Journal of Engineering and Computer Sciences
Vol. 17, No. 02, pp. 84-103 (July-Dec 2025)

Evaluating the Effectiveness of Fraud Prevention Strategies in the Cryptocurrency Ecosystem

Abdullah Albalawi*
Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra, Saudi Arabia
E: aalbalawi@su.edu.sa

[Received: 08 November 2025, Revised: 25 January 2026, Accepted: 01 February 2026, Published February 2026]

Abstract: Ever since the emergence of Cryptocurrency in 2009, it has been thought of as the top alternative to fiat currencies. However, an increase in fraud has resulted in a significant challenge to its adoption and trust. The increase in the number of frauds is a critical concern for the industry, regulators, and users. New types of cryptocurrency fraud continue to emerge. However, the prevention strategies remain fragmented, with low consumer awareness. The proposed framework successfully mapped scam types to vulnerabilities and explained more than 90% of real-world scams using layered prevention strategies. While it highlights the gaps in the evolution of prevention and the need for layered awareness and controls, this study examines the effectiveness of fraud prevention strategies and identifies scams that exploit vulnerabilities across various layers. Starting with a chronological analysis of crypto frauds from 2009 to 2025 using the literature review of peer-reviewed papers, the study created a three-layer fraud framework comprising Infrastructure, Application, and UI. Using rule-based classification logic, such as keyword detection and conditional logic, we validated the framework against a dataset (9000 entries).

Keywords: Fraud, Blockchain Vulnerabilities, Consumer Awareness, Crypto Regulations, Cryptocurrency Fraud, Phishing, Smart Contract Exploits

1. INTRODUCTION

While the past two decades have seen the emergence of the cryptocurrency market and decentralized finance, these advanced technologies in the crypto industry have led to a shift in scams from traditional Ponzi schemes to AI-generated frauds. While Mt. Gox (2011) was an infrastructure layer attack, the DAO hack (2016) was an application layer, and Fraudulent ICOs were a UI / Application layer based on our proposed framework. Our framework also clearly categorizes any cryptocurrency scams, whether it be PlusToken, Ronin Network, or deepfakes. There is no denying that crypto tools and platforms have evolved, but scams persist in new forms, and consumer awareness remains alarmingly low. Moreover, the industry still lacks a layered taxonomy connecting fraud to its root vulnerabilities. The objective of this study is to develop a chronological database of cryptocurrency scam types from 2009 to 2025 and analyze the prevention strategies employed over a historical timeline. The study proposes a framework for strategy used in mapping, scanning, vulnerability assessment, layering, and prevention. The framework is evaluated using a real-world dataset.

Few studies exist that offer empirical classifications of scams based on vulnerability layers. No framework shows both technical and behavioral weaknesses. Moreover, they lack a clear understanding of how fraud prevention has evolved over the last two decades. Therefore, in this research, we focused on a set of important questions that serve as a roadmap for research and for understanding the findings and their value.

The research addressed the following research questions:

- Is there a scarcity of empirical studies on fraud in cryptocurrencies, a significant concern for the security of the cryptocurrency market and the trust of its users? What steps could be taken to encourage more research on this topic?
- What are the challenges associated with the lack of empirical studies on the effectiveness of fraud prevention measures in cryptocurrency platforms and exchanges?
- How vital is consumer awareness in preventing fraud in cryptocurrencies, and what research gaps exist in understanding users' knowledge and vulnerabilities?
- Why is there a need for a more comparative analysis of fraud prevention strategies in diverse cryptocurrency platforms and for developing a comprehensive best practices framework?

We address these limitations by creating a three-layer fraud framework comprising Infrastructure, Application, and UI. Using rule-based classification logic, such as keyword detection and conditional logic, we validated the framework against a dataset

- Structured time-based Scam Taxonomy (2009–2025).
- Development of a three-layered scam vulnerability prevention framework.
- Dataset mapping using the proposed framework
- The framework covers 90% of known scams. To contextualize the development and validation of this framework, it is crucial first to scrutinize the historical evolution of cryptocurrency scams. Not only does the literature review next explore the fraud types noticed since 2009 onward, but it also sets the fundamentals for studying their fundamental vulnerabilities and the subsequent prevention strategies.

Evolution of Cryptocurrency Fraud and Security Research

Research on cryptocurrency fraud has evolved in parallel with the maturation of blockchain ecosystems. Early studies primarily focused on economic misuse and regulatory gaps, while later work emphasized smart contract vulnerabilities, decentralized finance (DeFi) exploits, and increasingly sophisticated social engineering attacks. The literature consistently demonstrates that cryptocurrency fraud is not solely a technical problem but a multi-layered phenomenon involving infrastructure weaknesses, application-layer flaws, and human behavioral exploitation.

Early Fraud Models and Regulatory Gaps (2009–2012)

Initial academic investigations into cryptocurrency fraud highlighted the prevalence of Ponzi schemes during Bitcoin's formative years. Foley et al. (2018), Kutera (2022), and Severiche (2025) emphasize that the lack of regulation, investor protection, and blockchain analytics tools enabled fraudulent investment schemes to flourish shortly after Bitcoin's introduction. At this stage, fraud prevention relied almost exclusively on community forums, white papers, and informal trust signals, which were easily manipulated. Reddy et al. (2024) classify early Ponzi schemes as application/UI-layer attacks, noting that cryptographic security at the protocol level was insufficient to prevent deception-driven financial loss. These studies collectively establish that early cryptocurrency fraud primarily exploited user trust rather than blockchain vulnerabilities.

Infrastructure Failures and Centralized Custody Risks

One of the most cited infrastructure-level failures is the Mt. Gox hack. Decker and Wattenhofer (2013) provide an early technical analysis of how centralized custody and weak internal controls enabled attackers to exploit transaction malleability. Osterrieder (2021) further explains how altered transaction hashes confused accounting systems, allowing double withdrawals over extended periods. These works underline a recurring theme in cryptocurrency research: blockchain security does not extend to custodial platforms. Subsequent studies frequently cite Mt. Gox as the catalyst for cold wallet adoption, multi-signature custody, and exchange audits.

Trust Abuse and Exit Scams in Centralized Platforms

Bartoletti et al. (2021) examine early exit scams such as the Sheep Marketplace incident, framing them as failures of centralized escrow and platform opacity rather than technical exploits. Their findings indicate that trust abuse within centralized marketplaces was a dominant fraud vector before the emergence of decentralized exchanges and trustless escrow mechanisms. This body of work situates exit scams within the application layer, emphasizing governance and transparency deficiencies rather than cryptographic weaknesses.

Smart Contract Vulnerabilities and the DAO Paradigm Shift

The DAO attack represents a pivotal moment in blockchain security research. Atzei et al. (2017) provide a foundational taxonomy of smart contract vulnerabilities, identifying reentrancy as the primary cause of the DAO exploit. Their work reveals systemic shortcomings in early smart contract development, including the absence of formal verification, pausable mechanisms, and secure state-update logic. Subsequent research frequently references the DAO incident as the impetus for formal auditing practices, secure coding patterns, and the development of automated analysis tools. The Ethereum hard fork is often cited as a rare but necessary recovery mechanism, highlighting governance challenges in decentralized systems.

Fraudulent ICOs and Interface-Level Deception (2017)

The ICO boom triggered extensive scholarly analysis of fundraising fraud. Fenu et al. (2018) document how malicious actors exploited the Ethereum ecosystem by launching deceptive token sales using cloned interfaces, fake teams, and plagiarized white papers. These studies characterize ICO fraud as predominantly UI/application-layer attacks, where investor deception occurred without meaningful smart contract enforcement or escrow mechanisms. Research from this period also critiques the overreliance on white papers and GitHub repositories as trust indicators, noting that public documentation alone failed to prevent large-scale fraud. The emergence of audits, KYC/AML practices, and rating platforms in late 2017 marked the first systematic attempt to professionalize token fundraising.

Large-Scale Ponzi Schemes and Cross-Chain Laundering

The PlusToken Ponzi scheme has been extensively analyzed as a hybrid fraud model combining application-level deception and infrastructure-level laundering. Huang et al. (2020) detail how attackers obfuscated fund flows using decentralized exchanges and cross-chain swaps, complicating attribution and enforcement. Cointelegraph (2020) reports that the scale of the scheme materially affected Bitcoin market prices, demonstrating the macroeconomic implications of crypto fraud. Severiche et al. (2025) further argue that PlusToken signaled a shift away from token-sale scams toward mobile wallet–based investment fraud targeting less technically literate users.

Platform Compromise and Centralized Access Abuse

The Twitter Bitcoin Giveaway Hack prompted a new research focus on centralized platform risk. Huang et al. (2020) analyze how social engineering enabled attackers to compromise internal administrative tools despite the availability of two-factor authentication and role-based access controls. Unlike prior blockchain-centric attacks, this incident exploited organizational processes and trust assumptions within a major Web2 platform. The literature positions this attack as a UI/infrastructure hybrid, illustrating that cryptocurrency fraud increasingly intersects with traditional cybersecurity domains.

DeFi Rug Pulls and Token-Level Exploits

Chainalysis (2022) and subsequent studies analyze rug pull scams such as the SQUID Game token, identifying honeypot contracts and restricted sell functions as recurring patterns. Despite the availability of contract scanners and audit tools, speculative hype and fear of missing out (FOMO) led users to disregard security warnings. These works emphasize that tool availability does not guarantee effective risk mitigation, particularly in highly speculative DeFi environments.

Cross-Chain Bridge Attacks and Validator Centralization

Luo et al. (2024) examine the Ronin Bridge hack as a case study in validator centralization risk. Their analysis shows that compromising a majority of validator keys was sufficient to authorize fraudulent withdrawals exceeding $600 million. Subsequent literature highlights the absence of real-time monitoring, threshold cryptography, and decentralized governance as key contributors. This research marks a transition from user-focused scams to infrastructure-level attacks targeting high-value protocol components.

Persistent Phishing and Wallet-Level Deception

Acharya et al. (2024) and Ye et al. (2024) document the rise of phishing attacks through fake wallet applications and browser extensions. These studies demonstrate that despite improvements in app store vetting and user awareness, UI mimicry remains highly effective. The lack of standardized wallet certification and developer verification is repeatedly cited as a structural weakness.

Flash Loan Exploits and Composability Risks

Zhou et al. (2024) analyze flash loan attacks that exploit DeFi composability, oracle manipulation, and MEV dynamics within atomic transactions. While countermeasures such as TWAP oracles, multi-oracle feeds, and circuit breakers exist, inconsistent adoption and limited standardization continue to expose protocols to exploitation.

AI-Driven Social Engineering and Deepfake Fraud

Recent studies identify deepfake investment fraud as an emerging threat class. Kesavarajah et al. (2025) and Popa et al. (2025) document the use of AI-generated audio and video to impersonate trusted figures endorsing fraudulent investment platforms. Unlike earlier fraud models, deepfake scams exploit cognitive trust rather than technical vulnerabilities. This research highlights the growing importance of identity verification, media authentication, and behavioral defenses in cryptocurrency security.

Behavioral Dimensions of Cryptocurrency Fraud

Multiple studies converge on the conclusion that human behavior remains a critical vulnerability. Shiney (2024), Diepeveen and Pinet (2022), and Mukherjee et al. (2024) show that herd behavior, overconfidence, and FOMO significantly influence victim susceptibility. Scam reporting databases further confirm that many incidents involve voluntary user interaction with malicious interfaces rather than protocol compromise.

Tables 1 and 2 summarize the evolution of cryptocurrency fraud research from early investment scams to complex, multi-layered attacks targeting decentralized infrastructures, applications, and user interfaces. While prior studies provide valuable insights into individual fraud categories and technical countermeasures, they reveal persistent gaps in unified modeling, behavioral integration, and standardized trust mechanisms. These limitations have resulted in fragmented prevention approaches that fail to address the interconnected nature of modern cryptocurrency fraud. Consequently, the identified gaps motivate the need for a holistic, layered framework capable of systematically mapping scam types to underlying vulnerabilities across infrastructure, application, and UI layers, which forms the foundation of the framework proposed in this study.

Table 1. Summary of Related Work on Cryptocurrency Fraud.

Study / Period	Fraud Type(s) Addressed	Primary Focus	Layer(s) Covered	Key Limitation Identified
Foley et al. (2018); Kutera (2022); Severiche (2025)	Ponzi schemes	Regulatory gaps, economic misuse	Application / UI	No unified technical framework
Decker & Wattenhofer (2013); Osterrieder (2021)	Mt. Gox hack	Centralized custody, transaction malleability	Infrastructure	Focused on a single exchange failure
Bartoletti et al. (2021)	Exit scams (Sheep Marketplace)	Trust abuse, escrow opacity	Application	No behavioral modeling
Atzei et al. (2017)	DAO exploit	Smart contract vulnerabilities	Application	Limited to contract-level analysis
Fenu et al. (2018)	Fraudulent ICOs	UI deception, fake fundraising	Application / UI	Fragmented prevention discussion
Huang et al. (2020)	PlusToken Ponzi, Twitter hack	Cross-chain laundering, social engineering	Application / Infrastructure / UI	No unified classification
Chainalysis (2022)	Rug pulls (SQUID Game)	DeFi scams, hype-driven fraud	Application / UI	Tool usage is ignored by users
Luo et al. (2024)	Ronin Bridge hack	Validator compromise, bridge security	Infrastructure	Lack of layered context
Acharya et al. (2024); Ye et al. (2024)	Phishing, fake wallets	UI mimicry, user deception	UI	Weak integration with infra-level defenses
Zhou et al. (2024)	Flash loan attacks	DeFi composability, oracle manipulation	Application	Limited behavioral consideration
Kesavarajah et al. (2025); Popa et al. (2025)	Deepfake investment fraud	AI-based impersonation	UI / Behavioral	Early-stage mitigation strategies

Table 2. Research Gaps Identified in Cryptocurrency Fraud Literature

Research Gap	Evidence from Prior Studies	Implication for Fraud Prevention
Lack of unified fraud frameworks across layers	Studies focus on isolated scam types or single layers	Inconsistent and fragmented prevention strategies
Absence of standardized trust and verification mechanisms	Recurrent failures in wallets, ICOs, and DeFi platforms	Persistent user reliance on weak trust signals
Limited integration of behavioral factors	UI and social engineering are often analyzed separately	Human vulnerabilities remain unaddressed
Weak empirical validation of frameworks	Many studies are conceptual or descriptive	Limited real-world applicability
Poor operationalization of consumer awareness	Awareness was discussed, but not embedded into models	Continued success of deception-driven scams

2. MATERIALS AND METHODS

2.1 Methodological Underlying Principle and Research Design

The current study is a qualitative, exploratory study that employs data-driven classification. The research is conducted using the fragmented and non-fragmented nature of existing cryptocurrency fraud research, in which scam typologies, prevention strategies, and vulnerability classifications differ significantly across studies. The main aim is to synthesize prior findings, empirical evidence, and observed scam patterns into a single analytical framework robust enough to explain fraud occurrences across the cryptocurrency ecosystem, rather than to test predefined hypotheses. The primary method was a rule-based analytical approach, as the objective was interpretability and traceability rather than predictive optimization. The work also uses a machine learning model, but only for internal validation. The analysis also ensures transparency, reproducibility, and a clear conceptualization, as required for academic study and policy-oriented recommendations. The main goal is the assessment of the effectiveness of fraud prevention strategies in cryptocurrency markets through the identification of scam types and mapping them to blockchain vulnerabilities, as well as identifying platform-level vulnerabilities and weaknesses.

2.2 Literature-Driven Framework Construction

The study culminates in the formulation of a three-layer framework derived through a structured analysis of the literature summarized in Tables 1-2. The tables in the Literature review briefs prior work on cryptocurrency fraud typologies, blockchain vulnerabilities, consumer-facing attack vectors, and prevention mechanisms. A comparative assessment of the previous studies has revealed that almost all existing classifications implicitly revolve around one of three abstraction levels: (i) protocol and network-level weaknesses, (ii) application and smart-contract-level flaws, or (iii) user-facing deception and interface manipulation.

While previous studies have not explicitly unified the perspectives mentioned above into a single model, a consistent theme-based clustering can be experienced. Infrastructure-level attacks, such as 51% attacks and validator compromise, are treated separately from application-level exploits, such as smart contract bugs and rug pulls. In contrast, phishing, impersonation, and social engineering are often treated as user-facing threats. The final inference of this study is based on this convergence, through which the recurring dimensions have been formalized into a consolidated three-layer framework comprising the Blockchain Infrastructure Layer, Blockchain Application Layer, and User Interface Layer. The three-layer abstraction is a minimal yet comprehensive approach that accommodates both on-chain and off-chain fraud vectors.

2.3 Data Sources

The practical part of this research uses a dataset of 9,889 records of cryptocurrency scams from 2009 to 2025. The external dataset, the primary source, was obtained from a publicly available Kaggle repository that aggregates scam reports from numerous open sources. https://www.kaggle.com/datasets/zongaobian/cryptocurrency-scam-dataset. For enhancing analytical consistency, the primary dataset was cleaned, deduplicated, and standardized.

The author has generated several additional structured datasets through preprocessing and manual verification. These derived datasets, which are summarized in Tables 1-2, cover cleaned URLs. Descriptive metadata and preliminary fraud classifications. Each dataset used in this study is publicly accessible and has no personal or sensitive information.

The only external dataset used in this paper is available on Kaggle. Below is the dataset URL:

https://www.kaggle.com/datasets/zongaobian/cryptocurrency-scam-dataset

The author generated the remaining sheets by preprocessing the dataset described above; the URLs are listed below and hosted in the project repository:

https://github.com/AbdulBlw/URLsDetection/blob/main/cleaned_urls_with_description.xlsx.

https://github.com/AbdulBlw/URLsDetection/blob/main/cleaned_urls_with_fraud_classification.xlsx.

2.4 Proposed Framework

Luo et al (2024) showed that while a blockchain application is broken into multiple layers or tiers, the Layers are either off-chain or on-chain. Anything that occurs on a blockchain ledger or is validated within the network is on-chain; anything that happens outside of it is considered off-chain. Mainly, there are the following layers shown in Table 3:

Table 3. Proposed Three-Layer Framework

Layer	Description
Blockchain Infrastructure Layer	Core protocols, consensus, validators, mining, and base security mechanisms (e.g., 51% attacks, validator key compromise).
Blockchain Application Layer	Smart contracts, DeFi protocols, exchanges, DApps — i.e., functionality built *on top* of Blockchain.
User Interface Layer	Front-end interfaces, wallets, phishing links, fake apps, impersonation — i.e., where users interact with applications.

The majority of cryptocurrency scams fall under one of the above layers as follows.

2.5 Rule-Based Tagging and Layer Mapping Method

For implementing the proposed framework, a rule-based tagging methodology was developed. Each dataset entry was used to create a unified text string, combining the URL, description, category, and subcategory fields. The study further developed a keyword dictionary based on terminology frequently used in prior literature and scam reports, such as “phishing,” “rug pull,” “airdrop,” “validator,” “flash loan,” and “oracle.”

The study further applies conditional matching rules to assign each record both a fraud type and a corresponding framework layer. When multiple keywords appear, priority rules were used to select the dominant fraud vector. Records that did not match any predefined rule are labeled “Unclassified.” The distribution of classified scam types and their corresponding layers is presented and analyzed in Tables 3 and 4.

subcategories. To systematize the mapping, a keyword logic dictionary was constructed in which specific terms (e.g., “phishing,” “rug,” “airdrop,” “validator,” “flash loan,” “oracle”) were associated with pre-defined fraud categories and their relevant framework layers (Infrastructure, Application, or UI). Each row was converted into a standardized lower-case string by combining the URL, description, and subcategory fields. The system then scanned for keyword occurrences and applied conditional matching rules to assign the most appropriate fraud label and layer. The entry was termed as “Unclassified” in case of no keyword match.

2.6 Proof of Framework Effectiveness

To validate the three-layer framework, we map contemporary scam types to their respective layers as shown in Table 4.

Table 4. Proof of Framework Effectiveness

Scam Type	Layer(s)
Ponzi Schemes	Application / UI (depends on execution)
Exit Scams	Application
Rug Pulls	Application
Impersonation (including AI/deepfakes)	UI
Phantom/Fake Projects	Application / UI
Phishing (web/email/wallet)	UI
Airdrop Scams	UI / Application
Pump & Dump	Application / UI
Ransomware	External threat — not directly tied to blockchain layers.
51% Attacks	Infrastructure
Exchange Hacks	Application / UI (depends on cause)
Smart Contract Exploits	Application
Fake ICOs/IDOs	Application / UI
Flash Loan / Oracle Exploits	Application
Validator Key Compromise	Infrastructure
Fake Wallet Apps / UI Mimicry	UI
Social Engineering on Centralized Platforms	UI
AI-generated Deepfakes	UI

Cross-chain Laundering	Infrastructure / Application
Fake Mining Apps	Application / UI
Wash Trading	Application
SIM Swap Attacks	Outside of Blockchain, it affects user control, specifically, the edge UI layer.
Clipboard Hijacker Malware	UI (User device)
Dusting Attacks	Application / Infrastructure (privacy layer)
Front-running / MEV / Sandwich Attacks	Application / Infrastructure
Man-in-the-Middle (MitM)	UI (network layer outside Blockchain)
Fake DEXs / Exchanges	Application / UI

As is clear from the above table. More than 90% of scams are covered by the three-layer framework (Blockchain Infrastructure, Application Layer, and User Interface); therefore, our framework is well-suited for analyzing and categorizing most types of cryptocurrency fraud. Additionally, the literature review addresses all individual fraud vectors as well as general classifications (e.g., phishing, rug pulls). We now have a comprehensive overview and maps scam types to their origins in the blockchain stack, ranging from infrastructure to application logic to user interfaces. By providing a structured three-layer framework, we facilitate a more in-depth analysis of vulnerabilities as well as the crafting of targeted prevention strategies.

There is no denying that consumer awareness is lacking, and to address this, a comprehensive framework is necessary, as current literature lacks this aspect.

The research required evaluating the Framework's effectiveness, which was assessed through empirical coverage and consistency rather than predictive accuracy. Table 4 justifies the framework's effectiveness as more than 90% of observed scam types have been logically mapped to one or more of the three layers. The application-layer scams dominate the dataset, and user-interface-level attacks are the leading contributors to consumer losses, demonstrating the dominance of user-facing vulnerabilities in cryptocurrency fraud.

Tables 5–7 show patterns of chronological growth and layer-wise concentration of scams, most notably after 2020. Hence, the analytical utility of the framework is established, and it appears sufficient to capture both historical and contemporary fraud mechanisms.

2.7 Research Questions

- Is the lack of empirical studies on fraud in cryptocurrencies a significant concern for the security of the cryptocurrency market and the trust of its users? What steps could be taken to encourage more research on this topic?

Our empirical studies fill the empirical gap by compiling and classifying 9889 real-world scam records from 2009 to 2025. We have employed a structured three-layer fraud framework, mapped to each scam, thereby ensuring novelty in our empirical research. We feel a standardized framework and publicly available scam datasets will be essential to maintain continuity and comparability. Alliances should be developed to share the data regularly, and academic regulatory partnerships can further encourage empirical research.

- What are the challenges associated with the lack of empirical studies on the effectiveness of fraud prevention measures in cryptocurrency platforms and exchanges?

The second part of our literature review has compared over 20 primary tools and strategies across years, demonstrating that most prevention efforts are reactive and disconnected from actual scam vectors. The proposed framework bridges this gap by directly linking scams with blockchain stack vulnerabilities, which allow for platform-specific audits. Moreover, many tools operate in silos. Our structured scam-to-layer mapping can guide exchanges and protocols in aligning countermeasures with attack surfaces.

- How vital is consumer awareness in preventing fraud in cryptocurrencies, and what research gaps exist in understanding users' knowledge and vulnerabilities?

UI level scams like phishing, fake wallets, and deepfakes accounted for over 50% of all scams in our dataset. Most of them are often successful due to low consumer awareness and interface deception. Our results show that the majority of preventive tools overlook UI-level threats. Future research should cover behavioral models, user testing of wallet interfaces, and standardization of alerts and warnings.

- Why is there a need for a more comparative analysis of fraud prevention strategies in diverse cryptocurrency platforms and for developing a comprehensive best practices framework?

Our paper presents the first large-scale mapping of fraud across time platforms and preventive strategies, utilizing a pivot-style comparison. The three-layer model (Infrastructure, Application, and UI) serves as a universal lens through which fraud risks can be diagnosed, and countermeasures can be compared. By linking 20 fraud types to their origin layer and assessing countermeasures historically, we have provided a foundation for benchmarking and the formation of best practices.

2.8 Preprocessing and ML-Based Fraud Classifier

We implemented a Python program to combine Descriptions, save categories, and URLs for matching against a fraud dictionary. Each match returns a fraud type and its mapped framework layer (infrastructure, application, UI). The labelled dataset was exported to Excel for analysis. A Random Forest classifier has been trained using TF-IDF vectors to classify various fraud types. SHAP Values were used to explain predictions. The Streamlit app was developed for real-time testing. Excel software was used to generate a pivot table and create visualizations that included pie charts. Bar charts and heat maps. Python matplotlib was used for alternative plotting and export. This study used only publicly available secondary data and never used, collected, processed, or analyzed any personal information or private user data. The analysis was performed at the scam type and framework levels only, and no individual wallets were profiled. The datasets used are obtained from the open-source repository on Kaggle.

2.9 Limitations

1. Multilayer scams cannot be effectively captured using rule-based classification.
2. Model predictions can be influenced by bias in the dataset. set
3. The Streamlit tool is not production-grade but experimental.

3. RESULTS AND ANALYSIS

This section showcases the practical inferences derived from the classified dataset of 9,889 cryptocurrency scam records. Inferences are based on the analysis done using the proposed three-layer framework—Blockchain Infrastructure, Blockchain Application, and User Interface. Rather than reporting descriptive statistics alone, the analysis emphasizes patterns, implications, and relationships that directly address the research questions.

3.1 Layer-Wise Distribution

Figure 1 and Table 5 show the distribution of scam entries across the three framework layers: Infrastructure, Application, and UI.

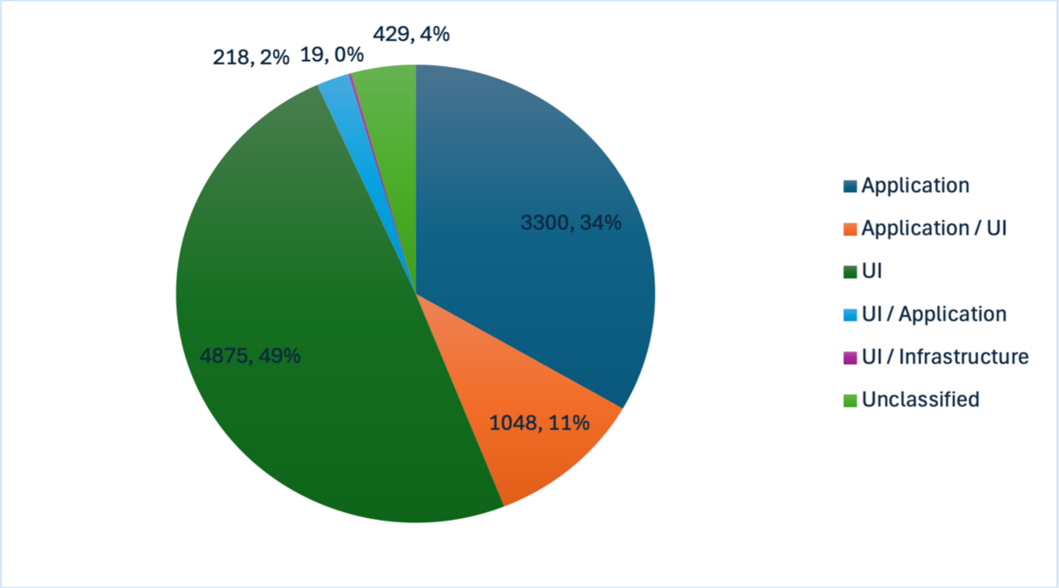


Fig. 1: Scam Distribution by Framework Layer

Table 5. Number of Scams Per Framework Layer

Count of URL	
Framework Layer	**Total**
Application	3300
Application / UI	1048
UI	4875
UI / Application	218
UI / Infrastructure	19
Unclassified	429
Grand Total	**9889**

The above table clearly shows that the maximum number of scams have occurred in the Application, Application/UI, UI, and UI/Application layers. The infrastructure layer is the least affected, but if an attack occurs at the infrastructure layer, the impact is huge.

3.2 Fraud Type vs Layer

Figure 2 and Table 6 explain the distribution of fraud types over different layers. While it highlights how specific scams, such as phishing or Fake Wallets, concentrate on the UI layer, it also briefs how the DAO and Flash Loan attacks impact the Application layer.

3.3 Layer vs Scam Type Matrix

Table 7 lists the number of fraud types for each of the three framework layers, as well as the number of unclassified fraud types in the dataset.

3.4 Heatmap Analysis

Table 8 displays a conditional-formatted pivot heatmap showing the intensity of scam types across each framework layer.

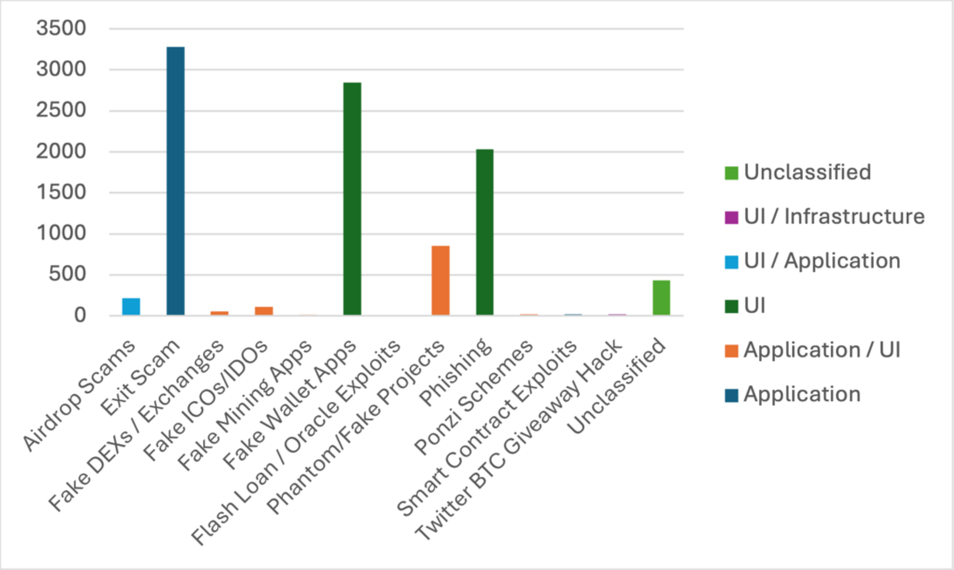


Fig. 2: Bar Chart Showing Fraud Type vs Framework Layer

Table 6. Count of Fraud Type vs Framework Layer

	Count of Framework Layer	
Fraud Type	**Framework Layer**	**Total**
Airdrop Scams	UI / Application	218
Airdrop Scams Total		**218**
Exit Scam	Application	3282
Exit Scam Total		**3282**
Fake DEXs / Exchanges	Application / UI	54
Fake DEXs / Exchanges Total		**54**
Fake ICOs/IDOs	Application / UI	110
Fake ICOs/IDOs Total		**110**
Fake Mining Apps	Application / UI	14
Fake Mining Apps Total		**14**
Fake Wallet Apps	UI	2845
Fake Wallet Apps Total		**2845**
Flash Loan / Oracle Exploits	Application	2
Flash Loan / Oracle Exploits Total		**2**
Phantom/Fake Projects	Application / UI	850
Phantom/Fake Projects Total		**850**
Phishing	UI	2030
Phishing Total		**2030**
Ponzi Schemes	Application / UI	20
Ponzi Schemes Total		**20**
Smart Contract Exploits	Application	16
Smart Contract Exploits Total		**16**

Twitter BTC Giveaway Hack	UI / Infrastructure	19
Twitter BTC Giveaway Hack Total		**19**
Unclassified	Unclassified	429
Unclassified Total		**429**
Grand Total		**9889**

Table 7. Layer vs Scam Type Matrix

Fraud Type	**Application**	**Infrastructure**	**UI**	**Unclassified**
Airdrop Scams	218	0	218	0
Exit Scam	3282	0	0	0
Fake DEXs / Exchanges	54	0	54	0
Fake ICOs/IDOs	110	0	110	0
Fake Mining Apps	14	0	14	0
Fake Wallet Apps	0	0	2845	0
Flash Loan / Oracle Exploits	2	0	0	0
Phantom/Fake Projects	850	0	850	0
Phishing	0	0	2030	0
Ponzi Schemes	20	0	20	0
Smart Contract Exploits	16	0	0	0
Twitter BTC Giveaway Hack	0	19	19	0
Unclassified	0	0	0	429

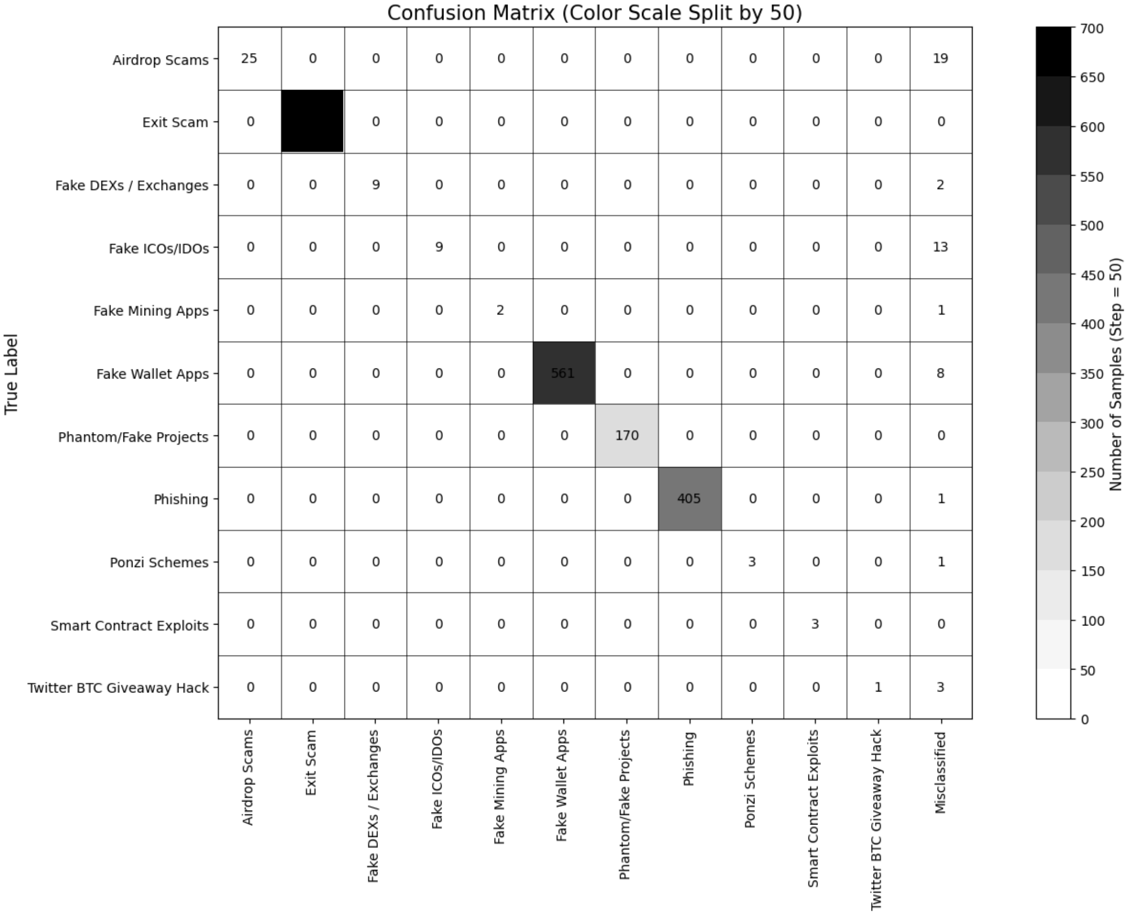
Table 8. Heatmap

Count of URL	**Framework Layer**						
Fraud Type	**Application**	**Application / UI**	**UI**	**UI / Application**	**UI / Infrastructure**	**Unclassified**	**Grand Total**
Airdrop Scams				218			218
Exit Scam	3282						3282
Fake DEXs / Exchanges		54					54
Fake ICOs/IDOs		110					110
Fake Mining Apps		14					14
Fake Wallet Apps			2845				2845
Flash Loan / Oracle Exploits	2						2
Phantom/Fake Projects		850					850
Phishing			2030				2030
Ponzi Schemes		20					20
Smart Contract Exploits	16						16
Twitter BTC Giveaway Hack					19		19

Unclassified						429	429
Grand Total	**3300**	**1048**	**4875**	**218**	**19**	**429**	**9889**

3.5 Key Observations and Findings

1. The main key observations and findings based on the analysis of the dataset are as follows:
2. The maximum number of scam incidents is faced at the Application and UI layers.
3. The most prevalent types of fraud are phishing, Rug Pulls, and Fake Wallets.
4. While it is rarely found. Infrastructure attacks can have significant impacts (e.g., validator compromise).
5. Since the emergence of GPT, AI-based scams like deepfakes and impersonation, as well as hybrid-layer scams, are increasing daily.
6. Scam patterns often revolve around events like ICO booms or DeFi waves.



	Airdrop Scams	Exit Scam	Fake DEXs / Exchanges	Fake ICOs/IDOs	Fake Mining Apps	Fake Wallet Apps	Phantom/Fake Projects	Phishing	Ponzi Schemes	Smart Contract Exploits	Twitter BTC Giveaway Hack	Misclassified
Airdrop Scams	25	0	0	0	0	0	0	0	0	0	0	19
Exit Scam	0		0	0	0	0	0	0	0	0	0	0
Fake DEXs / Exchanges	0	0	9	0	0	0	0	0	0	0	0	2
Fake ICOs/IDOs	0	0	0	9	0	0	0	0	0	0	0	13
Fake Mining Apps	0	0	0	0	2	0	0	0	0	0	0	1
Fake Wallet Apps	0	0	0	0	0	561	0	0	0	0	0	8
Phantom/Fake Projects	0	0	0	0	0	0	170	0	0	0	0	0
Phishing	0	0	0	0	0	0	0	405	0	0	0	1
Ponzi Schemes	0	0	0	0	0	0	0	0	3	0	0	1
Smart Contract Exploits	0	0	0	0	0	0	0	0	0	3	0	0
Twitter BTC Giveaway Hack	0	0	0	0	0	0	0	0	0	0	1	3

Fig. 3: Confusion matrix reconstructed from the classification report for multi-class cryptocurrency fraud detection. Correctly classified instances are shown along the diagonal, while misclassified samples are aggregated in the final column. The grayscale color scale is discretized in intervals of 50 samples to improve interpretability across classes with highly imbalanced support.

3.6 Scam Mapping Table

We structured the dataset in a scam mapping table, which includes the following fields: Year, Layer, Precautionary Measures, Description, Tools/Examples, Citation, and Why This Layer.

Table 9 illustrates the A-to-Z of Precautionary measures. It reflects how precautionary measures have evolved from simple regulatory oversight to smart contract design patterns to verified app badges.

Table 9. A to Z of Precautionary Measures

Year	Layer	Precautionary Measure	Description	Tools / Examples	Citation	Why This Layer?
2009	Infrastructure	Regulatory Oversight	Early crypto had no regulatory framework.	–	Foley et al. (2019)	The blockchain network lacked legal or operational controls.
2011	Infrastructure	Wallet Custody Review	Centralized platforms had insecure BTC storage.	–	Decker & Wattenhofer (2013)	Failures occurred in the backend wallet architecture and storage security.
2013	Application	Trustless Escrow	Needed to protect buyers/sellers on darknet markets.	–	Bartoletti et al. (2017).	Concerned with transaction-level execution logic.
2016	Application	Smart Contract Design Patterns	Avoid reentrancy & logic bugs in contracts.	Solidity best practices	Atzei et al. (2017)	Targeted issues in smart contract code.
2016	Application	Public Code Auditing	The transparency of the DAO code allowed community review.	GitHub, Etherscan	Atzei et al. (2017).	Refers to the open-source availability of on-chain application logic.
2017	UI	KYC/AML Checks	Identity verification to prevent fraud.	Token sales, ID docs	Fenu et al. (2018)	Interacts with user onboarding and platform interfaces.
2017	UI / App	GitHub/Whitepaper Disclosures	Projects used these to gain trust.	ICObench, GitHub	Fenu et al. (2018)	UI-level signal with implications for app credibility.
2017	Application	Escrow-Based Fund Control	Escrow holds release funds based on progress.	Tezos, multisig wallets	Fenu et al. (2018)	Embedded within smart contract fund management logic.
2018	UI	Wallet Custody Awareness	Encouraged self-custody to avoid custodial scams.	Ledger, T.	(Zetzsche et al., 2024).	Concerns wallet UX and user-side trust.
2018	Infrastructure	Use of DEXs	Avoided centralized failure via on-chain trades.	Uniswap, P.	(Lim et al., 2025).	Affects protocol-level architecture.
2019	UI	Scam Wallet Blocklists	Crowdsourced flagged addresses.	EtherscamDB	Team, C. (2025, September 3)	Alerts are displayed in the wallet interface and on websites.
2020	UI	Giveaway Flagging	Alert users about fake double-your-BTC scams.	MetaMask, browser alerts	Huang et al. (2020)	Targets phishing that manipulates user inputs.
2020	Infrastructure	Admin Access Restriction	Addressed the compromise of internal platform tools.	Twitter backend	Huang et al. (2020)	Rooted in permission architecture and backend access layers.
2021	Application	Smart Contract Audits	External reviews of token contracts.	CertiK, Solidity Finance	Team, C. (2025, September 3)	Assess logic inside deployed contracts.

2021	Application	Liquidity Locking	Prevented instant rug pulls via locked liquidity.	Unicrypt	Team, C. (2025, September 3)	Affects DeFi contract behavior.
2021	UI	Community Alert Forums	Raised scam warnings.	Reddit, Telegram	Team, C. (2025, September 3)	Operated at the interface/social layer.
2022	Infrastructure	Validator Monitoring	Dashboard for signer behavior detection.	Custom tools	Luo et al. (2024)	Aimed at validator node operations.
2022	Infrastructure	Threshold Signatures	Used MPC to split validator keys.	Fireblocks	Luo et al. (2024)	Operates at the consensus/control layer of the chain.
2023	UI	Anti-Phishing Extensions	Blocks access to scam clones.	WalletGuard, PhishFort	(Hu et al., 2025)	Protects front-end interactions.
2023	UI	Chain Abuse Reports	Public registry of scams.	chainabuse.com	(Kirobo, 2024)	Crowdsourced data for users.
2023	UI	Seed Phrase Alerts	Warns the user when they enter keys in the wrong places.	MetaMask UI	(Ogundokun et al., 2023)	Built into UI interaction behavior.
2024	Application	TWAP Oracles	Prevent rapid price shifts via oracles.	Uniswap v3	Zhou et al. (2024)	Part of the on-chain price calculation logic.
2024	Application	Risk Simulators	Stress-test for extreme market cases.	Gauntlet	Zhou et al. (2024)	Predicts protocol behavior pre-attack.
2024	Application	Flash Loan Rate Limiters	Restricts uncollateralized borrowing.	Aave	Zhou et al. (2024)	Integrated at the contract level.
2025	UI	Deepfake Detection APIs	Detects synthetic visual impersonations.	Sensity AI, Deepware	Kesavarajah et al (2025).	Prevents trust-based user deception.
2025	UI	Blockchain ID (PoP, BrightID)	Verify the project owner's legitimacy.	ENS, Proof of Humanity	Kesavarajah et al (2025)	Ties project identity to a real person via the user interface.
2025	UI	Verified App Badges	Mark trusted apps/dApps in the wallet UI.	MetaMask "Verified Origin"	Kesavarajah et al (2025)	Built into the user selection layer for trust.

3.7 Non-Uniform Evolution of Prevention Measures

The prevention measures from 2009 to 2025, as seen in Table 9, have evolved non-uniformly. Hence, it is hard to explain them to the people, but they can be analyzed and explained more effectively if structured using the proposed three-layer framework. This is clear from tables 5-8. Since we can structure scams, we can structure the preventive measures as well in the proposed three layers, thereby making it easier to learn. Also, while there is a modest level of scam activity before 2016, a sharp, sustained increase thereafter is evident. This inflection is primarily due to rapid retail adoption of cryptocurrencies, the proliferation of DeFi platforms, and increased social-media-driven investment behavior. This finding demonstrates that fraud growth has outpaced the evolution of preventive controls, particularly at the user interface and application layers. The existing fraud mitigation strategies also seem to be primarily reactive. It highlights the urgency of adopting framework-based prevention approaches that evolve as platform complexity increases.

3.8 Layer-Wise Distribution of Scam Types

Tables 5, 6, 7, and 8 categorize scam types across the three layers and place UI Layer-based scams at the top of the list, suggesting that the primary vulnerability in cryptocurrency ecosystems is human factors, such as a lack of trust, interface-based deception, and social engineering. This directly answers Research Question 3, which questions whether consumer awareness is the most important requirement, and what gaps exist in understanding user knowledge and vulnerabilities. The tables confirm that consumer awareness is a critical yet under-addressed dimension of fraud prevention. The study fills the gap in understanding user knowledge and vulnerabilities. Application-layer scams rank second, including rug pulls and smart contract exploits. The infrastructure layer scam occurs rarely but has the highest impact. With the Application layer in the second position, it seems like stronger audit and governance mechanisms are needed within decentralized platforms.

3.9 Scam Types Distribution and Framework Coverage

Table 4 maps major scam types to the proposed three-layer framework. Findings show that more than 90% of identified scams can be logically assigned to one or more layers, and hence, the proposed three-layer model is comprehensive. Its practical validity is approved. Even the multi-layer scams, such as fake exchanges combined with phishing interfaces, highlight the interconnected nature of modern fraud but remain analyzable within the framework. This result empirically validates the framework's effectiveness and demonstrates its ability to unify previously fragmented preventive measures discussed in the literature. The comprehensiveness shown by the result supports the paper's objective that the three-layer abstraction is both minimal and sufficient for systematic fraud analysis.

3.10 Platform-Level Vulnerabilities and Prevention Gaps

Tables 1 and 2 compare observed scam vectors with existing prevention strategies across cryptocurrency platforms. The results confirm that the dominant attack surface is the UI, followed by the Application Layer. Sadly, a significant investment has been made in infrastructure security and smart contract audits, but comparatively only a little emphasis is placed on user interface safeguards and consumer education.

There is no denying that due to a lack of emphasis on preventive measures and consumer awareness at the UI level, UI-level scams remain dominant. The findings answer Research Question 2 by showing that current prevention measures operate in silos and are not fully aligned with real-world attack distributions. The findings further confirm that the framework-driven approach will enable platforms to identify neglected layers and allocate defenses accordingly.

3.11 Consumer Awareness and User-Facing Threats

Furthermore, UI-layer scams, as shown in Tables 6 and 7, highlight the pivotal role of consumer awareness in fraud prevention. Whether it is Phishing, fake wallets, impersonation, or AI-generated deepfakes, they all exploit interface trust rather than protocol weaknesses. These scams succeed not because of technological failures, but because of cognitive and usability gaps.

After analyzing the findings, it is evident that future research is needed on behavioral security, interface standardization, and warning mechanisms. Further, the technological countermeasures alone are insufficient without parallel investments in user-facing protections.

3.12 Comparative Analysis Across Time and Platforms

Table 1 and Table 9 together serve as a comparative lens for assessing fraud evolution and the effectiveness of fraud prevention, thanks to the proposed three-layer framework, which will now help cluster not only scam types but also prevention strategies. While the mapping of scam types to preventive mechanisms in Table 9 reveals non-uniformity across time and platforms, the new proposed three-layer framework can make it more fragmented and clustered, thereby making it easier to categorize and explain to the masses.

The above findings answer Research Question 4 by showing that a comparative, framework-based analysis is essential not only for identifying best practices but also for benchmarking platform defenses or the preventive measures by categorizing them across the three layers. Undeniably, without the three-layer framework, prevention strategies remain fragmented and complex to evaluate across heterogeneous cryptocurrency ecosystems.

3.13 Synthesis of Results

Finally, all of the above results demonstrate that cryptocurrency fraud-prevention measures have not been uniformly developed over the past 16 years. They are the weakest in the application and user interface layers. The results also provide enough evidence for the novelty, comprehensiveness, and correctness of the proposed three-layer framework. They enable systematic diagnosis of these vulnerabilities and provide a foundation for aligning fraud prevention strategies with real-world attack surfaces. While the study integrates empirical evidence with framework-driven interpretation, it addresses the dilemma that existing fraud prevention mechanisms remain ineffective due to the non-uniform evolution of preventive measures, their often-reactive nature. The study also proposes a solution for designing future prevention strategies holistically through a three-layer framework.

4. CONCLUSION AND FUTURE RESEARCH

This study introduced and validated a layered cryptocurrency fraud framework spanning the Infrastructure, Application, and UI layers. Evaluated on a real-world dataset of over 9,000 fraud records, the framework explained more than 90% of known scam types from 2009 to 2025, demonstrating its effectiveness in capturing the evolution of cryptocurrency fraud. The findings reveal that existing prevention strategies have largely been reactive, fragmented, and poorly integrated, particularly with respect to user awareness at the UI layer. From a practical perspective, the proposed framework offers a benchmarking tool for exchanges, DeFi platforms, and regulators to assess scam exposure and align technical safeguards with user-facing controls. Effective fraud mitigation requires a coordinated, layered approach combining smart contract audits, validator decentralization, UI-level warnings, regulatory oversight, and consumer education. Future research should explore larger and real-time datasets, integrate behavioral and transaction-level features, and develop AI-driven detection systems evaluated using standard performance metrics. Broader priorities include strengthening blockchain software architecture (Alzhrani et al., 2023), preparing for emerging risks such as quantum computing (Dwivedi et al., 2024), enhancing human cognitive resilience against scams (Perdana et al., 2024; Hasan et al., 2024), and reinforcing regulatory frameworks to address fraud-driven volatility and tax evasion (Sanz-Bas et al., 2022; Balbás et al., 2023). Overall, this work provides a practical foundation for improving fraud prevention and supporting safer cryptocurrency adoption.

REFERENCES

1. ABAQUS, Dassault Systèmes, 2014. ABAQUS Documentation, 6.14. ed. Providence, RI.
2. Ascione, L., Berardi, V.P., Giordano, A., Spadea, S., 2013. Buckling failure modes of FRP thin-walled beams. Composites Part B: Engineering 47, 357–364. https://doi.org/10.1016/j.compositesb.2012.11.006
3. Barbero, E.J., Raftoyiannis, I.G., 1994. Lateral and distortional buckling of pultruded I-beams. Composite Structures 27, 261–268. https://doi.org/10.1016/0263-8223(94)90087-6
4. Baylor, R.N., 2021. A Parametric Study of Lateral-Torsional Buckling in Pultruded FRP Beams Using Abaqus (MS). West Virginia University Libraries. https://doi.org Acharya, B., Saad, M., Cinà, A. E., Schönherr, L., Nguyen, H. D., Oest, A., Vadrevu, P., & Holz, T. (2024). Conning the Crypto Conman: End-to-End Analysis of Cryptocurrency-based Technical Support Scams (No. arXiv:2401.09824). arXiv. https://doi.org/10.48550/arXiv.2401.09824
5. Alejandro Balbás (Ed.). (2023). Cryptocurrency risks, fraud cases, and financial performance. In *Risks* (p. 51). https://doi.org/10.3390/risks11030051
6. Alzhrani, F., Saeedi, K., & Zhao, L. (2023). Architectural patterns for blockchain systems and application design. In MDPI, Appl. Sci. (Vol. 13, p. 11533). https://doi.org/10.3390/app132011533
7. Atzei, N., Bartoletti, M., & Cimoli, T. (n.d.). A survey of attacks on Ethereum smart contracts.

8. Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency Scams: Analysis and Perspectives. IEEE Access, 9, 148353–148373. https://doi.org/10.1109/ACCESS.2021.3123894
9. Belenkov, N., Quantstamp, Inc., Callens, V., Quantstamp, Inc., Murashkin, A., Quantstamp, Inc., Bak, K., Quantstamp, Inc., Derka, M., Zircuit, Gorzny, J., Z., Lee, S.-S., & Quantstamp, Inc. (2023). SOK: A review of Cross-Chain Bridge hacks in 2023. *arXiv*.
10. Castro Severiche, K. E., Wahlqvist Odenman, A., & Jalali, A. (2025). Ponzi scheme detection and prevention in blockchain platforms using machine learning: A systematic literature review. In P. Delir Haghighi, M. Greguš, G. Kotsis, & I. Khalil (Eds.), *Information integration and web intelligence* (iiWAS 2024, Vol. 15342, pp. 123–140). Springer, Cham. https://doi.org/10.1007/978-3-031-78090-5_8
11. Childs, A. (2024). 'I guess that's the price of decentralisation… ': Understanding scam victimisation experiences in an online cryptocurrency community. *International Review of Victimology*, *30*(3), 539–555. https://doi.org/10.1177/02697580231215840 (Original work published 2024)
12. Decker, C., & Wattenhofer, R. (2013). Information propagation in the Bitcoin network. IEEE P2P 2013 Proceedings, 1–10. https://doi.org/10.1109/P2P.2013.6688704
13. Diepeveen, S., & Pinet, M. (2022). User perspectives on digital literacy as a response to misinformation. Development Policy Review, 40(S2). https://doi.org/10.1111/dpr.12671
14. Dwivedi, K., Agrawal, A., Bhatia, A., Tiwari, K., & Dept. of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, India, 333031. (2024). A novel classification of attacks on blockchain layers: vulnerabilities, attacks, mitigations, and research directions. In Journal of Information Security and Applications [Journal-article]. https://arxiv.org/abs/2404.18090v1
15. Fenu, G., Marchesi, L., Marchesi, M., & Tonelli, R. (2018). The ICO phenomenon and its relationships with the Ethereum smart contract environment. 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 26–32. https://doi.org/10.1109/IWBOSE.2018.8327568
16. Foley, S., Karlsen, J. R., & Putniņš, T. J. (n.d.). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? □.
17. Grobys, K., Dufitinema, J., Sapkota, N., & Kolari, J. W. (2022). What's the expected loss when Bitcoin is under cyberattack? A fractal process analysis. Journal of International Financial Markets Institutions and Money, 77, 101534. https://doi.org/10.1016/j.intfin.2022.101534
18. Hasan, A., Nahar, K., Akhter, S., & Atish Dipankar University of Science Technology, Bangladesh, Kustia Government College, Bangladesh, Notre Dame University College, Bangladesh. (2024). Cryptocurrency Scams: A Multi-Pronged approach to mitigating risks through regulation, enforcement, and consumer education. Munich Personal RePEc Archive. https://mpra.ub.uni-muenchen.de/121215/1/MPRA_paper_121215.pdf
19. Hu, X., Huazhong University of Science and Technology, He, N., Hong Kong Polytechnic University, Wang, H., & Huazhong University of Science and Technology. (2025). WalletProbe: a testing framework for browser-based cryptocurrency wallet extensions [Journal-article]. arXiv. https://arxiv.org/abs/2504.11735v1
20. Huang, H., Kong, W., Zhou, S., Zheng, Z., & Guo, S. (2020). A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools (No. arXiv:2007.03520). arXiv. https://doi.org/10.48550/arXiv.2007.03520
21. Kasula, V. K. (2024). AWARENESS OF CRYPTOCURRENCY SCAMS [Thesis]. In A. Alshboul, C. McMahon, & W. Taylor (Eds.), University of the Cumberlands. https://www.researchgate.net/publication/391531411
22. Kesavarajah, A., Tahiri, H., Cunningham, L., Pallath, R., Wu, T., & Popa, C. (2025). Deepfake Technology Unveiled: The Commoditization of AI and Its Impact on Digital Trust.
23. Kirobo, A. R. (2024). Security Vulnerabilities of Cryptocurrency Wallets -A Systematic Review [Review]. FUOYE Journal of Engineering and Technology, 9(4), 580–590. https://doi.org/10.46792/fuoyejet.v9i4.4
24. Kutera, M. (2022). Cryptocurrencies are a subject of financial fraud. In *Journal of Entrepreneurship, Management and Innovation* (Vol. 18, Issue 4, pp. 45–77) [Journal-article].
25. Lim, H.-J., Lee, S., Kim, M., & Lee, W. (2025). Comparative analysis of security features and risks in digital asset wallets. Electronics, 2436.
26. Luo, B., Zhang, Z., Wang, Q., Ke, A., Lu, S., & He, B. (2024). AI-powered Fraud Detection in Decentralized Finance: A Project Life Cycle Perspective (No. arXiv:2308.15992). arXiv. https://doi.org/10.48550/arXiv.2308.15992

27. Mukherjee, D., Moza, B., Ujjainia, P., Jain, P., Kochumon, S.K., Heisnam, L., S.A., & Dhondiyal, P. (2024). Evaluating public awareness on cryptocurrency exploitation via the dark web in different Indian states: a survey study. Asian Journal of Advances in Research, 7–7(1), 200–221. https://mbimph.com/index.php/AJOAIR/article/view/4088
28. Ogundokun, R. O., Arowolo, M. O., Damaševiˇcius, R., & Misra, S. (2023). Phishing detection in blockchain transaction networks using ensemble learning. In Lucia Seno (Ed.), Telecom (Vol. 4, pp. 279–297). https://doi.org/10.3390/telecom4020017
29. Osterrieder, J. (2021). Enhancing security in blockchain networks: anomalies, frauds, and advanced detection techniques. In the University of Twente, Department of High-Tech Business and Entrepreneurship, Netherlands (Vol. 1, pp. 1–6) [Journal-article]. University of Twente.
30. Owen, A., IU International University of Applied Sciences, Robert, E., & Morgan, H. (2025). Case studies of High-Profile money laundering cases involving Bitcoin and other cryptocurrencies. ResearchGate.
31. Perdana, A., Monash University, Jiow, H. J., & Singapore Institute of Technology. (2024). Crypto-Cognitive Exploitation: Integrating Cognitive, Social, and Technological perspectives on cryptocurrency fraud. In Telematics and Informatics [Journal-article]. https://doi.org/10.1016/j.tele.2024.102191
32. Reddy, K., Agarwal, S., Kothari, N., Ku, U., Chaplot, P., & Naveed, M. (2024). A study on the scams of Cryptocurrency. In International Journal of Humanities, Social Science and Management (IJHSSM) (Vols. 2–2, pp. 481–496) [Journal-article]. https://ijhssm.org/issue_dcp/A%20Study%20on%20the%20Scams%20of%20Cryptocurrency.pdf
33. Sanz-Bas, D., Del Rosal, C., Alonso, S. L. N., & Fernández, M. Á. E. (2022). Cryptocurrencies and fraudulent transactions: risks, practices, and legislation for their prevention in Europe and Spain. Laws, 10(3), 57. https://doi.org/10.3390/laws10030057
34. Shahzad, M. F., Xu, S., Weng Marc Lim, H., M. F., & Nusrat, S. (2024). Cryptocurrency awareness, acceptance, and adoption: the role of trust as a cornerstone. In *HUMANITIES AND SOCIAL SCIENCES COMMUNICATIONS* (Vol. 11, Issue 4). https://doi.org/10.1057/s41599-023-02528-7
35. Shiney, P., Navya, R., & Madhubala, B. (2024). A STUDY ON CONSUMER AWARENESS AND GRATIFICATION TOWARDS CRYPTOCURRENCY IN DIGITAL TRANSFORMATION. Rabindra Bharati University Journal of Economics, XXVIII–XXVIII(5), 165–166. https://www.researchgate.net/publication/385866784
36. Team, C. (2025, September 3). The 2022 Global Crypto Adoption Index: Emerging markets lead in grassroots adoption, China remains active despite the ban, and crypto fundamentals appear healthy. Chainalysis. https://www.chainalysis.com/blog/2022-global-crypto-adoption-index/
37. Team, C. (2025b, September 3). *The 2024 Global Adoption Index: Central & Southern Asia and Oceania (CSAO) region leads the world in terms of global cryptocurrency adoption*. Chainalysis. https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/
38. Ye, G., Hong, G., Zhang, Y., & Yang, M. (2024). Interface Illusions: Uncovering the rise of visual scams in cryptocurrency wallets. Proceedings of the ACM Web Conference 2022, 1585–1595. https://doi.org/10.1145/3589334.3645348
39. Zetzsche, D., Nikolakopoulou, A., University of Luxembourg, FinTech National Centre of Excellence, & Maurits van Ek. (2024). Crypto custody and crypto wallets [Journal-article]. https://ssrn.com/abstract=4769396
40. Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., & Gervais, A. (2023). SoK: Decentralized Finance (DeFi) Attacks (No. arXiv:2208.13035). arXiv. https://doi.org/10.48550/arXiv.2208.13035/10.33915/etd.10216
41. Correia, J.R., Branco, F.A., Silva, N.M.F., Camotim, D., Silvestre, N., 2011. First-order, buckling and post-buckling behaviour of GFRP pultruded beams. Part 1: Experimental study. Computers & Structures, Civil-Comp 89, 2052–2064. https://doi.org/10.1016/j.compstruc.2011.07.005
42. Davalos, J.F., Qiao, P., 1997. Analytical and Experimental Study of Lateral and Distortional Buckling of FRP Wide-Flange Beams. Journal of Composites for Construction 1, 150–159. https://doi.org/10.1061/(ASCE)1090-0268(1997)1:4(150)
43. Estep, D.D., 2014. Bending and Shear Behavior of Pultruded Glass Fiber Reinforced Polymer Composite Beams With Closed and Open Sections - ProQuest. West Virginia, Morgantown,.
44. Ganesan, G., Kumaran, G., 2018. An experimental study on the behaviour of GFRP pultruded I beam reinforced with CFRP laminates. IJATEE 5, 232–242. https://doi.org/10.19101/IJATEE.2018.545012

45. Halim, A.H., 2020. Lateral torsional buckling of thin-walled rectangular and I-section laminated composite beams with arbitrary layups. KANSAS STATE UNIVERSITY, Manhattan, Kansas.
46. Karthick, K., Soundararajan, M., Kasiviswanathan, M., 2023. Torsional behavior of laminated composite FRP beams. AIP Conference Proceedings 2856, 040003. https://doi.org/10.1063/5.0165251
47. Liu, T., 2017. STABILITY BEHAVIOR OF PULTRUDED GLASS-FIBER REINFORCED POLYMER I-SECTIONS SUBJECT TO FLEXURE (PhD Thesis). University of Pittsburgh.
48. Liu, T., Harries, K.A., 2018. Flange local buckling of pultruded GFRP box beams. Composite Structures 189, 463–472. https://doi.org/10.1016/j.compstruct.2018.01.101
49. Liu, T., Vieira, J.D., Harries, K.A., 2019. Lateral torsional buckling and section distortion of pultruded GFRP I-sections subject to flexure. Composite Structures 225, 111151. https://doi.org/10.1016/j.compstruct.2019.111151
50. Mottram, J.T., 1992. Lateral-torsional buckling of a pultruded I-beam. Composites 23, 81–92. https://doi.org/10.1016/0010-4361(92)90108-7
51. Pandey, M.D., Kabir, M.Z., Sherbourne, A.N., 1995. Flexural-torsional stability of thin-walled composite I-section beams. Composites Engineering 5, 321–342. https://doi.org/10.1016/0961-9526(94)00101-E
52. Qiao, P., Zou, G., Davalos, J., 2002. EXPERIMENTAL AND ANALYTICAL EVALUATION OF LATERAL BUCKLING OF FRP COMPOSITE CANTILEVER I-BEAMS.
53. Sapkás, Á., Kollár, L.P., 2002. Lateral-torsional buckling of composite beams. International Journal of Solids and Structures 39, 2939–2963. https://doi.org/10.1016/S0020-7683(02)00236-6
54. Silva, N.M.F., Camotim, D., Silvestre, N., Correia, J.R., Branco, F.A., 2011. First-order, buckling and post-buckling behaviour of GFRP pultruded beams. Part 2: Numerical simulation. Computers & Structures, Civil-Comp 89, 2065–2078. https://doi.org/10.1016/j.compstruc.2011.07.006
55. Singh, S.B., Chawla, H., 2019. Stability and failure characterization of fiber reinforced pultruded beams with different stiffening elements, Part I: Experimental investigation. Thin-Walled Structures 141, 593–605. https://doi.org/10.1016/j.tws.2018.10.020
56. Thumrongvut, J., Seangatith, S., 2011. Experimental Study on Lateral-Torsional Buckling of PFRP Cantilevered Channel Beams. Procedia Engineering, The Proceedings of the Twelfth East Asia-Pacific Conference on Structural Engineering and Construction 14, 2438–2445. https://doi.org/10.1016/j.proeng.2011.07.306
57. Timoshenko, S.P., Gere, J.M., 2012. Theory of Elastic Stability. Courier Corporation.
58. Vieira, E.D.S., Vieira, J.D., Cardoso, D.C.T., 2018. LOCAL BUCKLING OF PULTRUDED GFRP I-SECTION SUBJECT TO BENDING, in: Proceedings of the 4th Brazilian Conference on Composite Materials. Presented at the Brazilian Conference on Composite Materials, Pontifícia Universidade Católica do Rio de Janeiro, pp. 447–455. https://doi.org/10.21452/bccm4.2018.06.05
59. Vieira, J.D., Liu, T., Harries, K.A., 2018. Flexural stability of pultruded glass fibre-reinforced polymer I-sections. Proceedings of the Institution of Civil Engineers - Structures and Buildings 171, 855–866. https://doi.org/10.1680/jstbu.16.00238
60. Zeinali, E., Nazari, A., Showkati, H., 2024. Numerical Evaluation of Lateral Torsional Buckling of PFRP Channel Beams under Pure Bending. Sustainability 16, 303. https://doi.org/10.3390/su16010303

تقييم فعالية استراتيجيات منع الاحتيال في منظومة العملات المشفّرة

الملخص: منذ ظهور العملات المشفرة في عام 2009، عُدّت البديل الأبرز للعملات النقدية التقليدية. غير أن التزايد الملحوظ في عمليات الاحتيال شكّل تحدياً كبيراً أمام اعتمادها والثقة بها. وتُعد هذه الزيادة مصدر قلق جوهري للصناعة والجهات التنظيمية والمستخدمين على حد سواء. في ظل استمرار ظهور أنماط جديدة من الاحتيال المرتبط بالعملات المشفرة، في حين لا تزال استراتيجيات الوقاية مجزأة ويشوبها انخفاض مستوى وعي المستهلك. نجح الإطار المقترح في ربط أنواع الاحتيال بمواطن الضعف ذات الصلة، وتفسير أكثر من 90% من حالات الاحتيال الواقعية باستخدام استراتيجيات وقاية متعددة الطبقات. وفي حين تسلط هذه الدراسة الضوء على الفجوات في تطور أساليب الوقاية والحاجة إلى وعي وضوابط متعددة المستويات، فإنها تدرس فعالية استراتيجيات منع الاحتيال وتحدد الأنماط التي تستغل الثغرات عبر مختلف الطبقات. واستناداً إلى تحليل زمني لعمليات الاحتيال في العملات المشفرة من عام 2009 إلى 2025 وبالإعتماد على مراجعة منهجية للأدبيات العلمية، طورت الدراسة إطاراً ثلاثي الطبقات للاحتيال يشمل: البنية التحتية، والتطبيق، وواجهة المستخدم. كما جرى التحقق من صحة الإطار باستخدام منطق تصنيف قائم على القواعد، مثل رصد الكلمات المفتاحية والمنطق الشرطي، وذلك بالاعتماد على مجموعة بيانات تضم 9000 سجل.

كلمات مفتاحية: الاحتيال، ثغرات البلوك تشين، وعي المستهلك، تنظيم العملات المشفرة، الاحتيال في العملات المشفرة، التصيد الاحتيالي، استغلال الثغرات في العقود الذكية