CHAPTER I

INTRODUCTION

1.1 Background

The rapid development of digital technology has transformed various sectors, particularly in communication, financial transactions, and data management. However, this digital expansion is accompanied by rising cybersecurity threats, particularly regarding authentication systems. According to Verizon's 2023 Data Breach Investigations Report, 74% of breaches involved the human element, with 49% resulting from the use of stolen credentials, highlighting vulnerabilities in traditional authentication mechanisms. Traditional security measures, especially password-based systems, are increasingly vulnerable to sophisticated attacks.

Two-Factor Authentication (2FA) was introduced as an enhancement, combining two distinct authentication elements typically a password and an OTP (One-Time Password) sent via SMS, email, or generated by an authenticator app. However, recent studies (Bartłomiejczyk & El Fray, 2024) reveal that 2FA, especially OTP-based, remains susceptible to phishing, SIM-swapping, and man-in-the-middle (MITM) attacks. Research by Message Central (2024) shows that phishing attacks can trick users into giving up their OTP codes, allowing attackers to bypass the additional layer of security provided by 2FA. Other attack techniques, such as man-in-the-middle (MITM), have also been explored by Bonneau et al. (2012), who showed that the method of sending OTP codes via SMS or third-party applications has security holes that can be exploited by attackers. These threats exploit the transmission channels and central server dependencies inherent in traditional 2FA.

A notable case in 2023 involved the Scattered Spider hacker group, which employed social engineering techniques, including phishing and SIM-swapping, to bypass 2FA mechanisms. The group targeted major organizations such as MGM Resorts and Caesars Entertainment, demonstrating the effectiveness of these attack vectors and the vulnerability of traditional multi-factor systems (Cybersecurity and Infrastructure Security Agency [CISA], Federal Bureau of Investigation [FBI], & Multi-State Information Sharing and Analysis Centre [MS-ISAC], 2023).

Centralized authentication systems introduce a single point of failure; if the server storing user credentials is compromised, it can result in large-scale data breaches. The 2024 IBM Security report highlights that compromised credentials were responsible for 16% of data breaches and had the longest lifecycle to identify and contain, averaging 292 days. These incidents are among the costliest, with an average impact of USD 4.81 million per breach. Such findings underscore the risks inherent in traditional, centralized credential management systems, particularly in an era where attackers increasingly exploit stolen or leaked credentials. The dependency on a single device, such as a smartphone, presents a critical point of failure. If a user's phone is lost, stolen, or broken, they can be locked out of their accounts, leading to a frustrating and often complex recovery process.

Ethereum smart contracts can be used to cryptographically verify user actions without relying on centralized verification systems. Previous frameworks like those by Alghazzawi et al. (2019) showed promise but still relied on OTPs encrypted and validated on-chain. This research builds upon those ideas by eliminating OTPs entirely and introducing secondary wallet authentication, where verification is performed using dual cryptographic signatures from user-owned wallets.

Despite the widespread adoption of traditional two-factor authentication, the range of available alternatives remains notably limited. Most existing methods still rely on centralized systems or secondary devices that introduce additional points of failure or friction for users. As digital security threats evolve, the scarcity of secure and decentralized alternatives to conventional 2FA poses a significant challenge. This highlights the urgent need to explore innovative authentication mechanisms such as dual wallet-based approaches that can offer both strong security guarantees and user-friendly experiences without depending on vulnerable intermediaries.

This research proposes a fundamental shift in how we approach 2FA. Instead of tethering authentication to a physical device, we propose a system centred on the verifiable ownership of cryptographic private keys. By leveraging Ethereum smart contracts, this model introduces a decentralized 2FA system where authentication is confirmed via a cryptographic signature from a secondary digital wallet. This approach not only mitigates the security risks of OTPs but also provides unprecedented flexibility and user control. The user's identity is no longer trapped in a single piece of hardware but is defined by the keys they control, which can be securely managed and recovered across any number of devices.

The proposed approach integrates seamlessly with Ethereum Testnet (Sepolia) and utilizes a Node.js backend and React frontend with Web3.js for system interaction and testing. Through comprehensive testing, including penetration testing and static and fuzz analysis, this research evaluates the model's effectiveness compared to conventional 2FA systems.

1.2 Problem Identification

Based on the problem background previously outlined, this study will focus on the following identified issues:

1. Traditional 2FA Vulnerabilities: SMS and app-based 2FA methods are vulnerable to third-party cyberattacks, such as phishing, SIM swapping, and MITM.
2. Dependence on Central Authority: Storing user credentials on a centralized server creates a single point of failure.
3. Lack of Alternatives: Few viable solutions exist to replace traditional 2FA without compromising security or usability.

1.3 Research Questions

Based on the problem background and the identified issues above, the research questions can be formulated as follows:

1. How can a dual wallet-based two-factor authentication system reduce vulnerabilities found in traditional methods such as SMS and authenticator apps, especially against phishing, SIM swapping, and MITM attacks?
2. How can be decentralized using smart contracts to eliminate the single point of failure caused by centralized servers?

3. Can the proposed dual wallet-based 2FA model serve as a secure and usable alternative to traditional 2FA methods?

1.4 Scope of the Study

To ensure that this research remains focused and can be implemented well, the problem limitations are set as follows:

1. This research only uses Ethereum Testnet (Sepolia) for testing without involving the mainnet.
2. The authentication mechanisms used consist of: Secondary wallet authentication, where users must confirm actions using a secondary wallet that has been registered in the smart contract.
3. Testing focused on phishing and Man in The Middle attacks, without considering other attacks such as DoS or malware.
4. Does not address integration with biometric-based authentication methods or hardware security keys.

1.5 Research Objectives

Based on the problem formulation above, the objectives of this study are to:

1. To design a blockchain and smart contract-based two-factor authentication model that addresses security vulnerabilities in SMS and app-based 2FA by introducing secondary wallet authentication.
2. To implement a decentralized 2FA mechanism on the Ethereum Testnet (Sepolia) that eliminates reliance on centralized credential storage.
3. To evaluate the proposed system’s effectiveness as a secure and usable alternative, specifically in resisting phishing and Man in The Middle attacks.

1.6 Research Significance

From the research objectives above, this research is expected to provide several benefits as follows:

1.6.1 Theoretical Significance

Provides a new framework for developing dual wallet-based authentication systems that are empirically tested through a testnet. Enriches the literature on smart contract integration with secondary wallet authentication mechanisms for digital security.

1.6.2 Practical Significance

Provides a more secure, transparent, and cost-effective 2FA authentication solution for users and organizations. Minimizes risks and points of failure through decentralized architecture.