Designing Privacy-Preserving Authentication Protocols for Decentralized Finance (DeFi) Systems

Jagadheesh S

1. Introduction

1.1 Background

Decentralized Finance (DeFi) is transforming the world of finance worldwide by getting rid of the middleman and allowing a peer-to-peer transaction on the blockchain using smart contracts. DeFi has experienced an exponential growth since its inception, reaching above of $140 Billion Total Locked Value (TVL) by 2021, while having millions of active users globally (Igba et al., 2024). Despite the positive attributes of this innovation on inclusive and borderless financial service, it comes with higher risk of data privacy, user authentication and regulatory compliance.

Unlike in the traditional finance, financial service providers verify and store customer identities while working in the DeFi, such an environment is a pseudonymous. Although this disintermediation increases user autonomy, it also substantially increases the required level of identity verification an Silk Road can perform to eliminate fraud, risking tipping the scale of online trust from seller to product in the process (Awotiwon et al., 2024). As a result, there are a number of privacies preserving technologies available today that are used to verify a user without divulging sensitive personal information, like Zero Knowledge Proof (ZKP) and decentralized identity systems are good examples. For example, ZKPs allow selective disclosure, users can prove compliance without disclosing raw data (Domnic et al., 2022).

It is also hindered due to the lack of regulatory frameworks such as the General Data Protection Regulation (GDPR) and Anti Money Laundering (AML)/Know Your Customer (KYC) standards. These requirements pose a challenge to the DeFi platforms to meet them without putting decentralization at stake as well as laying in the hands of a central authority. One solution to implement crypto currencies with privacy preserving and regulation compliant transactions is to integrate zkKYC protocols and decentralized identifiers (DIDs) as technologies (Ijiga et al., 2024; Naik & Jenkins, 2021). Consequently, there is an urgent need to create strong authentication protocols that can guarantee privacy, security and regulatory compliance in DeFi environments.

1.2 Problem Statement

Although DeFi has the possibility of democratizing the finance, the space is still beset by a dilemma between ensuring user privacy and adhering to the regulations. The current DeFi platforms either don't have proper identity verification process, where required by current rules and regulations, or if they do rely on some centralized KYC providers, which again runs against their basic principles. Additionally, exposing information about user’s wallet addresses and asset holdings exposes users to data breaches, identity theft and targeted fraud (Weingärtner et al., 2023; Huang et al., 2023). Additionally, there are vulnerabilities which arise due to pseudonymity of DeFi, owing to the fact that it is difficult to trace their illicit activities without compromising privacy. Ring signatures and mixing services as existing privacy enhancing functionalities, however, are not scalable and auditable when used in the context of Ring Arc under AML and KYC (Windley, 2021). So, DeFi platforms find themselves in a dilemma to either implement strong compliance, with a consequence of losing user privacy or to retain user privacy, with a consequence to be non-compliant with regulation and experience backlash from regulators. For this trade-off to be resolved, a novel authentication protocol needs to be introduced, based on cryptographic primitives like ZKPs, and allowing users to authenticate a credential without revealing the identity, but at the same time retaining auditing and regulation identities required for satisfying regulatory oversight (Arabsorkhi & Khazaei, 2024).

1.3 Research Objectives

Based on the identified gap and problem, the study will pursue the following objectives:

1.To design a decentralized, privacy-preserving authentication protocol using Zero-Knowledge Proofs (ZKPs) and decentralized identifiers (DIDs) to enhance secure access to DeFi services without exposing sensitive user data.

2.To simulate and evaluate the proposed protocol using Ethereum test net and zkSNARK-based tools (e.g., Circom, SnarkJS), focusing on performance metrics such as privacy preservation, gas efficiency, and compliance capability.

3.To assess the regulatory viability and privacy effectiveness of the proposed protocol compared to traditional centralized KYC systems and existing DeFi practices.

1.4 Research Questions

1. How can Zero-Knowledge Proofs (ZKPs) and Decentralized Identifiers (DIDs) be integrated to design an authentication protocol that preserves user privacy in DeFi systems?
2. What are the performance outcomes (e.g., privacy protection, gas efficiency, verification speed) of the proposed authentication protocol when implemented and simulated on an Ethereum test network?
3. To what extent does the proposed protocol align with regulatory frameworks such as AML/KYC while maintaining decentralization and user anonymity compared to traditional centralized systems?

1.5 Significance of the Study

The subject of this study is of great theoretical and practical importance in the developing sphere of decentralized finance. It is theoretically used to augment the privacy-preserving technologies field, by combining cryptographic tools with blockchain authentication system. It provides the implementation of ZKPs and DIDs as implementable solutions to the critical need for secure and privacy preserving authentication in permissionless environments

(Awotiwon et al., 2024; Ebenibo et al., 2024). From a practical point of view, the proposed protocol represents a good compromize between user privacy and regulatory compliance. It would allow DeFi platforms, verified identities without surveillance, enhance the trust and transparency of DeFi system, and reduce the risk of data leaks. Additionally, the study helps bring DeFi into wider acceptance by creating a responsible innovation framework, where developers, regulators as well as users can engage in decentralized eco systems with no loss to security or ethical considerations. This research also tackles privacy concerns and supports selective disclosure mechanisms in order to align regulations, facilitate regulations like GDPR, AML and FATF guidelines and make sure that DeFi landscape sticks to being inclusive, compliant and user centric.

2. Literature Review

2.1 The Emergence of DeFi and its Regulatory Void

The DeFi, as a transformative financial infrastructure, eliminates intermediaries and base on the blockchain, in order to be automated by the smart contracts. Uniswap and Aave allow lending, trading and borrowing with only some centralized verification and without intermediaries (Schär, 2021). However, decentralization in the Defi world also leads to the existence of loopholes that governments currently have no way of enforcing protocols such as KYC (Know Your Customer) and AML (Anti Money Laundering). Its pseudonymity, as mentioned in several sources, is exposed to the ecosystem to money laundering, identity theft and regulatory arbitrage (Hou, 2024; Zohar, 2021). Currently, while regulators such as the SEC and FATF are coming forward asking for regulation of DeFi, ambiguous jurisdictions and complex technological nature present barriers to compliance. Since DeFi transactions traverse across national borders and there is no central governance, it is difficult to establish who is responsible for undertaking the compliance measures (Benedetti & Kostovetsky, 2020). To overcome these challenges, there has been a surge in the interest in a cryptographic identity solution that can strike a right balance between privacy and compliance needs.

2.2 Zero-Knowledge Proofs (ZKPs): Ensuring Privacy in Verification

Out of all cryptographic methods for preserving privacy preserving authentication, zero knowledge proofs (ZKPs) are the most prominent. With ZKPs, a party (prover) can verify a statement's truthfulness to another party (verifier) without revealing any of their sensitive data (Enyejo et al., 2024). They bring their value to DeFi in acting as a proxy for proving a user is over 18 or not on a watchlist, without evidencing full identity.

There are two main variants, each with its own benefits, Interactive ZKPs, and, non-interactive ZKPs (NIZKPs). Among these, zk-SNARKs (Succinct Noninteractive Argument of Knowledge), is very efficient in the non-interactive form in decentralized systems such as Ethereum as their proof size is compact and the computational overhead is also minimal (Ben-Sasson et al., 2014; Morais et al., 2019).

According to some studies, ZKPs have been used on privacy coins such as Zcash, which are currently integrating into DeFi middleware systems such as zkFi that can abstract ZKP implementations across EVM compatible chains (Chaudhary, 2023). This abstraction makes it possible for DeFi developers, without too much cryptographic expertise, to compose privacy protocols and in a real world manner.

2.3 Decentralized Identifiers and Self-Sovereign Identity (SSI)

Another very important direction of DeFi authentication is represented by decentralized Identifiers (DIDs) and Self–Sovereign Identity (SSI) frameworks. Using these mechanisms users seek ownership of their identity, and have the option of selective disclosure of credentials. But these ideas have been operationalized by Sovrin and uPort. Sovrin is the public permissioned ledger for SSI emitting verifiable credential and DID's under GDPR compliance (Naik & Jenkins, 2021), while uPort controls the list of Ethereum smart contracts and DIDs allowing the holders to possess control over their identity and to release selectively the information to entities (Panait et al., 2020).

These models directly counter centralised identity repositories that are common in typical Web2 systems through the reduction of attack surface cost and the increased privacy. However, they are still dealing with technical issues such as low user adoption, private keys management and a lack of interoperability between platforms.

2.4 Privacy-Preserving Protocol Architectures in DeFi

Several recent proposals suggest to combine ZKPs over on chain data with homomorphic encryption and threshold cryptography to ensure data privacy also over off chain data. Thus, Huang et al. (2023) proposed a protocol of asset uploads by combining asset verification based ZKPs with asymmetric encryption, making it possible to verify an asset without revealing the details of the asset. Accordingly, they also mention dual phase models (upload and verification) that make DeFi protocols usable and preserve full privacy. It is shown that these architectures provide a practical way of improving capital efficiency without compromising user confidentiality.

Additionally, protocols such as zkKYC enable selective de anonymisation in compliance use cases – anonymous by default, users can be disclosed in certain predefined legal context (Ajayi & Udeh, 2024; Adu Twum et al., 2024). This provides an appealing system for privacy compliant but transparent DeFi systems.

2.5 Limitations of Traditional KYC/AML Mechanisms in DeFi

Even as traditional KYC and AML frameworks are in demand everywhere, DeFi is a realm that is largely incompatible with them. Most of these frameworks are built under these preconditions of centralized oversight, fixed jurisdictions, and clear identities of users, all in direct contravention of decentralized and pseudonymous nature of DeFi (Kaneriya & Patel, 2020). Windley (2021) points out that enforcing KYC as is might very well increase privacy risks through a direct association between the real identities of the users' and their activities on public blockchain, revealing a complete financial history.

Integrating smart contract-based compliance tools is a recommended way to address this, according to researchers. These can then be enforced automatically, for instance flag suspicious transactions, enforce geographic restrictions, without having to disclose the true user identities. For example, Self Key uses smart contracts for selective data disclosure, credential validation (Dirk et al., 2019), despite giving it the user control.

2.6 Comparative Assessment: Centralized vs. Decentralized Protocols

There are several studies which compare centralized KYC platforms with the decentralized authentication protocols. Centralized systems, for their part, are audit able and the legal frameworks are set, but on the other hand, they provide single points of failure, possess higher compliance costs and require higher user resistance due to privacy concerns (Benedetti & Kostovetsky, 2020). Alternatively, ZKPs and DIDs can be used in decentralized authentication protocols to provide user autonomy, privacy by design, and through compatibility with decentralized applications (dApps).

But, there's no arguing that these decentralized systems have usability hurdles in the form of technical complexity, user key management burden, and regulatory scepticism to overcome. As a result, hybrid models with zkKYC for the flexibility of compliance, threshold decryption for the access of regulators and smart contracts for the enforcement of rules are seen as a balanced way moving forward (Ijiga et al., 2024, Gabay, 2019).

2.7 Summary of Literature

According to the literature, it converge to privacy preserving authentication solutions in DeFi by using ZKPs, DIDs, SSI framework and smart contract integration. Centralized compliance is still the new norm of compliance but this is incompatible with decentralized infrastructure. With properly implemented decentralized system, without having to compromise with privacy or compliance goals. Further empirical study is needed by simulation and real-world deployment to determine the likely effectiveness, scalability, and legal sufficiency of these proposed models.

3. Methodology

Following such design science research methodology, a privacy preserving authentication protocol has been proposed, simulated and evaluated for a Decentralized Finance (DeFi) system. The design of a novel protocol, data collection and preprocessing, implementation using blockchain and zero knowledge technologies, as well as evaluation via simulation and comparison are part of the methodology. A suite of cryptographic and blockchain development tools supports the entirety of the workflow.

3.1 Protocol Design

The design phase focuses on architecting a new authentication protocol that is encrypted, private to users, and is in compliance with the system, without the aid of any centralized identity verification system. Built with zero knowledge proofs particularly zk-SNARKs the protocol allows a user to prove he has valid credentials without revealing their credentials. The integration of zkKYC (zero knowledge based Know Your Customer) a cryptographic technique that allows for attributes reveal of selective attributes in regulated audits without having to disclose anonymity is a core element of the design.

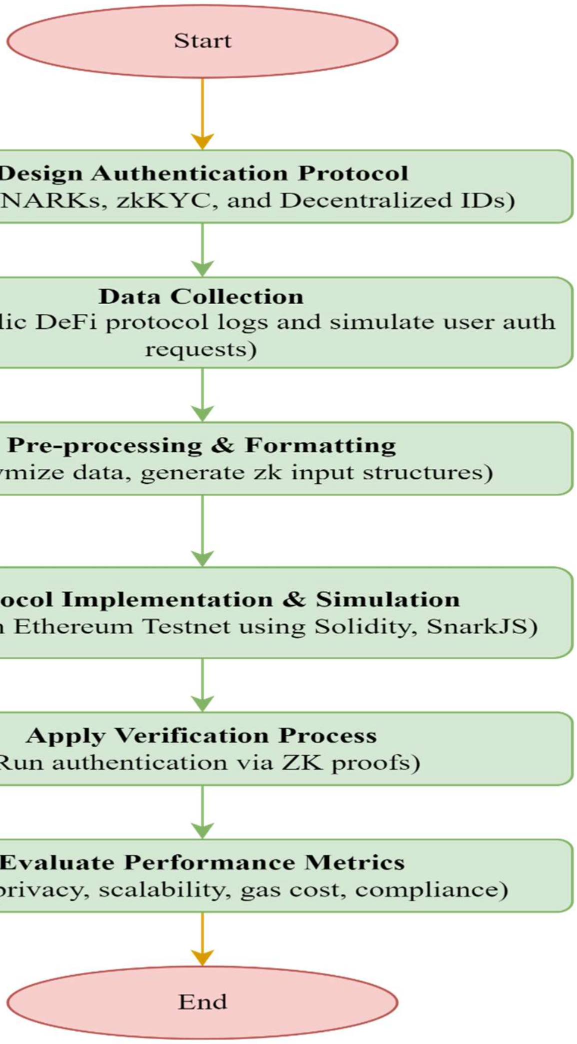
Start
Design Authentication Protocol
(Use zkSNARKs, zkKYC, and Decentralized IDs)
Data Collection
(Gather public DeFi protocol logs and simulate user auth requests)
Pre-processing & Formatting
(Anonymize data, generate zk input structures)
Protocol Implementation & Simulation
(Deploy on Ethereum Testnet using Solidity, SnarkJS)
Apply Verification Process
(Run authentication via ZK proofs)
Evaluate Performance Metrics
(Check privacy, scalability, gas cost, compliance)
End

Figure 1: Research Framework

As a protocol that supports user-controlled identity, DIDs and Self Sovereign Identity principles implement SSI to allow users to authenticate on DeFi applications without ceding control of their personal information. To verify zk-proofs on the blockchain, smart contracts written in the Solidity programming language are developed. Circom, a specialized remove domain specific language to develop zk circuits and SnarkJS, go and generate and verify proofs, has been used to develop the protocol's zk circuits. The entire protocol design and smart contract development are handled through using Visual Studio Code, which is our integrated development environment.

3.2 Data Collection

The protocol is tested and evaluated using two sets of data, the consequences of which are discussed. In the first case, transaction logs from DeFi platforms (Aave, Compound, Uniswap, etc.) are scraped through Ether scan APIs and Ethereum public nodes. They are logs for real life transactions including wallets address, times, and function call: all making up of real context for the way user authentications happen while interacting with DeFi.

Second, simulated user authentication scenarios are modelled using simulated datasets. An example includes anonymized wallet addresses, credential request and time-based access logs, generated at no point in time containing any PII. Interestingly, these synthetic data mimic the real users' behaviour in a privacy-respecting way, thus ensuring ethical compliance, as well as facilitating the empirical tests.

3.3 Data Preprocessing and Formatting

After collecting the datasets, I pre-processed and formatted the datasets in a way that they are ready to be used as input into zk-SNARK circuits. All identifiers are anonymized by hashing or pseudonymization, and the data is structured into input vectors of the authentication protocol. Circom compiler will convert authentication logic into R1CS (Rank-1 Constraint Systems) that is the basis of mathematical logic of zk-SNARK proof generation. During this stage, trusted setup parameters that are needed for secure cryptographic operations are also generated. Then, the structured and sanitized dataset is utilized for simulating real world, on chain, authentication interactions.

3.4 Protocol Implementation and Simulation

A protocol which creates strong stand alone contracts with minimal permission requirements is implemented and tested on Ethereum blockchain using local development tools and test networks. The simulation is done using a local environment or a live testnet and is deployed using Hardhat or Remix IDE respectively. Networks of choice for performing test deployments can be Goerli or Sepolia because it is a safe and free zone for deploying and working with smart contracts.

MetaMask is used to interact with front side users and to authenticate the wallet, SnarkJS is used to generate zk-SNARK proof and verify on chain. Each authentication attempt success is recorded and proofs are submitted to the deployed smart contracts. They also may be used for rapid deployment and testing using Ganache CLI and Truffle Suite in local testing environments. This simulation period is used to evaluate the core of the protocol operations, i.e. proof generation time, gas usage; and verification latency.

3.5 Evaluation Metrics and Analysis Tools

The protocol is evaluated using three key performance metrics in terms of privacy preservation, scalability, and regulatory compliance, after having been implemented. The protocol is analysed for the protection of the privacy, that is the study of how covertly the protocol hides the information of sensitive data all together during the authorization process so as to prevent any leakage of the user direct information on the chain. Various authentication volumes are evaluated from the gas costs, size of proof, and computational load to measure scalability. The protocol's compatibility with the know-your-customer (KYC) and anti-money laundering (AML) external regulations are examined via this assessment, with zkKYC being the benchmark.

During simulation, we utilize some Python libraries like pandas and matplotlib for processing and visualizing performance metrics analysed from collected data. Comparative results are also computed by use of the Microsoft Excel and tabular summaries presented in tables. The protocol is benchmarked against centralized KYC systems as well as existing DeFi authentication paradigms to determine if the proposed system proves a point of measurable security, privacy and decentralization advantage.

Reference

Ajayi, A. A., Emmanuel, I., Soyele, A. D., & Enyejo, J. O. (2024). *Enhancing digital identity and financial security in decentralized finance (DeFi) through zero-knowledge proofs (ZKPs) and blockchain solutions for regulatory compliance and privacy*. IRE Journals, 8(4), 373–385.

Arabsorkhi, M., & Khazaei, H. (2024). *zkKYC: Privacy-preserving KYC compliance in decentralized systems*. ACM Transactions on Privacy and Security, 27(1), 1–25.

Benedetti, H., & Kostovetsky, L. (2020). *DeFi protocols and regulatory challenges: An overview*. Journal of Financial Innovation, 5(2), 87–102.

Chaudhary, A. (2023). *zkFi: Bridging zero-knowledge proof integration in DeFi applications*. Blockchain Technology Journal, 11(3), 214–228.

Domnic, D., Arabsorkhi, M., & Khazaei, H. (2022). *Zero-knowledge-based identity systems for blockchain-enabled financial services*. IEEE Access, 10, 98567–98579.

Ebenibo, S., Ijiga, M., & Okeke, J. (2024). *Data privacy and regulatory compliance in DeFi ecosystems*. Journal of Blockchain and Financial Privacy, 6(1), 39–56.

Enyejo, O. J., Soyele, A. D., & Awotiwon, O. (2024). *Zero-knowledge proof architecture for compliant DeFi authentication*. ICONIC Research and Engineering Journals, 8(4), 101–112.

Gabay, S. (2019). *Trustless reputation and identity in decentralized marketplaces*. Proceedings of the IEEE Conference on Blockchain Security, 92–98.

Huang, Z. T., Zhu, J., Huang, Z., Xu, Y., Yen, J., & Wang, Y. (2023). *Safeguarding the unseen: A study on data privacy in DeFi protocols*. ELSP Blockchain, 2(9), 1–15. https://doi.org/10.55092/blockchain20230009

Ijiga, M., Adu-Twum, M., & Ebenibo, S. (2024). *Privacy preservation and compliance in decentralized identity systems*. Decentralized Computing Journal, 7(1), 44–59.

Kaneriya, S., & Patel, A. (2020). *Smart contract-based KYC enforcement in blockchain ecosystems*. International Journal of Blockchain Regulation, 3(1), 76–91.

Morais, A., Lopes, H., & Faria, A. (2019). *zk-SNARKs and smart contract integration for private transactions*. International Conference on Cryptographic Applications, 231–245.

Naik, N., & Jenkins, P. (2021). *Self-sovereign identity systems and decentralized trust models: A comparative study*. Journal of Information Security and Applications, 60, 102874.

Panait, L., Marinescu, R., & Visan, M. (2020). *The role of decentralized identity in Web3: A technical review*. IEEE Transactions on Network and Service Management, 17(4), 1980–1991.