POSTER: Towards an Identity Authentication Layer in CBDC Networks using Self-Sovereign Identities

Annonymous Submission

Abstract—**Central Bank Digital Currency (CBDC) is the digital form of a country's fiat currency, based on Decentralized Ledger Technology (DLT). The increasing interest in CBDCs raises the concern of how to verify user's identities for achieving regulatory demands, while maintaining user privacy in the CBDC Network. In this paper we explore Self-Sovereign Identities (SSI) as a way for users to have full control over credentials issued by trusted Financial Institutions in a CBDC Governance Framework. These credentials can then be used to generate privacy-preserving proofs by their holders to authenticate them in different service providers in the CBDC Network.**

Index Terms: **Authentication, Blockchain, CBDC, Self-Sovereign Identity**

I. Introduction

Building on the impact of blockchain technology in the financial sector [1] [2], the concept of CBDCs has emerged as a significant development, bridging traditional banking systems with the innovative potential of digital currencies [3]. CBDCs represent a digital form of a country's fiat currency, issued and regulated by the central bank, utilizing blockchain technology to facilitate secure and efficient transactions through the use of smart contracts [4].

However, CBDCs also raise significant privacy concerns [5]. Unlike decentralized cryptocurrencies such as Bitcoin and Ethereum [6] [7], CBDCs are centrally controlled, which could potentially allow governments to monitor individual financial transactions in real-time [8]. This surveillance capability raises questions about user privacy and the potential for misuse of personal financial data. Moreover, the integration of blockchain technology, while enhancing transaction security, does not inherently guarantee privacy [9]. The design and implementation of CBDCs thus necessitate a careful balance between the benefits of digital currencies and the protection of individual privacy rights.

The SSI framework offer a way to identify users and verify credentials in a decentralized network while preserving user privacy [10]. This approach leverages blockchain technology to create a secure, tamper-proof system where users can control their own identity information. In the SSI paradigm, individuals can prove their identity or certain attributes of their identity (like age or nationality) without revealing any additional personal information [11]. This method ensures that the central bank can fulfill its regulatory and security obligations such as Know Your Customer (KYC) regulations, while maintaining the privacy of individuals [12] defined in directives such as General Data Protection Regulation (GDPR) [13]. The integration of SSI with CBDCs could therefore represent a significant step towards combining the efficiency and innovation of digital currencies with the fundamental need for privacy in CBDC networks [14].

While different approaches to user authentication in blockchain-based systems have been addressed in studies like [15], [16], and [17], the adaptation of these methodologies to CBDC networks remains a novel area of research. This is largely because CBDC development, still in its early stages, is heavily influenced by unique regulatory and governance frameworks [3]. Presently, the primary focus of governments in this domain is on foundational aspects such as system robustness and scalability [18], [19], rather than on the specifics of user authentication.

Therefore, the Research Question (RQ) asked to address this research gap is:

How to provide a privacy-preserving user authentication process compliant with KYC regulations in a CBDC network?

II. Background

The SSI model is based on three pillars, which are necessary to understand the proposed model:

1) **Decentralized Identifiers (DIDs)**: are unique digital identities controlled by the user, created on a decentralized infrastructure, such as blockchain, to ensure security, privacy, and interoperability [20].
2) **Verifiable Credentials**: are the digital proof of various claims, such as qualifications, rights, or identity. What makes them unique is the ability to be digitally verified without the constant need to resort to the issuing authority [21].
3) **Trusted Registry**: Ensures that information and metadata about verifiable credentials and DIDs are stored in a way that they cannot be altered or hacked [10]. Usually is based on a blockchain.

III. Proposed Model

The main objective of this authentication layer is to allow the trusted institutions in the CBDC network to issue verifiable credentials that enable the user to access different financial services and to generate, from these credentials, zero-knowledge proofs (ZKPs) that demonstrate they are qualified to conduct transactions on the network.

Figure 1 illustrates the process of credential issuance in a decentralized identity system involving a user, their user agent (the app in their device, such as a digital wallet, to manage private keys and credentials), a trusted Financial Institution (FI) as the issuer, and a blockchain network.

The proposed model's execution process includes: Issuing and verifying credentials.

A. Issuing Credentials

Initially, the user accesses their user agent to interact with the financial institution. The FI, having registered as an issuer on the blockchain, has published its credential definition and schemas. The user's agent resolves the FI's public DID and requests DID information. In response, the FI provides its public DID document, which contains the FI's service endpoint. Following this, the user creates a pairwise DID and keys, which are used to establish a secure connection to the FI's service endpoint. Once the connection is established, the FI requests identity documents from the user. The FI, after verifying the documents, sends a credential offer to the user. The user confirms the credential offer, and the FI sends the credential to the user's agent. The user then stores these credentials securely in their user agent.

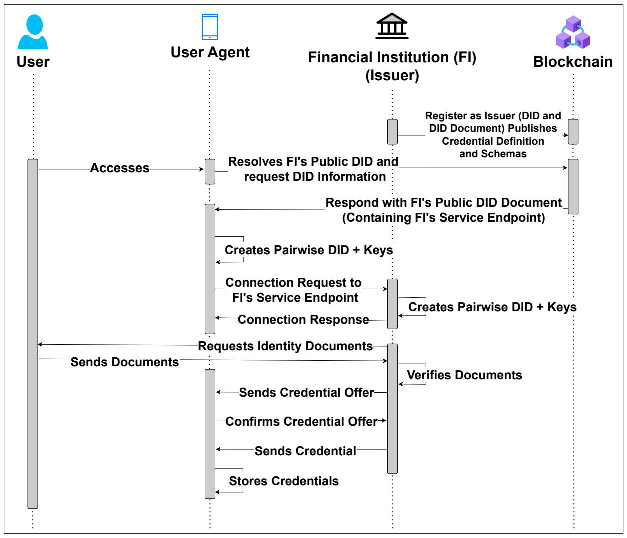
User
User Agent
Financial Institution (FI)
(Issuer)
Blockchain
Register as Issuer (DID and DID Document) Publishes Credential Definition and Schemas
Accesses
Resolves FI's Public DID and request DID Information
Respond with FI's Public DID Document (Containing FI's Service Endpoint)
Creates Pairwise DID + Keys
Connection Request to FI's Service Endpoint
Creates Pairwise DID + Keys
Connection Response
Requests Identity Documents
Sends Documents
Verifies Documents
Sends Credential Offer
Confirms Credential Offer
Sends Credential
Stores Credentials

Fig. 1. Credential Issuance Process: User requests connection with the chosen Institution and receive credential

B. Verifying Credentials

In the credential verification process illustrated in Figure 2, a user again employs their user agent to securely connect with an FI by resolving the FI's public DID and establishing a secure communication channel through a pairwise DID. Upon connection, the FI requests proof of the user's credentials, prompting the user's agent to send a verifiable presentation containing the necessary credentials and cryptographic proofs. The FI then validates these credentials by cross-referencing the signatures and proofs against the blockchain network, ensuring their authenticity and integrity. Upon validating the credentials, the FI can immediatly grant the user the access to financial services in the CBDC network.

This way, the end user is then able to interact with smart contracts in the CBDC network while protecting his privacy in a private blockchain setup environment.

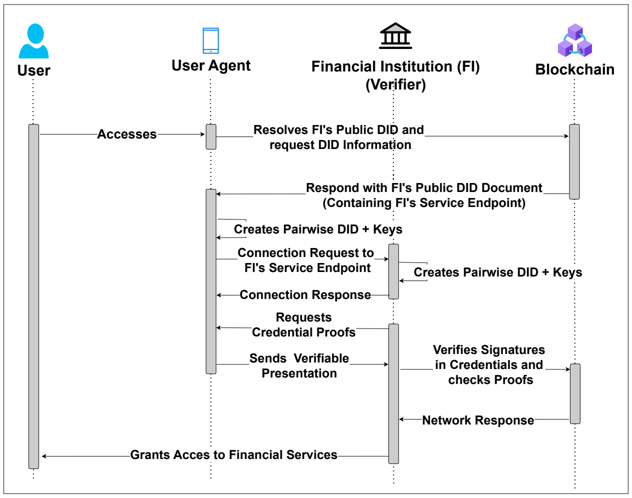
User
User Agent
Financial Institution (FI)
(Verifier)
Blockchain
Accesses
Resolves FI's Public DID and request DID Information
Respond with FI's Public DID Document (Containing FI's Service Endpoint)
Creates Pairwise DID + Keys
Connection Request to FI's Service Endpoint
Creates Pairwise DID + Keys
Connection Response
Requests Credential Proofs
Sends Verifiable Presentation
Verifies Signatures in Credentials and checks Proofs
Network Response
Grants Acces to Financial Services

Fig. 2. Credential Verification Process: Financial Institution Verifies User Credentials and grants access to financial services

IV. Evaluation

The tests were made using Hyperledger Aries Agents [22] communicating to simulate credential issuance and credential verification between an end user and a financial institution in the CBDC Network.

Also, the ledger used to simulate the blockchain environment of the CBDC authentication layer was Hyperledger Indy [23], specifically designed for handling metadata regarding DIDs and credential schemas [20] [21]. We used four Indy nodes to work as validators of a private blockchain network.

V. Conclusion

It is possible to conclude that the use of Self-Sovereign Identities for user authentication in a CBDC network is a good alternative for a more privacy-preserving digital financial system. For future works, we intend to interview specialist from blockchain and financial areas to understand more deeply their views regarding this topic and how this model could be aligned with existing systems.

REFERENCES

[1] R. Patel, M. Migliavacca, and M. E. Oriani, "Blockchain in banking and finance: A bibliometric review," *Research in International Business and Finance*, vol. 62, p. 101718, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0275531922001064

[2] F. A. Sunny, P. Hajek, M. Munk, M. Z. Abedin, M. S. Satu, M. I. A. Efat, and M. J. Islam, "A systematic review of blockchain applications," *IEEE Access*, vol. 10, pp. 59 155–59 177, 2022.

[3] J. Fernández-Villaverde, D. Sanches, L. Schilling, and H. Uhlig, "Central bank digital currency: Central banking for all?" *Review of Economic Dynamics*, vol. 41, pp. 225–242, 2021, special Issue in Memory of Alejandro Justiniano. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1094202520301150

[4] A. Nugroho, S. H. Supangkat, and A. A. Arman, "Central bank digital currency (cbdc) information technology system design : A literature review," in *2023 10th International Conference on ICT for Smart Society (ICISS)*, 2023, pp. 1–6.

[5] A. Jabbar, A. Geebren, Z. Hussain, S. Dani, and S. Ul-Durar, "Investigating individual privacy within cbdc: A privacy calculus perspective," *Research in International Business and Finance*, vol. 64, p. 101826, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0275531922002124

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[7] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," https://ethereum.org/en/whitepaper/, 2013.

[8] R. Bhaskar, A. I. Hunjra, S. Bansal, and D. K. Pandey, "Central bank digital currencies: Agendas for future research," *Research in International Business and Finance*, vol. 62, p. 101737, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0275531922001258

[9] V. Sethaput and S. Innet, "Blockchain application for central bank digital currencies (cbdc)," in *2021 Third International Conference on Blockchain Computing and Applications (BCCA)*, 2021, pp. 3–10.

[10] N. Naik and P. Jenkins, "Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems," in *2020 IEEE International Symposium on Systems Engineering (ISSE)*, 2020, pp. 1–6.

[11] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey," *IEEE Access*, vol. 10, pp. 113 436–113 481, 2022.

[12] E. Bandara, X. Liang, P. Foytik, S. Shetty, and K. D. Zoysa, "A blockchain and self-sovereign identity empowered digital identity platform," in *2021 International Conference on Computer Communications and Networks (ICCCN)*, 2021, pp. 1–7.

[13] GDPR-Info, "General data protection regulation (gdpr)," https://gdpr-info.eu/, 2018.

[14] N. Naik and P. Jenkins, "Your identity is yours: Take back control of your identity using gdpr compatible self-sovereign identity," in *2020 7th International Conference on Behavioural and Social Computing (BESC)*, 2020, pp. 1–6.

[15] L. Zhang, H. Li, L. Sun, Z. Shi, and Y. He, "Poster: Towards fully distributed user authentication with blockchain," in *2017 IEEE Symposium on Privacy-Aware Computing (PAC)*, 2017, pp. 202–203.

[16] Z. Yang, H. Ma, M. Ai, M. Zhan, G. Wu, and Y. Zhang, "A minimal disclosure signature authentication scheme based on consortium blockchain," in *2022 IEEE International Conference on Blockchain (Blockchain)*, 2022, pp. 516–521.

[17] J. Zhu, Y. Wei, and X. Shang, "Decentralized dynamic identity authentication system based on blockchain," in *2021 International Conference on Networking Systems of AI (INSAI)*, 2021, pp. 1–4.

[18] Reserve Bank of Australia, "Central bank digital currency," 2023, accessed: 2023-11-16. [Online]. Available: https://www.rba.gov.au/payments-and-infrastructure/central-bank-digital-currency/

[19] S. V. Kesavaraj, C. Mukund Jakhiya, and C. Nisha Bhandari, "A study on upcoming central bank digital currency: Opportunities, obstacles, and potential fintech solutions using cryptography in the indian scenario," in *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2022, pp. 1–10.

[20] W3C, "Decentralized Identifiers (DIDs) v1.0," https://www.w3.org/TR/did-core/, 2022, Accessed: 23 June 2023.

[21] ——, "Verifiable Credentials Data Model," https://www.w3.org/TR/vc-data-model/, 2022, Accessed: 12 June 2023.

[22] Hyperledger, "Hyperledger aries," https://github.com/hyperledger/aries, 2023, accessed: 2023-12-2.

[23] ——, "Hyperledger indy-node," https://github.com/hyperledger/indy-node, 2023, accessed: 2023-12-2.