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. Thanh-Chung Dao ______________

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: BKC Labs

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 3 tháng 8 năm 2023
Advisor's signature

Ph.D. 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, Ph.D. Thanh-Chung Dao. 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 (SSS) and Distributed Key Generation (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.

Students
(Sign and full name)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES