*—Most of the existing identity systems are built on top of centralized storage systems. Storing identity data on these types of centralized storage platforms(e.g cloud storage, central servers) becomes a major privacy concern since various types of attacks and data breaches can happen. With this research, we are proposing blockchain and self-sovereign identity based digital identity (KYC - Know Your Customer) platform "Casper" to address the issues on centralized identity systems. "Casper " is an Android/iOS based mobile identity wallet application that combines the integration of blockchain and a self-sovereign identity-based approach. Unlike centralized identity systems, the actual identities of the customer/users are stored in the customers' mobile wallet application. The proof of these identities is stored in the blockchain-based decentralized storage as a self-sovereign identity proof. Casper platforms' Self-Sovereign Identity(SSI)-based system provides a Zero Knowledge Proof(ZKP) mechanism to verify the identity information. Casper platform can be adopted in various domains such as healthcare, banking, government organization etc. As a use case, we have discussed building a digital identity wallet for banking customers with the Casper platform. Casper provides a secure, decentralized and ZKP verifiable identity by using blockchain and SSI based approach. It addresses the common issues in centralized/cloud-based identity systems platforms such as the lack of data immutability, lack of traceability, centralized control etc.**

***Index Terms*—Blockchain; Self-Sovereign Identity; Zero-Knowledge Proof; Cloud Computing**

1. Introduction

Most of the existing identity platforms used centralized data storage(e.g cloud stores) architecture. These centralized data storage comes with inherent security and privacy issues, in perspectives of control, immutability, and data provenance management. Due to these concerns, data fraud and attacks are easier and more likely to happen. Unauthorized third parties such as hackers, or employees of the cloud service company, may access the data and alter them. Whenever a large amount of data is stored in a central location it creates a greater incentive to attackers. In this regards, storing identity data on these types of centralized storage platforms(e.g cloud storage, central servers) becomes a major privacy concern. With this research, we are proposing blockchain and self-sovereign identity based digital identity platform, Casper, to address the issues on centralized identity systems. "Casper" comes with an Android/IOS based mobile identity wallet which is built on top of blockchain and self-sovereign identity-based approach. Unlike centralized identity systems, the actual identities of the customers/users stored in the customers' mobile application. The proof of these identities stored in the blockchain-based decentralized storage as a self-sovereign identity proof. Casper platform's self-sovereign identity-based system provides a zero-knowledge proof mechanism to verify the identity information. Casper platform can be adopted in various domains such as healthcare, banking, government organization etc. As a use case of Casper, we have implemented an inter-bank KYC platform for banking customers. With this system, banking customers can hold their own customer data on the mobile wallet. The customer identity which is known as DID(decentralized identity in SSI terms) embedded in the QR code in the mobile wallet. Customers can prove their identity and share the data with other entities(e.g banks, hospitals, government organizations etc) by using their mobile wallet. Other entities can verify the customers' identity by using Zero-Knowledge Proof. For credential verification, we provide mobile and web-based "Trace" application for admin entities in different organizations(e.g bank officer, healthcare company admins). In Casper, all user personal data is stored in users' physical mobile devices based on SSI architecture. Only the cryptographic identity proofs and artefacts will be stored in blockchain storage. In this way, the Casper platform addressed the above-mentioned issues with a cloud storage approach by providing Data Privacy, Confidentiality, Integrity, Authentication, Authorization security features. Following are our main contributions.

1) Blockchain and SSI empowered decentralized identity system has been introduced to address the challenges in centralized identity systems.
2) Android/IOS based mobile identity wallet has

been introduced to capture/verify the user identity proofs.
3) Introduced a mechanism to store user identity data and activity trace record data on blockchain platforms by using self-sovereign identity proofs.
4) Self-sovereign identity proof-based identity and consent storage address the common issues in cloud-based data storage(e.g lack of data privacy, lack of data immutability, lack of traceability, lack of data provenance [1], [2]).

The rest of the paper is organized as follows. Section 2 discusses the architecture of the Casper platform. Section 3 functionality of Casper platform. Section 4 performance evaluation, Section 5 surveys related work. Section 6 concludes the Casper platform with suggestions for future work.

2. Casper platform architecture

2.1. Overview

Casper is a blockchain and self-sovereign identity based digital identity platform that addresses the issues on centralized identity systems. "Casper" comes with an Android/IOS based mobile identity wallet which is built on top of blockchain using a self-sovereign identity-based approach. Unlike centralized identity systems, the actual identities of the customers/users stored in the customers' mobile application. The proof of these identities stored in the blockchain-based decentralized storage as a self-sovereign identity proof. Casper platforms' self-sovereign identity-based system provides a zero-knowledge proof mechanism to verify the identity information. As a use case of Casper, we are proposing an inter-bank KYC platform for bank customers. However, Casper is application agnostic and well-suited for diverse applications such as health data records, transport/delivery tracking platforms, user authentication/authorization platforms, etc. The Casper platform is built using a layered architecture shown in Figure 1 containing four main layers.

1) Distributed ledger - Where all user cryptographic artefacts for identity (DIDs) and proofs of activity are stored.
2) Smart contract layer - Ledger functions such as identity handling, permission handling, notification functions implemented in the smart contracts layer.
3) Credential layer - Where different entities in the platform(users, admins) create and exchange credentials for verification via credential layer.
4) Peer-To-Peer communication layer - Where peer to peer data exchange between user identity wallets happens within the DID communication layer.

2.2. Distributed ledger

Distributed ledger is the blockchain-based peer to peer storage system used in the Casper platform. The blockchain

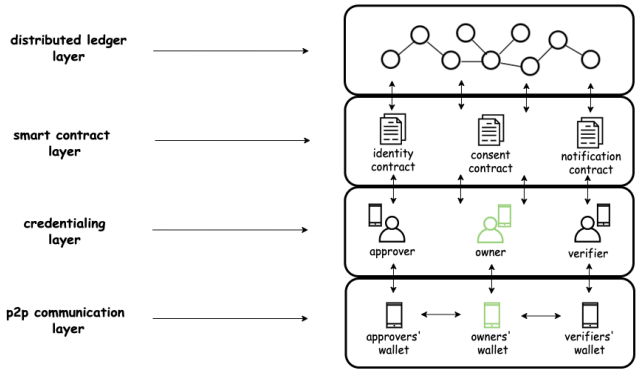


Figure 1: Casper platform layered architecture.

can be deployed among multiple organizations such as government organizations, hospitals, banks, identity authorities etc. Each organization in the network can run its own blockchain node, as shown in Figure 3. It stores all user digital identity proofs (which are identified as DID or decentralized identity proof [3]) and user consents(credential owners give permission for different entities in the platform to access their credentials) on the Casper platform. The user identity proofs and consents stored in one node will be synced with all other nodes by using the underlying blockchain consensus algorithm. The DID proof is generated by the credential owner and stored in the blockchain ledger. Then issuers approve it and update the status of the DID proof. The verifiers use the DID proofs to verify the user identity.

In this paper, Rahasak blockchain [4], [5] is used, which is a highly scalable blockchain targeted for big data as the distributed ledger of the Casper platform. Rahasak comes with functional programming [6] and actor [7], [8] based "Aplos" smart contract platform to facilitate blockchain functions [9], [10]. All blockchain functions of the Casper platform are implemented with Aplos smart contracts.

2.3. Smart Contract Layer

All the ledger functionalities in the Casper platform are implemented with smart contracts. The users in the platform(e.g credential owner, verifier, approver in layer 3) interact with these smart contracts functions. There are four main smart contracts a) identity contract, b) trace contract c) consent contract and d) notification contract. The self-sovereign identity functions are implemented by the identity contract. The credential owners give permission for different entities in the platform to access their credentials. These permission handling functions are implemented with the Consent contract. There are various notification scenarios in Casper, for example when a credential verifier needs to access the credential of a customer, a customer needs to be notified about it. These kinds of notifications are handled with the Notification contract. We have used Rahasak

blockchains Aplos smart contracts to implement the smart contract functions in the Casper.

2.4. Credential layer

There are two main types of users in the Casper platform, credential owners, admins(credential approvers and verifiers). Casper provides a self-sovereign identity based mobile wallet application for each type of user. Credential owners use the "Casper mobile wallet application" and admins use the "Trace mobile wallet application" and "Trace web application". Credential owners register their DID proofs on blockchain and enrol in the Casper platform with the Casper mobile application. Admins(credential approvers/verifiers) approves and verifies the credentials(DID proofs) via Trace application. All credential cryptographic information is stored on the blockchains distributed ledger. When performing DID register and credential verification, credential owners and verifiers interact with the underlying blockchain ledger to put and fetch credentials. The credential exchange process happens in the Credential layer, where credential owners and admins exchange the credentials for verification. It implements all credentialing functions such as credential creation, approval, and verification.

2.5. Peer-To-Peer communication layer

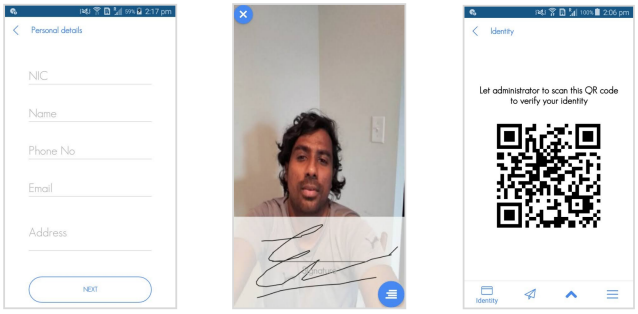
The peer-to-peer communication layer is used to exchange the actual credential information(such as user image, id numbers, etc) between the credential owners and admins(credential approvers and verifiers). Peer to peer data exchange between user identity wallets happens in this layer. When a user's identity needs to be verified/approved, the admin requests proof of identity from the holder, the holder consents and shares data along with cryptographic proof stored on the blockchain. The Casper mobile app fetches the identity information stored in local storage to send to the admins Trace mobile wallet. The admin can do further verification/approvals based on this information.

The peer to peer communications can be implemented with TCP/WebSocket based communication service or firebase [11] push notifications service. In the Casper platform firebase push notification service is used to implement the peer to peer communication between mobile wallets.

3. Casper Platform Functionality

3.1. Identity Registration

As a use case of Casper, we have built an inter-bank KYC(Know Your Customer) application for banking customers. With this application, banks can share customer information with other banks by granting permissions. The customer only needs to register with one bank, then they can access the functions(e.g loan requests, lease requests) with other banks through the Casper platform. Consider a scenario where five banks participate in the Casper platform.



(a) Add personal information (b) Capture photo and signature (c) User identity embed in QR code

Figure 2: Casper mobile wallet application.

The blockchain network deployed in five banks(Bank1, Bank2, Bank3, Bank4, Bank5). The admin officers at each bank have Trace mobile application and Trace web application. Assume User1 who is a customer of Bank1 registered in Casper platform with Casper mobile wallet application. On registration, the user needs to capture his personal information, tax details, occupation details, image and signature via the Casper mobile wallet application as shown in Figure 2. The image and signature can be used as additional proof which administrators can use to approve/verify the user identity. The captured information will be saved in secure storage in a mobile application and the proof of this information will be uploaded to the blockchain as a self-sovereign identity proof(DID proof). The user DID is generated based on the public key of the user. On registering, Casper mobile wallet will generate a public/private key pair for the user. The private key will be saved on the secure Keystore on the mobile application. The DID will be generated with the based58 hash of the public key and users' bank ID. In this scenario, User1 is a customer of Bank1, so the users' bank ID is Bank1. The generated DID format is described in Figure 3. It contains a user's bank and base58 hash of the public key. By using the DID anyone can identify the account holding bank of the user. The user generates the DID proof with the public key, DID and user role. Then the user digitally signs the DID proof with his/her private key and upload it to the blockchain ledger. Figure 3 shows the format of the DID proof on the Casper platform. The users' DID will be embedded in a QR code in the Casper mobile app, which the user can show to admin officers (e.g admin at bank, hospital) for verification. Figure 3 described the registration flow of the Casper.

3.2. Approve Identity

Once registered, a user needs to get approval for his/her identity before using it in the Casper platform. User can go to a branch of the bank with which the user has registered in the Casper platform and approve the identity by using the Casper mobile wallet. In the above scenario User1 is a customer of Bank1(User1 registered in Casper platform with Bank1), so the user can go to any branch of Bank1 and

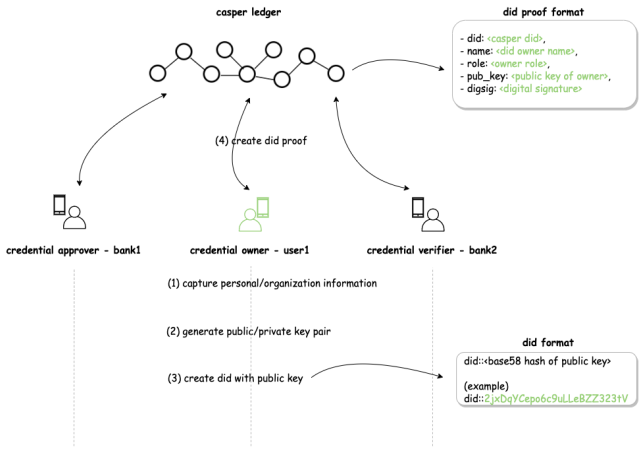
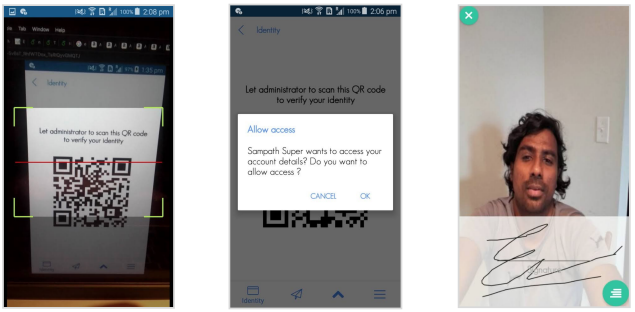


Figure 3: Casper Registration Flow



(a) Scan QR code and fetch identity

(b) Allow admin to access identity

(c) View user image

Figure 4: Trace mobile wallet application access user identity. The user needs to give permission to the admin to access the identity.

approve the identity. When the user visits the bank branch he/she shows the Casper wallet QR code(which embedded the user's DID) along with his/her government identity card, driver's license or passport. Then the admin officer at the bank scans the QR code using the Trace mobile wallet application and fetches the DID proof from the blockchain ledger. In order to approve the identity bank admin requests the user's actual identity information which resides on the user mobile wallet application. Then trace the application requests from the blockchain ledger. In order to access the identity information of the user, the requesting party needs to have consent from the user. When the admin requests the identity information blockchain ledger, it checks whether the admin(in this case Bank1) has the consent from the user to view the identity. If consent does not exist it will generate a notification to the users Casper mobile wallet application to get the Consent, Figure 4. Then the user can approve or reject the request. If the user accepts the request, the consent for Bank1 from User1 will be generated and saved in the blockchain ledger. These consent details will be shown in the users Casper mobile wallet application. At anytime user can revoke the consent via the mobile wallet. This consent gives permissions only for Bank1 to access the users' identity information. If other banks in the platform need to access the identity, the same consent process needs to happen between the bank and the user. Once consent is given, the bank admins' trace wallet directly fetches the user identity information from the users Casper mobile wallet by using the peer-to-peer communication layer. This fetched identity information will be displayed in the Trace mobile wallet application. To approve the identity admin needs to check the fetched identity information against the users' physical identity card. If the data is correct according to the passport/id card, the admin approves the identity of the user. When approving, it digitally signs the identity proof and updates the status of the identity proof to "Approved" in the blockchain. This is the first-time vetting process that needs to be done in order to approve the user identity saved in the blockchain is authentic and verified by a trusted source. Once identity is approved by an authorized administration user can use his/her identity wallet in any other place to prove his/her identity (e.g. in a bank, hospital etc). When approving the identity, it will use the Identity smart contract. The credential approving flow described in Figure 5. The bank admin officer has permission to revoke the approved identities once they got invalid or inactive.

3.3. Share Identity

Assume at some point user goes to Bank2 to apply for a loan. In this scenario, the user can prove his/her identity by using the Casper mobile wallet. The user needs to show his/her identity wallet QR code in order to prove identity at the bank. Then the admin at the bank scans the QR code, fetches the identity proof of the blockchain and verifies the user. Admin can see the user identity is already approved, so the users' identity can be used to apply for the loan in Bank2. In order to apply for the loan, Bank2 needs the users' identity information in their loan system. In this case, the bank admin enters the user's DID number in the Trace web application and requests the identity information from the blockchain ledger. Then ledger checks the Bank2 has the consent from the user to access the identity data. Since no consent has been given to Bank2 yet, it will generate push notification to users Casper mobile wallet about requesting permissions to Bank2. Then the user can approve that request and give permission to Bank2 to access the identity information. Then the bank system automatically fetches the user identity information from the users Casper mobile wallet. This information can be used as the customer data to process the loan approval. Then the user doesn't need to fill any customer data again in the Bank2 for the loan approval. Identity sharing happens in this approach. The identity sharing flow described in Figure 5.

The user identities can be shared with any other organization in the blockchain network. For example, the ledger can be linked with the motor traffic department. Then when the user goes to get his/her driving license, the identity can

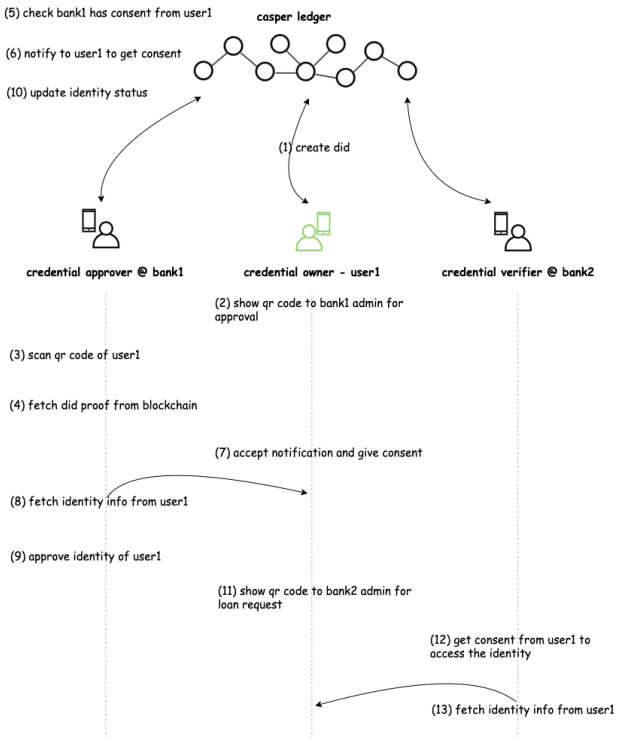


Figure 5: Casper platform functionality.

be proven with the Casper mobile wallet. In this way, the Casper platform provides privacy-preserving global identity for the users which can be shared with any third parties. All the identity information will be stored in the user's physical mobile wallet. When someone needs the identity data, they can get consent from the user can fetch the identities directly from the users Casper mobile wallet.

3.4. Data Privacy and Security

The Casper platform guarantees Privacy, Confidentiality, Integrity, Authentication, Authorization security features. To guarantee privacy, only the users' identity proof will be stored on the blockchain. Actual identity data such as id/passport numbers, image, and signature is stored on user's physical mobile phones. When this information is needed by officials for verification, it can fetch directly via the user's mobile application using push notifications(credential fetching process shown in the Figure 5). By using the SSI based approach, the Casper platform addresses the common issues in centralized cloud-based storage platforms(e.g. lack of data privacy, lack of data immutability, lack of traceability). To guarantee integrity, we have used RSA cryptography-based digital signature mechanism [12]. All data in the Casper platform are digitally signed by a corresponding party. We have used JSON Web Token(JWT) based authentication/authorization services to handle the authentication/authorization of the Casper platform.

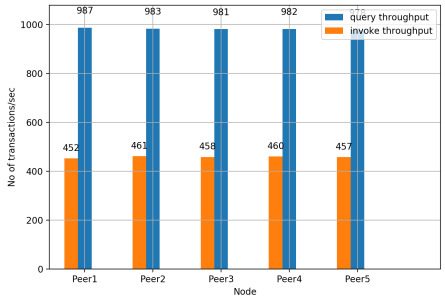


Figure 6: Invoke and Query transaction throughput.

4. Casper Implementation and Performance Evaluation

We have built the production version of the Casper platform using microservices architecture [13] to support high scalability and high transaction load. All the services are dockerized [14] and deployed using Kubernetes [15] container orchestration system. The platform is running as a permissioned blockchain system in a private cloud. For performance evaluation, we deployed the Casper platform with a multi peer Rahasak blockchain cluster(each blockchain node runs on a server with 16GB RAM and 8 CPUs). The evaluation results are obtained with a varying number of blockchain peers (1 to 5 peers) used in different evaluations.

4.1. Transaction throughput

For this evaluation, we recorded the number of DID proof create transactions and DID proof query transactions that can be executed in each peer in the Casper platform. When creating a DID, an invoke transaction will be executed in the underlying blockchain. Invoke transaction creates a record in the ledger and updates the status of the assets in the blockchain. The query searches the status of the underlying blockchain ledger. We flooded concurrent transactions for each peer and recorded the number of completed results. As shown in Figure 6 we have obtained consistent throughput in each peer on the Casper platform. Since queries are not updating the ledger status, it has high throughput(2 times) compared to invoke transactions.

4.2. Transaction execution rate

Next, we evaluate the transaction execution rate in the Casper platform. We tested the number of submitted transactions and executed transactions in different blockchain peers recording the time. Figure 7 shows how transaction execution rate varies when having a different number of blockchain peers in the Casper platform. When the number of peers increases, the rate of executed transactions is increased relatively. Figure 8 shows the number of executed transactions and submitted transactions in a single blockchain peer. There is a back pressure operation [16] between the rates of submitted transactions and executed

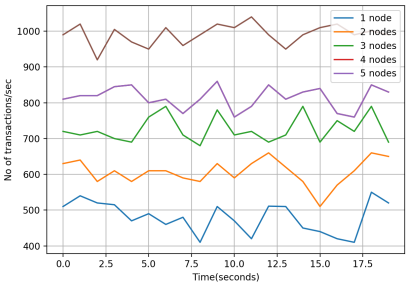


Figure 7: Transaction execution rate with no of blockchain peers in the Casper platform.

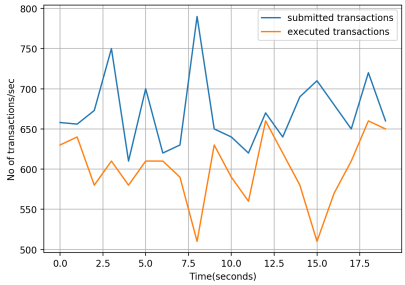


Figure 8: Transaction execution rate and transaction submission rate on one blockchain peer of Casper.

transactions. We have used a reactive streaming-based approach with Apache Kafka to handle these backpressure operations in the Casper platform.

4.3. Search performance

Casper provides the ability to search identity information and activity trace information via underlying Rahasak blockchains' Lucene Index-based search API. For this evaluation, we issued concurrent search queries into Casper and computed the search time. As shown in Figure 9, to search 2 million records, Casper took 4 milliseconds.

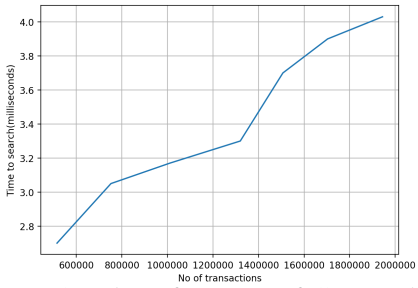


Figure 9: Search performance of Casper platform.

5. Related Work

Much research has been conducted to find new technologies to integrate self-sovereign identity concepts with blockchain technology [17]–[19]. In this section, we outline the main features and architecture of these research projects.

Portable Trust [20] is biometric-based authentication and blockchain storage for self-sovereign identity systems. They developed a biometric-based authentication prototype that is permissionless, autonomous, and open-source. This allows the user to securely store personal information that can only be accessed after successful biometric authentication. It integrates a permissionless blockchain with identity and key attestation to be used in mobile phones. This work, however, is focused on how to implement self-sovereignty but storing secret and biometric material in full user control rather than the generic scenario of ours which is enhancing current biometric systems with auditing capabilities of blockchains.

Horcrux [21] protocol is a method for securing biometric information registration and access. The protocol is generalized for two or more biometric shares that can be stored across mobile devices and personal storage providers with redundancy for availability and safety. The biometric data's owner is able to authorize others to get access to the data without permission from a third party. The owner can assert the identity transaction claim or authorize a verified and trusted third party to do so. The trust is diffused in itself sovereign environment and is not controlled by any single or grouped organizations. Blockchain helps enable this environment by creating multiple department nodes like organizations and governments. As a result, department nodes mutually form distributed consensus and data are recorded in different places and hence, resistant to mistakes

Jolocom [22] is an open-source protocol that is general in nature to facilitate identity records for the person and non-person entities. The protocol is designed to operate on public blockchain infrastructures such as Ethereum. Digital identifier information is stored on the blockchain and all personal information is stored off-chain in control of the user. The protocol currently exists as a working prototype on the Ethereum test network.

SIMS [23] which introduced as Self-Sovereign Identity Management System proposes a blockchain-based privacy-preserving identity management system based on a ZK-SNARK (Zero-Knowledge Succinct Non-interactive ARgument of Knowledge). SIMS can be implemented on Hyperledger, Bitcoin or Ethereum blockchain platforms using Hawk: Zero-Knowledge Proof based Privacy-Preserving Smart Contract platform. Using the proposed SIMS protocol, each user has the self-sovereignty to utilize personal information with preserving privacy. They discussed various applications which can be built on top of SIMS such as minor check, address check, transcript check, and working history proof.

Sora Identity [24] system proposes a mobile app-based identity system that utilizes blockchain technology to create a secure protocol for storing encrypted personal information,

as well as sharing verifiable claims about personal information. In this system hash values of users' personal information encrypted with a cryptographic key(that is owned by the user) and published in the blockchain. The proposed system built on top of Hyperledger Iroha permissioned blockchain. The Sora mobile apps allow the user to generate their cryptographic key, input their data, encrypt it, and publish salted hashes of their data to the blockchain. Users can then share their personal information of their own volition to institutions, such as banks or other organizations.

6. Conclusions and Future Work

With this research, we are proposing blockchain and self-sovereign identity based digital identity (KYC - Know Your Customer) platform "Casper" to address the issues on centralized identity systems. The Casper platform can be adopted in various domains such as healthcare, banking, government organization etc. As a use case, we have discussed building a digital identity wallet for banking customers with the Casper platform.

In the Casper platform, all personal data is stored in the users' physical mobile devices based on SSI architecture. Only identity proofs will be stored in the distributed blockchain storage. With this approach the Casper platform addresses security and privacy issues on cloud centralized storage(e.g lack of data privacy, lack of traceability, centralized control, lack of data provenance etc) providing Data Privacy, Confidentiality, Integrity, Authentication, and Authorization security features.

We have proven the scalability and transaction throughput features of the Casper platform with empirical evaluations. The 1.0 version of the Casper platform as described in this paper is currently running as a prototype.

Acknowledgements

This work is funded by the Department of Energy (DOE) Office of Fossil Energy (Federal Grant #DE-FE0031744).

References

[1] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 767–778, 2016.

[2] X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, and J. Liu, "Towards decentralized accountability and self-sovereignty in healthcare systems," in *International Conference on Information and Communications Security*. Springer, 2017, pp. 387–398.

[3] D. Baars, "Towards self-sovereign identity using blockchain technology," Master's thesis, University of Twente, 2016.

[4] E. Bandara, X. Liang, P. Foytik, S. Shetty, N. Ranasinghe, and K. De Zoysa, "Rahasak-scalable blockchain architecture for enterprise applications," *Journal of Systems Architecture*, p. 102061, 2021.

[5] E. Bandara, W. K. NG, K. DE Zoysa, N. Fernando, S. Tharaka, P. Maurakirinathan, and N. Jayasuriya, "Mystiko—blockchain meets big data," in *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018, pp. 3024–3032.

[6] J. Hughes, "Why functional programming matters," *The computer journal*, vol. 32, no. 2, pp. 98–107, 1989.

[7] C. Hewitt, "Actor model of computation: scalable robust information systems," *arXiv preprint arXiv:1008.1459*, 2010.

[8] Akka, "Akka documentation." [Online]. Available: https://doc.akka.io/docs/akka/2.5/actors.html

[9] E. Bandara, W. K. NG, K. De Zoysa, and N. Ranasinghe, "Aplos: Smart contracts made smart," *BlockSys'2019*, 2019.

[10] E. Bandara, X. Liang, P. Foytik, S. Shetty, N. Ranasinghe, K. De Zoysa, and W. K. Ng, "Saas-microservices-based scalable smart contract architecture."

[11] C. Khawas and P. Shah, "Application of firebase in android app development-a study," *International Journal of Computer Applications*, vol. 179, no. 46, pp. 49–53, 2018.

[12] J. Jonsson and B. Kaliski, "Public-key cryptography standards (pkcs)# 1: Rsa cryptography specifications version 2.1," RFC 3447, February, Tech. Rep., 2003.

[13] J. Thönes, "Microservices," *IEEE software*, vol. 32, no. 1, pp. 116–116, 2015.

[14] "Docker documentation," Aug 2018. [Online]. Available: https://docs.docker.com/

[15] B. Burns, B. Grant, D. Oppenheimer, E. Brewer, and J. Wilkes, "Borg, omega, and kubernetes," *Queue*, vol. 14, no. 1, pp. 70–93, 2016.

[16] A. Destounis, G. S. Paschos, and I. Koutsopoulos, "Streaming big data meets backpressure in distributed network computation," in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 2016, pp. 1–9.

[17] Y. Liu, G. Sun, and S. Schuckers, "Enabling secure and privacy preserving identity management via smart contract," in *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2019, pp. 1–8.

[18] M. Sharma and J. Lim, "A survey of methods guaranteeing user privacy based on blockchain in internet-of-things," in *Proceedings of the 2019 2nd International Conference on Data Science and Information Technology*, 2019, pp. 147–153.

[19] H. Gulati and C.-T. Huang, "Self-sovereign dynamic digital identities based on blockchain technology," in *2019 SoutheastCon*. IEEE, 2019, pp. 1–6.

[20] J. Hammudoglu, J. Sparreboom, J. Rauhamaa, J. Faber, L. Guerchi, I. Samiotis, S. Rao, and J. A. Pouwelse, "Portable trust: biometric-based authentication and blockchain storage for self-sovereign identity systems," *arXiv preprint arXiv:1706.03744*, 2017.

[21] A. Othman and J. Callahan, "The horcrux protocol: a method for decentralized biometric-based self-sovereign identity," in *2018 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2018, pp. 1–7.

[22] Jolocom, "Jolocom, a decentralized, open source solution for digital identity and access management," *white paper, Jolocom*, 2019. [Online]. Available: https://github.com/jolocom/jolocom-lib/wiki/Jolocom-Whitepaper

[23] J. Lee, J. Hwang, J. Choi, H. Oh, and J. Kim, "Sims: Self sovereign identity management system with preserving privacy in blockchain." *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 1241, 2019.

[24] M. Takemiya and B. Vanieiev, "Sora identity: secure, digital identity on the blockchain," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2. IEEE, 2018, pp. 582–587.