B.Sc. in Computer Science and Engineering Thesis

KYC-DRIVEN CRYPTOCURRENCY WALLET: A SOLUTION TO REGULATORY COMPLIANCE

Submitted by

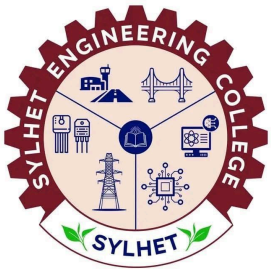
Mehadi Hasan
Registration No.: 2019331537

Ovi Talukder
Registration No.: 2019331548

Raisul Karim Saju
Registration No.: 2019331549

Supervised by

Md Lysuzzaman
Lecturer
Department of Computer Science and Engineering
Sylhet Engineering College



Department of Computer Science and Engineering
Sylhet Engineering College, Sylhet

Affiliated with
Shahjalal University of Science and Technology
Sylhet, Bangladesh

22 July 2025

Candidates' Declaration

This is to certify that the work presented in this thesis, titled **"KYC-Driven Cryptocurrency Wallet: A Solution to Regulatory Compliance"**, is the outcome of the investigation and research carried out by us under the supervision of **Md Lysuzzaman**.

It is also declared that neither this thesis nor any part thereof has been submitted anywhere else for the award of any degree or diploma.

A part of this research has been accepted and published in the proceedings of an IEEE-sponsored international conference.

Mehadi Hasan	**Ovi Talukder**	**Raisul Karim Saju**
Reg. No : 2019331537	Reg. No: 2019331548	Reg. No: 2019331549

Sylhet

Bangladesh

22 July 2025

Recommendation Letter from Thesis Supervisor

It is with great satisfaction that I confirm the acceptance and successful defense of the thesis titled **"KYC-Driven Cryptocurrency Wallet: A Solution to Regulatory Compliance"**, presented by the following group of students as a partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering on **22nd July 2025**.

Group Members:

1. **Mehadi Hasan**
2. **Ovi Talukder**
3. **Raisul Karim Saju**

The students conducted their research under my supervision, showcasing outstanding commitment, technical proficiency, and a strong understanding of the subject matter. Their project addresses crucial aspects of regulatory compliance in the cryptocurrency domain, proposing a practical KYC-integrated wallet solution to enhance financial transparency and security.

I hereby certify that this thesis is the result of their original and independent work, and I recommend it for academic recognition and future professional exploration.

.

Supervisor:

_____

Md Lysuzzaman
Lecturer
Department of Computer Science and Engineering
Sylhet Engineering College
Date: 22th July 2025

Certificate of Acceptance of the Thesis

This is to certify that the above-mentioned thesis entitled *"***KYC-Driven Cryptocurrency Wallet: A Solution to Regulatory Compliance***"* submitted by the students **Mehadi Hasan, Ovi Talukder, and Raisul Karim Saju** in **July 2025** as part of the requirements of the course **CSE-800**, has been approved by the **Department of Computer Science and Engineering** as partial fulfillment of the **B.Sc. (Eng.)** degrees of the mentioned students.

Supervisor
Md Lysuzzaman
Lecturer
Department of Computer Science and Engineering
Sylhet Engineering College

Internal
Md. Abu Naser Mojumder
Assistant Professor & Head of Department
Department of Computer Science and Engineering
Sylhet Engineering College

Internal
Md. Nagrul Islam
Assistant Professor
Department of Computer Science and Engineering
Sylhet Engineering College

Internal
Md. Rasel Ahmed
Assistant Professor
Department of Computer Science and Engineering
Sylhet Engineering College

Internal
Nayan Kumar Nath
Lecturer
Department of Computer Science and Engineering
Sylhet Engineering College

External
Mohammad Shahidur Rahman, PhD, SMIEE
Professor & Head of Department
Department of Computer Science and Engineering
Shahjalal University of Science and Technology

Acknowledgment

We would like to express our sincere gratitude to the **Department of Computer Science and Engineering, Sylhet Engineering College, Sylhet**, for providing us with the necessary support and resources throughout this research.

We are especially thankful to our honorable supervisor, **Md Lysuzzaman** (Lecturer, CSE, Sylhet Engineering College), for his continuous guidance, insightful feedback, and encouragement at every stage of our work.

We are also pleased to acknowledge that a part of this research has been accepted and published in the proceedings of an **IEEE-sponsored international conference**, which has further validated the relevance and impact of our work.

List of publications

Publications related to this thesis:

- Hasan, Mehadi, Ovi Talukder, Raisul Karim Saju, and Md Lysuzzaman. "KYC-Driven Cryptocurrency Wallet: A Solution To Regulatory Compliance." In *2024 27th International Conference on Computer and Information Technology (ICCIT)*, pp. 405-410. IEEE, 2024.
  DOI: 10.1109/ICCIT64611.2024.11022389

Contents

Abstract

Cryptocurrencies have transformed digital finance with decentralized, peer-to-peer systems prioritizing privacy and autonomy, but their rapid adoption has raised concerns about financial crimes, tax evasion, and illegal activities, leading to stringent regulations and bans. This paper proposes a solution integrating compliance standards into a centralized regulatory framework for cryptocurrency wallets, balancing decentralization with oversight. The proposed hybrid wallet model incorporates KYC, AML, NFC-enabled device verification, and taxation mechanisms under a Central Governing Committee overseeing transaction management and user verification. It employs biometric authentication and encrypted key management to ensure security, while NFC devices enhance user verification. This system aims to address concerns like money laundering, terrorism financing, and tax evasion, promoting responsible cryptocurrency use while maintaining financial stability. It offers a pathway for governments to adopt cryptocurrencies securely, ensuring compliance without stifling innovation, ultimately fostering a more inclusive and regulated digital financial ecosystem.

Index Terms—Cryptocurrencies, KYC (Know Your Customer), Anti-Money Laundering (AML), NFC (Near Field Communication), Centralized Regulatory System, Hybrid Crypto-Wallet Model, Financial Crime Prevention, Biometric Authentication, Encrypted Key Management.

Chapter One

Introduction

1.1 Overview

Blockchain technology is transforming industries by revolutionizing processes and enabling innovative applications. Its decentralized, transparent nature enhances efficiency, security, and trust in areas like supply chain management, data storage, document verification, and smart contracts. Central to blockchain are transactions, facilitating digital asset transfers and self-executing smart contracts, often powered by cryptocurrencies. Operating without intermediaries, cryptocurrencies enable secure, peer-to-peer interactions, transparent and immutable, making them vital in modern finance and diverse industries.[1][2]

Cryptocurrencies, integrated into blockchain systems, streamline processes by eliminating intermediaries, reducing costs, and enhancing transparency. They lower fraud risks and foster innovation in finance, healthcare, logistics, and governance. As blockchain technology advances, cryptocurrencies are vital to decentralized ecosystems, shaping global digital transactions despite regulatory challenges.[3][4]

This research paper addresses the challenge of integrating Know Your Customer (KYC) protocols in cryptocurrencies to ensure regulatory compliance. KYC procedures, commonly used in traditional financial institutions, verify customer identities and mitigate risks like money laundering, terrorism financing, and fraud. By incorporating KYC protocols into cryptocurrency wallets, this research aims to bridge the gap between cryptocurrencies' decentralized nature and regulatory requirements. The proposed framework balances user autonomy with centralized oversight, enabling cryptocurrencies to coexist with existing financial systems while addressing regulatory concerns.[5][6][7]

As cryptocurrencies continue to grow, robust regulatory frameworks are crucial to ensure mainstream acceptance and integration into global financial systems. Despite offering decentralization, anonymity, and financial autonomy, cryptocurrencies raise concerns over misuse in illicit activities due to the lack of regulatory oversight [8][9] and pseudonymous blockchain transactions, which facilitate money laundering, terrorism financing, and tax evasion. Consequently, many countries have imposed strict regulations or bans, citing threats to economic stability, consumer protection, and national security [10][11]. This paper proposes a KYC-driven framework for cryptocurrency wallets to address these regulatory concerns while preserving the benefits of digital currencies. By focusing on combating financial crime, enhancing consumer protection, and promoting economic stability, it aims to create a more secure and regulated cryptocurrency ecosystem.

This paper explores the following research questions:

1. How do KYC-driven crypto wallets support regulatory compliance and reduce financial crime risks?
2. How can centralized crypto regulations ensure oversight while preserving digital currency benefits?
3. What are the potential benefits and challenges of KYC implementations in crypto wallet?
4. How do biometrics and NFC-based ID verification enhance wallet security and compliance?
5. How can privacy tech like ZKPs and homomorphic encryption maintain anonymity in KYC wallets?
6. How do KYT protocols complement KYC to boost transparency and prevent illicit activities?

This research aims to integrate regulatory measures into cryptocurrency systems without compromising their core principles. It evaluates existing compliance frameworks, analyzes technological advancements for secure identity verification, and proposes a balanced regulatory framework that aligns digital currencies with legal financial structures. By addressing regulatory challenges, this study contributes to a secure, compliant, and scalable cryptocurrency ecosystem, supporting mainstream adoption and ensuring long-term viability. [12][13][14][15]

1.2 Research Objectives

The objectives of this research are to:

- Analyze the regulatory landscape for cryptocurrencies and identify compliance challenges.
- Propose a framework for KYC-driven cryptocurrency wallets, including components, processes, and technologies.
- Evaluate the impact of KYC-driven wallets on regulatory compliance, consumer protection, and cryptocurrency adoption.
- Assess the feasibility of biometric authentication and NFC-based identity verification for enhanced security and compliance.
- Examine the role of privacy-preserving technologies like ZKPs and homomorphic encryption in balancing user anonymity with regulatory requirements.
- Evaluate the potential of AI and ML in enhancing fraud detection and risk assessment in KYC-driven wallets.
- Explore the challenges of implementing a globally standardized KYC framework for cryptocurrencies.

Chapter Two: Background Study

Background Study

This section introduces a centrally governed cryptocurrency wallet solution, offering an innovative approach to integrating cryptocurrencies into existing financial infrastructures. It emphasizes a hybrid model that merges decentralized cryptocurrencies with the necessary oversight and regulation, ensuring compliance without sacrificing the core benefits of digital assets. The system is designed to balance the needs of consumers, financial institutions, governments, and regulatory bodies, facilitating cryptocurrency adoption while maintaining control over illicit activities.

2.1 Crypto-Wallet

Cryptocurrency, a form of digital currency secured by advanced cryptographic techniques, operates on decentralized blockchain networks, offering a high level of transparency and security. A crypto-wallet is a specialized digital storage solution used to manage these cryptocurrencies, enabling users to securely store their cryptographic keys (private and public keys) instead of relying on physical storage methods. These wallets allow users to perform various functions such as managing their digital assets, checking balances, and facilitating transactions.

When a user initiates a transaction using a crypto-wallet, the process begins by presenting the transaction details to the user for confirmation. Once the user authorizes the transaction, it is signed with the user's private key, ensuring the security and authenticity of the transaction. The signed transaction is then sent to the blockchain network for validation and processing. The role of the wallet is critical in this process, as it enables the secure transmission of data to the blockchain while ensuring that the transaction is performed only by the rightful owner of the wallet.

Crypto-wallets can generally be categorized into two types:

1. **Custodial Wallets**: These wallets are managed by third-party service providers such as cryptocurrency exchanges. In this type of wallet, the user does not directly control their private keys; instead, the third-party service retains control over them. While custodial wallets offer ease of use and convenience, they also introduce a level of trust dependency on the service provider. If the provider experiences a security breach or failure, the user’s funds could be at risk.
2. **Non-Custodial Wallets**: In contrast, non-custodial wallets allow users to maintain full control over their private keys. This means that the user has complete authority over their

digital assets, and no third party is involved in the management of the wallet. While this approach provides increased autonomy and security, it also places the onus of safeguarding the keys on the user.

There are two common types of implementations for crypto-wallets:

- **Hardware Wallets**: These are physical devices that store private keys offline. By keeping the keys disconnected from the internet, hardware wallets offer heightened security against online attacks such as hacking or malware.
- **Software Wallets**: These are applications or programs that store private keys digitally. They can be implemented on mobile phones, desktops, or as browser extensions. Software wallets are more accessible but may be susceptible to online threats.

The proposed system in this paper introduces a hybrid software wallet, which combines the benefits of both custodial and non-custodial models. The idea is to offer users the autonomy of managing their cryptocurrency while ensuring that the system has centralized oversight for regulatory compliance. This hybrid wallet will allow users to maintain control over their private keys while incorporating necessary security measures and regulatory features, such as Know Your Customer (KYC) protocols and transaction monitoring, to comply with financial regulations. This balance between decentralized control and centralized oversight seeks to address concerns about security, regulatory compliance, and illicit activity while maintaining the advantages of blockchain-based digital currencies.

2.2 Cryptocurrency and Wallet Regulation

The proposed cryptocurrency wallet system integrates a Central Governing Committee to oversee and regulate all aspects of the cryptocurrency ecosystem. This committee is responsible for monitoring key components, including user wallets, transaction activities, currency exchanges, databases, and servers. Its primary role is to ensure that the system adheres to established regulatory standards while preserving the essential features of cryptocurrency transactions, such as decentralization, user privacy, and security.

The system incorporates several key regulatory measures to address concerns related to illicit activities, fraud, and money laundering while promoting transparency and compliance with international financial standards. These regulatory measures include:

1. **Mandatory Biometric Verification**: The system mandates the use of biometric data, such as facial recognition or fingerprint scans, to verify the identity of users. This layer of security ensures that only authorized individuals can access the wallet and perform transactions.
2. **Near Field Communication (NFC) Verification**: For added security and ease of use, users must employ an NFC-enabled device for verification during account setup and transaction processing. NFC technology ensures that the user is physically present during transactions, minimizing the risk of remote fraud.

3. **Know Your Customer (KYC) Compliance**: KYC verification is required for all users during account registration. This process helps confirm the identity of users, preventing identity theft, fraud, and money laundering. The system collects and verifies user data, such as government-issued identification and address proof, to meet the regulatory requirements of financial institutions.
4. **Transaction Limits and Invoice Verification**: The system places limits on the amount of cryptocurrency that can be exchanged or transferred within a specified period. These limits help monitor large transactions that could indicate suspicious activity. Additionally, invoice verification protocols ensure that money transfers are legitimate and align with agreed-upon transaction terms.
5. **Enhanced Anti-Money Laundering (AML) Protocols**: The system employs advanced anti-money laundering measures, such as transaction monitoring, risk scoring, and sanction screening, to identify and prevent illegal activities like money laundering or terrorist financing. These protocols analyze transaction patterns, flag suspicious behavior, and initiate investigations if necessary.

By integrating these regulatory controls, the system balances the decentralized nature of cryptocurrencies with the need for effective regulation. This hybrid approach addresses the concerns of governments, financial institutions, and regulatory bodies while preserving the benefits of cryptocurrency, including fast, low-cost transactions and financial inclusivity. The goal is to foster a regulatory environment that supports innovation and adoption of digital assets, without compromising on security or compliance.

2.3 Summary

This section provides an overview of a centrally governed cryptocurrency wallet solution designed to integrate digital assets into traditional financial systems through a hybrid model. It highlights the balance between decentralized control and centralized oversight, ensuring regulatory compliance while preserving the inherent benefits of cryptocurrencies. The discussion covers the fundamentals of crypto-wallets, distinguishing between custodial and non-custodial types, and introducing a hybrid wallet that merges user autonomy with regulatory features like KYC protocols and transaction monitoring. Additionally, it outlines the role of a Central Governing Committee and key regulatory measures such as biometric verification, NFC-enabled security, AML protocols, and transaction limits. This comprehensive background establishes the foundation for the proposed system's methodology and its regulatory framework in subsequent sections.

Chapter Three

Literature Review

3.1 Previous Work

In this section, we present an overview of the findings from various research papers and studies related to cryptocurrencies and their regulation. A wide range of prior works has been examined to understand global perspectives, regulatory approaches, economic impacts, and governance factors influencing cryptocurrency adoption. The following subsections summarize the key insights from these studies.

3.1.1 Global Impact and Regulatory Challenges of Cryptocurrencies

Cryptocurrencies have fundamentally transformed financial transactions, providing unprecedented levels of privacy and decentralization. However, this innovation has also introduced significant challenges related to regulatory compliance, anti-money laundering efforts, and the prevention of terrorism financing by providing the features of conducting transactions anonymously between crypto-users worldwide.[16] While cryptocurrencies have become popular worldwide, not all countries have adopted this digital trend. Some of them instead see this as a potential threat to their economies and completely prohibit the use of cryptocurrencies, citing concerns over lack of control and associations with illicit ties. [17]

3.1.2 Country-Specific Cryptocurrency Restrictions

Countries like Argentina, Colombia, Iran, and Taiwan have instituted implicit bans, permitting individuals to hold or mine digital assets while prohibiting banks from accepting them as payment methods. On the other hand, some Muslim countries, such as Iraq, Egypt, Indonesia have banned cryptocurrency transactions due to their adherence to Islamic Economic Laws.[18] This is because cryptocurrency lacks a central regulatory authority, uncertainty, experiences volatile value fluctuations, and has been associated with gambling, money laundering and terrorist financing, which are seen as incompatible with Islamic financial principles. On the other hand, countries like United States, Canada, Japan, Australia uses cryptocurrency for its innovation potential, economic growth and technological advancement. [19]

3.1.3 Research Gaps in Cryptocurrency Regulation

In recent years, there has been a growing focus in the space of cryptocurrency regulation, Anti-Money Laundering, and combating terrorism financing. Although much of the recent research has concentrated on the technical aspects of cryptocurrency transactions,[20][21][22] few have comprehensively examined the integration of regulatory measures with crypto-wallets, particularly in preventing illicit activities.

3.1.4 Cryptocurrency Pricing and Economic Impact

This paper [23] explores the role of cryptocurrency pricing relative to standard currencies as a foreign currency, analyzing factors influencing the "Kimchi premium" in foreign exchange markets and how introducing a new cryptocurrency can affect money supply, interest rates, and exchange rates.

3.1.5 Decentralized Approaches to Cryptocurrency Regulation

This study [24] explores challenges of regulating Bitcoin within traditional legal frameworks due to its decentralization. It proposes a decentralized regulatory approach that leverages existing financial regulations and intermediaries like banks, payment service providers, exchanges, and large node operators. Instead of directly regulating cryptocurrencies, the study targets their use cases, ensuring compliance through financial market participants. This approach aims to create a more effective and adaptable regulatory framework for decentralized cryptocurrencies.

3.1.6 Governance Factors in Cryptocurrency Adoption

Another paper [25] analyzes governance factors using PLS-SEM across 33 countries to examine the influence of national institutions on cryptocurrency adoption. Strong government efficiency and regulatory quality discourage use, while political stability and accountability have a smaller negative impact. Rule of law and corruption control promote adoption by fostering trust in digital assets. A well-functioning welfare state discourages reliance, while robust legal enforcement and financial oversight encourage legitimate transactions.

3.1.7 Shifting Regulatory Approaches in Cryptocurrency Markets

This study examines the technological foundation of cryptocurrencies and the growing need for regulatory intervention. While countries like India have attempted to ban cryptocurrencies due to perceived economic risks, increasing investment and fintech interest have led governments to reconsider outright prohibitions. Highlighting the shift from restrictive policies to frameworks balancing financial stability with innovation, the paper emphasizes the necessity of structured oversight in the evolving crypto market [26].

3.1.8 Blockchain for Automating KYC Processes

A systematic review explores blockchain’s automation of Know Your Customer (KYC) processes. Traditional KYC methods are labor-intensive and costly, especially for financial institutions. Blockchain’s decentralized nature improves efficiency by enhancing speed, reducing onboarding time, and minimizing risks and costs. The study highlights platforms like Ethereum and Hyperledger as effective blockchain-based KYC solutions. [27]

3.1.9 e-KYC TrustBlock: Blockchain and CP-ABE Integration

Addressing data security, interoperability, and efficiency challenges in the e-KYC framework, the proposed "e-KYC TrustBlock" utilizes blockchain and CP-ABE (Ciphertext-Policy Attribute-Based Encryption) for tamper-resistant KYC verification. This system introduces a one-time access key and consent-based mechanism, empowering users with

data control, outperforming existing systems in security, efficiency, and user-centric features [28].

3.1.10 Decentralized KYC with Hybrid Blockchain Model

A blockchain-based KYC system enhances transparency, security, and efficiency through a decentralized framework. Integrating permissioned and open blockchains, the system employs smart contracts for user registration, document uploads via IPFS, and administrative validation. Automating approval processes ensures tamper-proof data storage, streamlining KYC procedures while maintaining regulatory compliance [29].

3.1.11 Blockchain Solutions for Banking KYC Inefficiencies

Research highlights how blockchain can transform traditional KYC processes in banking, addressing inefficiencies and high costs. By storing and monitoring KYC information on decentralized networks, blockchain mitigates issues like fraud, scalability, and privacy concerns, reducing intermediaries and enhancing security [30].

3.1.12 Regulating Cryptocurrency Exchanges in DeFi

Regulation of cryptocurrency exchanges within decentralized finance (DeFi) landscapes is examined, noting that many platforms still rely on traditional institutions, exposing investors to risks. The study critiques the focus on regulating ICOs, advocating instead for formal registration requirements for exchanges to balance decentralization benefits with investor protection and systemic risk management [31].

3.1.13 Financial Regulatory Tools for Cryptocurrency Oversight

The necessity and feasibility of government regulation in the cryptocurrency sector are explored through financial regulatory tools tailored to electronic money. Analyzing fraudulent schemes, the study proposes frameworks to help governments monitor cryptocurrency movements, detect suspicious transactions, and enhance security and transparency [32].

3.1.14 Taxation Policies on Cryptocurrency Income

Taxation of income from cryptocurrency transfers highlights the need for individuals earning over 600 lei annually from cryptocurrencies to report income and, in some cases, pay taxes. Gains are classified as taxable income, requiring declaration through a Single Taxation Statement. Holding cryptocurrencies without using them exempts individuals from taxation [33].

3.1.15 Bitcoin’s Role Post-Financial Crisis and Taxation

Bitcoin’s emergence post-2008 financial crisis is discussed, focusing on its role as an investment tool amid financial risks, digitalization, and geopolitical tensions. The paper examines its popularity, the challenges of tracking illicit activities via blockchain, and varying global taxation practices, offering suggestions for Turkey’s cryptocurrency taxation approach [34].

3.1.16 Cryptocurrency and Global AML Efforts

This article examines the impact of crypto-coins, such as Bitcoin, on global anti-money laundering (AML) efforts, arguing that the main challenge lies not in their illicit use but in the opportunities offered by blockchain technology [35]. Highlighting the Financial Action Task Force's (FATF) risk-based approach, the article underscores its importance in balancing threats and opportunities associated with digital assets, despite certain limitations. Continuous monitoring and investigation of the ethical implications of crypto-coins are recommended.

3.1.17 Cryptocurrency, Blockchain, and Law Enforcement

Exploring the intersection of cryptocurrency, blockchain technology, and law enforcement, this paper focuses on criminal activities enabled by these technologies, noting that amateur investors are frequent targets of investment scams [36]. Based on interviews with law enforcement practitioners, it discusses illicit uses of cryptocurrencies in money laundering and cashing out illegal profits. The paper proposes a simplified classification of crypto-related crimes and stresses the importance of privacy in protecting against scams and cybercrimes.

3.1.18 Cryptocurrency in Money Laundering and Regulatory Responses

The integration of cryptocurrencies into money laundering processes and the regulatory responses are examined in this paper [37]. With the anonymity of blockchain technology attracting criminal networks, the paper emphasizes the urgency for additional regulation to mitigate associated risks. It contributes to the debate on preventing cryptocurrency misuse and advocates for stronger regulatory measures against illicit transactions.

3.1.19 Blockchain Regulation in the EU and USA

Key regulatory challenges around blockchain technology in the EU and USA are the focus of this paper, which utilizes qualitative analysis from statutes and case studies [38]. It finds that the hands-off regulatory approach fosters innovation, efficiency, and financial inclusiveness in blockchain technologies, underlining their broader economic potential beyond virtual currencies.

3.1.20 Comparative AML Strategies Across Regions

This study compares anti-money laundering strategies through cryptocurrencies across the USA, EU, Japan, and Singapore [39]. The USA employs a technology-driven approach, the EU emphasizes regulatory harmonization, Japan focuses on strict surveillance, and Singapore integrates advanced technology with rigorous oversight. The research concludes that a combined strategy of technology, regulation, and international cooperation is vital for combating cryptocurrency-related money laundering.

3.1.21 Securing Private Keys in Cryptocurrency Systems

Addressing the challenge of securing private keys in cryptocurrency systems, this paper highlights issues like the irreversibility of compromised transactions and inadequate backup mechanisms in wallets [40]. Building on prior research, it proposes enhanced cryptographic schemes and multilayered security frameworks to improve both security and usability.

3.1.22 Privacy-Enhancing Technologies for Blockchain Compliance

Privacy-enhancing technologies (PETs) such as Zero-Knowledge Proofs (ZKPs) and multiparty computations (MPCs) are analyzed for their roles in balancing blockchain privacy with regulatory compliance [41]. While ZKPs and MPCs face computational and communication challenges, researchers suggest optimizing cryptographic methods and employing AI for bias detection. This study further proposes a tiered privacy approach for improved efficiency and compliance.

3.1.23 Security and Privacy Challenges in Digital Currencies

This chapter examines security and privacy challenges in digital currencies, focusing on blockchain's security features like cryptographic hashing, decentralized consensus, and immutability. While these features enhance security, vulnerabilities persist. Case studies like Mt. Gox and the DAO attack [42] illustrate these risks and countermeasures like multi-signature and hardware wallets. Privacy concerns center on pseudonymity and blockchain forensics, with coins like Monero and Zcash enhancing anonymity through ring signatures and zero-knowledge proofs. Regulatory tensions balance privacy with compliance under AML and KYC laws, impacting the digital currency ecosystem.

3.1.24 Vulnerabilities in Cryptocurrency Wallets

A study on cryptocurrency wallet vulnerabilities categorizes attack vectors into six areas: memory/storage, operating systems, software, networks, blockchain protocols, and others (43]. It reveals a gap between available countermeasures and their adoption, highlighting existing threats, proposing mitigation strategies, and suggesting future research directions to enhance wallet security.

3.1.25 Global Adoption and Security Challenges of Blockchain

The rise of blockchain and cryptocurrency is reviewed, emphasizing decentralized finance benefits and global adoption efforts [44]. The study analyzes security challenges, regulatory limitations, and varying national stances—some countries ban cryptocurrencies while others embrace them as secure payment methods. It compares cryptocurrency security with traditional systems and proposes solutions for security concerns while exploring the future of adoption.

3.1.26 Challenges of Traditional KYC/AML in the Crypto Era

Traditional KYC/AML practices face challenges balancing efficiency, innovation, financial inclusion, and compliance [45]. This chapter examines how cryptocurrency transactions and digital identity affect these regulations, particularly for the unbanked. It concludes by exploring new KYC/AML approaches and technological innovations to address these challenges.

3.1.27 Protocol Design for Secure Cryptocurrency Wallets

Addressing cryptocurrency wallet vulnerabilities, this study proposes a key protocol design to enhance transaction security and user privacy [46]. Integrating a session key for blockchain data and using the Federated Byzantine Agreement for secure key exchange, the protocol

demonstrates optimal security with improved computation costs. It's applicable beyond decentralized exchanges, strengthening distributed network security.

3.1.28 Defense-in-Depth Architecture for Private Key Protection

Protecting private keys in cryptocurrency wallets is tackled through a multilayered Defense-in-Depth architecture [47]. The design uses three restricted layers with distinct protection mechanisms to prevent a single breach from compromising the entire fund and allow quick user responses. A proof-of-concept on smart card hardware and Android wallets showed no performance penalty, with security analyzed using two adversary models.

3.1.29 Hot and Cold Wallets for Mobile Transactions

Digital wallets are categorized into hot (online) and cold (offline) wallets, with efficiency being key for mobile transactions due to speed and security [48]. These wallets reduce costs compared to traditional methods, driving demand through peer-to-peer transactions without third parties. The chapter also addresses rising security concerns, current market status, and future improvement prospects.

3.1.30 Global Regulatory Reactions to Cryptocurrencies

Cryptocurrency, a global fintech innovation, evokes mixed reactions from central banks and governments [49]. While China bans virtual currencies, Japan legalizes them as payment methods. Cryptocurrencies rely on cryptographic security and decentralized blockchain ledgers maintained by global volunteers. The mining process adds transactions, creating new currency units, and poses unique regulatory challenges for central banks.

3.1.31 Bitcoin Price Influences and Policy Impacts

Factors influencing Bitcoin's high price and governmental policy impacts on the crypto market are explored [50]. The paper examines U.S., European, Chinese, and Salvadoran policies, analyzing their effects on Bitcoin's price. It concludes that Bitcoin’s price may decrease regardless of policy support or restrictions.

3.1.32 Terrorist Financing and Hybrid Regulation Approaches

The misuse of cryptocurrencies by terrorist groups and criminal syndicates for financing illicit activities is discussed [51]. Countries respond with varying regulations—China bans virtual assets, while others regulate. Pakistan’s ban cites concerns over tax evasion and cybercrimes, but the paper suggests a hybrid regulatory approach to balance risks and benefits, advocating for cautious, long-term planning.

3.1.33 Cryptocurrency and AML Challenges

Cryptocurrencies' role in money laundering, due to their decentralized and pseudonymous nature, poses challenges for AML efforts [52]. This paper highlights these issues, using Liberty Reserve as a case study to illustrate how criminals bypass traditional AML measures.

3.1.34 Hyperledger Fabric for Optimized KYC

Optimizing the traditional KYC process using a Hyperledger Fabric network is proposed to address security and cost inefficiencies [53]. Tested with Hyperledger Composer, the system accelerates KYC transfers, reduces redundancies, secures data sharing, lowers costs, and enhances transparency.

The existing literature has identified challenges and potential solutions, but further research is required to integrate these elements within crypto-wallets. Our paper aims to fill this gap by proposing a solution that ensures compliance with regulatory requirements while enhancing security against money laundering and terrorism funding, preserving the user experience, and maintaining the core principles of cryptocurrency.

3.2 Systematic literature review

Ref	Findings	Features	Limitations
[16] Amsyar et al. (2020)	Highlights challenges of cryptocurrency adoption, including regulatory gaps and illicit activities.	Systematic review of crypto risks, focus on decentralization and anonymity.	Lacks technical solutions for compliance.
[55] Rezaeighaleh et al. (2020)	Proposes multi layered defense architecture for crypto wallets.	Multi-layer cryptography, secure key storage, transaction monitoring.	No integration of biometric authentication or NFC-based verification.
[56] Hughes & Middlebrook (2015)	Advocates for Article 4A UCC as a regulatory model for crypto exchanges.	Legal framework for Defining rights/ liabilities of crypto users.	Overlooks technical integration with wallets; theoretical focus.
[57] He et al. (2018)	Social-network-based wallet management for	Semi-trusted social networks, shared	Limited privacy enhancements; no

	collaborative recovery.	wallet control.	KYC/AML integration.
[58] Moreno et al. (2021)	Surveys KYC/AML methods for crypto transactions.	Hardware wallets with digital certificates, risk-based transaction limits.	Relies on physical hardware; lacks biometric verification.
[59] Togggle KYC (2024)	Token-based KYC verification for crypto wallets.	Simplified identity verification using tokens.	Tokenization compromises privacy; no homomorphic encryption support.
[60][61] MiCA (2024)	EU's Markets in Crypto-Assets regulation framework.	FATF-aligned AML standards, consumer protection mechanisms.	Rigid structure; lacks adaptability to non-EU jurisdictions.
[62] Barbereau & Bodó (2023)	Proposes copyright law for regulating noncustodial wallets.	Principles-based framework for secondary liability.	Limited technical implementation guidance.
[63] Perlman (2019)	Model crypto-asset framework to avoid regulatory arbitrage.	Categorizes cryptoassets, assigns regulators.	Does not address wallet-level compliance mechanisms.
[64] Hou et al.	Stochastic volatility	Correlated jump	Focuses on finance,

(2020)	model for pricing crypto options.	model for volatility prediction.	not compliance or wallet design.
[65] Guan et al. (2020)	Privacy-preserving crypto transactions using zk-SNARKs.	Zero-knowledge proofs for transaction anonymity.	High computational overhead; no KYC integration.
[66] Villanueva Collao et al. (2024)	Decentralized finance (DeFi) compliance protocols.	Automated AML checks via smart contracts.	Limited scalability for cross-border transactions.

Chapter Four: Methodology

Methodology

4.1 Proposed Crypto-Wallet Scheme

This section introduces a centrally governed cryptocurrency wallet solution, offering an innovative approach to integrating cryptocurrencies into existing financial infrastructures. It emphasizes a hybrid model that merges decentralized cryptocurrencies with the necessary oversight and regulation, ensuring compliance without sacrificing the core benefits of digital assets. The system is designed to balance the needs of consumers, financial institutions, governments, and regulatory bodies, facilitating cryptocurrency adoption while maintaining control over illicit activities.

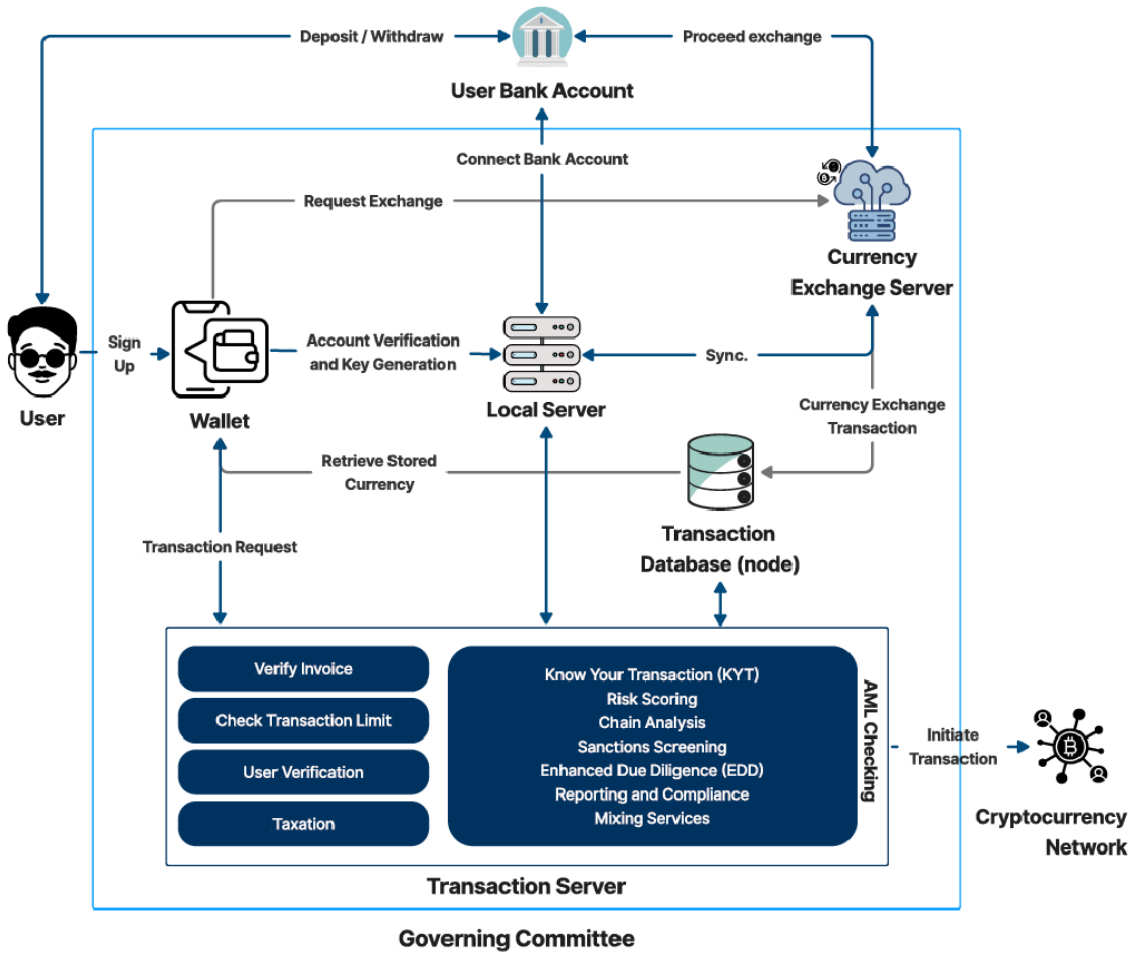


Figure 1: Proposed System

4.2 Crypto-Wallet Entities

The proposed cryptocurrency wallet system consists of multiple interconnected entities, each playing a crucial role in ensuring secure, compliant, and efficient transactions. These entities collaborate to establish a regulated and user-friendly digital asset management framework. The key entities involved in the system are as follows:

4.2.1 User

The User is the primary entity interacting with the wallet system. They initiate all actions, including account registration, cryptocurrency transactions, and currency exchanges. To ensure regulatory compliance and security, users must complete a comprehensive verification process, which includes identity authentication and bank account linking. Users are responsible for managing their digital assets securely, following system policies, and complying with regulatory guidelines.

4.2.2 Crypto-Wallet

The Crypto-Wallet is a software-based application that serves as the user interface for managing digital assets. It enables users to store, send, receive, and exchange cryptocurrency while ensuring security through advanced authentication mechanisms. The wallet requires an NFC-enabled device for authentication and transaction approvals. Unlike traditional wallets, the proposed solution offers a hybrid model, combining user control over private keys with centralized oversight for compliance and fraud prevention.

4.2.3 Account Setup and Authentication

The account creation process in the proposed system follows a multi-layered authentication mechanism to prevent unauthorized access. The setup involves:

- **Device and Document Requirements:** Users must possess an NFC-enabled device and a Machine-Readable Passport (MRP) for identity verification.
- **Three-Tier Verification Process:**
    - **KYC (Know Your Customer) Verification:** Ensures legitimacy through identity proof and government-issued documents.
    - **NFC Verification:** Users scan the NFC chip embedded in their passport to match their digital signature against official records.
    - **Biometric Authentication:** Users complete a facial scan, which is verified against government records using Application Programming Interfaces (APIs).
- **Key Generation & Secure Storage:** Upon successful verification, the system generates private and public keys, a unique wallet address, and securely stores the encrypted keys

locally. A Key Management System (KMS) server further ensures security by generating mnemonic keys linked to the database records.

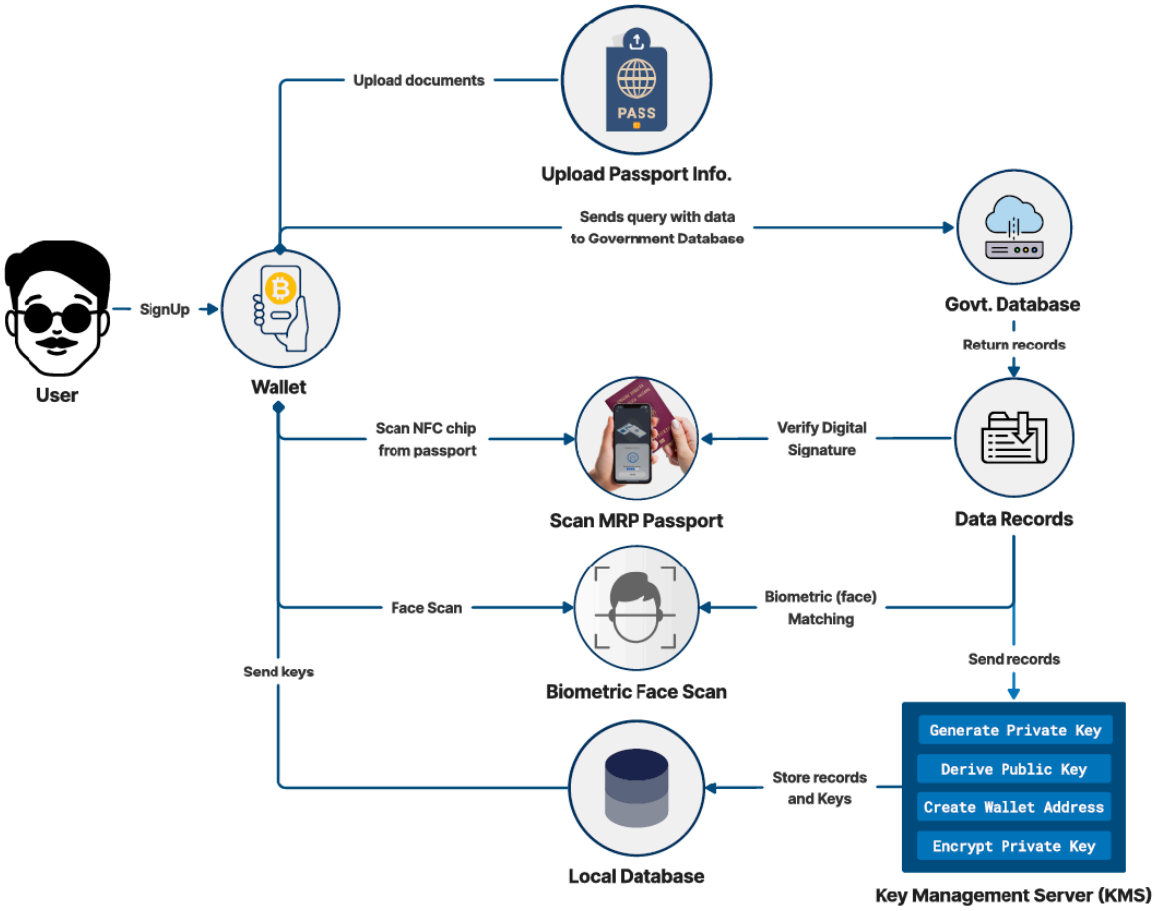


Figure 2: Authentication Server - Account Creation

4.2.4 Local Server

The Local Server functions as the centralized repository for storing user information, including account details, verification status, linked bank accounts, and authentication logs. This server is responsible for initial user authentication, data encryption, and secure communication between different system components.

4.2.5 Transaction Server

The Transaction Server processes and verifies all incoming and outgoing transactions by performing the following functions:

- **Invoice and Transaction Verification:** Confirms the authenticity of fund transfers and detects anomalies.

- **Risk Scoring and Fraud Detection:** Implements Know Your Transaction (KYT), Enhanced Due Diligence (EDD), and chain analysis to prevent money laundering.
- **Regulatory Compliance Checks:** Screens transactions against sanctions lists, tax policies, and AML (Anti-Money Laundering) regulations.
- **Transaction Execution:** Once verification is complete, the server submits the cryptocurrency transaction to the blockchain network for processing and provides real-time feedback to the user.

4.2.6 Transaction Database

The Transaction Database maintains a secure and immutable record of all executed transactions, ensuring compliance and traceability. It serves as:

- A storage system for exchange transactions, fund transfers, and receipts.
- A node in the cryptocurrency network, facilitating real-time transaction validation and audit logging.

4.2.7 Exchange Server

The Exchange Server acts as a bridge between fiat currency and cryptocurrency. It processes exchange requests initiated by users and enables seamless conversion between traditional bank accounts and digital wallets. Functions of the Exchange Server include:

- **Currency Exchange:** Allows users to convert fiat currency (e.g., USD, EUR) into cryptocurrency and vice versa.
- **Real-Time Rate Calculation:** Retrieves live exchange rates and applies conversion fees.
- **Bank Integration:** Facilitates transactions between users' bank accounts and their crypto wallets.

4.2.8 Cryptocurrency Network

The Cryptocurrency Network represents the external blockchain infrastructure responsible for processing and validating transactions. It ensures that:

- Transactions are securely recorded on the blockchain following consensus protocols.
- The system maintains transparency, immutability, and decentralized verification.

4.2.9 Central Governing Committee (CGC)

The Central Governing Committee (CGC) is a regulatory authority that oversees the entire cryptocurrency wallet system. Its responsibilities include:

- **Monitoring Transactions and User Activities:** Ensuring compliance with financial regulations, AML laws, and tax policies.
- **Setting Transaction Policies:** Defining rules such as transaction limits, exchange policies, and risk thresholds.
- **Overseeing Security Measures:** Enforcing security protocols such as NFC authentication, biometric verification, and fraud prevention mechanisms.
- **Maintaining System Integrity:** Continuously auditing the transaction server, wallet database, and exchange server to detect and mitigate potential risks.

The proposed cryptocurrency wallet system integrates multiple layers of security, verification, and compliance measures to establish a robust and regulated digital asset management platform. By leveraging advanced cryptographic protocols, multi-factor authentication, and centralized oversight, the system ensures secure, compliant, and scalable transactions.

Each entity within the system plays a critical role in ensuring:

- User authentication and fraud prevention
- Regulatory compliance and AML enforcement
- Seamless cryptocurrency and fiat currency exchanges
- Transparent and auditable transaction processing

By implementing this architecture, the system bridges the gap between the decentralized nature of cryptocurrencies and the regulatory requirements of financial institutions and governments.

4.3 Privacy Mechanisms

The Privacy Mechanisms of the proposed cryptocurrency wallet system integrate advanced cryptographic techniques to ensure secure and regulatory-compliant transactions while preserving user confidentiality. Homomorphic encryption allows sensitive data, such as transaction details and risk scores, to be processed without being decrypted, ensuring privacy while maintaining system functionality. Zero-Knowledge Proofs (ZKPs) enable users to authenticate their identity and prove adherence to Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations without exposing private information. Additionally, the system employs multi-layered encryption protocols, including end-to-end encryption and secure key storage via a centralized Key Management System (KMS), to protect cryptographic keys and prevent unauthorized access. Mandatory biometric authentication, combined with Near Field Communication (NFC)-based verification, further strengthens user identity protection, reducing the risk of fraud and identity theft. These privacy measures not only safeguard user data but also ensure compliance with international regulatory frameworks, enhancing the system's security, scalability, and trustworthiness in financial transactions.

4.4 Workflow Sequence

This workflow sequence outlines the interactions between different entities in the system, including new and verified users, the wallet application, wallet servers, authorized banks, and the cryptocurrency network. The system ensures security, regulatory compliance, and efficient transaction management through a structured series of steps.

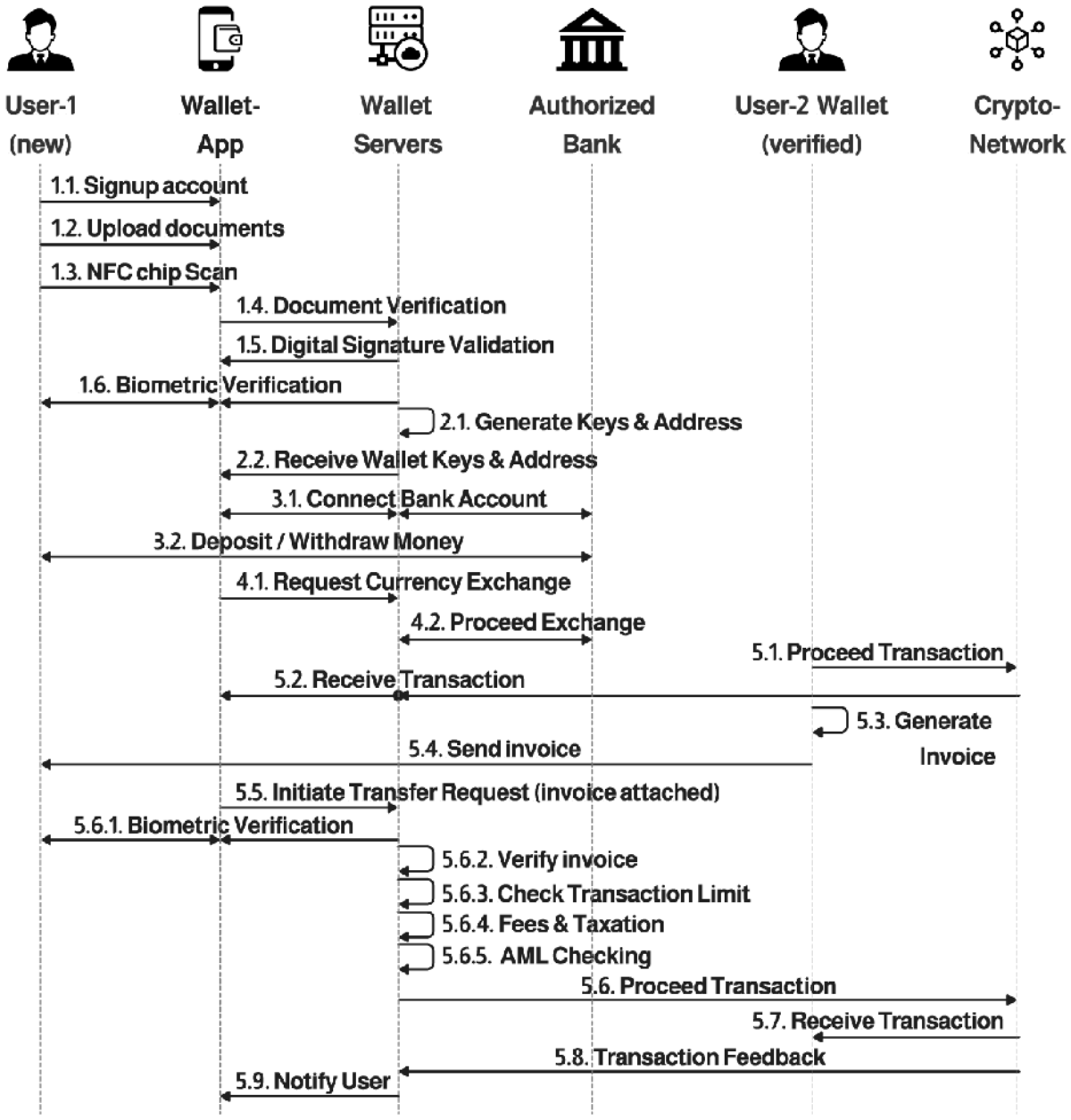


Figure 3:Workflow Sequence

4.4.1 User Registration and KYC Verification

The process begins when a new user registers for an account within the wallet application. This involves:

- **Step 1.1:** The user signs up for an account by providing basic details.
- **Step 1.2:** The user uploads identity documents for verification in accordance with Know Your Customer (KYC) requirements.
- **Step 1.3:** The system scans the NFC chip in the user's government-issued identity card to extract identity details securely.

Once the documents are uploaded, the system performs several verification steps:

- **Step 1.4:** The uploaded documents undergo verification against authoritative sources to ensure authenticity.
- **Step 1.5:** The system validates the digital signature present on the documents, ensuring they have not been tampered with.
- **Step 1.6:** The system conducts biometric verification using government APIs to confirm the user's identity, adding an extra layer of security.

4.4.2 Wallet Creation and Key Generation

Upon successful verification of identity:

- **Step 2.1:** The system generates unique cryptographic wallet keys and assigns a wallet address to the user.
- **Step 2.2:** The generated wallet credentials are securely provided to the user, enabling them to engage in financial transactions within the system.

4.4.3 Bank Account Integration and Fund Management

To facilitate seamless deposits and withdrawals:

- **Step 3.1:** The user links their bank account to their cryptocurrency wallet. This step ensures that fiat-to-crypto transactions can be conducted in compliance with financial regulations.
- **Step 3.2:** The user can now deposit or withdraw money between their bank account and the crypto wallet, enhancing liquidity and accessibility.

4.4.4 Currency Exchange Process

Once the user’s account is fully set up and verified, they can:

- **Step 4.1:** Request a currency exchange within the wallet application, allowing them to convert fiat currency to cryptocurrency or vice versa.

- **Step 4.2:** The system processes the exchange request by connecting with financial institutions and cryptocurrency exchanges, ensuring fair conversion rates and compliance with anti-money laundering (AML) policies.

4.4.5 Transaction Management and Compliance Checks

Users can send and receive funds through a structured transaction process:

- **Step 5.1:** A verified user initiates a transaction request, instructing the system to proceed with fund transfers.
- **Step 5.2:** The system processes the incoming transaction, ensuring that funds are securely delivered to the recipient's wallet.
- **Step 5.3:** The system generates an invoice, which serves as proof of transaction and ensures transparency.
- **Step 5.4:** The invoice is sent to the receiving party for verification. To complete the transaction, the system performs multiple compliance checks:
- **Step 5.5:** The sender must initiate a transfer request, attaching the invoice as proof.
- **Step 5.6.1:** The system conducts biometric verification of the sender to prevent unauthorized transactions.
- **Step 5.6.2:** The system verifies the invoice details, ensuring consistency between the sender's intent and the recipient's wallet address.
- **Step 5.6.3:** The system checks whether the transaction adheres to predefined limits set by regulatory authorities.
- **Step 5.6.4:** Fee and taxation calculations are performed in accordance with jurisdictional requirements.
- **Step 5.6.5:** AML screening is carried out to prevent fraudulent activities such as money laundering or terrorism financing.
- **Step 5.6:** Once all checks are successfully completed, the system proceeds with the transaction.

4.4.6 Transaction Finalization and User Notification

- **Step 5.7:** The recipient's wallet receives the funds after successful validation.
- **Step 5.8:** The system processes transaction feedback, ensuring that any discrepancies or failures are reported to the appropriate parties.
- **Step 5.9:** The user is notified of the transaction completion, providing a detailed breakdown of the exchange.

Chapter Five

Implementation

5.1 Algorithms

The proposed cryptocurrency wallet system aims to provide secure and efficient transaction management through a multi-server architecture, which facilitates user transactions, currency exchange with banks, and compliance with cryptocurrency regulations through a central governing committee. This prototype focuses on the implementation of two key algorithms responsible for managing user accounts, currency exchanges, and cryptocurrency transactions. These algorithms ensure secure registration, verification, and transaction processes.

Algorithm 1 Account Creation

```
1:  function CREATEACCOUNT(email)
2:      user ← SignUp(email)
3:      if not VerifyEmail(user.email) then
4:          return failure
5:      end if
6:      userInfo ← CollectUserInfo(user)
7:      govRecord ← QueryGovernmentDB(userInfo)
8:      if govRecord = null then
9:          return failure
10:     end if
11:     nfcData ← ScanPassportNFC()
12:     if not MatchDigitalSignature(govRecord, nfcData)
        then return failure
13:     end if
14:     faceData ← ScanUserFace()
15:     if not MatchBiometrics(govRecord, faceData) then
16:         return failure
17:     end if
18:     SendToKMSServer(userInfo, govRecord)
19:     privateKey ← GeneratePrivateKey()
20:     publicKey ← DerivePublicKey(privateKey)
21:     walletAddress ← GenerateWalletAddress(publicKey)
        mnemonicKeys ← GenerateMnemonicKeys()
22:     localDatabase ← EncryptedData(user, privateKey,
        publicKey, walletAddress)
23:     User ← mnemonicKeys return success
```

24: **end function**

The Account Creation algorithm initiates when a user provides an email address. The process starts by verifying the email and collecting user information. The QueryGovernmentDB function ensures that the information is valid by cross-referencing with a government database. Once verified, the system performs additional security checks using NFC and biometric scanning. The user's facial recognition data is matched against government records. Upon successful verification, elliptic curve cryptography is used to generate a private key and public key, which are used to create a wallet address. The keys are then stored in the local database, which is encrypted using homomorphic encryption for added security. Finally, mnemonic keys are generated for the user, and the account creation process is complete, ensuring a secure setup for cryptocurrency transactions.

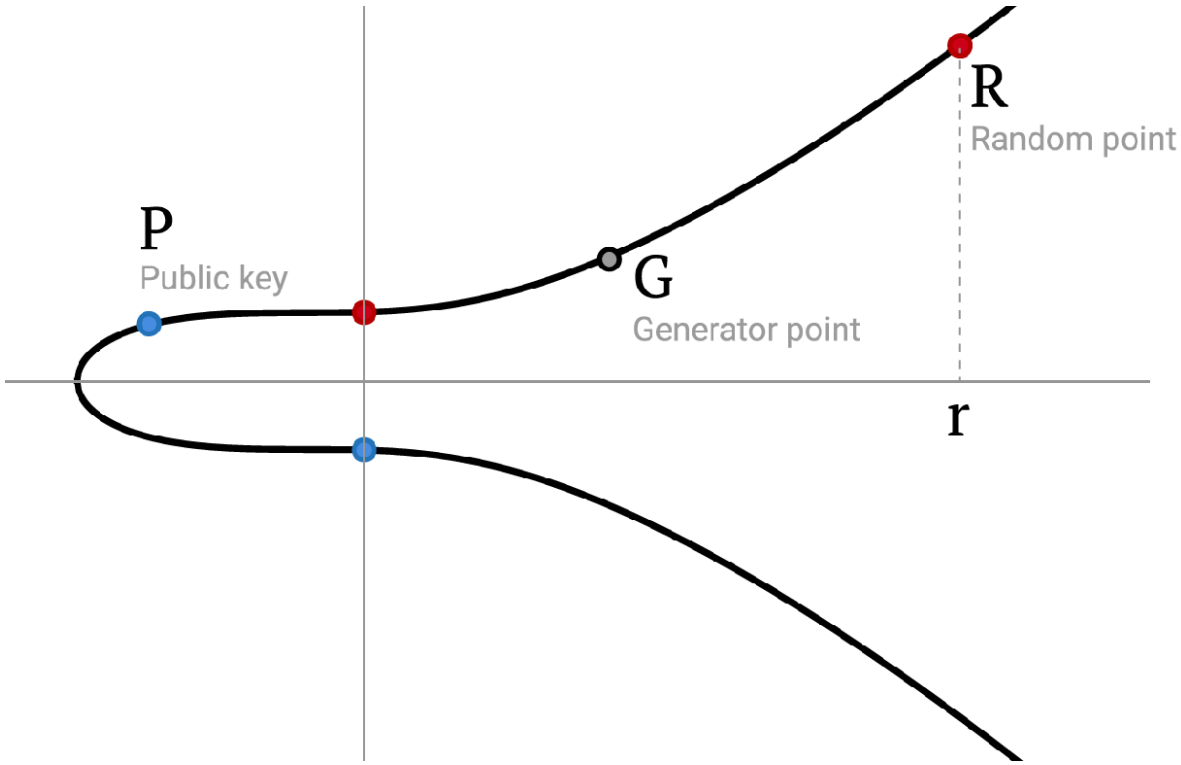


Figure 4 : Elliptic Curve

This figure illustrates the Elliptic Curve Cryptography (ECC) mechanism used for secure key generation within our prototype implementation. ECC is essential for creating robust cryptographic keys that underpin the wallet's security framework. By generating a pair of keys (private and public) using ECC, the system ensures that each user's wallet is uniquely secured and capable of signing transactions reliably. The implementation of ECC in our account creation algorithm not only enhances security with smaller key sizes and faster computation but also ensures that all transactions are verifiably authentic and resistant to unauthorized access. This

integration of ECC underscores our commitment to employing advanced cryptographic standards to safeguard digital assets.

Algorithm 2 ML-Integrated Transaction Validation Process

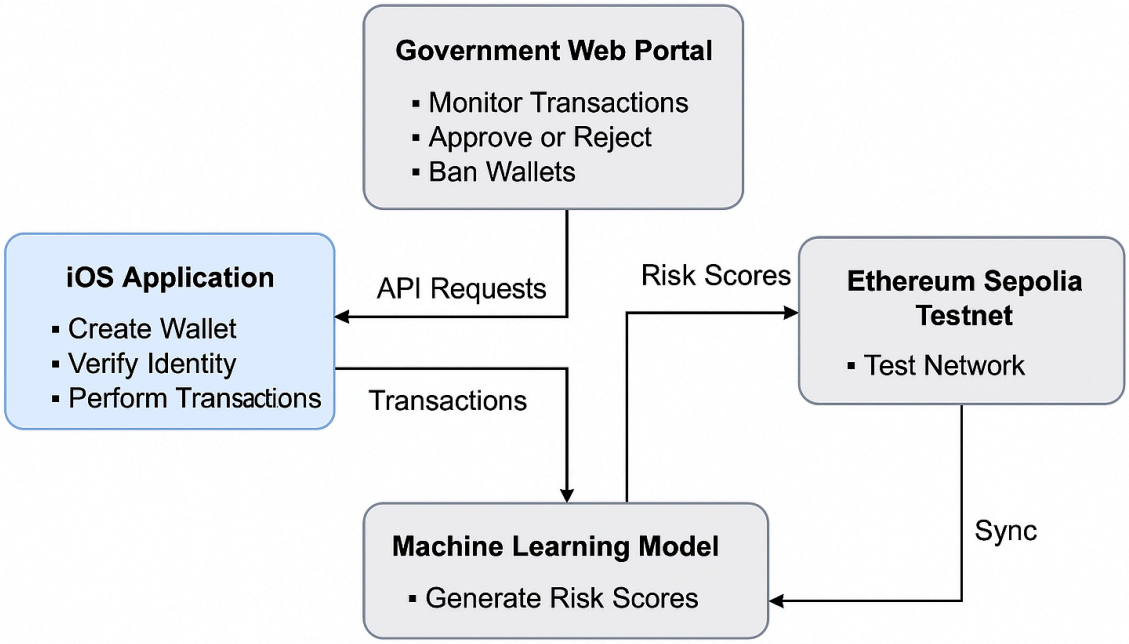
```
1:  function SMARTTRANSACTION(user, bankAccount, amount, targetCurrency, txnInfo)
2:      if not IsAccountVerified(user) then
3:          return failure
4:      end if
5:      if not IsBankAccountConnected(user, bankAccount) then
6:          ConnectBankAccount(user, bankAccount)
7:      end if
8:      features ← ExtractFeatures(txnInfo, user)
9:      riskModel ← LoadTrainedModel("risk_model.joblib")
10:     score, prediction ← PredictRisk(riskModel, features)
11:     if score ≥ riskThreshold then
12:         FlagTransaction(txnInfo, score)
13:         return blocked_due_to_risk
14:     end if
15:     request ← CreateExchangeRequest(user, amount, fromCurrency, toCurrency)
16:     result ← ProcessExchange(request)
17:     if result.success then
18:         UpdateUserBalance(user, result.newBalance)
19:         RecordTransaction(user, result)
20:     else
21:         return failure
22:     end if
23:     receiveTxn ← ReceiveTxn(walletAddress)
24:     if receiveTxn then
25:         UpdateTxnDB(user, txnInfo, txnResult)
26:     else
27:         return failure
28:     end if
29:     invoiceVerified ← VerifyInvoice(txnInfo.invoice)
30:     if not invoiceVerified then
31:         return failure
32:     end if
33:     return success
```

Algorithm 2 outlines a secure, AI-enhanced transaction workflow that integrates identity verification, banking validation, and machine learning–based risk scoring to ensure regulatory compliance within the KYC-driven crypto wallet. It begins by checking whether the user's identity and bank account are verified. Once verified, transaction metadata—such as amount,

user behavior history, biometric/NFC status, and recipient credibility—is extracted and fed into a trained Random Forest model. If the predicted risk score exceeds a predefined threshold (e.g., 0.70), the transaction is flagged and blocked. If deemed safe, the system creates an exchange request, processes the transaction through the backend, updates the user's balance, and logs the event. It then verifies if the transaction has reached the wallet and ensures the invoice is legitimate before confirming success. This algorithm strengthens anti-money laundering (AML) measures by embedding real-time predictive intelligence within the transaction flow, offering a layered and automated approach to fraud prevention in digital financial systems.

5.2 System Architecture Overview

The iOS application serves as the primary user interface within a three-component government-compliant cryptocurrency wallet ecosystem. The application integrates with multiple external systems to ensure regulatory compliance while maintaining user accessibility and security.



5.3 iOS Application

5.3.1 SwiftUI Framework Implementation

SwiftUI serves as the primary user interface framework, providing declarative interface development that ensures consistency and maintainability across all application screens. The framework's reactive programming model aligns perfectly with the real-time nature of cryptocurrency transactions and compliance monitoring. The declarative syntax enables clear

expression of user interface requirements while automatically handling state management complexities. This proves particularly valuable for displaying dynamic transaction status, real-time balance updates, and compliance approval workflows that require immediate user feedback.

SwiftUI's built-in accessibility features ensure that the application meets government accessibility requirements without requiring extensive additional development. NFC support, Camera support, dynamic type scaling, and high contrast modes are automatically implemented across all interface elements. The framework's animation capabilities provide smooth user experience transitions during critical workflows including biometric verification, transaction submission, and document scanning processes. These animations guide users through complex procedures while maintaining engagement and reducing cognitive load. State management in SwiftUI utilizes @State, @StateObject, and @ObservedObject property wrappers that automatically update interface elements when underlying data changes. This reactive approach ensures that transaction status, verification progress, and compliance updates appear immediately without requiring manual interface refresh operations.

5.3.2 Wallet Creation & Restoration

The application implements two distinct user pathways to accommodate both new users requiring full verification and returning users with existing credentials.

```swift
import Foundation
import BigInt
import CryptoSwift
import CryptoKit
import secp256k1

class EthereumWallet: ObservableObject {
    @Published var address: String = ""
    @Published var balance: String = "0"
    @Published var isLoading: Bool = false
    @Published var errorMessage: String = ""
    @Published var privateKeyHex: String = ""
    @Published var fetchedTransactions: [TransactionItem] = []

    private var privateKey: Data?
    private let rpcURL = "https://sepolia.infura.io/v3/5c13cec41a9d4475bdd2c744a636a822"
    private let etherscanApiKey = "EM9MKXCQRUMVU37HKXFCU8679QNP4PWHVQ"

    init() { ••• }

    static let secpContext: OpaquePointer = {
        secp256k1_context_create(UInt32(SECP256K1_CONTEXT_SIGN | SECP256K1_CONTEXT_VERIFY))
    }()

    func createWallet(from mnemonic: String, passphrase: String = "") {
        let seed = seedFrom(mnemonic: mnemonic, passphrase: passphrase)
        let privKey = deriveEthPrivateKey(from: seed)
        self.privateKey = privKey
        self.privateKeyHex = privKey.toHexString()
        self.address = generateAddress(from: privKey)
    }


    func importWallet(from mnemonic: String, passphrase: String = "") throws {
        let words = mnemonic.trimmingCharacters(in: .whitespacesAndNewlines).lowercased().components(separatedBy: .whitespaces).filter { !$0.isEmpty }

        guard words.count == 12 || words.count == 24 else {
            throw WalletImportError.invalidWordCount
        }
        guard Bip39.basicValidate(mnemonic: words) else {
            throw WalletImportError.invalidWordList
        }

        let seed = seedFrom(mnemonic: words.joined(separator: " "), passphrase: passphrase)
        let priv = deriveEthPrivateKey(from: seed)
        let addr = generateAddress(from: priv)
    }
```

5.3.3 Biometric Face ID Verification with Persona

To verify user identity, the app integrates the PersonaInquirySDK2, allowing users to complete live biometric facial verification. Once initiated, the SDK presents a native flow to capture a selfie and match it against uploaded ID documents. The results are returned securely via delegate callbacks, ensuring compliance with KYC standards.

```swift
class BiometricVerificationManager: ObservableObject {
    @Published var verificationResult: VerificationResult?
    @Published var isVerifying = false

    func startBiometricVerification() {
        isVerifying = true

        let inquiryConfiguration = InquiryConfiguration(
            templateId: Config.personaTemplateId
        )

        inquiryConfiguration.theme = InquiryTheme()
        inquiryConfiguration.theme?.accentColor = UIColor.systemBlue

        let inquiry = Inquiry(config: inquiryConfiguration)

        inquiry.onComplete = { [weak self] inquiryId, status, fields in
            DispatchQueue.main.async {
                self?.handleVerificationComplete(inquiryId, status, fields)
            }
        }

        inquiry.onError = { [weak self] error in
            DispatchQueue.main.async {
                self?.handleVerificationError(error)
            }
        }

        inquiry.start(from: UIApplication.shared.windows.first?.rootViewController)
    }

    private func handleVerificationComplete(_ inquiryId: String, _ status: InquiryStatus, _ fields: [String: Any]) {
        isVerifying = false

        switch status {
        case .completed:
            verificationResult = .success(inquiryId: inquiryId)
            syncVerificationWithBackend(inquiryId, fields)
        case .failed:
            verificationResult = .failed(reason: "Verification failed")
        default:
            verificationResult = .pending
        }
    }

    private func syncVerificationWithBackend(_ inquiryId: String, _ fields: [String: Any]) { ••• }
}
```

5.3.4 Document Verification with NFC

The application supports NFC-based document authentication for ePassports. It uses Apple's `CoreNFC` framework to scan the Machine Readable Zone (MRZ) and read data from the embedded NFC chip. The chip's digital signature is validated on-device to ensure the document's authenticity and integrity, enhancing the security of identity verification.

```swift
import CoreNFC

class NFCVerificationManager: NSObject, ObservableObject {
    @Published var verificationStatus: NFCVerificationStatus = .idle
    @Published var documentData: DocumentData?

    private var readerSession: NFCTagReaderSession?

    func startNFCVerification() { ••• }
}

extension NFCVerificationManager: NFCTagReaderSessionDelegate {
    func tagReaderSession(_ session: NFCTagReaderSession, didDetect tags: [NFCTag]) {
        guard let tag = tags.first else { return }
        session.connect(to: tag) { error in
            if let error = error {
                session.invalidate(errorMessage: "Connection failed: \(error.localizedDescription)")
                return
            }
            self.readDocumentData(from: tag, session: session)
        }
    }

    private func readDocumentData(from tag: NFCTag, session: NFCTagReaderSession) {
        guard case let .iso7816(iso7816Tag) = tag else {
            session.invalidate(errorMessage: "Unsupported tag type")
            return
        }
        let selectCommand = NFCISO7816APDU( ••• )
        iso7816Tag.sendCommand(apdu: selectCommand) { data, sw1, sw2, error in
            if let error = error {
                session.invalidate(errorMessage: "Failed to select application: \(error.localizedDescription)")
                return
            }
            guard sw1 == 0x90 && sw2 == 0x00 else {
                session.invalidate(errorMessage: "Document selection failed")
                return
            }
            self.performBasicAccessControl(iso7816Tag, session)
        }
    }

    private func performBasicAccessControl(_ tag: NFCISO7816Tag, _ session: NFCTagReaderSession) { ••• }

    private func readDataGroup1(_ tag: NFCISO7816Tag, _ session: NFCTagReaderSession) { ••• }

    private func processDocumentData(_ data: Data) { ••• }
}
```

5.3.5 Mnemonic Key Generation with BIP39

The wallet uses a 12-word mnemonic phrase conforming to the BIP39 standard for deterministic key generation. In this process, a secure random seed is generated using strong cryptographic algorithms, ensuring high entropy and resistance to brute-force attacks. This seed is then mapped to a predefined wordlist consisting of 2048 unique words, carefully selected to minimize confusion and enhance memorability. The resultant mnemonic phrase enables users to back up and recover their wallets effortlessly, providing an intuitive method for key restoration even in the event of device loss or failure. This approach ensures both accessibility and robust security, as the mnemonic can regenerate the same cryptographic keys without storing sensitive information directly on the device. Additionally, users are encouraged to store their mnemonic phrases securely, as possession of this phrase equates to full access to the associated wallet and funds.

```swift
class BIP39Manager {
    static let wordlist = loadWordlist()

    static func validateMnemonic(_ mnemonic: String) -> Bool {
        let words = mnemonic.trimmingCharacters(in: .whitespacesAndNewlines)
            .components(separatedBy: .whitespaces)

        guard words.count == 12 else { return false }

        guard words.allSatisfy({ wordlist.contains($0) }) else { return false }

        return validateChecksum(words)
    }

    static func mnemonicToSeed(_ mnemonic: String, passphrase: String = "") -> Data {
        let saltString = "mnemonic" + passphrase
        let saltData = saltString.data(using: .utf8)!
        return Data(PBKDF2<SHA512>.deriveKey(
            from: mnemonic.data(using: .utf8)!,
            salt: saltData,
            using: SHA512.self,
            outputByteCount: 64,
            rounds: 2048
        ))
    }

    private static func validateChecksum(_ words: [String]) -> Bool {
        let binaryString = words.compactMap { word in
            guard let index = wordlist.firstIndex(of: word) else { return nil }
            return String(index, radix: 2).leftPadding(toLength: 11, withPad: "0")
        }.joined()

        let entropyBits = String(binaryString.prefix(128))
        let checksumBits = String(binaryString.suffix(4))
        let entropyData = Data(stride(from: 0, to: entropyBits.count, by: 8).map { index in
        let startIndex = entropyBits.index(entropyBits.startIndex, offsetBy: index)
        let endIndex = entropyBits.index(startIndex, offsetBy: 8)
        return UInt8(entropyBits[startIndex..<endIndex], radix: 2)!
        })

        let hash = SHA256.hash(data: entropyData)
        let expectedChecksum = String(hash.first!, radix: 2).prefix(4)

        return checksumBits == expectedChecksum
    }
}
```

5.3.6 Fetch Balance

The current ETH balance is fetched by calling a JSON-RPC method (eth_getBalance) on the Sepolia Ethereum node. The balance is retrieved in Wei and converted into ETH. Additional conversion is performed to show the balance in USD and BDT, offering users localized currency context

5.3.7 Send Transaction

To send ETH, the app builds a raw transaction object containing the nonce, gas limit, recipient, and value. The transaction is hashed and signed locally using the private key via the `secp256k1` library. The signed transaction is then broadcast to the Sepolia testnet using `eth_sendRawTransaction` over JSON-RPC

```
178     func sendTransaction(to: String, amount: String) {
179         guard let privateKey = privateKey else {
180             errorMessage = "Wallet not initialized"
181             return
182         }
183 
184         guard to.hasPrefix("0x") && to.count == 42 else {
185             errorMessage = "Invalid recipient address"
186             return
187         }
188 
189         guard let amountDouble = Double(amount), amountDouble > 0 else {
190             errorMessage = "Invalid amount"
191             return
192         }
193 
194         isLoading = true
195         errorMessage = ""
196 
197         Task {
198             do {
199                 let txHash = try await sendRawTransaction(to: to, amount: amount, privateKey: privateKey)
200                 await MainActor.run {
201                     self.isLoading = false
202                     print("Transaction sent: \(txHash)")
203                     self.getBalance()
204                 }
205             } catch {
206                 await MainActor.run {
207                     self.errorMessage = "Transaction failed: \(error.localizedDescription)"
208                     self.isLoading = false
209                 }
210             }
211         }
212     }
```

5.4 Government Monitoring Web Portal

5.4.1 System Overview and Architecture

This platform is a fullstack application designed to provide secure crypto wallet management, user risk profiling, and compliance monitoring. It comprises two main components: a backend API built with Node.js and Express, and a frontend UI developed with React and Tailwind CSS.

- **Backend Architecture:** The backend interacts with a PostgreSQL database (via Supabase) to store user data, wallets, transactions, and alerts. It exposes RESTful API endpoints secured with authentication tokens, supporting functions such as user management, transaction retrieval, and compliance alert handling.
- **Frontend Architecture:** The frontend is a React-based Single Page Application (SPA) that communicates with the backend via Axios. It features a responsive UI with components for dashboards, user lists, detailed user views, and alerts.
- **External Systems & Dependencies:** The system integrates with Supabase for database management, blockchain explorers for transaction verification, and utilizes Tailwind CSS for styling the interface

```
CryptoCompliance/
├── crypto-compliance-frontend/   # React + Tailwind CSS frontend
│   ├── src/
│   │   ├── pages/                # Dashboard, Users, Alerts, etc.
│   │   ├── components/           # Table, Modal, Badge, NavBar, etc.
│   │   └── services/api.js       # API abstraction (Axios)
│   └── ...
├── crypto-compliance-backend/    # Node.js + Express backend
│   ├── server.js                 # Main server and API routes
│   ├── db.js                     # Supabase client setup
│   └── ...
└── ...
```

5.4.2 Wallet Management & Transaction Monitoring

The platform stores wallet data and transaction histories, with transactions embedded as JSONB arrays in the database.

```
CREATE TABLE wallets (
id SERIAL PRIMARY KEY,
wallet_address VARCHAR(42) UNIQUE,
user_id INTEGER REFERENCES users(id),
transactions JSONB,
invoice_id VARCHAR(64)
);
```

```
// Retrieve transactions for a user
app.get('/api/users/:id/transactions', async (req, res) => {
const { id } = req.params;
const { data } = await supabase
.from('wallets')
.select('transactions')
.eq('user_id', id);
res.json(data);
});
```

5.4.3 Compliance & Monitoring

The system is designed to enhance compliance by continuously monitoring transactions and user activity to generate real-time alerts for suspicious activities, large transactions, or KYC issues. Additionally, it features functionality to freeze or unfreeze user accounts, acting as a compliance measure to restrict access during investigations or violations, with API endpoints for managing freeze status and maintaining an audit trail.

5.4.4 Additional Components & Technical Details

Security, data integrity, and scalability are ensured through strategic architectural choices. Environment variables (.env) manage sensitive information, while API endpoints are safeguarded with token middleware to prevent unauthorized access. CORS is enabled to support seamless frontend-backend communication. Additionally, the modular design emphasizes separation of concerns with dedicated components for user management, transactions, alerts, and API services, promoting scalability and ease of maintenance.

Chapter Six

Result And Discussion

6.1 New User Registration Process

New users begin with document type selection, where they choose from supported identity documents including passports, national identification cards, and driver's licenses. The interface prioritizes passport verification due to its standardized international format and enhanced security features.

Following document selection, users capture a high-quality photograph of their chosen identification document using the device camera. The application implements automatic edge detection and image quality validation to ensure optimal conditions for subsequent verification steps. Image preprocessing includes rotation correction, brightness adjustment, and resolution optimization.

The biometric verification phase requires users to complete a live face scan using the PersonaInquirySDK2 integration. This process captures multiple facial angles and performs liveness detection to prevent spoofing attempts. The SDK handles secure transmission of biometric data to Persona's verification servers while maintaining user privacy through encrypted communication channels.

NFC verification represents the final authentication step for documents equipped with NFC chips. Users position their document against the device's NFC reader, enabling the application to extract machine-readable zone data and validate digital signatures embedded within the document's secure element. This process verifies document authenticity and ensures that the physical document matches the photographed version.

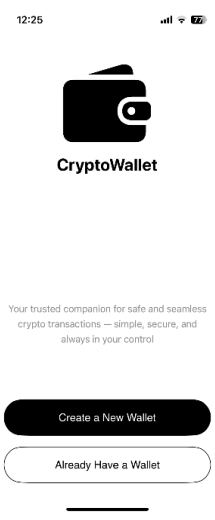
Upon successful verification, the application generates a new Ethereum wallet using cryptographically secure random number generation. The system creates a 12-word BIP39 mnemonic phrase that serves as the master seed for key derivation. Users must manually transcribe and confirm their mnemonic phrase before proceeding, ensuring they understand the critical importance of backup security.

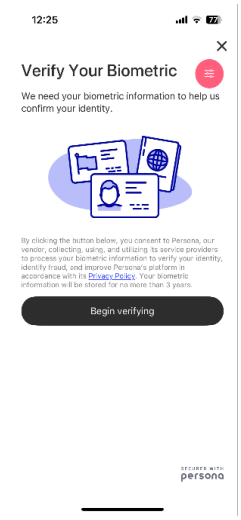
6.2 Returning User Authentication

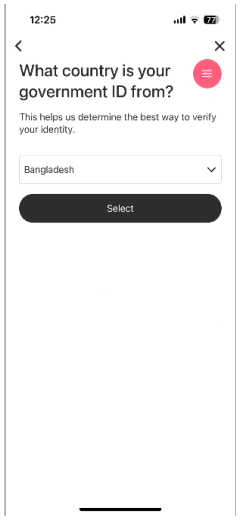
Existing users authenticate by entering their 12-word mnemonic phrase through a secure input interface that obscures individual words until validation. The application derives the corresponding private key using BIP39 and BIP44 derivation paths, enabling access to the previously created wallet without requiring re-verification of identity documents.

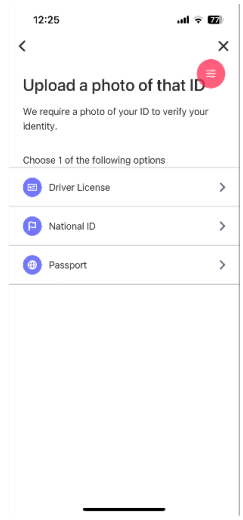
6.3 Biometric Face Verification

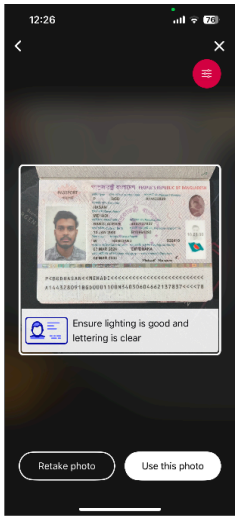
PersonaInquirySDK2 provides the core biometric verification functionality through its comprehensive identity verification platform. The integration involves initializing inquiry

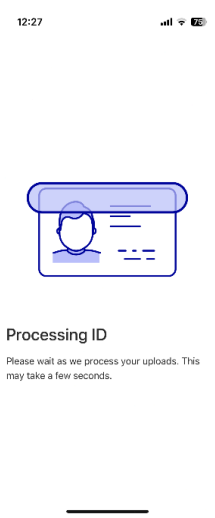

12:25
CryptoWallet
Your trusted companion for safe and seamless crypto transactions — simple, secure, and always in your control
Create a New Wallet
Already Have a Wallet

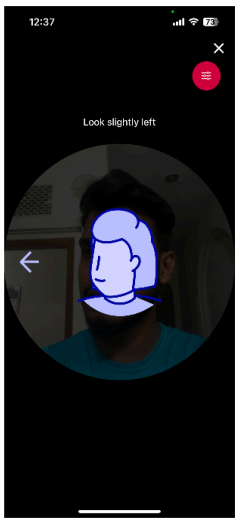

12:25
Verify Your Biometric
We need your biometric information to help us confirm your identity.
Begin verifying


12:25
What country is your government ID from?
This helps us determine the best way to verify your identity.
Bangladesh
Select


12:25
Upload a photo of that ID
We require a photo of your ID to verify your identity.
Choose 1 of the following options
Driver License
National ID
Passport

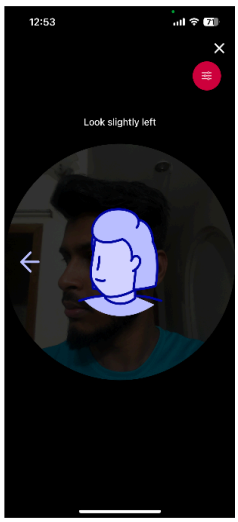

12:26
Ensure lighting is good and lettering is clear
Retake photo
Use this photo

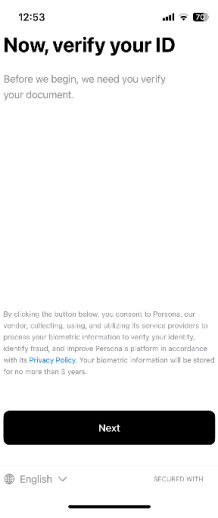

12:27
Processing ID
Please wait as we process your uploads. This may take a few seconds.

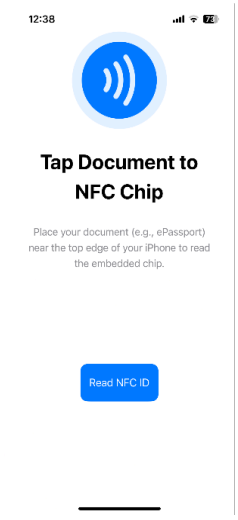

12:37
Look slightly left

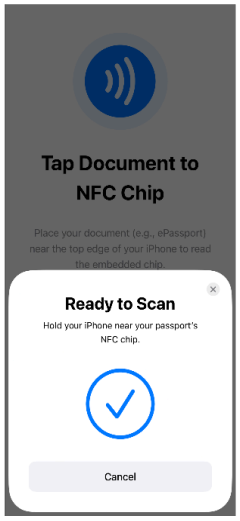

12:38
Hold still...
1


12:38
Look slightly right

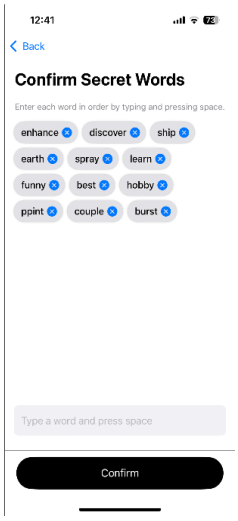

12:53
Look slightly left


12:53
Now, verify your ID
Before we begin, we need you verify your document.
By clicking the button below, you consent to Persona, our vendor, collecting, using, and utilizing its service providers to process your biometric information to verify your identity, identify fraud, and improve Persona's platform in accordance with its Privacy Policy. Your biometric information will be stored for no more than 3 years.
Next
English
SECURED WITH


12:38
Tap Document to NFC Chip
Place your document (e.g., ePassport) near the top edge of your iPhone to read the embedded chip.
Read NFC ID


Tap Document to NFC Chip
Place your document (e.g., ePassport) near the top edge of your iPhone to read the embedded chip.
Ready to Scan
Hold your iPhone near your passport's NFC chip.
Cancel


12:40
Secret Recovery Words
Your Secret Recovery Phrase (SRP) is a unique 12-word phrase that is generated when you first set up Crypee. Your funds are connected to that phrase.
1. enhance
2. discover
3. ship
4. earth
5. spray
6. learn
7. funny
8. best
9. hobby
10. point
11. couple
12. burst
Copy to Clipboard
Ok, I saved


12:41
Back
Confirm Secret Words
Enter each word in order by typing and pressing space.
enhance
discover
ship
earth
spray
learn
funny
best
hobby
ppint
couple
burst
Type a word and press space
Confirm

sessions with specific templates configured for government compliance requirements. The SDK manages the entire verification workflow, including live face capture, comparison against government-issued photo identification, and liveness detection algorithms.

The implementation configures the SDK with custom UI themes matching the application's design language while maintaining security protocols. Verification results include confidence scores, fraud detection flags, and detailed analysis of facial feature matching. These results integrate with the broader compliance system to determine user approval status.

6.4 NFC-Based Document Verification

NFC verification utilizes Core NFC framework capabilities to communicate with electronic passport and identification card chips. The implementation supports ISO 14443 Type A and Type B communication protocols commonly used in government-issued documents.

The verification process begins by establishing secure communication with the document's NFC chip using Basic Access Control (BAC) or Password Authenticated Connection Establishment (PACE) protocols. Authentication keys derive from machine-readable zone data extracted during the document photography phase.

Once authenticated, the application reads DataGroup 1 (containing machine-readable zone information), DataGroup 2 (containing facial image data), and DataGroup 15 (containing public key information for digital signature validation). The system validates document authenticity by verifying digital signatures using public keys from the appropriate country's certificate authority.

6.5 Document Type Support

The application implements specialized handlers for each supported document type. Passport verification follows ICAO Doc 9303 standards, supporting all passport formats compliant with international civil aviation requirements. National ID verification adapts to specific country formats while maintaining consistent security validation procedures. Driver's license verification focuses on jurisdictions with standardized NFC implementation and digital signature capabilities.

6.6 Main Screens & Features Implementation

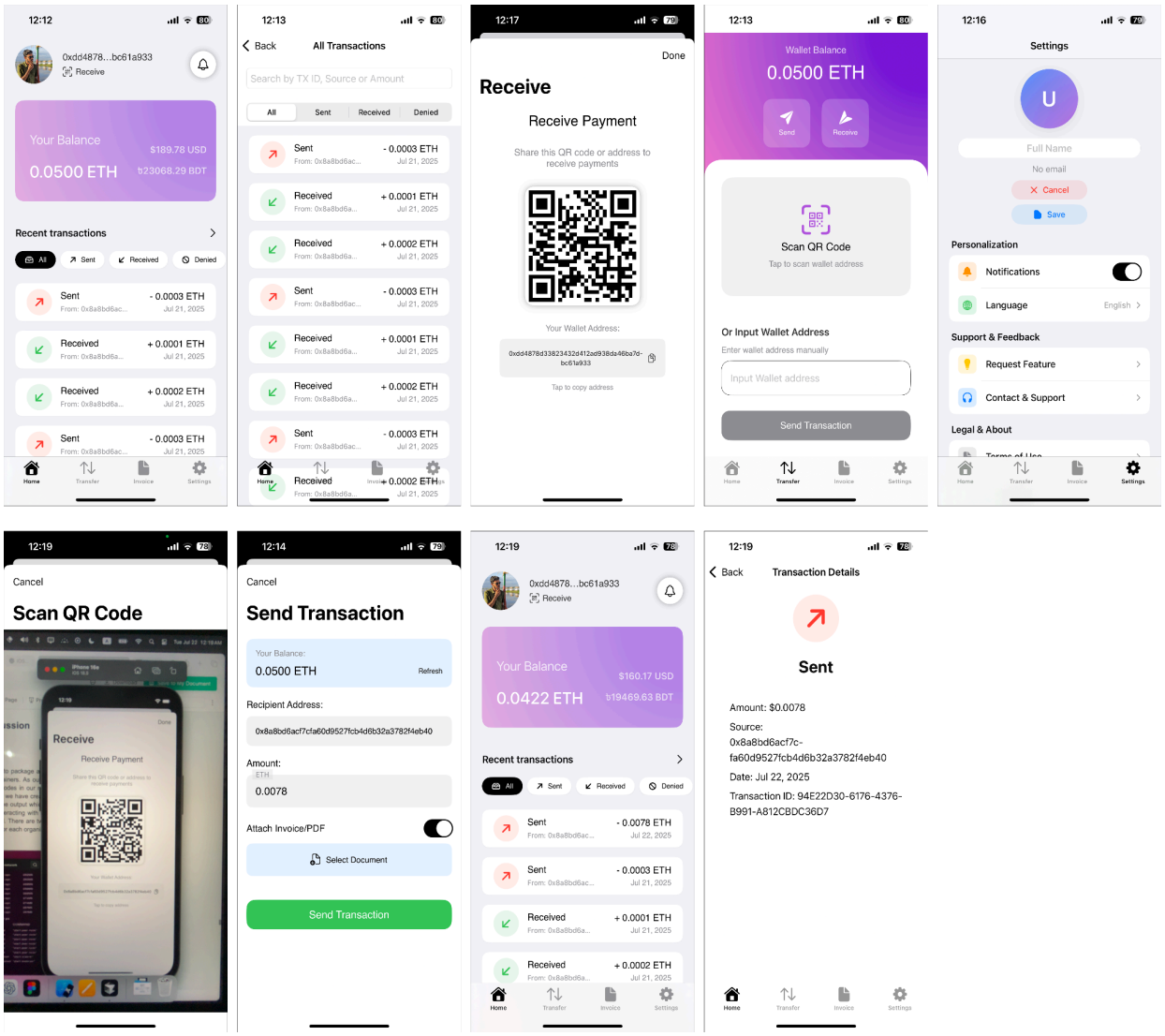
The application's user interface centers around four primary screens, each optimized for specific user workflows and integration requirements.

6.6.1 Home Screen Architecture

The home screen serves as the primary dashboard, displaying essential wallet information and providing navigation to other application features. The Ethereum address presentation includes both full address display and QR code generation for easy sharing. Balance information appears in multiple denominations including ETH, USD, and BDT, with real-time exchange rate updates through integrated price feeds.

Transaction history implementation provides comprehensive filtering and search capabilities, allowing users to locate specific transactions by date range, amount, transaction type, or recipient address. Each transaction entry displays status information including confirmation count, gas

fees, and compliance approval status. Integration with the government monitoring system provides additional metadata indicating regulatory review status.



6.6.2 Transfer Screen Implementation

The transfer functionality integrates QR code scanning capabilities through the CodeScanner library, enabling users to capture recipient addresses quickly and accurately. The scanner supports multiple QR code formats including standard Ethereum addresses, EIP-681 payment requests, and custom invoice formats generated by other application users.

Manual address entry includes comprehensive validation ensuring addresses conform to Ethereum standards and pass checksum verification. The interface provides real-time feedback during address input, highlighting potential errors before transaction submission.

Amount specification supports multiple input methods including direct ETH entry, fiat currency conversion, and percentage-based wallet balance selection. Gas fee estimation provides users

with transaction cost information before confirmation, with options for standard, fast, and custom gas price selection.

Invoice attachment functionality enables users to associate supporting documentation with transactions for compliance and record-keeping purposes. The system supports image uploads, PDF documents, and text descriptions that sync with the government monitoring portal for regulatory review.

6.6.3 CodeScanner Implementation

CodeScanner provides SwiftUI-native QR code and barcode scanning functionality integrated throughout the application's payment workflows. The library's implementation offers camera access management, real-time scanning feedback, and support for multiple barcode formats commonly used in cryptocurrency applications.

Integration within the transfer screen enables rapid recipient address capture while maintaining user experience consistency with the broader SwiftUI interface design. The scanner includes automatic focusing, torch control, and scan area customization to optimize scanning success rates across various lighting conditions and QR code sizes.

Custom validation logic processes scanned codes to distinguish between standard Ethereum addresses, EIP-681 payment requests, and application-specific invoice codes. Error handling provides clear feedback when scanned codes don't match expected formats or contain invalid data.

6.6.4 Invoice Management Implementation

The invoice system enables users to create payment requests with detailed specifications including amount, description, due date, and compliance metadata. Generated invoices include QR codes containing all necessary payment information, simplifying the payment process for recipients.

Invoice tracking provides real-time status updates as payments progress through the compliance review process. Users receive notifications when invoices are paid, when payments require additional verification, or when regulatory authorities flag transactions for review.

Sharing capabilities integrate with iOS native sharing functionality, allowing invoice distribution through email, messaging applications, or direct QR code display. The system maintains privacy by ensuring that sensitive compliance information remains accessible only to authorized parties.

6.6.5 Settings Screen Configuration

The settings interface provides comprehensive application customization including security preferences, notification management, and compliance reporting options. Users configure biometric authentication requirements, transaction approval workflows, and privacy settings affecting data sharing with government monitoring systems.

6.7 Ethereum Network

6.7.1 Sepolia Testnet Result

Ethereum Sepolia testnet integration provides a controlled environment for testing transaction functionality while maintaining compatibility with production Ethereum networks. The implementation connects to multiple Sepolia nodes ensuring availability and redundancy during testing operations.

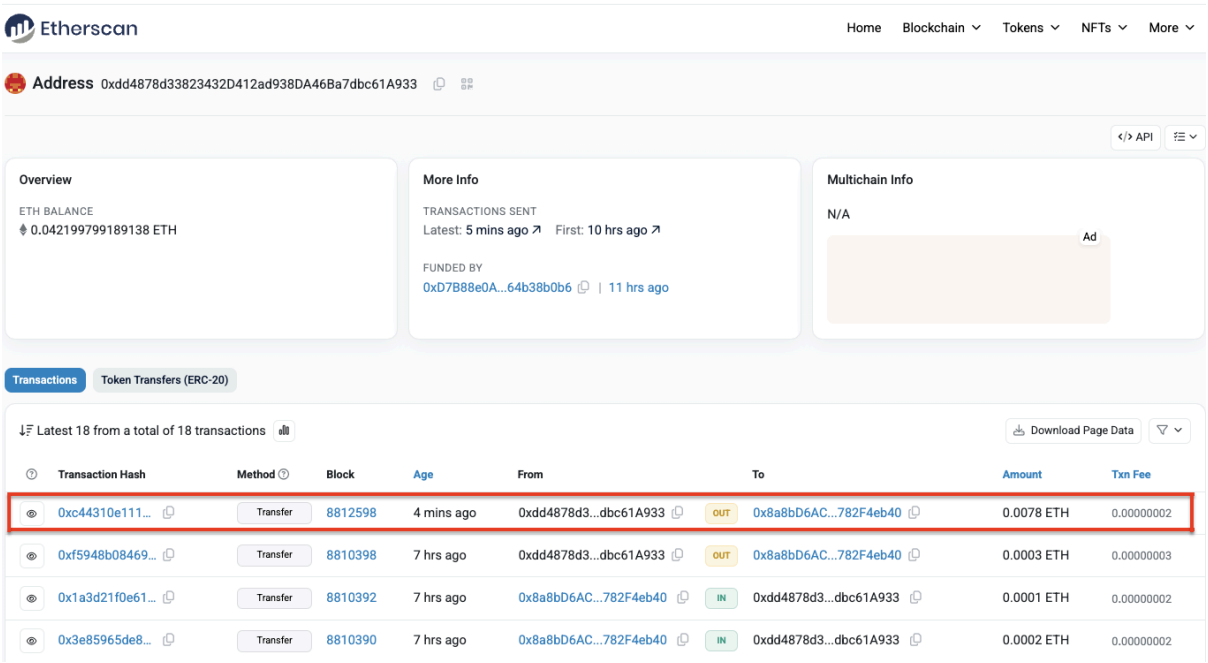
Transaction submission utilizes Web3 provider interfaces that abstract blockchain communication complexity while providing comprehensive error handling for network conditions, gas estimation failures, and transaction rejection scenarios. The system includes retry logic for transient network failures while preventing duplicate transaction submission.

Gas estimation implementation provides users with accurate transaction cost information before submission. The system queries current network conditions and adjusts gas price recommendations based on desired confirmation speed and network congestion levels.

6.7.2 Transaction Tracking and Compliance

Each transaction generates a unique hash upon successful submission to the Sepolia network, providing immutable tracking capability throughout the compliance review process. The application monitors transaction confirmation status and provides real-time updates to users regarding approval progress.

Compliance integration ensures that transaction metadata synchronizes with government monitoring systems immediately upon submission. This includes transaction amounts, recipient addresses, attached documentation, and risk assessment results from the machine learning evaluation module.



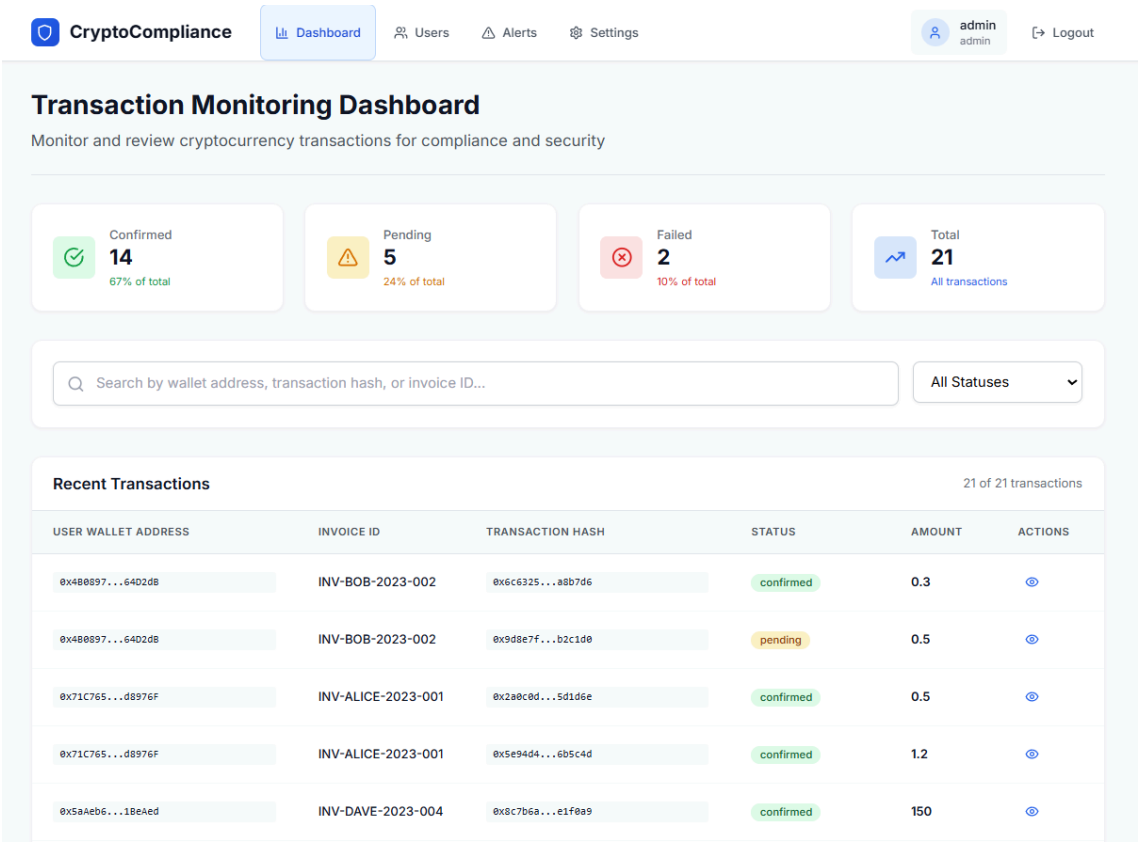
External tracking capability enables users and authorities to verify transaction details using standard Ethereum block explorers and analysis tools. The application provides direct links to transaction details while maintaining user privacy regarding wallet associations.

The implementation includes comprehensive logging of all blockchain interactions ensuring regulatory audit capabilities while maintaining user privacy protections. Transaction logs include timing information, gas usage, confirmation details, and compliance review outcomes providing complete transaction lifecycle documentation.

6.8 Monitoring Transaction and Compliance

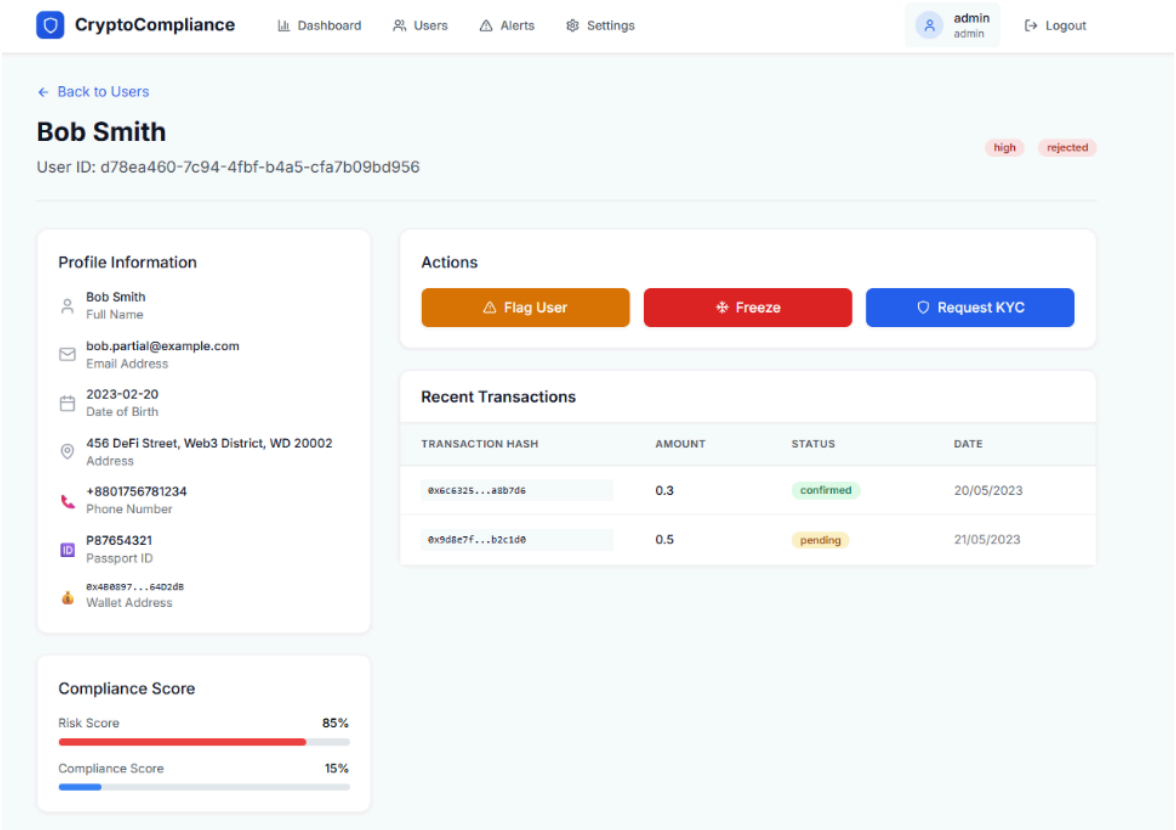
6.8.1 Transaction Monitoring Dashboard

The dashboard, a real-time compliance command center, displays a continuous stream of transactions with relevant metadata. Color-coded status indicators provide immediate insights into transaction legitimacy. Enhanced search and filtering tools allow users to perform targeted queries based on transaction hash or status, aiding anomaly investigations. Expandable transaction models or side panels offer comprehensive data for audit and decision-making. The dashboard supports key compliance functions, including AML by identifying and triaging suspicious transactions, taxation compliance through invoice and hash tracking for traceability, and user behavior analytics by revealing transaction volume and frequency patterns.



6.8.2 User Compliance

The profile view consolidates KYC data, user identity attributes, and transaction history into a centralized interface with a KYC badge, user photo, and verified personal data. A compliance score indicator summarizes the user's risk level based on historical flags and transactions. Administrators can flag users, request KYC updates, or freeze accounts. The interface supports verified and modifiable user identity statuses, AML responses, and behavior analytics. It meets modern crypto regulatory environments by detecting, analyzing, and acting on suspicious activity. It manages user compliance profiles at a granular level, supporting anti-money laundering protocols, KYC obligations, and behavior-based risk assessments. The responsive, role-ready design empowers proactive compliance enforcement. The modular build using React ensures future needs like integration with machine learning risk models or automated reporting systems.



Chapter Seven

Conclusion & Future Work

7.1 Conclusion

This research presents a novel KYC-driven cryptocurrency wallet that bridges digital currencies with global financial systems. Incorporating robust KYC protocols, NFC verification, biometric authentication, and machine learning-based transaction risk scoring, it ensures AML and taxation compliance while maintaining user autonomy and security. The iOS app prototype with a full-stack backend demonstrates efficient registration, secure key management, and real-time compliance monitoring, featuring ECC for key generation and pre-transaction validation for enhanced security and scalability. Its effectiveness in user authentication, transaction processing, and compliance checks is validated by findings from the 2024 27th International Conference on Computer and Information Technology (ICCIT). Future work will optimize transaction speeds, conduct large-scale testing, explore cross-jurisdictional compliance, and integrate advanced privacy techniques, paving the way for a secure, compliant, and inclusive cryptocurrency ecosystem.

7.1 Future Work

The future work for this research will focus on enhancing the functionality, security, and regulatory compliance of the proposed KYC-driven cryptocurrency wallet. The key areas of development include:

1. **Advanced Machine Learning & Security:** This will involve implementing refined machine learning algorithms, such as Random Forest, to improve Anti-Money Laundering (AML) risk assessments. Additionally, efforts will be made to strengthen security through advanced cryptographic protocols designed to counter emerging threats.
2. **Financial Integration & Cryptocurrency Compatibility:** The focus will be on achieving seamless interoperability with traditional financial systems to foster adoption and trust. Furthermore, the scope of compatibility will be expanded to support major cryptocurrencies like Bitcoin, addressing both technical and regulatory challenges.
3. **User Experience & Regulatory Compliance:** Work in this area will concentrate on optimizing the user interface for enhanced accessibility and faster transaction processing. Moreover, global regulatory frameworks will be explored to ensure compliance across various jurisdictions.
4. **Privacy-Preserving Techniques:** Methods such as zero-knowledge proofs will be incorporated to balance user privacy with regulatory obligations.

These developments aim to create a robust, secure, and inclusive cryptocurrency ecosystem.

Chapter Eight

Reference

[1] Lewis, Rebecca, John McPartland, and Rajeev Ranjan. "Blockchain and financial market innovation." Economic Perspectives 41, no. 7 (2017): 1-17.

[2] Schär, Fabian. "Decentralized finance: On blockchain-and smart contract-based financial markets." FRB of St. Louis Review (2021).

[3] Yuan, Yong, and Fei-Yue Wang. "Blockchain and cryptocurrencies: Model, techniques, and applications." IEEE Transactions on Systems, Man, and Cybernetics: Systems 48, no. 9 (2018): 1421-1428.

[4] Yadav, Satya Prakash, Krishna Kant Agrawal, Bhoopesh Singh Bhati, Fadi Al-Turjman, and Leonardo Mostarda. "Blockchain-based cryptocurrency regulation: An overview." Computational Economics 59, no. 4 (2022): 1659-1675.

[5] Parra Moyano, José, and Omri Ross. "KYC optimization using distributed ledger technology." Business & Information Systems Engineering 59 (2017): 411-423.

[6] Malhotra, Diksha, Poonam Saini, and Awadhesh Kumar Singh. "How blockchain can automate KYC: Systematic review." Wireless Personal Communications 122, no. 2 (2022): 1987-2021.

[7] Arner, Douglas W., Dirk A. Zetzsche, Ross P. Buckley, and Janos N. Barberis. "The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities." European business organization law review 20 (2019): 55-80.

[8] Wronka, Christoph. "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight." Journal of Banking Regulation 25, no. 1 (2024): 84-93.

[9] Yadav, Yesha. "Toward a Public-Private Oversight Model for Cryptocurrency Markets." Vanderbilt Law Research Paper 22-26 (2022).

[10] Zaghloul, Ehab, Tongtong Li, Matt W. Mutka, and Jian Ren. "Bitcoin and blockchain: Security and privacy." IEEE Internet of Things Journal 7, no. 10 (2020): 10288-10313.

[11] Karame, Ghassan, and Srdjan Capkun. "Blockchain security and privacy." IEEE Security & Privacy 16, no. 04 (2018): 11-12.

[12] Inshyn, Mykola, Leonid Mohilevskyi, and Oleksii Drozd. "The issue of cryptocurrency legal regulation in Ukraine and all over the world: a comparative analysis." Baltic Journal of Economic Studies 4, no. 1 (2018): 169-174.

[13] Cumming, Douglas J., Sofia Johan, and Anshum Pant. "Regulation of the crypto-economy: Managing risks, challenges, and regulatory uncertainty." Journal of Risk and Financial Management 12, no. 3 (2019): 126.

[14] Wronka, Christoph. "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight." Journal of Banking Regulation 25, no. 1 (2024): 84-93.

[15] Sandner, Philipp G., Agata Ferreira, and Thomas Dunser. "Crypto Regulation and the case for Europe." In Handbook on Blockchain, pp. 661-693. Cham: Springer International Publishing, 2022.
[16] I. Amsyar, E. Christopher, A. Dithi, A. N. Khan, and S. Maulana, “The challenge of cryptocurrency in the era of the digital revolution: A review of systematic literature,” Aptisi Transactions on Technopreneurship (ATT), vol. 2, no. 2, pp. 153–159, 2020.
[17] S. Agarwal, “Virtual currencies: Understanding the ban,” Available at SSRN 3301129, 2018.
[18] M. Masithoh and A. I. Hambali, “Virtual money exchange (cryptocurrency) with real money (rupiah) based on sharia economic law perspective,” International Journal of Social Service and Research, vol. 2, no. 6, pp. 518–525, 2022.
[19] “Which countries have banned crypto, and why?.”
[20] Vishawjyoti, “E-wallet,” Blockchain for Business: How It Works and Creates Value, pp. 97–111, 2021.
[21] K. Karantias, “Sok: A taxonomy of cryptocurrency wallets,” Cryptology ePrint Archive, 2020.
[22] M. Palatinus, P. Rusnak, A. Voisine, and S. Bowe, “Mnemonic code for generating deterministic keys,” Online at https://github.com/bitcoin/bips/blob/master/bip-0039. mediawiki, 2013.
[23] J. H. Oh, “The foreign exchange market with the cryptocurrency and” kimchi premium”,” 2018.
[24] Nabilou, Hossein. "How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency." International Journal of Law and Information Technology 27, no. 3 (2019): 266-291.
[25] Gonzálvez-Gallego, Nicolás, and María Concepción Pérez-Cárceles. "Cryptocurrencies and illicit practices: The role of governance." Economic Analysis and Policy 72 (2021): 203-212.
[26] Saundal, Sumit. "Cryptocurrencies: analysis of the technology and need for its regulation." Available at SSRN 3903787 (2021).
[27] Malhotra, Diksha, Poonam Saini, and Awadhesh Kumar Singh. "How blockchain can automate KYC: Systematic review." Wireless Personal Communications 122, no. 2 (2022): 1987-2021.
[28] Mandava, Suman, Joseph Savio Pereira, and S. Janagiraman. "Know Your Customer Verification using Blockchain and CPABE Algorithm." In 2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 262-266. IEEE, 2023.
[29] Panjaitan, Ria, Diana Putri Lazirkha, Mustofa Kamil, Ruli Supriati, and Wahyu Nur Wahid. "Design of Know Your Customer (KYC) Using Blockchain Technology." In 2022 IEEE Creative Communication and Innovative Technology (ICCIT), pp. 1-6. IEEE, 2022.
[30] Mansoor, Nafees, Kaniz Fatema Antora, Priyata Deb, Tarek Ahammed Arman, Azizah Abdul Manaf, and Mahdi Zareei. "A review of blockchain approaches for kyc." IEEE Access (2023).

[31] Johnson, Kristin N. "Decentralized finance: Regulating cryptocurrency exchanges." Wm. & Mary L. Rev. 62 (2020): 1911.
[32] Semenikhin, Andrey, Igor Morkovkin, Elena Kolosova, Elena Rudakova, Alexander Galushkin, and Lyudmila Rudenko. "The Role of Government in a Crypto-currency World." In 3rd International Conference on Judicial, Administrative and Humanitarian Problems of State Structures and Economic Subjects (JAHP 2018), pp. 64-67. Atlantis Press, 2018.
[33] Cernușca, Lucian, Bogdan Cosmin Gomoi, Raluca Simina Bilți, and Robert Cristian Almași. "Study on the taxation of the income obtained from the cryptocurrency transfer." Journal of Legal Studies 26, no. 40 (2020): 173-188.
[34] Yereli, Ahmet Burçin, and Işıl Fulya Orkunoğlu-Şahin. "Cryptocurrencies and taxation." In Proceedings of the 5th International Annual Meeting of Sosyoekonomi Society, vol. 25, p. 27. 2018.
[35] Campbell-Verduyn, Malcolm. "Bitcoin, crypto-coins, and global anti-money laundering governance." Crime, Law and Social Change 69 (2018): 283-305.
[36] Courtois, Nicolas T., Kacper T. Gradon, and Klaus Schmeh. "Crypto currency regulation and law enforcement perspectives." arXiv preprint arXiv:2109.01047 (2021).
[37] Albrecht, Chad, Kristopher McKay Duffin, Steven Hawkins, and Victor Manuel Morales Rocha. "The use of cryptocurrencies in the money laundering process." Journal of Money Laundering Control 22, no. 2 (2019): 210-216.
[38] Yeoh, Peter. "Regulatory issues in blockchain technology." Journal of Financial Regulation and Compliance 25, no. 2 (2017): 196-208.
[39] Rustamaji, Muhammad, and Faisal Faisal. "Law Enforcement Strategies Against Money Laundering Through Cryptocurrency: Comparative Studies in Several Countries." In International Conference on Cultural Policy and Sustainable Development (ICPSD 2024), pp. 560-572. Atlantis Press, 2024.
[40] Rezaeighaleh, Hossein. "Improving security of crypto wallets in blockchain technologies." (2020).
[41] Joseph, Sunday. "Balancing data privacy and compliance in blockchain-based financial systems." Journal of Engineering Research and Reports 26, no. 9 (2024): 10-9734.
[42] Arnone, Gioia. "Security and Privacy in the Digital Currency Space." In Navigating the World of Cryptocurrencies: Technology, Economics, Regulations, and Future Trends, pp. 63-77. Cham: Springer Nature Switzerland, 2024.
[43] Houy, Sabine, Philipp Schmid, and Alexandre Bartel. "Security aspects of cryptocurrency wallets—a systematic literature review." ACM Computing Surveys 56, no. 1 (2023): 1-31.
[44] Pandya, Suhag, Murugan Mittapalli, Sri Vallabha Teja Gulla, and Ori Landau. "Cryptocurrency: Adoption efforts and security challenges in different countries." HOLISTICA–Journal of Business and Public Administration 10, no. 2 (2019): 167-186.
[45] Moreno, Suzana MBM, Jean-Marc Seigneur, and Gueorgui Gotzev. "A survey of KYC/AML for cryptocurrencies transactions." In Handbook of Research on Cyber Crime and Information Privacy, pp. 21-42. IGI Global, 2021.

[46] Sung, Soonhwa. "A new key protocol design for cryptocurrency wallet." ICT Express 7, no. 3 (2021): 316-321.
[47] Rezaeighaleh, Hossein, and Cliff C. Zou. "Multilayered defense-in-depth architecture for cryptocurrency wallet." In 2020 IEEE 6th International Conference on Computer and Communications (ICCC), pp. 2212-2217. IEEE, 2020.
[48] Nowroozi, Ehsan, Seyedsadra Seyedshoari, Yassine Mekdad, Erkay Savaş, and Mauro Conti. "Cryptocurrency wallets: assessment and security." In Blockchain for Cybersecurity in Cyber-Physical Systems, pp. 1-19. Cham: Springer International Publishing, 2022.
[49] Agarwal, Shivani. "Virtual Currencies: Understanding the Ban." Available at SSRN 3301129 (2018).
[50] Huo, Yunchen. "The Effect of Government Policies on Cryptocurrency Market." In 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022), pp. 459-465. Atlantis Press, 2022.
[51] Ibrahim, Salman Ali. "Regulating cryptocurrencies to combat terrorism-financing and money laundering." Stratagem 2, no. 1 (2019).
[52] Mabunda, Sagwadi. "Cryptocurrency: The new face of cyber money laundering." In 2018 international conference on advances in big data, computing and data communication systems (icabcd), pp. 1-6. IEEE, 2018.
[53] Ullah, Nazir, Kawther A. Al-Dhlan, and Waleed Mugahed Al-Rahmi. "KYC optimization by blockchain based hyperledger fabric network." In 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), pp. 1294-1299. IEEE, 2021.
[54] Khan, Tanvir Ahmed, ASM Touhidul Hasan, Qingshan Jiang, and Qiang Qu. "A hybrid blockchain-based zero reconciliation approach for an effective mobile wallet." In 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), pp. 1-6. IEEE, 2020.
[55] H. Rezaeighaleh and C. C. Zou, “Multilayered defense-in-depth architecture for cryptocurrency wallet,” in 2020 IEEE 6th International Conference on Computer and Communications (ICCC), pp. 2212–2217, IEEE, 2020.
[56] S. J. Hughes and S. T. Middlebrook, “Advancing a framework for regulating cryptocurrency payments intermediaries,” Yale J. on Reg., vol. 32, p. 495, 2015.
[57] S. He, Q. Wu, X. Luo, Z. Liang, D. Li, H. Feng, H. Zheng, and Y. Li, “A social-network-based cryptocurrency wallet-management scheme,” IEEE Access, vol. 6, pp. 7654–7663, 2018.
[58] S. M. Moreno, J.-M. Seigneur, and G. Gotzev, “A survey of kyc/aml for cryptocurrencies transactions,” in Handbook of Research on Cyber Crime and Information Privacy, pp. 21–42, IGI Global, 2021.
[59] “Crypto wallet kyc: Ensuring compliance security.” https://www.togggle.io/
[60] “Guide 2024: Aml/kyc compliance implementation in crypto - unicsoft.” https://unicsoft.com/blog/aml-kyc-compliance-in-crypto/
[61] “Aml and kyc guidance for crypto exchanges and wallets – sanction scanner.”

[62] T. Barbereau and B. Bod´o, “Beyond financial regulation of crypto-asset wallet software: In search of secondary liability,” Computer Law & Security Review, vol. 49, p. 105829, 2023.
[63] L. Perlman, “A model crypto-asset regulatory framework,” 2019.
[64] A. J. Hou, W. Wang, C. Y. Chen, and W. K. H¨ardle, “Pricing cryptocurrency options,” Journal of Financial Econometrics, vol. 18, no. 2, pp. 250–279, 2020.
[65] Guan, Zhangshuang, Zhiguo Wan, Yang Yang, Yan Zhou, and Butian Huang. "BlockMaze: An efficient privacy-preserving account-model blockchain based on zk-SNARKs." *IEEE Transactions on Dependable and Secure Computing* 19, no. 3 (2020): 1446-1463.
[66] Villanueva Collao, Vanessa. "DeFi: a framework of the automated financial system." *Tul. J. Tech. & Intell. Prop.* 26 (2024): 75.