HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

GRADUATION THESIS

A social login solution for Web3 using Shamir's secret sharing and verified DKG

NGUYEN TUAN MINH

minh.nt184294@sis.hust.edu.vn

Major: ICT Global

Specialization: Information Technology

Supervisor: Ph.D Dao Thanh Chung ________________

Signature

Department: Computer Engineering

School: Information and Communications Technology

HANOI, 06/2022

Requirements for the thesis

Student information
Student name: Nguyen Tuan Minh
Tel: 0915871399 Email: minh.nt184294@sis.hust.edu.vn
Class: ICT02.K63 Program: Global ICT

This thesis is performed at: 21st floor, Charmvit Tower

Goal of the thesis
This thesis focus on addressing the challlenges associated with decentralized identity and authentication in blockchain applications, providing developers with a convenient and standardized way to implement secure and user-friendly authentication mechanism.

Main tasks
In this thesis, I will disscuss blockchain, smart contracts, and social login for Web3 Application. Next, I will describe in detail the architecture and design of the Social login system using Shamir's secret sharing and verified DKG. Lastly, i will conduct some experiments to evaluate and querying the efficacy of the solution.

Declaration of student
Nguyen Tuan Minh - hereby attests that the work and presentation in this thesis were carried out by myself under the direction of Ph.D Thanh-Chung Dao. All results presented in this thesis are authentic and have not been plagiarized. All references in this thesis, including images, tables, figures, and quotations, are cited in the bibliography in a plain and comprehensive manner. I will assume full responsibility for any copy that violates school regulations, even if it is only one.

Advisor's confirmation of the completion and defense permission

Hanoi, Ngày 6 tháng 7 năm 2023
Advisor's signature

Dr.Thanh-Chung Dao

ACKNOWLEDGMENTS

I would like to express my profound appreciation to my family, friends and significant other for their unwavering support and patince throughout the process of writing my thesis. Their love, encouragement, and confidence in my abilities have been an inexhaustible source of fortitude and inspiration for me.

Thank you for always being there for me, providing me with a nurturing enviroment, and teaching me the importance of perserverance and diligence. Your unconditional affection and encouragement have inspried me to pursue my academic objectives.

Thank you for solid friendship and for being an unending source of motivation. During the difficult times of thesis writing, your presence, laughter, and words of encouragement have brought me pleasure and helped me maintain a healthy work-life balance.

Lastly, i would like to express my sincerest gratitude to my supervisor, Dr. Dao Thanh Chung. Your direction, expertise and commitment have been indispensable to my research and academic development. Your guidance has not only increased my expertise in the field, but has also inspired me to achieve new heights of intellectual inquiry. Even when the research appeared daunting, your perseverance, encouragement, and unwavering faith in my ability propelled me forward. I am extremely appreciative of the opportunities you have afforded me and the invalueable lessons I have gained under your direction. Thank you for being an outstanding mentor and for your unwavering support throughout the process of writing my thesis.

ABSTRACT

The blockchain has emerged as a revolutionary technology with the potential to transform numerous industries by providing a decentralized and transparent platform for recording transactions and data securely. The administration of identities and authentication remains a significant challenge within the blockchain ecosystem, despite its many benefits. In order to resolve this issue, it is necessary to create software that bridges the gap between conventional web authentication methods and blockchain-based systems. This bridge software would facilitate a more user-friendly and accessible blockchain ecosystem, ensuring that users can access blockchain-based services and applications with seamless identity verification. Blockchain is renowned for its rigorous security features, and any software implementation must maintain this level of security while integrating with standard web authentication protocols. A failure to adequately resolve security concerns could undermine the trustworthiness of blockchain technology. Innovative approaches, such as Shamir's Secret Sharing[1] (SSS) and Distributed Key Generation[2] (DKG), have considerable potential for addressing these issues. SSS is a cryptographic technique that divides a secret into multiple portions before distributing them to participants. This strategy ensures that no single entity has complete access to the secret, thereby enhancing security and reducing the likelihood of unauthorized access. DKG enables the collaborative generation of cryptographic keys without requiring a singular trusted party. This distributed method adds another layer of security and decentralization to the authentication procedure. I intend to develop a social authentication solution for decentralized applications (DApps) using SSS and DKG techniques. This solution would allow users to authenticate using their social network accounts while assuring their privacy and security through the use of secure and distributed authentication protocols. I will design the system architecture, implement the required software components, and assess the solution's performance and efficacy.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

BIP	Bitcoin Improvement Proposal
Dapp	Decentralize application
DeFi	Decentralize finance
DKG	Distributed Key Generation
HTTP	Hyper Text Transfer Protocol
IaaS	Infrastructure as a Service
OAuth	Open Authenticate 2.0
PoS	Proof of Stake
PoW	Proof of Work
SSS	Shamir’s secret sharing

CHAPTER 1. INTRODUCTION

1.1 Motivation

Blockchain technology, as exemplified by Bitcoin [3] and Ethereum [4] networks, has experienced significant growth and garnered widespread attention due to its unique characteristics and prospective benefits. Blockchain has revolutionized many industries, including finance, supply chain, healthcare, and more, by providing a decentralized, transparent, and immutable platform for record-keeping and value transmission. However, conventional web technologies and systems offer their own set of benefits and advantages. Bridging the gap between blockchain and conventional web technologies can unleash a wealth of opportunities and synergies, resulting in a more robust and adaptable digital ecosystem.

One of the key benefits of blockchain technology lies in its ability to provide trust and transparency. The Bitcoin network, for instance, enables peer-to-peer transactions without the need for intermediaries, fostering trust among participants and reducing transaction costs. Ethereum, on the other hand, extends blockchain capabilities by supporting programmable smart contracts, enabling decentralized applications (DApps) with a wide range of use cases. Meanwhile, traditional web technologies offer a well-established infrastructure, user-friendly interfaces, and extensive compatibility with existing systems. By combining the benefits of both blockchain networks like Bitcoin and Ethereum and traditional web technologies, we can create a powerful hybrid solution that leverages the transparency of blockchain while maintaining the usability and familiarity of the traditional web. By facilitating self-sovereign identities and data control, blockchain technology promotes decentralization and empowers individuals. Users can have ownership and control over their digital assets and personal data, decreasing their dependence on centralized entities. This paradigm shift is facilitated by Bitcoin's decentralized network architecture and Ethereum's decentralized application platform. Traditional web technologies, on the other hand, provide users with convenience and familiarity via centralized authentication systems, social logins, and widespread standards. As demonstrated by Bitcoin and Ethereum, integrating these features into the blockchain ecosystem can improve user experience, encourage adoption, and bridge the gap between conventional web users and blockchain applications.

The growth and benefits of blockchain technology, exemplified by networks like Bitcoin and Ethereum, combined with the advantages of traditional web technologies, highlight the importance of bridging the gap between the two. By leveraging the strengths of both systems, we can create a hybrid solution that harnesses the transparency, security, and decentralization of blockchain while maintaining the usability, compatibility, and familiarity of the traditional web. This convergence unlocks new possibilities, expands the reach of blockchain applications, and paves the way for a more interconnected and inclusive digital future. Consequently, the objective of this thesis, a social login solution for Dapps using SSS and verified by DKG, is to combine the advantages of blockchain technology and conventional web authentication.

1.2 Contributions

Due to the fact that this solution is a large undertaking involving the implementation of numerous modules by numerous individuals, it is evident that I did not design and construct the system alone and that other developers participated in its creation. In addition, I was responsible for devising and implementing the mechanisms for the executors to share secrets and generate private keys for end users. I implement the majority of the project's features, with the exception of Shamir's algorithm for sharing secrets and the Distributed Key Generation protocol. In addition, I designed and implemented the majority of the data structures contained in smart contracts and the decentralized storage called Eueno. In addition, this system has a unique architecture for securing and enriching the user experience, as well as enabling developers to integrate existing Dapps seamlessly.

1.3 Thesis structure

The present thesis is organized into six distinct chapters, each of which fulfills a specific objective in the comprehensive investigation of the research subject matter. Chapter 1 serves as the introductory section of this thesis, wherein the underlying motivation driving the study is established. Furthermore, this chapter highlights the significant contributions made by the research and provides a comprehensive outline of the overall structure of the thesis. Chapter 2 of this thesis aims to establish a comprehensive understanding of fundamental concepts that are crucial to the subject matter. These concepts include blockchain, transactions, blocks, wallets, Shamir's secret sharing, distributed key generation, smart contracts, executor for decentralized applications (DApps), and social login for Web3. By delving into these concepts, this chapter lays the groundwork for the subsequent analysis and exploration of the topic at hand. Chapter 3 of this study presents the proposed solution, which outlines an innovative approach that has been adopted to effectively tackle the challenges that have been identified. Chapter 4 delves into an in-depth analysis of the technical issues and design considerations encountered throughout the implementation process. This chapter aims to address and shed light on the various challenges that were confronted during the execution of the project. Chapter 5 of this study presents a comprehensive evaluation of the proposed solution, offering valuable insights into its performance and usability. In conclusion, Chapter 6 serves as the final segment of this thesis, wherein the findings are succinctly summarized and potential avenues for future research are deliberated upon. The inclusion of a reference section within a thesis serves the purpose of meticulously documenting all the sources that have been cited throughout the research, thereby upholding the academic integrity of the study.

CHAPTER 2. BACKGROUND

The background section of this thesis provides a comprehensive overview of the key concepts and technologies that serve as the foundation for our proposed solution. This chapter examines the fundamental characteristics of blockchain technology, what social login for Web3 is, what a smart contract is, and the fundamental comprehension and utilization scenarios of Shamir's secret sharing and distributed key generation. Understanding these concepts is crucial for appreciating our solution's motivations and its potential impact on the decentralized digital landscape.

2.1 Blockchain

Blockchain technology has emerged as a revolutionary innovation with the potential to transform industries and revolutionize how digital transactions are conducted. It provides a decentralized and transparent platform for secure and unchangeable record-keeping, eliminating the need for intermediaries and facilitating peer-to-peer interactions. This chapter provides a concise introduction to blockchain technology, highlighting its historical context, the problem it seeks to solve, and the primary contributions of its first author. In 2008, an anonymous person or group of people using the alias Satoshi Nakamoto [3] introduced the concept of blockchain for the first time. The seminal whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto outlined the fundamental principles and architecture of blockchain technology as a solution to the issues of trust and decentralized digital currency. Bitcoin's introduction of blockchain represented a significant milestone in the evolution of cryptocurrencies and decentralized systems. Traditional centralized systems' lack of trust and security is the issue blockchain seeks to address. The reliance of centralized systems on a single trusted authority to validate and authenticate transactions leaves room for manipulation, deception, and censorship. Blockchain technology addresses these issues by establishing a decentralized network of nodes where consensus mechanisms guarantee the validity and integrity of transactions without requiring a central authority. The first author, Satoshi Nakamoto, introduced a secure and decentralized framework for digital currency transactions, laying the groundwork for blockchain technology. Combining existing cryptographic techniques, such as hash functions and digital signatures, with a distributed ledger system was Nakamoto's most significant innovation. This innovation facilitated the creation of a transparent and tamper-resistant ledger of transactions, ensuring the integrity and immutability of blockchain data. Since Nakamoto's original work, blockchain technology has expanded beyond cryptocurrencies such as Bitcoin. It has implications in numerous industries, including finance, supply chain management, and healthcare, among others. The blockchain's decentralized nature provides opportunities for greater transparency, efficiency, and trust in these industries, paving the way for innovative solutions and new business models.

2.1.1 Transactions

"Transactions are the most important part of the Bitcoin system. Everything else in bitcoin is designed to ensure that transactions can be created, propagated on the network, validated, and finally added to the global ledger of transactions (the blockchain). Transactions are data structures that encode the transfer of value between participants in the Bitcoin system. Each transaction is a public entry in bitcoin's blockchain, the global double-entry bookkeeping ledger" according to "Mastering Bitcoin: Unlocking Digital Cryptocurrencies" by Andreas M. Antonopoulos [5], which implies that transactions are fundamental components of blockchain technology, serving as the building blocks for the transfer and exchange of digital assets. Blockchain networks' security and trustworthiness rely heavily on transactions. They are intended to be verifiable and immutable, providing a transparent and auditable log of all blockchain activities. By recording each transaction on the distributed ledger, participants are able to trace the history and origin of digital assets, fostering accountability and preventing double spending. Multiple stages are involved in the creation of a transaction. The sender initiates the transaction by specifying the recipient's address and the desired transfer amount. The originator then signs the transaction with their private key, ensuring the transaction's authenticity and integrity. Once the transaction has been digitally signed, it is disseminated to the network for validation and inclusion in a block. The validation procedure involves verifying the digital signature of the transaction using the sender's public key, thereby ensuring that the transaction has not been tampered with and that the originator has sufficient funds to complete the transfer. The transaction is submitted to a pool of pending transactions awaiting confirmation after validation. Miners, who are tasked with safeguarding the blockchain, select transactions from the pool and incorporate them into a new block. A consensus mechanism, such as proof-of-work or proof-of-stake, is then used to add the transaction to the blockchain.The creation of transactions on the blockchain enables participants to transmit digital assets without the need for intermediaries in a transparent and secure manner. It assures the system's integrity by employing cryptographic techniques to authenticate and authorize transactions, thereby rendering the process tamper-proof and fraud-resistant.

2.1.2 Blocks

A block in a blockchain is a fundamental element that is crucial to the network's structure and functionality. It functions as a repository for a collection of transactions and other pertinent data. Each block is comprised of a block preamble, which includes metadata such as the block's unique identifier, timestamp, and a reference to the previous block, establishing a chronological order. The block contains transactions, which represent numerous actions within the blockchain network. These transactions include sender and recipient addresses, digital signatures for authentication, and additional pertinent information. The block also contains a Merkle tree root [6], which provides an efficient method for verifying the validity of transactions contained within the block. In addition, each block is allocated a unique block hash that is generated by a cryptographic hash function. This block hash serves as a digital fingerprint for the block's content and ensures its immutability. In proof-of-work consensus algorithms, for instance, miners compete to find a nonce value that, when combined with the block header, satisfies specific criteria, thereby adding a layer of security through the solution of computational puzzles. The block functions as the fundamental unit of the blockchain, enabling secure, transparent, and efficient transaction storage and verification.

2.1.3 Wallet

2.1.3.1 Key and address

Key and address are foundational concepts pertaining to user identification and transaction security in the context of blockchain technology and cryptocurrencies. A key, also known as a cryptographic key, is a fragment of information utilized in cryptographic algorithms for a variety of purposes, including encryption, decryption, and digital signatures. Typically, in the context of blockchain, keys are used to secure access to digital assets and to authenticate transactions. There are various mathematically related key categories, including private and public keys. A private key is a secret, randomly generated number that is kept covert by the user. It is used to generate digital signatures, which verify the integrity and authenticity of transactions. The private key should be stored in a secure location and never shared with anyone. If a third party obtains access to the private key, they may be able to take control of the associated digital assets. On the other hand, an address is a cryptographic representation of a user's public key. In a blockchain network, it is a string of alphanumeric characters that functions as a unique identifier for receiving transactions or messages. The public key is used to generate addresses, but they do not disclose any information about the private key. When sending a transaction to a particular user in a blockchain network, the recipient's address is used as the destination. The address functions as a pseudonymous identifier, providing privacy and security. The recipient can then access and manage the digital assets associated with that address using their private key.

2.1.3.2 Wallet

A cryptocurrency wallet is a software application or hardware device that enables users to store, administer, and interact with their digital assets in a secure manner. Wallets play a crucial role in the adoption and use of cryptocurrencies by both consumers, enhancing the overall experience with a variety of advantages. Wallets provide a convenient and intuitive interface for managing digital assets. They provide a secure solution for storing private keys, which are required for accessing and controlling cryptocurrencies. Wallets enable users to transfer and receive funds, track their transaction history, and monitor their account balances by storing private keys securely. Wallets typically include features such as address book administration, transaction history, and real-time market data, providing users with a comprehensive set of tools for managing their cryptocurrency holdings. One important aspect of wallet security is the implementation of industry standards, such as the BIP39 specification [7], in the generation and management of mnemonic phrases or seed phrases. The BIP39 specification ensures that wallets adhere to a standardized method for generating mnemonic phrases, which are human-readable sets of words. These phrases can be used to derive the cryptographic keys necessary to access and manage cryptocurrency funds. By adopting the BIP39 specification, wallets provide users with a consistent and reliable way to backup and restore their wallets, offering an additional layer of security and ease of use. MetaMask [8] is a prominent example of a cryptocurrency wallet. MetaMask is a wallet extension for web browsers that enables users to interact with Ethereum-based decentralized applications (DApps) directly from the browser. It provides a user-friendly and secure interface for interacting with Ethereum accounts and the blockchain. MetaMask provides a straightforward and intuitive interface that integrates seamlessly with popular web browsers such as Chrome, Firefox, and Brave. Within minutes, users can install the MetaMask extension and configure their Ethereum wallet. After configuring the wallet, users can access their Ethereum accounts, view their token balances, and conduct transactions.

2.1.4 Consensus

The concept of consensus holds paramount importance in the realm of blockchain technology as it serves to guarantee the agreement and validity of transactions throughout the network. This mechanism encompasses a process by which decentralized nodes within the network collectively establish agreement regarding the current state of the blockchain. This paper examines two prevalent consensus algorithms, namely Proof of Work (PoW) and Proof of Stake (PoS).

PoW consensus algorithm, initially pioneered by Bitcoin [3], serves as the foundational mechanism for validating transactions and maintaining the integrity of the blockchain network. In the context of PoW, the participants referred to as miners engage in a competitive process aimed at solving intricate mathematical puzzles. In the realm of blockchain technology, the initial miner who successfully unravels the intricate puzzle is duly acknowledged and bestowed with a reward, subsequently appending a novel block to the existing chain of transactions. The aforementioned process necessitates a substantial amount of computational resources and incurs a considerable level of energy expenditure. The security of a blockchain system is upheld through the utilization of PoW, which effectively deters malicious entities from tampering with previous transactions. This is achieved by imposing a significant computational burden on any attempts to modify the blockchain's historical records.

PoS [4] consensus algorithm serves as a viable alternative to the PoW mechanism, with the primary objective of mitigating the concerns pertaining to energy consumption commonly associated with PoW. In the PoS consensus mechanism, the selection of validators to generate new blocks is determined by their cryptocurrency holdings and their willingness to "stake" said holdings as collateral. The selection of validators is typically conducted through a deterministic procedure, which frequently takes into consideration factors such as the magnitude of their stake and the duration for which they have maintained it. PoS consensus mechanism is widely acknowledged for its superior energy efficiency in comparison to the PoW mechanism, primarily due to its reduced reliance on intensive computational resources.

The utilization of both PoW and PoS consensus mechanisms presents distinct benefits and limitations. PoW consensus mechanism is renowned for its robust security measures, albeit at the cost of significant resource consumption. Conversely, the PoS protocol boasts energy efficiency advantages, yet it may exhibit vulnerability to specific forms of attacks. The selection between PoW and PoS is contingent upon the distinct objectives and prerequisites of a blockchain network.

2.2 Shamir's secret sharing

Shamir's secret sharing is a cryptographic algorithm that divides a secret into multiple shares, which can then be distributed to various participants. The secret can only be reconstructed by combining a substantial number of shares. The algorithm was created in 1979 by Adi Shamir and is based on polynomial interpolation. To implement Shamir's secret sharing, a secret is first selected, and then a polynomial of a specific degree is generated with the secret as the constant term. The polynomial is subsequently evaluated at particular points to generate the shares. Each participant receives a portion of the polynomial curve that corresponds to a specific point. Any subset of shares, so long as it satisfies a certain threshold, can be used to reconstruct the original secret, according to Shamir's secret sharing scheme.

Here is a straightforward illustration of how Shamir's secret sharing works. Suppose we wish to divide a secret value of 42 into 5 portions with a threshold of 3. By evaluating a polynomial at various points, the shares are generated. Share 1: (1, 17), Share 2: (2, 23), Share 3: (3, 38), Share 4: (4, 14) Share 5: (5, 7) x represents the point on the polynomial curve, while y is the value of the polynomial at that point. Now, we need at least three shares to reconstruct the secret. Consider the shares 2, 3, and 4. We can use these shares to interpolate the polynomial and determine the value at x = 0 that corresponds to our confidential value of 42 by employing interpolation. Using the Lagrange interpolation formula [9], the secret can be calculated:

$$\text{Secret} = \frac{23 \cdot (0-3) \cdot (0-4)}{(2-3) \cdot (2-4)} + \frac{38 \cdot (0-2) \cdot (0-4)}{(3-2) \cdot (3-4)} + \frac{14 \cdot (0-2) \cdot (0-3)}{(4-2) \cdot (4-3)}$$

After simplifying the equation, the hidden value is determined to be 42.

2.3 Distributed Key Generation

The Distributed Key Generation (DKG) protocol is a cryptographic mechanism that allows multiple parties to generate a shared secret key collaboratively without relying on a single trusted authority. It ensures that no one party has complete knowledge of the secret key, thereby enhancing security and decreasing the likelihood of a single point of failure. In a DKG protocol, the participating parties collaborate to generate and distribute portions of the secret key. Combining these shares mathematically yields the final confidential key. Protocol phases include key generation, distribution, verification, and reconstruction. The primary benefits of DKG protocols are their security and resilience. The protocol mitigates the risk of a single party compromising the confidential key by distributing the key generation process across multiple parties. Even if some parties are compromised, the final key will remain secure if a minimum number of trustworthy parties are involved. Protocols for Distributed Key Generation have applications in numerous disciplines, including secure multi-party computation, cryptographic key management, threshold cryptography, and secure communication protocols. They provide a robust mechanism for establishing shared secret keys in situations where there is little or no trust between participants.

The Pedersen DKG protocol, proposed by Torben Pedersen [10] in 1991, was used in the thesis. The Pedersen DKG protocol utilizes polynomial interpolation techniques and cryptographic primitives to achieve secure and distributed key generation. It provides a robust mechanism for establishing shared secret keys without relying on a trusted central authority. The protocol involves several steps, including key generation, sharing, verification, and reconstruction.The Pedersen DKG protocol utilizes polynomial interpolation techniques and cryptographic primitives to achieve secure and distributed key generation. It provides a robust mechanism for establishing shared secret keys without relying on a trusted central authority. The protocol involves several steps, including key generation, sharing, verification, and reconstruction.

2.4 Smart contract

2.4.1 History and defination

Smart contracts are agreements that automatically carry out their obligations because they are encoded in code. By eliminating the need for middlemen and supplying a safe and decentralized method to facilitate and enforce agreements or transactions, these contracts automatically execute and enforce themselves. The idea of smart contracts has been around since the 1990s, and computer scientist Nick Szabo [11] is credited with coining the term. However, smart contracts did not receive much attention or widespread use until the advent of blockchain technology, particularly with the launch of Ethereum [4] in 2015. A Turing-complete programming language was introduced by Ethereum, a decentralized blockchain platform, allowing for the creation and execution of sophisticated smart contracts. This innovation paved the way for the development of decentralized applications (DApps) that might use smart contracts to secure and automate a variety of activities, including voting systems, supply chain management, and financial transactions. Since then, smart contracts have become more well-known and are being investigated in a variety of sectors and industries for their potential to transform conventional corporate operations. Their immutability and transparency, along with the ability to automate processes and get rid of middlemen, have the potential to improve workflow, boost productivity, and cut costs.

2.4.2 Practical use cases

Smart contracts have become a game-changing technology with several real-world applications in a wide range of industries. These self-executing contracts, which are inscribed on a blockchain, allow for secure and automated transactions, doing away with the need for middlemen and enhancing participant trust. Smart contracts have transformed lending platforms, decentralized exchanges, and yield farming protocols in the field of DeFi [12]. Smart contracts offer a transparent and effective ecosystem for decentralized financial applications by automating financial transactions and following established regulations. Likewise, supply chain management has benefited from smart contracts. By facilitating seamless tracking and verification of commodities along the supply chain, these contracts improve traceability, lower fraud, and streamline logistical operations. Smart contracts have simplified real estate transactions by enabling property transfers, escrow services, and rental agreements. Smart contracts increase efficiency and transparency in the real estate sector by doing away with middlemen and automating repetitive operations.

In this thesis, the smart contract plays a pivotal role in the ecosystem by fulfilling a multitude of significant responsibilities. The storage and maintenance of configuration updates for the Perdesen Distributed Key Generation (DKG) protocol is a primary responsibility. The smart contract is responsible for managing a whitelist of decentralized applications (DApps) that utilize the aforementioned solution. This mechanism ensures that only authorized DApps are able to participate in the protocol. The smart contract is designed to enable the asynchronous execution of the Perdesen DKG protocol rounds, which is a fundamental feature of its functionality. The process entails the antecedent creation of cryptographic keys through the secure retention of encrypted shares for each node involved in the operation. The implementation of a smart contract facilitates the asynchronous execution of the key generation procedure, thereby enhancing operational efficiency and scalability. The transparent management of the key generation process is regarded as a fundamental characteristic of the smart contract. The implementation of transparency in the process is paramount to guaranteeing the privacy and security of participants' private keys. The provision of transparency enables participants to authenticate the advancement and soundness of the key generation procedure while upholding the confidentiality of their private key data. The smart contract assumes a crucial function in the verification of signatures from nodes that are involved in the process. The implementation of a verification process within the Perdesen Distributed Key Generation (DKG) protocol serves to guarantee that exclusively legitimate users are allocated roles during each round of the cryptographic scheme. Through the process of signature verification, the smart contract ensures the integrity and authenticity of the nodes involved, thereby augmenting the overall security and dependability of the protocol.

2.5 Executor for DApps

An essential part of enabling the execution of transactions on the blockchain network is played by the executor of a DApp. The backend element tasked with connecting with the blockchain and carrying out transactions on behalf of users is referred to as the executor in the context of DApps. The user's private key or mnemonic being kept in the backend is one typical method for carrying out transactions in a DApp. The private key, which is used to sign transactions and verify identities, is represented by a series of phrases known as the mnemonic. The executor can access the mnemonic when necessary to sign transactions on behalf of the frontend by securely keeping it in the backend. The executors play a specific role in the thesis as the verifiers and assigners of a Perdesen DKG protocol round within the smart contract. The decentralized system's executors serve as dependable parties and are in charge of assuring the fairness and security of the round assignment procedure.

2.6 Social login for Web3

2.6.1 Web3 and Dapps

Web3 and Decentralized Applications (DApps) have emerged as critical components of the evolution of the internet and digital ecosystems. Web3 is the vision of a more decentralized and user-centric internet, in which individuals have greater control over their data, identity, and digital interactions. It is a collection of technologies, protocols, and frameworks designed to empower users, cultivate trust, and facilitate peer-to-peer interactions. DApps, on the other hand, are applications that are created on top of decentralized networks and typically utilize blockchain technology. These applications inherit Web3's fundamental principles, including decentralization, transparency, and user ownership. From financial services and governance platforms to gaming and social media applications, they provide a variety of features. The development and adoption of Web3 and DApps have been supported by a growing body of research and innovation. Several academic papers and technical publications have contributed to the advancement of these technologies. For instance, the paper by Wood et al. titled "Ethereum: A Secure Decentralized Generalized Transaction Ledger" provides a comprehensive overview of the Ethereum platform and its underlying principles [4]. Another significant contribution is the work by Swan, who explores the concept of "Token Economy" in his book "Token Economy: How the Web3 Reinvents Value Exchange." The book delves into the transformative potential of tokenization and its implications for various industries [13]. Moreover, the paper by Buterin et al. titled "A Next-Generation Smart Contract and Decentralized Application Platform" introduces the Ethereum platform, highlighting its unique features and use cases [14]. This paper serves as a foundational reference for understanding the capabilities and potential of DApps built on Ethereum.

2.6.2 Social login and OAuth

Social login is a prevalent method of authentication that enables users to log in to websites and applications using their existing social media accounts. Users are no longer required to establish new accounts and remember additional login credentials. Instead, users can merely click on a social media button, such as "Sign in with Facebook" or "Sign in with Google," to authenticate themselves. Social registration is supported by the OAuth2 (Open Authorization 2.0) [15] protocol, which provides a secure and standardized authentication framework. When a user logs in with a social media account, the website or application sends them to the respective social media platform for authentication. The user is then presented with a consent interface that describes the data to which the website or application requests access. Once the user grants permission, the social media platform provides the website or application with an access token that can be used to retrieve user information and authenticate the user's identity. Using OAuth2 for social authentication has multiple advantages. It increases security by removing the need for websites and applications to store user credentials. Instead, the obligation for authentication falls on the shoulders of the most reputable social media platforms. Second, social login streamlines the user experience by allowing users to log in with a few clicks and avoid the inconvenience of creating new accounts. It also allows websites and applications to utilize the extensive user profile data available on social media platforms, including user names, profile pictures, and email addresses, for personalization and customization.

2.6.3 Social login benefits DApps

Web3's technical complexity is one of the most significant obstacles it presents to normal consumers. The underlying technologies, such as blockchain, cryptographic keys, and smart contracts, can be complex and challenging for non-technical individuals to comprehend. Comprehending and traversing these

complexities can be an impediment to entry, impeding widespread adoption and utility. In addition, the decentralized nature of Web3 platforms may result in fragmented user experiences and inconsistent user interfaces, making it difficult for non-technical users to effectively navigate and interact with decentralized applications. Simplifying the user experience and enhancing the accessibility of Web3 technologies will be crucial for overcoming these obstacles and ensuring that regular users can reap the full benefits of Web3.
This thesis proposes a solution to improve the usability of Web2 [16] applications by integrating smart contracts, the Pedersen Distributed Key Generation (DKG) protocol, and Shamir secret sharing. The present study endeavors to propose a solution that seeks to mitigate the difficulties encountered by laypersons in comprehending and maneuvering the intricate technicalities of Web3. Additionally, the solution endeavors to guarantee the secure generation and distribution of cryptographic keys, as well as the safeguarding of data.

CHAPTER 3. SOLUTION

3.1 System's characteristics

This study examines the efficacy and adaptability of a system that utilizes conventional social login methods to augment the UX of DApps. The following characteristics can be more detailed:

Security - combining the potential benefits of blockchain smart-contract, SSS, and Pedersen DKG protocol. The security infrastructure of the system is established upon the utilization of blockchain smart contracts. Programmable contracts, operating on a decentralized network, guarantee the attributes of transparency, immutability, and tamper-proof execution of operations. Shamir secret sharing is used to fortify the protection of cryptographic keys and other forms of private information. This method entails breaking up a secret into smaller pieces and giving them to several parties. The Petersen DKG protocol distributes and secures cryptographic key generation, ensuring system security. This system lets a group of people generate a shared cryptographic key without anyone having the full key.

Efficacy and adaptability - By leveraging blockchain's decentralized nature, Web3Auth eliminates the reliance on centralized identity providers, reducing the potential for single points of failure and enhancing security. Additionally, blockchain-based identity systems enable instant verification of user credentials, eliminating the need for lengthy verification processes and reducing transaction times. The open solution's architecture enables seamless integration with any DApps, making it easier for developers to adopt and implement with their products.

User-friendly - This solution supports popular authentication mechanisms such as social login which are widely used in the traditional web. This familiarity allows users to leverage their existing accounts and authentication methods, reducing the learning curve and providing a seamless transition into the Web3 space. Users can easily authenticate their identities across multiple DApps using a unified and standardized protocol, without the need to remember and manage multiple usernames and passwords. This eliminates the hassle of creating and maintaining numerous accounts, making the user experience more streamlined and efficient.

Scalability - Compatible with any type of social authentication, including Facebook, Google, and Twitter. Utilizing a decentralized architecture increased the request's performance and volume by spreading it across multiple executors and parallel handling processes.

3.2 Overall of system

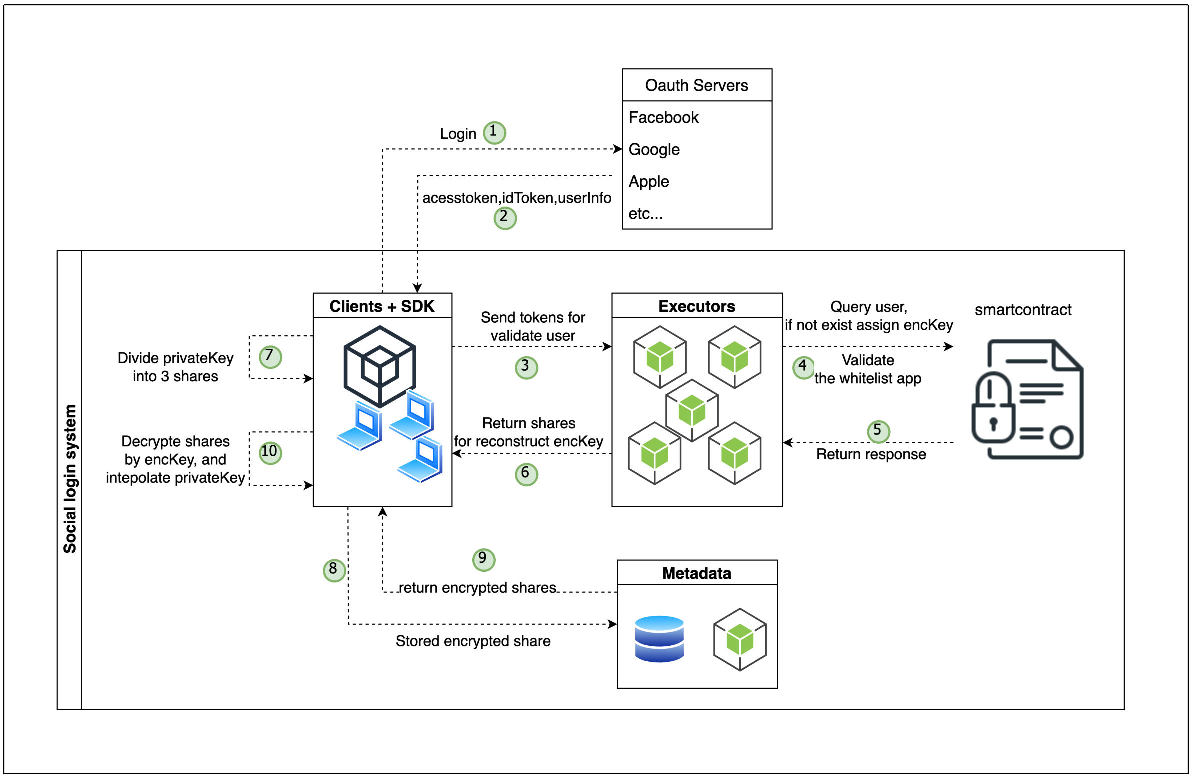
Oauth Servers
Facebook
Google
Apple
etc...
Login 1
acesstoken,idToken,userInfo
2
Social login system
Clients + SDK
Divide privateKey into 3 shares
7
Decrypte shares by encKey, and intepolate privateKey
10
Send tokens for validate user
3
Return shares for reconstruct encKey
6
Executors
Query user, if not exist assign encKey
4
Validate the whitelist app
smartcontract
5
Return response
8
9
return encrypted shares
Stored encrypted share
Metadata

Figure 3.1: Overall the system

Figure 3.1 depicts the overall processing of a request from a user utilizing the social login system. Because the process is more complex, it has been divided into three sub-processes for clarity.

3.3 Oauth2 connection

3.4 Requesting encKey for Executors

3.5 Generating and Storing Shares in Metadata

3.6 The Contribution of Executors to Pedersen's DKG Protocol

CHAPTER 4. TECHNICAL ISSUES AND DESIGN

CHAPTER 6. CONCLUSION AND FUTURE WORK

6.1 Conclusion

6.2 Future work

REFERENCE

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[2] M. Abadi *et al.*, "Distributed key generation in the wild: A practice-oriented study," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2016, pp. 257–269.

[3] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008. [Online]. Available: `https://bitcoin.org/bitcoin.pdf` (visited on 06/19/2023).

[4] V. Buterin and G. Wood, *Ethereum: A next-generation smart contract and decentralized application platform*, 2014. [Online]. Available: `https://ethereum.org/whitepaper/` (visited on 06/19/2023).

[5] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, 2014.

[6] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Advances in Cryptology - CRYPTO'87*, Springer, 1987, pp. 369–378. DOI: `10.1007/3-540-48184-2_32`.

[7] Bitcoin BIP-0039 Contributors, *Bip39: Mnemonic code for generating deterministic keys*, Bitcoin Improvement Proposal, Accessed on 2023-06-19, 2013. [Online]. Available: `https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki`.

[8] MetaMask, *Metamask: Ethereum wallet and gateway to blockchain apps*, Website, 2023. [Online]. Available: `https://metamask.io/` (visited on 06/19/2023).

[9] R. L. Burden and J. D. Faires, *Numerical Analysis*, 10th. Boston, MA: Cengage Learning, 2015, ISBN: 978-1-305-27108-9.

[10] T. P. Pedersen, "A threshold cryptosystem without a trusted party," in *Advances in Cryptology — EUROCRYPT'91*, Springer, 1991, pp. 522–526.

[11] N. Szabo, "Formalizing and securing relationships on public networks," in *First Monday*, vol. 2, University of Illinois at Chicago Library, 1997. DOI: `10.5210/fm.v2i9.548`. [Online]. Available: `http://firstmonday.org/ojs/index.php/fm/article/view/548/469`.

[12] C. van der Veen, *DeFi and the Future of Finance: A Comprehensive Guide to Decentralized Finance*. Packt Publishing, 2021, ISBN: 978-1801073687.

[13] M. Swan, *Token Economy: How the Web3 Reinvents Value Exchange*. 2018.

[14] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," 2014.

[15] Internet Engineering Task Force, *Oauth 2.0*, `https://tools.ietf.org/html/rfc6749`, Accessed: June 19, 2023, 2012.

[16] T. O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*. O'Reilly Media, 2005.