frontiers | Frontiers in Blockchain

TYPE Review
PUBLISHED 27 November 2025
DOI 10.3389/fbloc.2025.1713637

OPEN ACCESS

EDITED BY
Nader Sohrabi Safa,
University of Worcester, United Kingdom

REVIEWED BY
Shalini Singh,
Christ University, India
Ademola Salako,
Sam Houston State University, United States

*CORRESPONDENCE
S. P. Meenakshi,
spmeenakshi@vit.ac.in
Akinlemi Olushola,
akinlemi.o2022@vitstudent.ac.in

RECEIVED 26 September 2025
REVISED 01 November 2025
ACCEPTED 10 November 2025
PUBLISHED 27 November 2025

CITATION
Olushola A and Meenakshi SP (2025) Cybersecurity crimes in cryptocurrency exchanges (2009–2024) and emerging quantum threats: the largest unified dataset of CEX and DEX incidents.
Front. Blockchain 8:1713637.
doi: 10.3389/fbloc.2025.1713637

Cybersecurity crimes in cryptocurrency exchanges (2009–2024) and emerging quantum threats: the largest unified dataset of CEX and DEX incidents

Akinlemi Olushola* and S. P. Meenakshi*

School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Cryptocurrency exchanges are integral to the digital asset economy; however, their rapid growth has been accompanied by recurrent high-impact cyberattacks that erode trust and inflict substantial losses. Guided by the PRISMA-ScR framework, this review systematically screened peer-reviewed and industry sources to construct a validated dataset of 220 major incidents (2009–2024) across centralized (CEX) and decentralized (DEX) exchanges. We classify attack vectors, analyze repeated high-impact patterns, and identify systemic vulnerabilities spanning cryptographic mechanisms and exchange infrastructure. Across CEX platforms, four of ten identified attack types accounted for 62 of the 80 incidents and approximately $1.764 billion in losses (42.1% of the $4.191 billion CEX total). Across DEX platforms, five of eighteen attack types were responsible for 120 of 140 incidents, totaling $3.755 billion (87.3% of the $4.303 billion DEX total). The overall losses sum to $8.494 billion across 220 incidents (80 CEX; 140 DEX). Repeated vectors comprised 182/220 incidents and $5.519 billion (65.0%) of losses, dominated by wallet/key compromise (78 incidents; $2.394 billion) and DEX system/server/protocol exploits (56 incidents; $1.939 billion); these two classes account for 134/182 repeated incidents (79.1%) and $4.333 billion (78.5%) of repeated losses. We examine the susceptibility of cryptographic defenses to emerging quantum adversaries and assess the exchange readiness for post-quantum threats. This study is the first to systematically compile and quantitatively analyze cybercrime incidents affecting both centralized and decentralized cryptocurrency exchanges in a unified dataset, enabling unprecedented comparability of systemic risks with actionable insights for cybersecurity researchers, regulators, and exchange operators seeking quantum-safe infrastructure evolution.

KEYWORDS

cryptocurrency exchanges, cybersecurity incidents, centralized vs. decentralized exchanges, wallet/key compromise, system/server exploit, smart contracts, PRISMA-ScR, post-quantum cryptography

1 Introduction

Cryptocurrencies and cryptocurrency exchange platforms (CExPs), encompassing both centralized (CEX) and decentralized (DEX) exchanges, are intrinsically linked, with exchanges providing the essential infrastructure that facilitates transactions and drives global adoption (Kim and Lee, 2018). In this study, we used CExPs when referring to exchanges generically and CEX/DEX when distinguishing between the two types. Cryptocurrency has become a global phenomenon in the 21st century (Corbet et al., 2019b) and has attracted increasing levels of cybercrime, particularly against CExPs, which serve as the primary conduits for cryptocurrency transactions (Vital, 2022; Manimuthu et al., 2019; Connolly and Wall, 2019). Despite the challenges of transacting outside formal venues, the sustained growth in the acceptance of cryptocurrencies as an alternative to fiat currency is underpinned by the security and trust provided by exchanges (Bucko et al., 2015; Kawai et al., 2023). In practice, CExPs expand cryptocurrency usability by offering user-friendly rails for liquidity, rapid settlement, and broad accessibility (Oliva et al., 2019; Arli et al., 2021) (Supplementary Tables S1, S2).

Since 2009, at least 220 high-impact cyberattacks have been reported in exchanges, with a total of approximately $8.494 billion (Chainalysis, 2022; Vidal-Tomás, 2022; Giechaskiel, 2016). These incidents span both centralized exchanges (CEXs) and decentralized exchanges (DEXs), the two dominant architectures in the ecosystem, where CEXs are custodial order-book venues and DEXs are non-custodial smart-contract protocols (e.g., AMMs or on-chain order books). Together, CEX and DEX represent the core infrastructure of the global cryptocurrency economy, serving over 500 million users by 2024 and facilitating the majority of cryptocurrency liquidity and settlement (IMARC Group, 2023; Jani, 2018). Other venues, such as OTC desks, P2P platforms, and custodial brokers, exist, but their transaction volumes and user bases remain marginal compared to CEX and DEX. Hence, this study focused on these two dominant exchange types.

Exchanges are integral to digital finance, enabling the buying, selling, and conversion of assets such as Bitcoin and Ethereum (Marella et al., 2021; Rejeb et al., 2021), and they play a central role in liquidity formation, price discovery, and on-/off-ramping between fiat and crypto (Chutipat et al., 2023). As of May 2024, over 500 exchanges were operating globally (CoinMarketCap, 2023; Future Market Insights, 2023; Triple-A Technologies Pte. Ltd., 2024). Binance led spot and derivatives activities, often processing tens of billions of dollars in daily volume across markets, while other major venues, including Coinbase, Bybit, and Kraken, contributed materially to market liquidity and user trust (Cambridge Centre for Alternative Finance, 2017a).

By late 2024, the global crypto market capitalization was approximately $2 trillion (Chainalysis, 2023b). Annual trading volumes further highlight the market's scale: in 2024 alone, the top-15 centralized spot exchanges (CEXs) processed $18.8 trillion; the top-10 decentralized exchanges (DEXs) handled $1.76 trillion; and derivatives trading volumes were even higher, reaching $58.5 trillion on the top-10 centralized exchanges offering perpetual contracts and $2.9 trillion on their decentralized counterparts (CCData, 2025; DefiLlama, 2025a; DefiLlama, 2025b; DefiLlama, 2025c). In parallel, user adoption is expected to expand to an estimated 600 million global crypto users by the end of 2024 (IMARC Group, 2023; Jani, 2018). The growing participation of both retail and institutional investors further amplifies the systemic importance of crypto exchanges (Coinpedia, 2023; Chainalysis, 2023a).

The same characteristics that make exchanges efficient, high-throughput, deep liquidity, and global access also increase their attractiveness to attackers (Al-Amri, 2019; Oosthoek, 2021; Ahuja, 2023; Basilan, 2024). As the value of assets under custody increases, there is an incentive for sophisticated attacks (Rot and Blaicke, 2019). The pseudonymity and cross-jurisdictional nature of blockchain flows complicate asset tracing and recovery, whereas weaknesses in wallet/key management, authentication, and transaction-validation pipelines remain persistent pressure points (Crystal Blockchain, 2024b; Hedge with Crypto, 2024; Crystal Blockchain, 2024a; Sigurdsson et al., 2020; Adamik and Kosta, 2019; Shaji et al., 2022). Historically, attacks have included phishing, credential theft, malware, insider abuse, protocol and smart contract exploits, and large-scale DDoS events that exploit the gaps in both operational controls and cryptographic guardrails (Feder et al., 2017; Alia, 2014). In 2024 alone, over ten major breaches were recorded, with losses exceeding $1.018 billion (Berry, 2022); a notable example is the WazirX incident of July 2024 (approximately $230million) (Crystal Intelligence, 2024). These incidents further reveal critical weaknesses in wallet security (Erinle et al., 2023), authentication protocols, and transaction validation mechanisms (Homoliak and Perešíni, 2024), and continue to drive regulatory responses (e.g., KYC/AML regimes) across jurisdictions (Mohsin, 2022; Mateen, 2023; Ruiz et al., 2022; Zhou et al., 2023; Soana, 2024), which often address symptoms rather than root causes in the system architecture.

An additional risk acceleration is the prospective impact of quantum computing (Faruk et al., 2022; Bergstrom, 2024). Algorithms such as Shor and Grover threaten the hardness assumptions of widely deployed schemes (RSA and ECC) with implications for key custody, signatures, and consensus security (Fernández-Caramés, 2020; Easa et al., 2023; Vasavi and Latha, 2019). Given the "harvest-now, decrypt-later" risk, the key material exfiltrated today can be decrypted by future quantum adversaries, thereby increasing the urgency for migration to post-quantum cryptography (PQC) (Roy, 2019; Thanalakshmi et al., 2023). Leading PQC families, including lattice-based KEMs and signatures, hash-based signatures, and multivariate schemes, offer candidates for hardening key exchanges, authentication, and protocol design.

Against this backdrop, prior reviews have often conflated exchange-related incidents with wallet-only breaches or broader DeFi exploits, limiting comparability and obscuring systemic vulnerabilities specific to exchange infrastructure. Wallet-only breaches are often driven by end-user errors, such as private key mismanagement or phishing, whereas exchange breaches expose deeper architectural flaws in custodial systems, smart contracts and liquidity protocols. By isolating exchange-specific incidents, this study provides the first PRISMA-ScR scoping review that systematically maps systemic risks across CEX and DEX platforms. Furthermore, the 220 incidents analyzed not only revealed recurrent attack vectors but also highlighted the fragility of cryptographic mechanisms that face existential threats from quantum-capable adversaries. Linking historical breach patterns to quantum-era risks strengthens the case for urgent migration to

post-quantum cryptography in exchange infrastructure. This dual focus, systemic cyber risk, and quantum-era cryptographic fragility position the study to inform both immediate resilience strategies and long-term PQC migration pathways.

Despite the growing body of research on blockchain security, two critical research gaps remain unaddressed. First, the literature lacks a unified, longitudinal synthesis that isolates exchange-specific cyber incidents and compares systemic vulnerabilities across CEX and DEX architectures. Second, very few studies integrate post-quantum cryptographic readiness into the analysis of exchange security, even though quantum threats directly challenge the cryptographic foundations of trading, custody, and consensus. Addressing these interlinked gaps is essential to align historical evidence with the technological transition toward quantum-resilient infrastructures and to guide both academic inquiry and regulatory preparedness in the digital-asset domain.

This review critically investigates the evolving cybersecurity dynamics of cryptocurrency exchanges by examining both their historical vulnerabilities and their readiness for quantum-era threats. In direct response to the identified research gaps, the study pursues two overarching aims: first, to provide a unified, exchange-specific synthesis that compares systemic vulnerabilities across centralized (CEX) and decentralized (DEX) platforms; and second, to evaluate the preparedness of exchange cryptographic infrastructures for post-quantum migration. Specifically, we (i) conduct a systematic review and classification of repeated high-impact incidents involving exchanges from 2009 to 2024, (ii) identify common vulnerabilities and recurring attack vectors that have compromised exchange security, (iii) assess quantum-era risks to current cryptographic infrastructures, and (iv) offer actionable post-quantum–ready recommendations for exchanges and policymakers (Navarro, 2019). Unless otherwise stated, dollar amounts are USD (nominal, not inflation-adjusted), and reported volumes refer to calendar year 2024 benchmarks (CCData, 2025; DefiLlama, 2025a; DefiLlama, 2025b; DefiLlama, 2025c).

Beyond addressing these gaps, this study contributes to both theory and practice. Theoretically, it extends the understanding of cybersecurity resilience in digital-asset infrastructures by providing a longitudinal, exchange-specific taxonomy of high-impact incidents. Methodologically, it demonstrates how a PRISMA-ScR framework can be adapted to synthesize technical breach data across heterogeneous blockchain ecosystems. Managerially and for policy, the findings generate actionable insights for exchange operators, cybersecurity agencies, and regulators seeking to strengthen governance standards and guide post-quantum transition strategies. Collectively, these contributions position the review as a reference baseline for future empirical, regulatory, and cryptographic research on exchange security.

The remainder of this paper is organized as follows: Section 2 reviews the background and related studies. Section 3 details the PRISMA-ScR scoping methodology and data extraction pipeline. Section 4 briefly introduces exchange platforms (CEX/DEX), security/architecture, and frames the high-impact crimes. Section 5 presents the incident corpus and results (taxonomy, trends, cross-platform comparisons, losses, and repeated vectors). Section 6 analyzes the attack techniques and patterns, whereas Section 7 emphasizes classical cryptographic vulnerabilities and defenses. Section 8 expands on post-quantum threats and the PQC readiness of the CExPs. Section 9 discusses the synthesis of the results, limitations, research gaps, and recommendations. Finally, Section 10 concludes the study.

2 Background and related work

Although many publications discuss cryptocurrencies and related crimes, relatively few have analyzed the detailed mechanics of crimes against cryptocurrency exchange platforms (CExPs). Therefore, we review the literature most relevant to exchange security, emphasizing recent studies (2018–2024), which are summarized in Table 1.

Rising concerns over CExP security have driven studies on scams, cyberattacks, authentication, and cryptography, aimed at improving transparency, accountability, and resilience against both classical and quantum-enabled threats (Shalini and Santhi, 2019). The literature is synthesized below by theme:

2.1 Cryptocurrency exchange vulnerabilities and attacks

Vasek and Moore classified scams into four categories: fraudulent exchanges, Ponzi schemes, mining scams, and scam wallets, highlighting definitional challenges and the absence of systematic classifications (Vasek and Moore, 2018; Nabilou, 2020). Trozze et al. identified 29 types of fraud across academic and gray sources, underscoring research growth and the need for clearer definitions and collaboration (Trozze et al., 2022). Bartoletti et al. propose automated scam detection but note noisy labels and lack of a universal taxonomy (Bartoletti et al., 2021). Sigurdsson et al. (2020) and Chohan (2022) examined vulnerabilities (DDoS, phishing, social engineering, malleability, and double spending) paired with cost-raising countermeasures. Feder et al. analyzed the impact of DDoS on Bitcoin exchanges (Feder et al., 2017), whereas Abhishta et al. found that the activity typically normalizes within a day (Arli et al., 2021). Vasek et al. further highlighted malware and extortion, noting that theft declines after security upgrades (Vasek et al., 2014). Gottipati (2020) designed a defense model using Runtime Application Self-Protection (RASP) and Hardware Security Modules (HSMs), but focused only on centralized exchanges. Smith and Kahn De Saint Guilhem et al. (2020) proposed a composable framework for key exchange against man-in-the-middle attacks, although there is a lack of deployment evidence.

Gap: These studies propose defenses but none compile a longitudinal, unified dataset of high-impact crimes across both CEX and DEX.

2.2 Authentication and security in cryptocurrency exchanges

Chenchev et al. (2021) surveyed wallet authentication methods such as passwords, biometrics, MFA, blockchain-based methods, and stress persistent weaknesses. Homoliak and Perešíni, 2024 introduced "k-factor" authentication using threshold cryptography but focused narrowly on wallets. Doe and Smith Zhang et al. (2024) propose a privacy-preserving, threshold authentication framework, though centralization and scalability remain issues. Alghamdi et al. (2024)

TABLE 1 Review studies on cryptocurrency exchange vulnerabilities (2014–2024). Panel A reports yearly counts; Panel B lists study-level details.

Panel A – Yearly review-paper counts on cryptocurrency exchanges (2014–2024)										
Year	2014	2015	2017	2018	2019	2020	2021	2022	2023	2024
Papers	1	1	1	3	3	3	2	2	2	3

Panel B – Review studies on cryptocurrency exchange vulnerabilities (2014–2024)					
S/N	Year	Author	Coverage	Review type	References
1	2014	Vasek et al.	DoS attacks in bitcoin ecosystem	Empirical analysis	Vasek et al. (2014)
2	2015	Muthukumar Arunachalam et al.	Biometric authentication with cryptography	Survey	CoinMarketCap (2023)
3	2017	Bayu Adhi Tama	Blockchain applications and challenges	Critical review	Fernández-Caramés (2020)
4	2018	Kim and Lee	Risk management in cryptocurrency exchanges	Review	Kim and Lee (2018)
5	2018	Mauro Conti et al.	Bitcoin security and privacy	Survey	Conti et al. (2018)
6	2018	Aaron Higbee et al.	Crypto-currency in cybercrime	Survey	Higbee et al. (2018)
7	2019	Shalini and H. Santhi et al.	Attacks in bitcoin and cryptocurrency	Survey	Arunachalam et al. (2015)
8	2019	Arunmozhi M. Animuthu et al.	Bitcoin as a global phenomenon	Literature review	Animuthu et al. (2019)
9	2019	Ahmed Afif Monrat	Blockchain applications and opportunities	Survey	Monrat et al. (2019)
10	2020	Fernández-Caramés and Fraga-Lamas	Post-quantum blockchain security	Review	Fernández-Caramés (2020)
11	2020	Shaen Cobet	Crypto cybercriminality	Survey	Corbet et al. (2019a)
12	2020	Gudmundur Sigurdsson et al.	Cryptocurrency security breaches	Survey	Sigurdsson et al. (2020)
13	2021	Massimo bartoletti et al.	Cryptocurrency scams	Survey	Bartoletti et al. (2021)
14	2021	Kyle Soska et al.	Cryptocurrency derivatives — BitMEX	Case study survey	Soska et al. (2021)
15	2022	Aditya Vikram Singh et al.	Cryptocurrencies as financial assets	Systematic analysis	Corbet et al. (2019b)
16	2022	O. Pal	Post-quantum blockchain cryptography	Review	Mosca et al. (2024)
17	2023	Chenchev et al.	Authentication mechanisms	Literature survey	Chenchev et al. (2021)
18	2023	Raya Jasim Easa	Quantum cybersecurity protection	Survey	Easa et al. (2023)
19	2024	U. Sumalatha et al.	Multimodal biometric authentication	Comprehensive review	Sumalatha et al. (2024)
20	2024	Olaiya et al.	Encryption techniques in fintech applications	Comprehensive review	Olaiya et al. (2024)
21	2024	Homoliak and Perešíni	Cryptocurrency wallets authentication methods	Security review	Homoliak and Perešíni (2024)

show multimodal biometric fusion reduces attack success rates but overlook governance and regulation. Goh et al. (2022) developed a multimodal fingerprint/iris framework with Adaptive Feature Hashing, offering unlinkability but lacking exchange-scale testing. Brown et al. (2020) integrate biometrics with blockchain and ML but omit stress tests and compliance considerations. Vasavi and Latha (2019) explored multimodal fusion with RSA, achieving accuracy but at the cost of latency.

Gap: Authentication research is fragmented and not systematically tied to large-scale CEX/DEX breach data.

2.3 Encryption techniques and their challenges

Olaiya et al. (2024) surveyed symmetric, asymmetric, hybrid, and homomorphic encryption and noted the performance, key management, and integration trade-offs, whereas advanced paradigms (homomorphic and PQC) remain early in deployment. However, empirical benchmarks and migration strategies are lacking.

Gap: Few works map encryption weaknesses directly to the high-impact vectors observed in CEX/DEX incidents.

2.4 Quantum threats and post-quantum cryptography (PQC)

Shor-type attacks expose RSA/ECDH/ECDSA, prompting studies on PQC for exchanges (Gill et al., 2022). Chen (2024) advocated for PQC signatures (Dilithium) but omitted broader PQC families or hybrid migration paths. Saha et al. integrate lattice- and hash-based PQC into blockchain, showing performance gains but neglecting multivariate/code-based families and live deployment (Saha et al., 2023). Other studies have highlighted PQC's importance of PQC against Shor and Grover (Rosch-Grace and Straub, 2021). Chen Dharminder et al. (2023) proposed an RLWE-based protocol with

TABLE 2 Summary of problems addressed and limitations in prior studies.

Problem addressed	Technique used	Issue solved	Limitation	References
Cryptocurrency Exchange scams	Classification of frauds (fraudulent exchanges, Ponzi schemes)	Identification of various scams and fraudulent activities	Lack of detailed analysis of fraudulent websites and applications	Xia (2020)
Bitcoin fraud	Review of 29 types of fraud via academic and gray literature	Understanding the types and scale of bitcoin fraud	Need for better definitions and cross-sector collaboration	Charoenwong et al. (2022); Vasek and Moore (2018)
Automated scam detection	Automated system based on a dataset of thousands of scams	Classification of scams to aid detection systems	Inaccurate data and lack of a universally accepted taxonomy	Bartoletti et al. (2021)
Security vulnerabilities in exchanges	Analysis of phishing, social engineering, DDoS, double-spending	Identification of attack vectors and suggestions for mitigation	Focus on vulnerabilities but no definitive solutions for all threats	Chohan (2022); Sigurdsson et al. (2020)
DDoS attacks on exchanges	Metrics like skewness and kurtosis, economic analysis	Measured the effects of DDoS on bitcoin exchanges' transaction volume	Short-term recovery, but no deep analysis on long-term effects	Feder et al. (2017); Abhishta et al. (2019)
Cryptocurrency Exchange security risks	Security protocols for malware, extortion, and DDoS attacks	Identified key risks and solutions like security improvements	Limited to centralized exchanges, ignoring decentralized exchanges	Vasek and Moore (2018); Conti et al. (2018)
Phishing and man-in-the-middle attacks	Key exchange protocols, RASP, and HSMs	Prevents man-in-the-middle and replay attacks	Limited to centralized exchanges and lacks empirical validation	Oosthoek et al. (2020); Purohit et al. (2023)
Biometric authentication in wallets	Password-based, biometric, multi-factor authentication	Improved authentication security and fraud prevention	Lack of standardization and challenges in real-world applications	Hendrix and Lewis (2021); Brown et al. (2020); Chenchev et al. (2021)
Authentication for cryptocurrency wallets	k-factor authentication, threshold cryptography	Provided a framework for evaluating wallet security	Did not address exchange-level security or decentralized wallets	Vasek et al. (2014)
Privacy-preserving authentication	Threshold authentication, Schnorr's protocol	Balances anonymity with traceability	Centralization risk, scalability concerns	Crystal Blockchain (2024a)
Multimodal biometric fusion	Fusion of fingerprint, face, age, gender biometrics	Enhanced security and robustness over unimodal methods	Lack of scalability testing, privacy concerns	Amirthalingam et al. (2014)
Adversarial attacks on biometric systems	Multimodal biometric fusion and attack resistance	Increased security against adversarial biometric attacks	Did not explore privacy and compliance issues	Kathed et al. (2019)
Encryption for cryptocurrency systems	Symmetric, asymmetric, hybrid, and homomorphic encryption	Addressed encryption efficiency, key management issues	Computational inefficiencies, lack of real-world deployment benchmarks	Yang et al. (2023); Olaiya et al. (2024)
Post-quantum cryptography for blockchain	Lattice-based, hash-based PQC algorithms	Secures cryptocurrency systems against quantum computing threats	Limited to specific PQC methods, no large-scale testing	Fernández-Caramés (2020); Gill et al. (2022); Chen (2024)
Post-quantum blockchain security	Lattice-based key exchange protocols (RLWE)	Protects key exchanges from quantum attacks	No advanced features like zero-knowledge proofs, scalability concerns	Fernández-Caramés (2020); Dharminder et al. (2023); Easa et al. (2023); Roy (2019)
Quantum threats to blockchain	Dilithium PQC, elliptic curve cryptography (ECC) comparison	Improved resistance to quantum attacks, faster transactions	Lacks broader PQC exploration, scalability for large exchanges uncertain	Easa et al. (2023); Chen (2024); Yang et al. (2023); AL-Mubayedh et al. (2019)
Consumer Trust after cyber-attacks	Analysis of compensation, transparency, and customer engagement	Provided strategies to regain consumer trust post-breach	No focus on the long-term effect on user behavior and trust rebuilding	Marella et al. (2021); Arli et al. (2021); Ku-Mahamud (2019)
Regulation and standards for exchanges	Regulatory frameworks, certification bodies like C4	Improved credibility and user trust through standardized practices	Lack of global enforcement and compliance issues	Arli et al. (2021); Kim and Lee (2018); Mohsin (2022); Mateen (2023)

good performance, but it lacked privacy features and large-scale optimization. Yi (2022) applies lattice-based cryptography to SIoT, improving key exchange, but exchange-scale feasibility is untested.

Gap: PQC studies focus on design but rarely connect with empirical exchange breach data which our dataset provides this missing link.

2.5 Consumer trust and accountability in exchanges

Marella et al. (2021), Arli et al. (2021) showed that trust recovery requires compensation, not apologies. Chohan (2022) called for transparency, monitoring, and accountability.

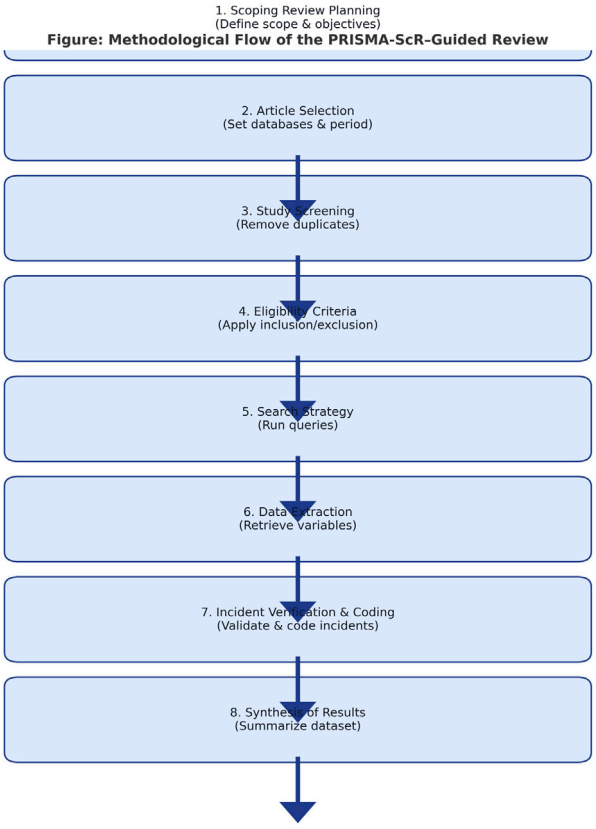

FIGURE 1
Workflow showing the major stages of the PRISMA-ScR methodology used in this study.

Gap: Trust research seldom links erosion directly to the repeated scale of CEX/DEX incidents.

2.6 Regulatory measures and global standards

Bucko et al. (2015) discussed certification bodies (e.g., C4) and global harmonization efforts (Xiong and Luo, 2024; Caliskan, 2022).

Gap: Regulatory work proposes frameworks but lacks quantitative grounding in the historical trajectory of high-impact incidents.

Synthesis of Gaps: Collectively, prior research covers scams, authentication, encryption, PQC, trust, and regulation. However, there is no comprehensive longitudinal dataset of high-impact incidents across the CEX and DEX. This study addresses this gap by compiling the largest unified dataset of 220 exchange-specific incidents (2009–2024), enabling cross-architecture comparisons, identification of repeated vectors, and contextualization of quantum-era risks (Table 2).

3 Review methodology

Figure 1 presents an overview of the PRISMA-ScR–guided methodology adopted in this study, illustrating the sequential stages from scoping and article selection to eligibility screening, data extraction, incident verification, and synthesis of results.

3.1 Scoping review

Scoping reviews systematically map the breadth and nature of research on established or emerging topics using an iterative, structured approach (Sarkis-Onofre et al., 2021; Mattos et al., 2023). This study aimed to analyze, evaluate, and classify existing studies on crimes against cryptocurrency exchange platforms (CExPs). We reviewed both peer-reviewed and gray literature sources (Vergara-Merino et al., 2021) on cybercrimes against exchanges (Souza et al., 2022). The review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses for Scoping Reviews (PRISMA-ScR) guidelines, with eligibility criteria defined *a priori* to ensure scope alignment and reproducibility (Tricco et al., 2016). In this study, "crime" is defined as any act (fraud, hacking, theft, or cyber-attack) committed to gain financial or asset benefits from exchanges.

3.2 Article selection methods

We conducted a scoping review of the academic and gray literature on crimes against cryptocurrency exchange platforms, focusing on repeated high-impact attack vectors affecting centralized (CEX) and decentralized (DEX) exchanges between 2009 and 2024. This review adhered to the PRISMA-ScR guidelines (Munn et al., 2018; Munn et al. 2022). Eligibility was determined based on publication type, language, topical relevance, and direct linkage to exchange securities.

3.3 Study selection

Searches were performed in the Web of Science, Scopus, and Google Scholar databases until 31 December 2024. In total, we identified 735 records (630 academic and 105 Gy literature articles). Duplicates were removed in Microsoft Excel using a two-pass procedure (pass 1: DOI-normalized exact match; pass 2: title-normalized + year for records without a DOI). All unique titles and abstracts were screened.

Academic literature. Of the 630 screened academic records, 301 underwent full-text reviews. After screening, 214 articles met all inclusion criteria and were retained, while 87 were excluded.

Gray literature. Of the 105 Gy records screened, 95 proceeded to full-text eligibility, 78 were finally included, and 17 were excluded during the title/abstract screening.

A total of 292 sources (214 academic and 78 Gy) met the inclusion criteria and were included in this review. The authors independently screened the studies, and disagreements were resolved through discussion. As shown in Figure 2, these counts align with the PRISMA-ScR flow diagram, ensuring full transparency at each stage.

3.4 Eligibility criteria

Although cryptocurrency security breaches occur across wallets, tokens, and broader DeFi protocols, this review explicitly focuses on exchange-centric incidents (centralized exchanges (CEX) and

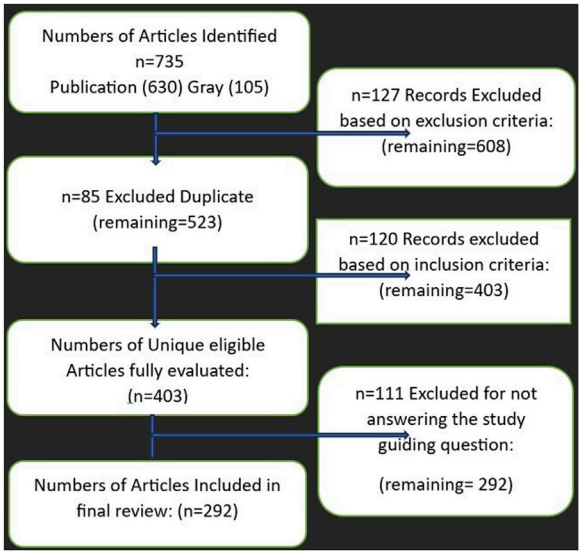

FIGURE 2
PRISMA-ScR flow diagram for study selection.

decentralized exchanges (DEX)). Wallet-only breaches were excluded because they primarily involve user-side vulnerabilities (e.g., private key mismanagement and phishing) rather than systemic flaws in the exchange infrastructure. Including such cases would blur the scope and reduce the comparability of the aggregated loss data. By restricting the inclusion to exchange-focused incidents, the review maintains analytic consistency with PRISMA-ScR and ensures that the findings remain directly relevant to exchange resilience, regulatory oversight, and post-quantum preparedness.

Only studies written in English were included. Eligible sources comprised peer-reviewed journal articles, conference papers, and formal reports (e.g., CERT advisories, technical white papers, and documented incident post-mortems) classified as gray literature. Editorials, opinion pieces, marketing materials, newsletters, and news articles were excluded from the study.

Topically, the included studies had to address crimes against CExPs (CEX or DEX) or their direct security posture (e.g., wallet/key management within exchanges, smart contract exchange logic, or bridges/oracles when tied to exchange incidents). We also included studies on quantum threats relevant to exchanges when they explicitly connected PQ/quantum risks (e.g., RSA/ECC compromise, Grover-related symmetric considerations) to exchange infrastructures or incident classes.

3.5 Search strategy

The complete database-specific queries are listed in Supplementary Table S3. Because Google Scholar restricts queries to approximately 256 characters, we executed the query set as multiple searches using the quoted phrases to control drift. The search was restricted to records published between January 2009 and December 2024. For gray literature, we restricted the results to English-language PDF files to ensure reproducibility. Both academic and gray searches included peer-reviewed articles, conference papers, theses, monographs, and technical reports. Duplicates across databases were systematically resolved using the two-pass procedure described above. Disagreements at the full-text inclusion stage were resolved by consensus.

3.6 Procedure for data extraction

As presented in Supplementary Table S4, we meticulously retrieved pertinent information for the scoping review by conducting structured searches across the Web of Science, Scopus, and Google Scholar. Multiple search strings were combined to extract relevant records. Google Scholar, which offers broader indexing coverage, provided the most robust results among the databases consulted.

3.7 Incident verification and coding

As shown in Figure 1, all steps were executed sequentially to ensure methodological transparency and reproducibility. Each incident was cross-verified across at least two independent sources such as exchange post-mortems, auditor reports, and regulatory filings to ensure authenticity and avoid double counting. Incidents were classified as major if the reported or independently confirmed financial loss exceeded USD 50,000 or caused service disruption exceeding 24 h. A standardized coding sheet was developed to capture the following variables: year, exchange type (CEX/DEX), loss magnitude, attack vector, recurrence status, and cryptographic relevance. Two reviewers independently coded all incidents, and intercoder agreement was assessed using percentage concordance (97%). Any discrepancies were resolved by discussion to maintain reliability and alignment with PRISMA-ScR transparency principles.

3.8 Scoping review results

Using the PRISMA-ScR framework (Stovold et al., 2014; Page et al., 2021), our systematic review process identified 735 sources (630 academic and 105 Gy). After removing duplicates and applying title/abstract and full-text screening, we included **292** sources (214 academic, 78 Gy). As shown in Figure 2, these numbers are aligned with the PRISMA-ScR flow diagram.

4 Brief history of cryptocurrency exchanges and cybersecurity crimes

4.1 Historical overview of cryptocurrency exchanges

When Bitcoin (BTC) was launched in 2009, it had no fixed market value and could only be obtained through mining or high-risk trades (Nakamoto, 2009; Wang et al., 2024b). The early exchange history was marked by fraud, hacks, and legal challenges, laying the groundwork for today's global

infrastructure (Al-Amri, 2019; Caliskan, 2021). Currently, more than 600 exchanges operate globally (Bartoletti et al., 2021; CoinMarketCap, 2025). Early transactions, such as those between Hal Finney and Satoshi Nakamoto on 12 January 2009, were experimental (Ruoti et al., 2020).

Before the 2008 Bitcoin white paper and 2009 Genesis Block Nakamoto (2009), trading occurred informally via forums or IRC and relied on trust. The first exchange, *bitcoinmarket. com*, was launched in March 2010 (Cryptohopper, 2023; World.org, 2023). By 2011, Mt. Gox had become the largest exchange and the site of the first major cybercrime (CoinDesk, 2023; Morin et al., 2023; Dimpfl and Flad, 2020). Hackers exploited a compromised hot wallet, crashing BTC prices from $17 to nearly zero and leaking user data. Despite this, Mt. Gox still handled 70% of global Bitcoin trade in 2013 before registering with FinCEN. Over time, exchanges have evolved with a greater focus on user experience and security (Gayathri et al., 2023; Fang et al., 2022). Leading platforms have introduced secure trading procedures (Watorek et al., 2020), although the regulatory burdens vary across jurisdictions (Mohsin, 2022).

4.1.1 CEX and DEX platforms

Cryptocurrency exchanges are privately run platforms in which users trade cryptocurrencies against fiat currencies or other assets (Czapliński et al., 2019; Bhaskar and Chuen, 2024). Orders can be executed at set prices or spot rates (Bentov et al., 2019; Keller and Scholz, 2019). Two main models exist: centralized (CEX) and decentralized (DEX) (Takahashi et al., 2019). Both aim to ensure liquidity, security, and rapid settlement, with some exchanges evolving into full trading platforms that offer analytical tools.

4.1.2 Centralized exchanges (CEXs)

In CEXs, a single authority manages the accounts and transactions (Zhou et al., 2022). They function like digital stock markets, earning fees and commissions (Patashkova et al., 2021). Its advantages include high liquidity, faster fund recovery, and selective asset listings. Drawbacks include custodial risks, centralized storage of sensitive data, and a history of price manipulation. The major CEXs include Binance, Bybit, Coinbase, Kraken, and KuCoin (Fu et al., 2022; Eigelshoven et al., 2021).

4.1.3 Decentralized exchanges (DEXs)

DEXs operate on distributed ledger technology without a central authority (Jain et al., 2021; Victor and Weintraud, 2021). Users control their keys and trade directly from their wallets, bypassing intermediaries and KYC requirements (Xu et al., 2023). They typically allow swaps within the same blockchain, such as Ethereum-based tokens. Its strengths include full custody, lower fees, higher privacy, and distributed hosting (Patel et al., 2019; Tripathi et al., 2023). Its weaknesses include low liquidity and limited interoperability. Examples include Uniswap, PancakeSwap, dYdX, and Kyber (Corbet et al., 2019a).

4.2 Overview of exchange security

4.2.1 Exchange architecture

Exchanges integrate multiple layers to enable asset trading, such as Bitcoin and Ethereum (Marella et al., 2021; Navarro, 2019). Their design combines security and efficiency across interconnected components. Supplementary Table S8 summarizes the layers, definitions, threats and defenses.

5 Cybersecurity incidents in cryptocurrency exchanges

From 2009 to 2024, cryptocurrency exchange platforms reported at least 220 high-impact security incidents, including hacks, thefts, scams, fraud, and breaches, arising from exploited vulnerabilities (Scharfman, 2023; Murugappan et al., 2023). The quantified losses across these incidents totaled $8.494 billion from 2009 to 2024 (Chainalysis, 2022; Chainalysis 2023b; Charoenwong et al., 2022; Chainalysis Team, 2024). As of 25 August 2023, the ecosystem comprised ≥16,500 cryptocurrencies and ≥600 active cryptocurrency exchanges (CoinMarketCap, 2023; CoinMarketCap, 2025), for which the 24-h trading volume was approximately 34.30 billion, with ≈68 million crypto-wallet owners and ≈430 million users (Bergstrom, 2024; Paganini, 2018). The scale and liquidity of these markets have made exchanges attractive targets, leading to repeated high-impact attacks and losses for users and platforms, thereby eroding confidence in cryptocurrencies as a fiat alternative worldwide (Hamrick et al., 2021). To the best of our knowledge, this study compiles the largest unified dataset of exchange-only crimes, covering both CEX and DEX incidents from 2009 to 2024. Unlike prior reviews that mixed exchanges with wallets or generalized DeFi exploits, our focus isolates exchange-specific breaches, enabling an unprecedented comparison of systemic risks across architectures.

Supplementary Table S1 (CEX) and S2 (DEX) outline the full set of 220 major incidents with a cumulative loss of $8.494 billion from 2009 to 2024 (Aspris et al., 2021; Manthovani et al., 2023). Of these, 80 incidents involved CEX and 140 involved DEX (Navamani, 2021).

5.1 Incidents classification

Tables 3, 5 summarize the incident taxonomy and counts for CEX and DEX respectively; the full record of 220 incidents (CEX 80; DEX 140) is provided in Supplementary Table S1 (CEX) and S2 (DEX).

5.1.1 Corpus and sources

We compiled incidents from 2009–2024 using peer-reviewed studies and preprints, auditor/forensic and blockchain-analytics reports, official exchange disclosures and post-mortems, regulatory/court materials, reputable industry media, and security research blogs. This comprehensive multi-source triangulation ensures that the resulting dataset is not only the broadest compiled to date but also systematically validated and de-duplicated, distinguishing it from earlier fragmented surveys. The specific sources that populated the database were as follows: Corbet et al. (2019b); Manimuthu et al. (2019); Connolly and Wall (2019); Bucko et al. (2015); Chainalysis (2022); Vidal-Tomás (2022); Marella et al. (2021); Chohan (2022); Chainalysis (2023b); Chainalysis (2023a); Oosthoek (2021); Anita (2019); Bartoletti et al. (2021); Crystal Blockchain (2024b); Hedge with Crypto

TABLE 3 Summarized high impact CEX exchange crimes from 2009–2024. Full list of incidence in Supplementary Table S1.

Date	Exchange	Platform	Cause of hack	Loss (M$)
31/05/2024	DMM bitcoin	CEX	Private key hack	305
22/06/2024	BtcTurk	CEX	Hot wallet hack	55
18/07/2024	WazirX	CEX	Phishing tactics	230
20/09/2024	BingX Exchange	CEX	Security breach	26
11/09/2024	Indodax	CEX	Hot wallet security breach	22
09/04/2023	GDAC	CEX	Access to hot wallet	13
12/11/2022	FTX	CEX	Unauthorized access	600
01/11/2022	Deribit	CEX	Access to hot wallet	28
17/01/2022	Crypto.com	CEX	Unknown	34
09/01/2022	LCX	CEX	Access to hot wallet	6.8
11/12/2021	AscendEX	CEX	Access to hot wallet	80
05/12/2021	BitMart	CEX	Access to hot wallet	150
19/08/2021	Liquid	CEX	Access to hot wallet	97
28/01/2015	Bitstamp	CEX	Social engineering	5

(2024); Crystal Blockchain (2024a); Sigurdsson et al. (2020); Feder et al. (2017); Berry (2022); Crystal Intelligence (2024); Navarro (2019); Shalini and Santhi (2019); Trozze et al. (2022); Vasek et al. (2014); CoinMarketCap (2025); Bit2Me Academy (2016); Cryptohopper (2023); World.org (2023); CoinDesk (2023); Fu et al. (2022); Eigelshoven et al. (2021); Corbet et al. (2019a); Charoenwong et al. (2022); Chainalysis Team (2024); Hamrick et al. (2021); Aspris et al. (2021); Manthovani et al. (2023); Abhishta et al. (2019); Panjwani (2023); Bhusal (2021); Blockchain (2022); Minto (2022); Badaw et al. (2020); Sengupta et al. (2020); Nabilou (2020); Patel (2022); Horch et al. (2022); Conti et al. (2018); Xia (2020); Oosthoek et al. (2020); Kasera (2020); Tandon and Nayyar (2019); Astrakhantseva et al. (2021); Shevchenko et al. (2022).

5.1.2 Inclusion and exclusion

We included exchange-platform security incidents (CEX or DEX) with (i) a clearly described compromise vector and (ii) a documented or conservatively estimated their financial impacts. We excluded non-exchange scams with no platform compromise, purely off-chain fraud that does not involve exchange infrastructure or duplicates.

5.1.3 Screening and de-duplication

All candidate items were screened and then de-duplicated by matching venue + date/time window + transaction or On-chain evidence and narrative details. Conflicting loss figures were reconciled by preferring primary disclosures and multi-source concordance, and unresolved ranges were conservatively recorded. This process yielded 220 unique incidents.

5.1.4 Normalization and coding

For each incident we coded: platform type (CEX/DEX), venue, date (UTC), region, attack vector (mapped to the 10-vector CEX and 18-vector DEX taxonomies), loss amount (USD; normalized at the time of reporting), and citation set. Ambiguous geography is tagged as unknown/global. The resulting database underlies all the figures and tables in §5.1.7.1–§5.1.7.6.

5.1.5 Focus on repeated high-impact vectors

From this corpus, we flagged vectors that recurred more than four times and caused losses exceeding $50,000 per incident (excluding non-property crimes). Applying this dual threshold ensures an analytical focus on patterns that are both persistent and financially material while filtering out one-off or low-impact breaches. These repeated high-impact records (CEX top-4; DEX top-5) drive the comparative analyses and the bar charts in §5.1.7.5–5.1.7.6, including the cross-platform private key (CEX + DEX) aggregate (78 incidents; ≈2.40B). This approach, consistent with incident analysis practices in breach reporting and cybercrime research (Shevchenko et al., 2022; Chainalysis, 2023a), allowed for the first rigorous identification of recurrent and high-impact attack vectors across both CEX and DEX. This provides a level of longitudinal granularity and cross-platform comparability that has previously been absent from the literature.

5.1.6 Data generation and curation

The curated incident lists for CEX (Supplementary Table S1; 2009–2024) and DEX (Supplementary Table S2; 2014–2024) constituted the canonical dataset used in this study. Each record includes the event date, venue, platform type, region, attack vector (mapped to the CEX 10-vector/DEX 18-vector taxonomies), loss amount (USD), and source citations. All figures and tables in §5.1.7.1–§5.1.7.6 are reproducible from these two supplementary tables by grouped aggregation over the vector, platform, year, and region fields. Tables 3, 5 define the taxonomies used to construct the summaries, and any total reported in the text (e.g., private key (CEX + DEX) = 78 incidents; ≈2.40B) can be recomputed directly from S1+S2 under these mappings. The complete source list for the

dataset is provided in the citations above, and the full 220-incident inventory is presented in Supplementary Tables S1, S2.

5.1.7 Incident results: taxonomy, trends, insights, and impact (2009–2024)

These analyses were enabled by a unified dataset of 220 incidents (the largest exchange-only compilation to date), which provides a longitudinal basis for trend analysis and cross-platform insights. Drawing on the curated 220-incident dataset (Supplementary Tables S1, S2) and the sources cited above, we analyzed, extracted, and categorized the exchange security incidents as follows:

1. Crimes on centralized exchanges (2009–2024): incident taxonomy and counts. See Section 5.1.7.1.
2. Crimes on decentralized exchanges (2009–2024): incident taxonomy and counts. See Section 5.1.7.2.
3. Annual losses on CEX and DEX platforms (2009–2024). See Section 5.1.7.3.
4. CEX–DEX incident comparison (and most-attacked platforms). See Section 5.1.7.4.
5. Repeated and common high-impact attacks on CEX and DEX. See Section 5.1.7.5.
6. Most common attack vector across all exchanges. See Section 5.1.7.6.
7. Incident trends over time. See Section 5.1.7.7.
8. Repeated attacks over time. See Section 5.1.8.
9. Financial impact and loss distribution. See Section 5.1.9.

5.1.7.1 Crimes on centralized exchanges (2009–2024)

As summarized in Table 3; Supplementary Table S1, we identified 80 major CEX incidents between 2009 and 2024. Our taxonomy comprises ten attack vectors, including hot wallet/private key compromise, compromised systems/servers, insider exploits, data leaks, and phishing via fake sites. Less frequent categories included protocol/implementation vulnerabilities and 2FA bypass. In aggregate, the quantified CEX losses totaled $4.191 billion; the top four vectors account for 62 of 80 incidents and approximately $1.764 billion (42.1%) of losses (Hong, 2019; Abhishta et al., 2019) (see Table 7 for aggregate losses and Table 4 for vector frequencies). Among the ten identified vectors, hacking/unauthorized access to hot wallets was the most prevalent (Panjwani, 2023; Bhusal, 2021), with 39 of the 80 incidents (nearly 50%). Internal mistakes have a low recurrence rate, whereas compromised servers and hot-wallet access remain persistent vulnerabilities. In 2022, the largest CEX loss was the FTX unauthorized transaction incident, exceeding $400M (Fu et al., 2022; Sigalos, 2023).

5.1.7.2 Crimes on decentralized exchanges (2009–2024)

As summarized in Table 5; Supplementary Table S2, we identified at least 140 DEX incidents spanning 18 distinct attack vectors between 2009 and 2024. Representative vectors include smart contract/protocol exploits (e.g., re-entrancy, logic bugs, oracle/manipulation errors), social engineering attacks, price-manipulation schemes (Blockchain, 2022), rug pulls, website/UI vulnerabilities, private-key compromise (admin/treasury/multisig), cross-chain and bridge weaknesses, double-spend attempts, malicious governance proposals, and flash-loan-enabled exploits.

TABLE 4 Common Attack vectors on CEX platforms and their frequency.

Common attack vectors CEX	Attack frequency
Hack/Access to hot wallet	39
Compromised System/Servers	10
Insider Exploit	7
Data leak/Breach	6
Bugs and Re-entrancy attack	5
Malware	4
Vulnerability in protocol	3
Bypass 2FA on the server Host	2
Unauthorized transactions	2
Internal Staff Error/Mistake	2
Total attacks	**80**

Total attacks represent the cumulative frequency of all documented CEX attack vectors from 2009–2024.

As shown in Table 6, system exploits (n = 56, 40.0%) and server/private key hacks (n = 39, 27.9%) are by far the most recurrent, together accounting for 95 of the 140 incidents (67.9%). These are followed by flash loan exploits (n = 12, 8.6%), price manipulation attacks (n = 6, 4.3%), and smart contract exploits (n = 7, 5.0%). Collectively, the top five vectors represented 120 of 140 attacks (85.7%). Recent DEX incidents have also produced large aggregate losses relative to many CEX events, thereby reflecting the scale and composability of on-chain protocols (Barbon, 2021). In aggregate, quantified DEX losses totaled $4.303 billion; the top five vectors account for approximately $3.755 billion (87.3%) of the losses (Hong, 2019; Abhishta et al., 2019); see Table 7.

5.1.7.3 Annual losses on CEX and DEX platforms (2009–2024)

Centralized exchanges (CEX) preceded the later arrival of decentralized exchanges (DEX), and their early adoption made CEX the dominant trading model. In 2023, CEX platforms reported an estimated 80 million regular unique users, compared with a peak of 7.5 million unique DEX users in 2021 (Coinweb, 2023; Makridis et al., 2023; Pandya et al., 2019). The broad adoption of both models has attracted persistent criminal activity since 2009 (Collins, 2022; Higbee et al., 2018; Vidal-Tomás, 2021).

CEX yearly losses: Figure 5 illustrates the yearly losses on the CEX platforms grouped by our study's attack-vector taxonomy. From 2009 to 2022, at least 80 reported incidents resulted in officially reported losses of over $4.191 billion. The largest annual losses occurred in 2018 ($869 million), followed by 2022 ($668.8 million), and 2016 ($628.8 million). From 2014 onward, CEX platforms experienced steady yearly attacks, while incident counts fell during 2019–2022 (13 → 12 → 5 → 4), 2022 still produced a major spike in financial losses Chainalysis (2022), Chainalysis (2023b). The most recurrent CEX vector is the private key/hot wallet/server compromise, accounting for 41 of 80 incidents (51%) and nearly $0.99 billion in aggregate losses (Chainalysis, 2022; Chainalysis 2023b).

DEX yearly losses. Figure 3 shows a breakdown of the total amount lost per year since DEX's inception of DEX in 2014 owing to

TABLE 5 Summarized high impact dex exchange crimes from 2009–2024. Full List of incidence in Supplementary Table S1.

Date	Exchange	Platform	Cause of hack	Loss (M$)
10/06/2024	UwU Lend	DEX	Hack	19.3
19/04/2024	Hedgey finance	DEX	Security breach	44
09/02/2024	PlayDapp	DEX	Private key vulnerability	290
03/09/2024	Penpie breach	DEX	Market manipulation	27
02/05/2023	Level finance	DEX	Security breach	1
28/04/2023	0vix	DEX	Flash-loan exploit	2
27/04/2023	Merlin	DEX	Hack	1.82
15/04/2023	Hundred finance	DEX	Hack	7.4
13/04/2023	Yearn	DEX	Exploit	11
09/04/2023	SushiSwap	DEX	Exploit	3.3
01/04/2023	AllBridge	DEX	Exploit	0.573
29/03/2023	SafeMoon	DEX	Manipulation	9
13/03/2023	Euler finance	DEX	Flash loan attack	200
09/03/2023	Hedera	DEX	Smart contract exploit	n/a
06/03/2023	PeopleDAO	DEX	Social engineering hack	0.12
27/02/2023	LaunchZone	DEX	Exploit	0.7
22/12/2021	Visor finance	DEX	Smart contract exploit	8.1

different crimes perpetrated against DEX platforms. In aggregate, the quantified losses on DEX totaled $4.303 billion, with 2022 recording the largest annual loss at over $1.918 billion. In recent years, attacks on DEX platforms have increased, reflecting multiple exploitable vulnerabilities in composable on-chain protocols (Badaw et al., 2020).

Peak year across platforms. As shown in Figure 6, the single largest combined annual loss occurred in 2022, totaling $2.587 billion across exchanges–$1.918 billion on DEX and $668.8 million on CEX. This peak substantially exceeds adjacent years (e.g., 2021 at ~$1.823 billion and year-to-date 2024 at ~$1.018 billion) and coincides with clusters of high-impact DEX exploits and major CEX losses.

Overall total loss. Across 2009–2024, the cumulative losses across exchanges amounted to $8.494 billion ($4.191 B CEX; $4.303 B DEX), consistent with the "Total" bars in Figure 4.

5.1.7.4 CEX–DEX incident comparison (and most-attacked platforms)

Figure 3C compares the incident frequencies of the CEX and DEX platforms. The data show that DEX venues experienced more cybersecurity incidents than CEX venues. Although DEXs provide decentralization, permissionless access, and user autonomy, these benefits come with reduced centralized oversight and weaker runtime controls, smart contract vulnerabilities, composability risks, and the absence of centralized monitoring, exposing DEXs to repeated high-impact attacks Chainalysis, 2022; Chainalysis 2023b; Chainalysis Team, 2024).

In contrast, CEXs, despite high-value breaches, tend to operate with stronger operational safeguards (custodial monitoring, layered access control, and compliance/audit programs) that lower the relative frequency of successful incidents (Chohan, 2022). However, both models remain materially exposed and require continuous hardening to ensure their reliability.

Most-attacked platforms. Figure 5 shows venue-level dispersion. In our dataset, the Uniswap DEX platform recorded the highest incidence of attacks, whereas the Binance CEX platform recorded the lowest among the major venues. This aligns with the mechanism-of-risk distinction above: DEX venues inherit smart contracts and composability risk (including human error and governance/upgrade pitfalls), whereas CEX venues benefit from centralized monitoring and coordinated incident responses.

5.1.7.5 Repeated and common high-impact attacks on CEX and DEX

As discussed in Section 5.1.5, we define repeated high-impact attacks as vectors that (i) recur more than four times (> 4 distinct occurrences) and (ii) cause losses exceeding $50,000 per incident. Non-property crimes were excluded from this analysis. We enumerated all incidents, tagged recurrent vectors, and tracked both frequency and loss (Tables 7, 8) (McCorry et al., 2018; Holub et al., 2018; Shevchenko et al., 2022). An attack is considered to have a high impact only when it satisfies both criteria.

CEX (repeated high-impact). Using the 10-vector taxonomy (Table 4), four vectors, as shown in Figure 4a exceeded the recurrence threshold and dominated the losses: Unauthorized Wallet Access (39), Server Exploit (10), Insider Exploit (7), and Data Leak/Breach (6). Together, they account for 62 of the 80 incidents (77.5%) and approximately $1.764 billion of $4.191 billion total CEX losses (42.1%). The dominant pattern

TABLE 6 Common Attack Vectors on DEX platforms and their frequency.

Common attack vectors on DEX	Attack frequency
System Exploit	56
Server/Private keys hacks	39
Flash-loan Exploit	12
Smart contract Exploit	7
Price manipulation attack	6
Manipulation	5
Access to the private keys	4
Security breach	2
Rugpull	2
Social engineering hack	1
Code that was in the wrong order	1
Vulnerability website Exploit	1
Malicious governance proposal	1
Platform security incident	1
Fake Token	1
Arbitraging for huge Profits	1
Re-entrancy attack	1
Double-spend attack	1
Total attacks	**140**

Total attacks represent the cumulative frequency of all documented DEX attack vectors from 2009–2024.

involves access to hot wallets, which is often enabled by phishing or social engineering techniques (Agarwal et al., 2023).

DEX (repeated high-impact): Of the 18 attack types forming the 140 total DEX incidents (Table 6), five clear the recurrence threshold: System Exploit (56), Server/Private Keys Hacks (39), Flash-Loan Exploit (12), Smart Contract Exploit (7), and Price Manipulation Attack (6). These top five accounted for 120 of 140 incidents (85.7%) and $3.755 billion of $4.303 billion total DEX losses (87.3%) (see Figure 4b; Table 7.)

Combined view. Across both platforms, the repeated high-impact vectors sum to 182 of 220 incidents (82.7%) and $5.519 billion of $8.494 billion combined losses (65.0%), as shown in Figure 4d. This persistence indicates the structural weaknesses that adversaries repeatedly exploit.

Most common attack vectors(CEX vs. DEX): Figures 3d, 6b From our findings, attackers commonly use five attack vectors including API exploits, insider threats, phishing, smart-contract exploits, and unauthorized wallet breaches across CEX and DEX. In CEX, repeated high-impact categories frequently manifest as wallet breaches (often delivered through phishing/API misuse) and insider/API problems. On DEX, smart contracts are exploited, and wallet breaches are dominant. These patterns align with the architectural risk surfaces of each platform (custody and server-side signing on CEX; contract logic, oracles, governance, and cross-chain bridges on DEX).

5.1.7.6 Most common attack vector across all exchanges

As shown in Figures 6a,b and Table 7), the dominant repeated vector across platforms is a wallet/key compromise (private key, hot wallet, or server access). This occurred 78 times (39 CEX; 39 DEX): 35.5% of all incidents (78/220) and 42.9% of repeated incidents (78/182), with combined losses of $2.394 B (43.4% of repeated-vector losses and 28.2% of the $8.494 B overall). The next most frequently repeated vectors are the system or server exploits of CEX(10) and DEX(56), that is, (66/182 repeated incidents with $1.979 B lost). Together, these two vectors account for 144/182 repeated incidents (79.1%) and $4.333 B of $5.518 B repeated losses (78.5%); that is, approximately 51% of the overall losses($8.494 B) across 220 incidents) as seen in Figure 6a.

The other repeated vectors (in Figure 4c). Beyond the two platform leaders, four additional repeated vectors show the material impact, listed in the same order as the chart: CEX

TABLE 7 Repeated and high impact attacks vectors on CEX and DEX (2009–2024). Data extracted from Supplementary Tables S1, S2.

Attack vector	Loss (millions $)	Platform	Frequency
Unauthorized wallet access	1208.413	CEX	39
Syetem or servers Exploit	39.135	CEX	10
Data leak	291.027	CEX	6
Insider Exploit	225.380	CEX	7
Total	**1763.955**		**62**
Flash loan Exploit	448.272	DEX	12
Price manipulation	168.560	DEX	6
System or server Exploit	1939.855	DEX	56
Smart contract Exploit	12.070	DEX	7
Unauthorized wallet access	1186.469	DEX	39
Total	**3755.226**		**120**

CEX totals include aggregated financial losses and incident counts for 2009. DEX totals include aggregated financial losses and incident counts for 2009–2024.

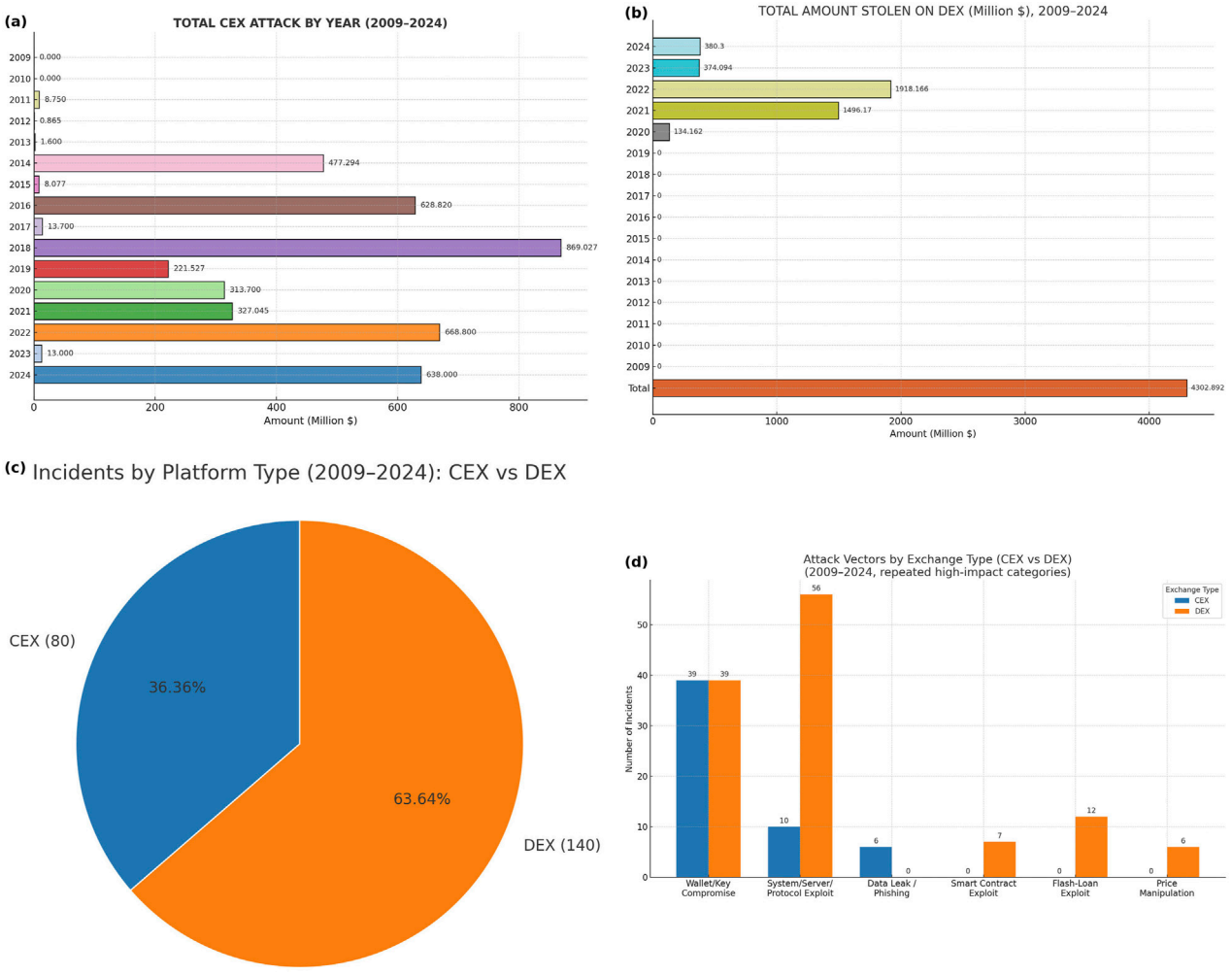

FIGURE 3
(a) Total CEX attack 2009_2024 **(b)** Total DEX 2009_2024 **(c)** CEX vs. DEX incidents **(d)** Attack vectors CEX vs. DEX.

Insider/Trusted (7 incidents; $0.23 B; ≈$32.9 M/incident), CEX Data Leak/Breach (4; $0.28 B; ≈$70 M/incident), DEX Flash loan (9; $0.41 B; ≈$45.6 M/incident), and DEX Private key/hot wallet/server (repeated subset count) (5; $0.55 B; ≈$110 M/incident).

Two patterns stand out: (i) although less frequent than re-entrancy, DEX private-key compromises are the costliest per incident, and (ii) on CEX, data-leak breaches are rarer but unusually severe on a per-event basis.

The appeal of key and wallet compromise remains clear: attackers obtain signing authority via phishing, social engineering, credential theft, or by breaching the server-side signing infrastructure (Bartoletti et al., 2021; Crystal Blockchain, 2024b; Hedge with Crypto, 2024; Crystal Blockchain, 2024a). A high-profile case is the FTX unauthorized transaction incident in 2022 (approximately $600 M) Fu et al. (2022), after which the platform leadership was criminally prosecuted (Minto, 2022). These observations reinforce the need to harden custody architecture and server-side signing (e.g., HSM/MPC) on CEX while prioritizing secure smart contract development, auditing, and runtime monitoring on DEX.

5.1.7.7 Incidence trends over time

Figure 5a shows the incident counts per year (2009–2024) across all exchanges. Incidents started near zero in 2009–2010 and then rose modestly through 2014 (7) and 2018 (9), before a sharp increase in 2020 (28) and a peak in 2021 (66). The activity remained elevated in 2022 (45) and retreated in 2023 (19) and 2024 (9, year-to-date). Overall, the series showed episodic surges followed by partial pullbacks, consistent with cyclical exposure to a small set of recurrent vectors (see §5.1.7.5).

Figure 6d shows incidents by region (2009–2024). Asia and North America accounted for the largest share, with 60 (27.3%) and 59 (26.8%) incidents, respectively, followed by unknown/global 56 (25.5%), Europe 33 (15.0%), Oceania 10 (4.5%), and Africa 2 (0.9%). The concentrations in Asia and North America likely reflect the scale of their crypto ecosystems and attack surfaces (Cambridge Centre for Alternative Finance, 2017b).

5.1.8 Repeated attacks over time

Figure 6c summarizes the recurrent attack patterns from 2009 to 2024 across five representative vectors: API Exploits,

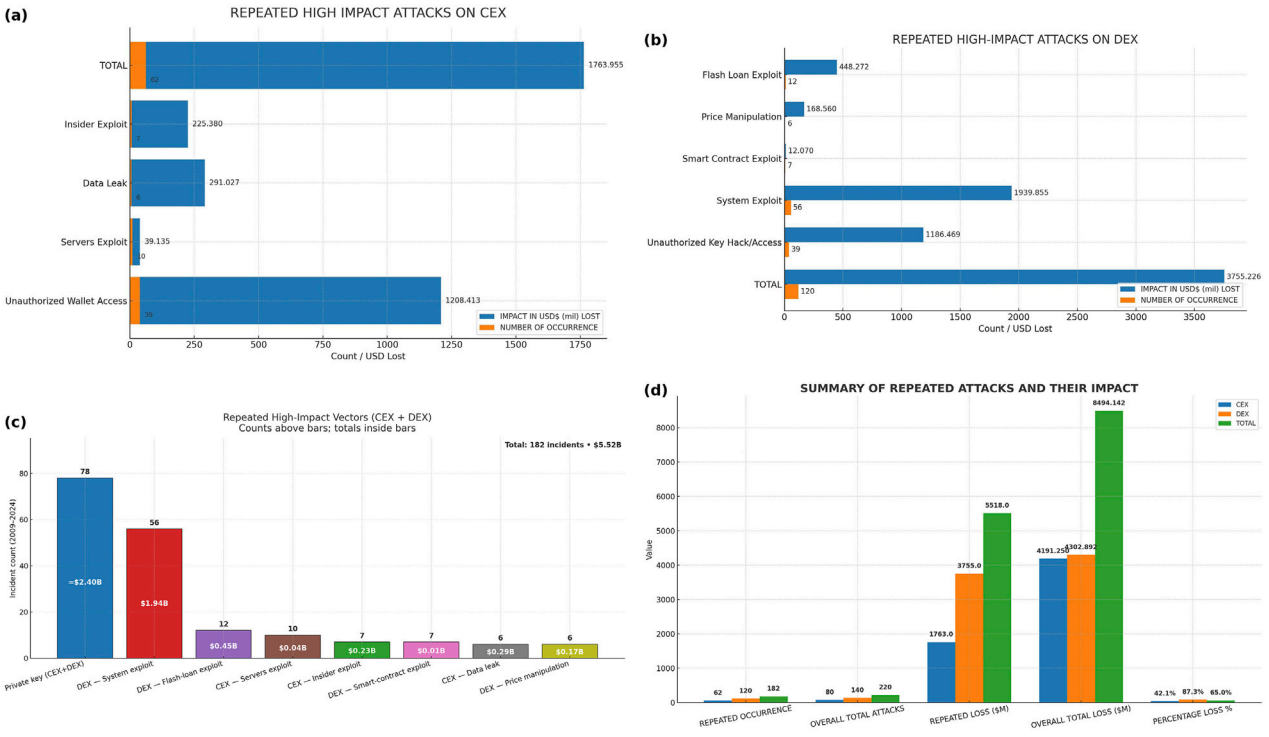

FIGURE 4
Repeated high impact attacks: **(a)** repeated high impact attacks CEX **(b)** repeated high impact attacks DEX **(c)** high impact vectors CEX_DEX **(d)** summary_repeated attacks.

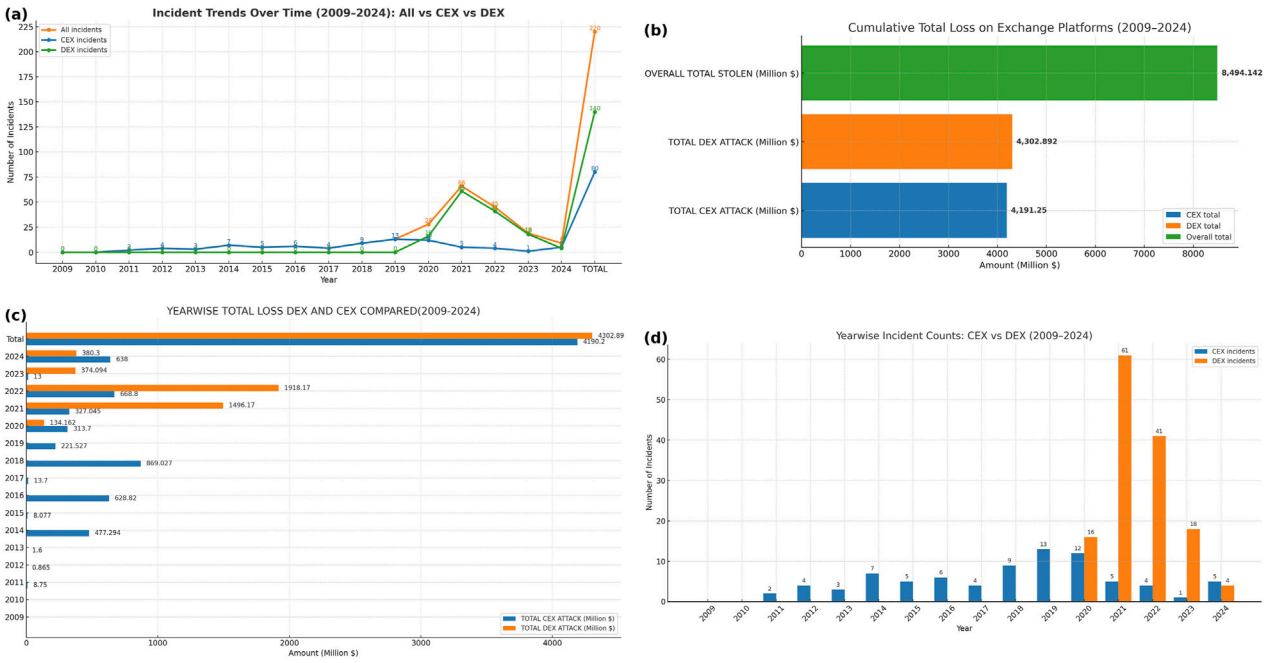

FIGURE 5
(a) Incident trends **(b)** Cumulative loss **(c)** Year-wise CEX DEX **(d)** Incidents by year.

TABLE 8 Attack vectors, methodologies, evolution, primary targets, defensive mechanisms, and references.

Attack vector	Methods	Evolution	Target	Classical defenses	Quantum defenses	References
Phishing	Social engineering, fake websites, phishing emails	Early: basic deceptive emails evolved: spear-phishing, advanced social engineering	User credentials and keys	Multi-factor authentication (MFA), training	AI-based detection, quantum-safe encryption	Birthriya et al. (2024); Gupta et al. (2024b); Ayeni et al. (2024); Bucko et al. (2015); Crystal Intelligence (2024); Holub et al. (2018); Bhusal (2021); Prendi et al. (2023); Mohsin (2022)
API exploits	Unsecured APIs, exposed keys	Early: Key theft evolved: Credential stuffing, misconfigs	Exchange APIs, trading bots	Rate-limiting, API authentication	PQC-based API authentication	Kamruzzaman et al. (2024); Gupta et al. (2024a); Homoliak and Perešíni (2024); Sigurdsson et al. (2020); Munn et al. (2022); Oliva et al. (2019)
Smart contracts	Re-entrancy, oracle manipulation	Early: simple coding bugs evolved: front-running, complex exploits	Smart contracts	Formal verification, bug bounty	PQC tools, AI bug detection	Jiao et al. (2024); Shou et al. (2024); Wang et al. (2024a); Bashir (2020); Gorkhali et al. (2020); Feder et al. (2017); Easa et al. (2023); Animuthu et al. (2019)
Wallet breaches	Malware, phishing, weak storage	Early: poor key storage evolved: malware attacks	Hot and custodial wallets	Hardware wallets, encryption, multisig	PQC wallets, cold storage	Alauthman et al. (2024); Santhosh and Subramanian (2024a); RANI (2024); Kawai et al. (2023); Olaiya et al. (2024); Faruk et al. (2022)
Insider threats	Unauthorized access, collusion	Early: negligence evolved: insider–external collab	Internal infra, funds	Zero-trust, privileged access mgmt	Real-time PQC anomaly detection	Inayat et al. (2024); Alzaabi and Mehmood (2024); Zewdie et al. (2024); Arli et al. (2021); Homoliak and Perešíni (2024); Fernández-Caramés (2020)
DDoS	Botnets, amplification	Early: simple floods evolved: amplified botnets	Exchange uptime	Load balancing, anti-DDoS	Distributed quantum networks	Kumar et al. (2024); Falowo et al. (2024); Poonia and Tinker (2024); Chen (2024); Crystal Intelligence (2024); Cherniei et al. (2021)
Sybil attacks	Fake nodes, consensus manipulation	Early: small network evolved: resource-heavy	Blockchain consensus	PoS, monitoring	PQC consensus protocols	Zhang et al. (2019); Antony and Revathy (2024); Bhatt and Sisodia (2024); Chutipat et al. (2023); Rosch-Grace and Straub (2021); Collins (2022)
Malware	Keyloggers, trojans, cryptojacking	Early: basic malware evolved: multi-stage malware	User devices	Antivirus, endpoint security	AI + PQC detection	Shandilya et al. (2024); Mohammadi et al. (2024); Edwards (2024); Chainalysis (2022); Berry (2022); Alfieri (2022)
Double-spending	51% attacks, timing manipulation	Early: low-hash networks evolved: PoW exploits	Blockchain transactions	High hash rates, multisig	PQC consensus, secure payments	Santhosh and Subramanian (2024b); Behzadi and Joseph (2024); Asare (2024); Limdrian et al. (2024); Chen (2024); Munn et al. (2022); Bentov et al. (2019)
Social Eng	Impersonation, fake requests	Early: simple scams evolved: complex manipulation	User trust	Education, behavior analysis	AI-driven anomaly detection	Birthriya et al. (2024); Hasan et al. (2024); Olaniyan and Ogunola (2024); Zaoui et al. (2024); Bucko et al. (2015); Ruiz et al. (2022); Wang et al. (2023)

Insider Threats, Phishing, Smart Contract Exploits, and Wallet Breaches. Wallet Breaches are the most frequent and peak notably in 2012 and 2023. Smart contract exploits show consistent activity, with a high point in 2020. Phishing peaked between 2012 and 2020 and subsequently declined, whereas Insider Threats remained relatively stable with minor fluctuations. A modest increase was observed in the discovered API Exploits. Overall, these trends indicate that adversaries repeatedly return to a small set of structurally exposed vectors, which is consistent with the high-impact concentrations quantified in §5.1.7.5.

5.1.9 Financial impact of incidents

Figure 4c summarizes the total loss caused by repeated attack vectors (2009–2024). Using a harmonized taxonomy over the merged dataset, cumulative losses (USD billions) are as follows: Smart-contract exploits ≈$2.216 B; Wallet breaches/key-access ≈$2.108 B; Flash loans ≈$0.440 B; Data leaks/breaches ≈$0.276 B; Phishing/social engineering ≈$0.230 B; Insider/trusted ≈$0.225 B; Compromised system/server ≈$0.039 B; and other/unspecified ≈$2.958 B. Thus, smart contract–related failures and key material compromise together explain roughly ~4.32 *B* (~51%) of the ~8.494 *B* cross-platform baseline.

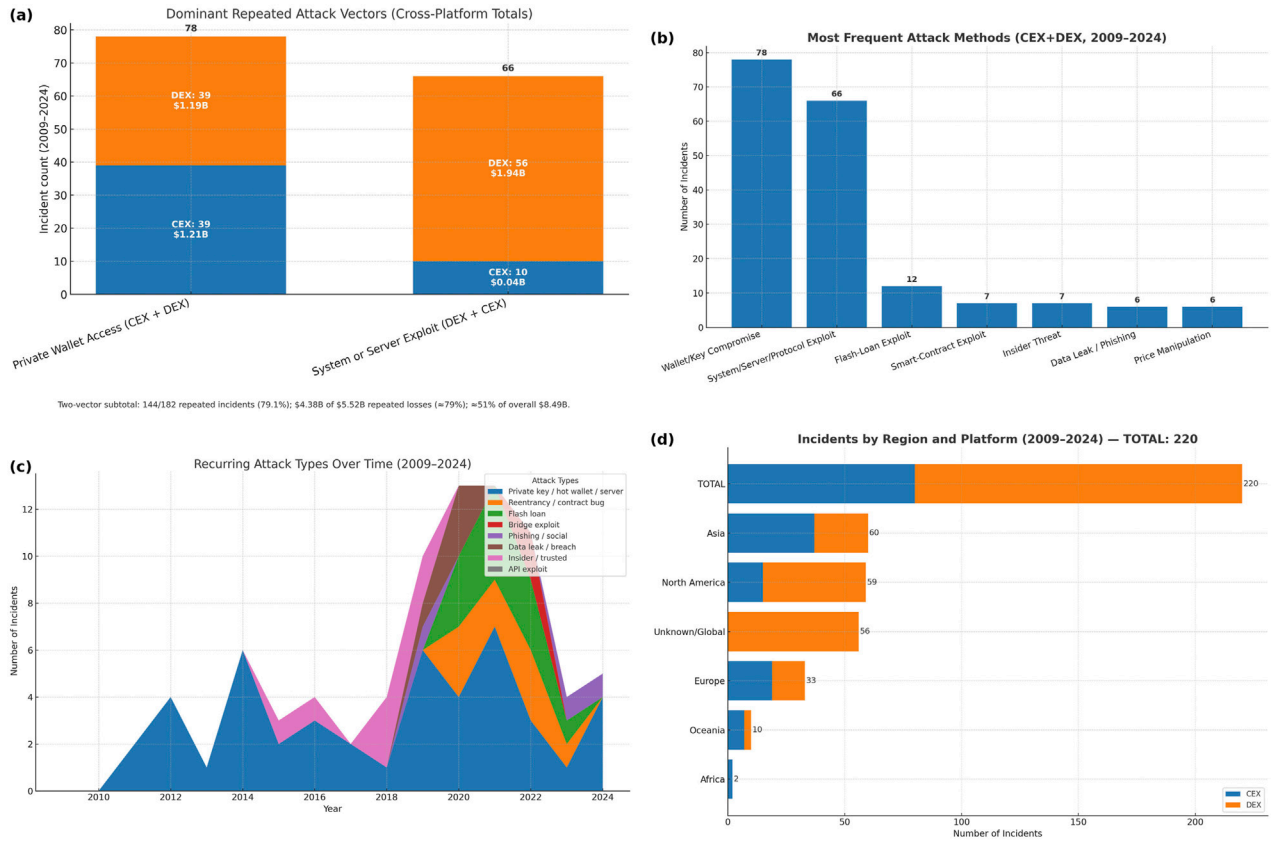

FIGURE 6
Attack vectors/types: **(a)** dominant attack vectors cex VS dex **(b)** most frequent attack methods **(c)** recurring attack types over time **(d)** Incidents by region and platform.

Figure 7a shows the annual losses across exchanges. Loss peaks in 2022 at ~2.587 *B*, remain elevated in 2021 (~1.823 *B*) and 2018 (~0.869 *B*), and are relatively low in 2019 (~0.222 *B*) and 2016 (~0.629 *B*). Year-to-date 2024 total ~1.018 *B*.

Figure 7b details the regional loss distribution (2009–2024): Asia ~4.146 *B*, North America ~2.196 *B*, Unknown/Global ~1.029 *B*, Europe ~0.786 *B*, Africa ~0.301 *B*, and Oceania ~0.036 *B*. Asia registered the largest cumulative losses, whereas Oceania had minimal cumulative losses during the period.

6 Analysis of attacks techniques and patterns

Table 8 presents an in-depth analysis of numerous attack vectors, methodologies, evolutions, classical defence mechanisms, and widely used quantum defence mechanisms.

As the ecosystem surrounding cryptocurrencies grows in size and development, criminals seeking to identify vulnerabilities in these systems have a level of sophistication (Magizov et al., 2019). The tactics applied by these attackers have grown dynamically, from hacks, phishing, and social engineering to breaches. Quantum computing, which is slowly becoming more prevalent, will open up additional issues, particularly in cryptographic systems tasked with ensuring CExP security. To protect against both classical and quantum attacks, it is important to integrate quantum-safe cryptographic algorithms (Mosca et al., 2024), AI-based anomaly detection, and strong security authentication measures, such as multi-factor authentication and cold storage solutions (Badaw et al., 2020). By following these procedures, cryptocurrency exchanges can strengthen their defenses and mitigate the risks of current and future cyberattacks.

6.1 Impact of cybersecurity attacks on users, exchanges, and the industry

Cyberattacks on cryptocurrency exchanges have serious consequences for users, exchanges, and the broader ecosystem (Navarro, 2019; Alfieri, 2022). Their impacts include:

6.1.1 Impact on users

1. Financial Losses: Phishing, wallet breaches, and malware can lead to direct loss of funds and private keys (Purohit et al., 2023).
2. Loss of Trust: High-profile hacks erode user confidence, as in the Mt. Gox collapse (Bucko et al., 2015).
3. Personal Data Exposure: Breaches often leak sensitive information (emails, phone numbers, IDs), enabling identity theft and further attacks (Arli et al., 2021).

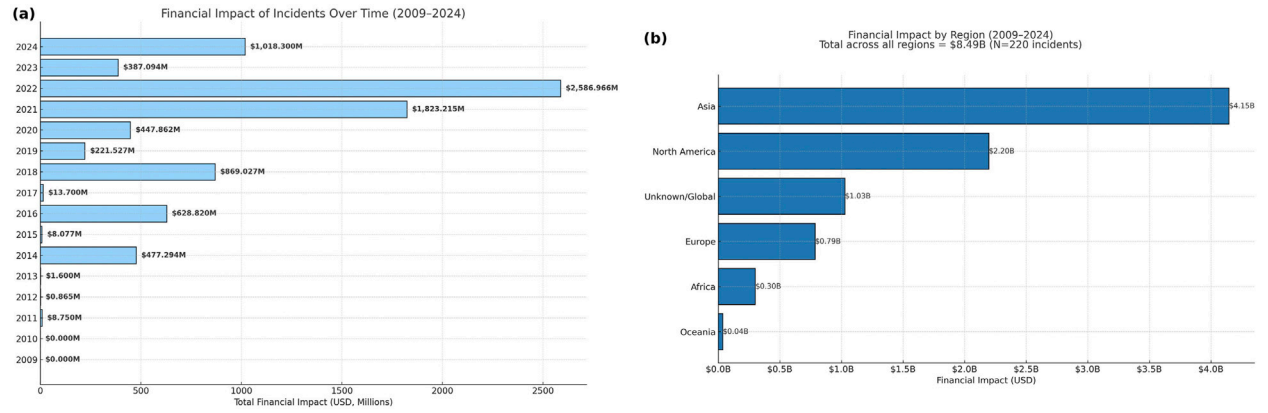

FIGURE 7
Financial impact views: **(a)** Financial Impact Over Time **(b)** Financial Impact by Region.

4. Psychological Impact: Anxiety and stress may drive users away from cryptocurrencies.

6.1.2 Impact on exchanges

1. Reputation Damage: Breaches harm credibility and deter new users (Marella et al., 2021).
2. Regulatory Scrutiny: Attacks trigger stricter oversight, often requiring stronger KYC/AML compliance (Mohsin, 2022; Mateen, 2023).
3. Financial Costs: Exchanges face compensation, restoration, and investigation expenses (Prendi et al., 2023).
4. Operational Downtime: Attacks often halt trading, withdrawals, and deposits, affecting liquidity and user activity.

6.1.3 Impact on the ecosystem

1. Reduced Adoption and Trust: Frequent attacks damage public confidence and slow adoption (Illia et al., 2023).
2. Higher Compliance Costs: Regulations like EU MiCA and FATF proposals increase operational costs (Cherniei et al., 2021).
3. Innovation Slowdown: Post-breach investigations divert resources from R&D.
4. Cybersecurity Investment: Exchanges invest heavily in bug bounties, AI anomaly detection, and quantum-safe cryptography (Sengupta et al., 2020).

6.1.4 Broader economic impacts

1. Market Volatility: Breaches intensify sell-offs and price drops (e.g., Mt. Gox 2014) (Li et al., 2022).
2. Migration to DEXs: Security concerns push users from CEXs to decentralized platforms, though DEXs face smart-contract risks (Krafft et al., 2018).

Having quantified the prevalent attack vectors, we next examine the security of the cryptographic primitives underpinning exchanges, both classical and quantum-resilient.

7 Classical cryptographic vulnerabilities and their defense in cryptocurrency exchanges

Classical cryptography defines conventional methods for data and communication security, in which established cryptographic algorithms are applied. Many of these methods are widely applied in the modern digital world to protect information, although they are vulnerable to the growing power of quantum computing (Szymanski, 2022). The following is an overview of classical cryptographic methods. The following is an overview of classical cryptography methods.

7.1 Classical cryptographic mechanisms

Traditional cryptographic measures in cryptocurrency exchanges include public-key encryption, hashing algorithms, multi-signature wallets, and digital signatures (Supplementary Table S5). All these security measures help protect users' cash, ensure the integrity of transactions, and create a safe channel of communication between exchanges and users (Subramani et al., 2023). They also encounter different challenges, such as the requirement for careful key management to avoid losses and vulnerabilities from cryptographic attacks. In any case, both of the above solutions will certainly play a substantial role in further development and help maintain consistency and security of exchanges in the cryptocurrency ecosystem (Banoth and Regar, 2023).

7.2 Various defense measures on exchanges

Supplementary Table S6 explains the different measures of defence in exchanges.

1. Public-Key Encryption: It finds wide applications in securing transactions, wallets, and messages due to the fact that it offers confidentiality and authentication (Subramani et al., 2023).

2. Symmetric Encryption: The most used symmetric encryption algorithm is Advanced Encryption Standard, generally known as AES. Although AES is more resistant to quantum attacks compared to RSA, larger key sizes are preferred, such as AES-256, for better security (Banoth and Regar, 2023).
3. Homomorphic Encryption: A technique performs computation over encrypted data without revealing sensitive information.
4. Two-Factor Authentication: Used mostly with exchanges, 2FA will ask for two types of identity/password and something else-OTP, biometrical data-before allowing the user to log into their accounts. This approach provides increased security and is most common in protecting accounts from phishing and theft of credentials (Kiraz, 2016).
5. Multi-Factor Authentication (MFA): In supplementing the Two-Factor Authentication (2FA) with additional authentication levels, the MFA uses biometric or hardware tokens to finally reduce the possibility of an unwanted account access, in case of a password compromise (Tom et al., 2023).
6. Advanced Security Protocols Tokenization: Sensitive data, such as credit card numbers or user information, is replaced with random tokens. Tokens, even if intercepted, possess no intrinsic value, thus diminishing the possible consequences of a breach.
7. Hardware Security Modules, better known as HSMs, are physical devices involved in the process of creating, storing, and managing keys for cryptocurrency payments. They are a must in protecting exchange wallets and the cash that users have on their accounts due to the high level of security offered for cryptographic keys (Bentov et al., 2019; Rezaeighaleh and Zou, 2020).
8. Security protocols, such as Transport Layer Security (TLS) and Virtual Private Networks (VPNs), ensure that all data transferred between users and exchanges is encrypted, hence reducing the likelihood of data being intercepted while it is being transmitted.

Cryptographic systems are fundamental to ensuring the security of cryptocurrency exchange systems. However, attackers can exploit several weaknesses and vulnerabilities. Table 6 summarizes the key vulnerabilities and defense strategies.

8 Post-quantum cryptography and cryptocurrency exchanges

8.1 From classical defenses to quantum threats

Cryptocurrency exchanges currently rely on classical cryptographic mechanisms and layered defence strategies to secure their platforms and protect users from cyberattacks (Weichbroth et al., 2023). These include public key encryption, hashing algorithms, multi-signature wallets, and digital signatures that underpin authentication, transaction integrity, and custodial security. Although these defenses remain effective against current adversaries, they are increasingly strained by the growing sophistication of attacks.

Simultaneously, advances in quantum computing have led to a paradigm shift in cryptographic security. By applying the principles of quantum physics, quantum computers can perform computations beyond the capacity of classical machines (Gill et al., 2022; Rosch-Grace and Straub, 2021). Unlike binary bits, quantum bits (qubits) exist in superposition and enable massive parallelism, thereby allowing quantum systems to solve certain problems exponentially faster than classical systems (Gyongyosi and Imre, 2019; Preskill, 2018). This creates both opportunities and threats: algorithms such as Shor's and Grover's jeopardize the hardness assumptions underlying RSA and ECC, exposing exchange infrastructure to harvest-now and decrypt-later risks. Consequently, post-quantum cryptography (PQC) has emerged as a critical frontier for improving exchange resilience.

8.2 Post-quantum cryptography

Post-quantum Cryptography(PQC) denotes cryptographic algorithms designed to withstand the computational power of quantum computers (Fernández-Caramés, 2020; Chen, 2024). Quantum computing poses a potential threat to classic systems, including RSA, ECC, and DH, because their security depends on mathematical problems that any quantum computer can efficiently solve using methods such as Shor's algorithm. Given the recent advances in quantum computing, the security of conventional cryptography public-key systems has become increasingly insecure. Therefore, quantum-resistant cryptography protocols are urgently required (Mosca et al., 2024; Yi, 2022; National Institute of Standards and Technology, 2024).

The urgency of PQC arises not only from theoretical concerns but also from real-world practices such as "harvest now, decrypt later" attacks, where adversaries store encrypted blockchain traffic today with the intent to decrypt it in the quantum future (Marchsreiter and Sepúlveda, 2023). In response, the NIST PQC standardization project selected lattice-based Kyber (ML-KEM) and Dilithium (ML-DSA) as primary standards (Chen, 2024; Cherkaoui et al., 2024; National Institute of Standards and Technology, 2024), while also advancing Falcon and SPHINCS + for specific use cases (Chen, 2024). This marks a critical turning point in the integration of post-quantum algorithms into the cryptocurrency ecosystem. Crypto-agility, the ability to swiftly migrate to stronger schemes, is now viewed as essential for blockchain protocols (Marchsreiter and Sepúlveda, 2023).

8.3 Types of post-quantum cryptographic algorithms

Table 9 summarizes the different types of post-quantum cryptographic(PQC) algorithms used.

1. Lattice-Based Cryptography: Lattice-based cryptography protects digital systems from classical and quantum attacks (Wang et al., 2023; Bandara et al., 2022). Security relies on the intractability of solving problems such as LWE and SVP, which remain impractical even for quantum computers (Zheng, 2022; John et al., 2023). Lattice-based schemes resist quantum

algorithms, such as Shor's algorithm, unlike RSA and ECC. Features include fully homomorphic encryption (FHE) for multiparty computation with the leading standards CRYSTALS-Kyber (key exchange) and CRYSTALS-Dilithium (digital signatures) (Chen, 2024; National Institute of Standards and Technology, 2024). Despite barriers such as large key sizes and computational overheads, lattice-based cryptography is a core component of quantum-safe infrastructure for exchanges, wallets, and blockchains.

2. Code-Based Cryptography: Proposed by McEliece in 1978, code-based cryptography relies on the difficulty of decoding linear error-correcting codes without a private key (Weger et al., 2022; Wachter-Zeh et al., 2022). Classic McEliece, BIKE, and HQC remain strong candidates, though their large public keys challenge lightweight implementation. Applications include wallet encryption, key management, and authentication (Singh, 2022). Research has aimed to reduce overhead and improve scalability (Horlemann, 2023; Gueron et al., 2022); Ren and Zhang, 2022), while keeping code-based schemes relevant for post-quantum security.
3. Multivariate Polynomial Cryptography: This approach makes it difficult to solve nonlinear multivariate equations in finite fields (Kuang et al., 2022; Sobral, 2022). It enables high-speed signing and efficient verification and is suitable for IoT and embedded devices (Dey and Dutta, 2023; Ikematsu et al., 2023). Examples include Rainbow, a former NIST finalist known for its compact signatures. The benefits include efficiency and low verification cost, whereas the challenges include key-size optimization and algebraic attack resistance (Kuang et al., 2022; Gong, 2024). In contrast, multivariate schemes support user authentication, integrity, and key management.
4. Hash-Based Cryptography: Hash-based schemes use one-way collision-resistant functions, avoiding algebraic structures vulnerable to quantum algorithms such as Shor's algorithm (Fathalla and Azab, 2024; Srivastava et al., 2023; Nagarajan et al., 2024; Algazy et al., 2024). SPHINCS+ is a leading stateless hash-based signature scheme that provides strong guarantees without requiring state management. Exchanges use this for transaction signing, wallet authentication, and blockchain verification. Its limitations include large signatures and slower key generation; however, ongoing research has improved its efficiency, making hash-based cryptography a reliable option (Panthi and Bhuyan, 2023; Mamatha et al., 2024).
5. Isogeny-Based Cryptography: Isogeny-based schemes derive security from the difficulty of computing isogenies between elliptic curves, which are resistant to Shor's algorithm (Dey et al., 2022; Drzazga and Krzywiecki, 2022). SIKE is a notable candidate in the NIST process, valued for its compact keys and low bandwidths (Veroni, 2023; Leroux, 2022b). Although vulnerabilities exist, they offer lightweight solutions for IoT and mobile wallets (Reijnders, 2023). With further research, isogeny-based systems can protect exchanges from quantum threats (Leroux, 2022a).
6. Quantum-Secure Symmetric Algorithms: Symmetric algorithms are less vulnerable to quantum attacks but face Grover's algorithm, which halves the effective security. AES-256 and SHA-3 remain quantum-safe by relying on larger key lengths (María, 2024; Malviya et al., 2022; Pan et al., 2024; Khosravi and Eghlidos, 2023). They secure wallets, transactions, and blockchain communication and are efficient in IoT and mobile environments. Research has explored improving key management and resilience to ensure robustness against future attacks (Nosouhi et al., 2024; Feng et al., 2022).
7. Hybrid Cryptographic Systems: Hybrid systems combine classical schemes (RSA and ECC) with PQC algorithms (lattice, hash, or code-based) to provide both short- and long-term security (Ricci et al., 2024; Giron et al., 2023). They support wallet authentication, key exchange, and TLS protocols and blend ECC for real-time use with Kyber or Dilithium for quantum resistance. This transitional approach balances current deployment with future security demands (Cherkaoui et al., 2024; Zeng et al., 2024).

Currently, research is being conducted to make hybrid systems more efficient in terms of performance, scalability, and efficiency to ensure resistance against emerging threats while providing a smooth transition towards a totally post-quantum-secure setting.

8.4 Impact of quantum computing on classical cryptography

Most cryptocurrency exchange transactions rely on RSA and ECC (Rezaeighaleh and Zou, 2020; Islam et al., 2018); however, quantum computing poses a significant threat to these systems. Shor's algorithm (Faruk et al., 2022; Kapoor and Thakur, 2022) can efficiently solve the difficult problems underlying these schemes, which modern classical computers cannot (Hussain, 2023; Sharma et al., 2022).

RSA's security of RSA is based on the difficulty of factoring large numbers (Gangele, 2024); however, Shor's algorithm can break it in polynomial time, rendering RSA insecure for future quantum adversaries (Vasavi and Latha, 2019; Moussa, 2020). Similarly, ECC, built on the hardness of the discrete logarithm problem, is equally vulnerable to Shor's algorithm, thereby significantly compromising its security (Olaiya et al., 2024; Padhiar and Mori, 2022). Thus, widely deployed cryptography is obsolete in the quantum era, underscoring the urgency of quantum-resistant alternatives.

8.5 Emerging quantum threats

Quantum computing introduces threats that undermine the foundations of cryptography (See Supplementary Table S7). Mosca (2018); Mosca et al. (2024) warned that the timeline for "Q-day" may be shorter than expected, stressing the need for proactive migration through the inequality of data shelf-life and cryptographic transition. More recently, Reynolds (2025) reported that experts estimate a significant chance of Q-day before 2035, underscoring the urgency of adopting post-quantum defenses and preparing for harvest-now-decrypt-later (HN-DL) attacks.

TABLE 9 Post-quantum cryptographic algorithms.

Cryptography type	Algorithms used	Description	Security	References
Lattice-based	NTRU, kyber, SABER, dilithium	Based on the hardness of lattice problems, such as the shortest vector problem (SVP)	Resistant to quantum attacks, efficient for key exchange	Wang et al. (2023); Bandara et al. (2022); Zheng (2022); John et al. (2023)
Hash-based	XMSS, SPHINCS+	Utilizes cryptographic hash functions for digital signatures	Quantum-safe, robust for authentication	Fathalla and Azab (2024); Srivastava et al. (2023); Nagarajan et al. (2024); Algazy et al. (2024)
Multivariate	UOV, rainbow	Relies on solving systems of multivariate polynomial equations	Secure for signatures/ encryption, though rainbow was broken	Kuang et al. (2022); Sobral (2022); Dey and Dutta (2023); Ikematsu et al. (2023)
Code-based	McEliece, niederreiter	Uses error-correcting codes for secure encryption	Quantum-resistant but requires large key sizes	Weger et al. (2022); Wachter-Zeh et al. (2022); Horlemann (2023); Singh (2022)
Isogeny-based	SIDH, SIKE	and elliptic curve isogeny-based	Compact key exchange, but SIKE has been broken	Dey et al. (2022); Drzazga and Krzywiecki (2022); Veroni (2023); Leroux (2022b)
Symmetric key	AES, SHA-3	Standard encryption and hashing algorithms	Secure with doubled key lengths against Grover's algorithm	María (2024); Malviya et al. (2022); Pan et al. (2024); Khosravi and Eghlidos (2023)
Hybrid systems	Classical + PQC combinations	Integrates PQC with classical schemes for compatibility	Transition path with enhanced security	Cherkaoui et al. (2024); Zeng et al. (2024); Ghinea et al. (2023); Marchsreiter and Sepúlveda (2023)

1. Quantum Decryption: Shor's algorithm enables efficient factoring and discrete logarithm solutions, undermining encryption protocols and exposing exchange transactions (Faruk et al., 2022).
2. Quantum-Enhanced Brute Force: Grover's algorithm accelerates brute-force key searches, weakening symmetric encryption and reducing key lifetimes (Fernández-Caramés, 2020; Easa et al., 2023).

8.6 Challenges in the post-quantum ERA

Quantum computing challenges can be addressed in several ways.

1. Smart Contract Vulnerability: Contracts secured with classical cryptography become exposed to quantum-enabled attacks (Chen, 2024).
2. Migration Complexity: Integrating PQC into deployed systems requires extensive testing for compatibility (Wang et al., 2023).
3. Scalability: Many PQC algorithms demand more resources, reducing transaction throughput (Dharminder et al., 2023).
4. Lack of Standardization: Consensus on quantum-safe algorithms remains pending, complicating adoption (Yi, 2022).
5. Time Sensitivity: Rapid migration is needed to pre-empt harvest-now, decrypt-later attacks.

Backward compatibility further complicates adoption. Many exchanges rely on ECC for wallets and smart contracts (Ghinea et al., 2023). Migration often requires hybrid approaches (e.g., ECC with Kyber or Dilithium), which increase the payload size and computation, stressing mobile and IoT devices (Ghinea et al., 2023; Cherkaoui et al., 2024; National Institute of Standards and Technology, 2024; Marchsreiter and Sepúlveda, 2023).

8.7 Post-quantum cryptography for cryptocurrency exchanges

Given the reliance on public key cryptography for signatures and secure communication, exchanges must transition to PQC (Chen, 2024; Marchsreiter and Sepúlveda, 2023). Therefore, phased adoption is recommended.

1. Quantum-Resistant Signatures: Schemes such as XMSS and LMS protect transactions in a quantum era (National Institute of Standards and Technology, 2024).
2. Quantum-Secure Key Exchange: Kyber can replace ECDH for secure channel establishment (Cherkaoui et al., 2024).
3. Lattice-Based Encryption: Ensures sensitive data remain safe even if classical schemes are broken (John et al., 2023).

8.8 Threat timeline and policy implications

Although the exact timeline for scalable quantum computers remains uncertain, experts have estimated practical threats within 10–15 years (Chen, 2024). Harvest-now and decrypt-later risks require immediate preparation (Marchsreiter and Sepúlveda, 2023). Regulators such as NIST, ETSI, and NSA encourage proactive PQC migration (Chen, 2024; National Institute of Standards and Technology, 2024). Exchanges must implement crypto-agility and begin testing NIST-approved schemes to mitigate systemic risks (Marchsreiter and Sepúlveda, 2023).

9 Discussion

9.1 Research gaps

This review highlights that despite substantial progress in cryptography and blockchain research, important gaps remain in securing cryptocurrency exchanges against classical and quantum adversaries. By curating the first PRISMA-ScR-guided dataset of 220 exchange-only breaches drawn from academic studies, industry reports, and technical disclosures, this study provides a structured evidence base that was absent in previous studies. Our synthesis demonstrates that vulnerabilities are not isolated events but recur systematically; however, existing scholarship has not sufficiently addressed this. These observations build directly on the dataset of 220 validated exchange-only incidents summarized in Section 5, which revealed that vulnerabilities frequently recurred across platforms and years, confirming the systemic nature of the risks discussed here.

First, relatively few studies have examined how the authentication infrastructure of exchanges is exposed to both classical and quantum threats (Chainalysis, 2022; Chainalysis 2023b; IMARC Group, 2023; Oosthoek, 2021; Faruk et al., 2022; Vasavi and Latha, 2019; Olaiya et al., 2024; Sarkis-Onofre et al., 2021). Second, quantum-safe cryptographic algorithms are rarely tailored to the operational realities of exchanges, where latency, throughput, and interoperability are critical (Faruk et al., 2022; Fernández-Caramés, 2020; Easa et al., 2023). Third, multimodal or hybrid post-quantum authentication frameworks are virtually absent in the literature, even though exchanges remain high-value targets (Olaiya et al., 2024; Chen, 2024; Saha et al., 2023; Dharminder et al., 2023; Yi, 2022). Beyond algorithms, practical deployment is rarely simulated in live or large-scale exchange environments (Bucko et al., 2015; De Saint Guilhem et al., 2020; Zhang et al., 2024; Chen, 2024; Saha et al., 2023; Yi, 2022; Panthi and Bhuyan, 2023; Mamatha et al., 2024). Moreover, economic assessments of migration remain underdeveloped, and few studies have quantified the cost-benefit trade-offs of PQC adoption across heterogeneous blockchain ecosystems (Saha et al., 2023; Yi, 2022). Scalability also persists as a problem, with most post-quantum crypto systems untested under high-throughput real-world conditions (Rezaeighaleh and Zou, 2020; Prabakaran and Ramachandran, 2022; Nagarajan et al., 2024; Cherkaoui et al., 2024). Finally, the integration pathways for legacy systems are not clearly articulated, leaving exchange operators without transition roadmaps (John et al., 2023; Dey et al., 2022; Giron et al., 2023). Together, these gaps indicate that both technical design and sociotechnical adoption strategies require further research attention.

9.2 Repeated and dominant attack vectors

Hot wallet compromises are disproportionately prevalent because of the inherent trade-off between accessibility and security issues. Exchanges must maintain hot wallets online to ensure continuous liquidity and rapid settlement; however, this design exposes the private keys to adversaries. Even with safeguards such as multi-signature schemes or withdrawal limits, the online nature of hot wallets increases their susceptibility to theft (Crystal Blockchain, 2024b); Erinle et al., 2023; Sigurdsson et al., 2020). As a result, attackers repeatedly exploit these systemic vulnerabilities, making hot wallet breaches a dominant incident vector. This interpretation aligns with the results showing that wallet and key-management breaches accounted for 78 of the 220 incidents (35%) and approximately $2.39 billion in cumulative losses, confirming their disproportionate impact.

For decentralized exchanges (DEXs), the higher frequency of incidents (140 for DEX vs. 80 for CEXs) yet comparable aggregate losses can be explained by the concentration of attacks on protocols with significant Total Value Locked (TVL). When numerous small-scale exploits occur, adversaries disproportionately target high-value liquidity pools and automated market makers. A single breach in a system protocol with billions of TVL can generate losses equivalent to those in custodial CEX incidents (DefiLlama, 2025a; Chainalysis, 2023b; Nabilou, 2020). This reflects a systemic difference: CEX incidents are commonly tied to custodial infrastructure and authentication, whereas DEX breaches stem from protocol-level weaknesses in smart contracts and governance. As detailed in Table 7; Figure 4, DEX platforms accounted for 140 total incidents, of which 120 (85.7%) were repeated high-impact attacks. Despite the decentralized architecture, these attacks concentrated on high-TVL (Total Value Locked) protocols platforms holding large volumes of user funds, resulting in aggregate losses comparable to centralized exchanges.

9.3 Security of exchanges in the quantum era

Approximately 12% of the incidents in the dataset involved cryptographic or key-management weaknesses, providing the empirical foundation for assessing how quantum algorithms could amplify these vulnerabilities. Our analysis of the incident vectors underscores the need for exchanges to prioritize quantum resilience. Wallet and private key compromises and DEX protocol exploitation dominate historical breaches. In the quantum era, these vectors have become even more dangerous: Shor's algorithm threatens RSA and ECC, whereas Grover's algorithm reduces the effective strength of symmetric primitives. As Mosca (2018) warned, the timeline for "Q-day" may be shorter than expected, requiring proactive migration rather than reactive defence.

Our findings have led to the emergence of practical strategies. Continuous monitoring of quantum algorithmic progress must be institutionalized by the exchange operators. Gradual migration to lattice-based encryption (e.g., Kyber) and hash-based signatures (e.g., XMSS and SPHINCS+) should occur through hybrid deployments that preserve backward compatibility with existing RSA/ECC infrastructure. Exchanges must also upgrade Hardware Security Modules (HSMs), authentication servers, and wallet architectures to support PQC natively. Regular quantum-aware risk assessments coupled with third-party audits are essential for validating compliance with emerging standards. Importantly, quantum security cannot be achieved in isolation; collaboration with cybersecurity firms and standardization bodies, such as the NIST, will be vital to ensure interoperability and coordinated adoption.

In this study, post-quantum readiness was assessed using a structured set of indicators derived from both technical and

organizational dimensions. At the technical level, we analyzed the proportion of incidents linked to cryptographic or key-management weaknesses (12% of the dataset) (Suga et al., 2020; Oosthoek et al., 2020; Monrat et al., 2019) and evaluated the extent to which exchanges had adopted or tested quantum-safe primitives such as lattice-, hash-, and isogeny-based schemes (Leroux, 2022b; Reijnders, 2023; Ricci et al., 2024; Giron et al., 2023; Singamaneni and Muhammad, 2024). At the organizational level, readiness was gauged through the presence of formal migration planning, use of hardware security modules (HSMs) with PQC compatibility, and evidence of alignment with emerging frameworks such as the NIST PQC standardization roadmap and ETSI QSC guidelines (National Institute of Standards and Technology, 2024; Nosouhi et al., 2024; Mosca, 2018). These indicators collectively formed the basis for evaluating institutional preparedness and quantum-era migration maturity within the exchange ecosystem.

9.4 Implications for operators and regulators

For exchange operators, the dataset shows that 67.9% of recorded incidents stem from two repeated vectors: key compromise and system exploitation. This concentration of risk reflects underlying structural weaknesses in exchange architecture–particularly hot wallet custodianship, key management, and protocol-level controls–that continue to enable repeated exploitation. This finding corresponds to the quantitative pattern in which two repeated vectors–wallet/key compromise and protocol exploitation–jointly accounted for 65% of total recorded losses, highlighting where mitigation should concentrate. Therefore, operators must adopt hybrid PQC schemes in the near term while preparing to transition fully once the standards stabilize. Investments in training, simulation of quantum attacks, and joint R&D with academic partners will accelerate preparedness.

These longitudinal findings, drawn from the 2009–2024 dataset, emphasize that regulatory interventions must address historically recurrent weaknesses rather than isolated breaches. For regulators, this dataset offers a rare longitudinal map of systemic vulnerability. This evidence highlights the urgency of regulatory harmonization, echoing trends seen in frameworks such as the EU Markets in Crypto-Assets (MiCA) regulation and MAS oversight in Singapore. Regulators should define explicit PQC adoption timelines, mandate quantum security audits, and develop incident response protocols that are adapted for quantum-enabled breaches. Without coordinated oversight, fragmented PQC adoption risks leaving exchanges, and, by extension, retail investors are exposed to asymmetric quantum advantages, which highlights the urgency of harmonized oversight, as emphasized in efforts to build standards from past exchange failures (Suga et al., 2020; Johnson, 2020).

9.5 Recommendations for exchange security

The following recommendations derive from empirical patterns identified in Section 5, particularly the dominance of wallet/key and protocol-exploitation vectors responsible for most repeated incidents and financial losses. Several best practices flow directly from this analysis. First, operators must prioritize quantum-resistant cryptography (lattice-based, isogeny-based, and hash-based schemes) for transaction signing and custodianship. Second, mandatory multi-factor authentication must extend beyond SMS or app tokens to include biometric and hardware devices. Third, penetration testing and security audits must explicitly evaluate the implementation of PQC under realistic workloads. Fourth, APIs should be secured through strong authentication, rate limiting, and encryption to reduce the attack surface. Fifth, robust key management practices, including key rotation, segmentation, and HSM-backed cold storage, must be enforced. Finally, layered defense strategies, user education campaigns, and continuous engagement with regulators provide the depth required to withstand both classical and quantum threats.

9.6 Overall significance of the review

This systematic review contributes to the advancement of exchange security scholarship on three levels. Theoretically, it extends cyber-risk and cryptographic migration literature by linking recurrent attack vectors to the technological horizon of quantum computing. Managerially, it provides a longitudinal evidence base that exchange operators can use to prioritize investment in post-quantum architectures, authentication frameworks, and incident-response design. For policy and regulation, it offers empirical benchmarks to inform harmonized oversight, PQC adoption timelines, and audit standards. Collectively, these insights strengthen both scholarly understanding and institutional decision-making for building resilient, quantum-secure digital-asset ecosystems. Together, these contributions position this review as a foundational empirical reference for guiding the secure and quantum-ready evolution of global cryptocurrency exchange infrastructure.

9.7 Limitations

This study has several limitations that should be acknowledged. First, the dataset relies on publicly reported breaches, which may omit incidents suppressed for legal, regulatory, or reputational reasons, introducing a degree of under-reporting bias. Second, the analysis focuses specifically on CEX and DEX platforms, excluding broader DeFi protocols and Layer-2 scaling systems that may exhibit distinct vulnerability patterns and data incompleteness. Third, the evaluation of post-quantum readiness remains forward-looking, as PQC schemes have yet to be widely deployed and tested in live exchange environments. Despite these constraints, the systematic scope of this review provides a robust empirical foundation for future research and policy development.

9.8 Future research directions

Future studies should address these gaps in several ways. Technical research should benchmark PQC schemes under high-throughput exchange workloads to provide empirical evidence of

latency and cost effects. Research on crypto-agility,the ability to rapidly switch between cryptographic algorithms, is crucial for managing transitions as PQC standards evolve. Sociotechnical studies are needed to evaluate the user acceptance of PQC-enabled multi-factor authentication, particularly for retail investors. Finally, comparative policy studies should analyze how different jurisdictions mandate PQC migration with a view towards harmonization. Addressing these questions will accelerate scholarly understanding and practical readiness for quantum-secure financial ecosystems.

10 Conclusion

10.1 Summary of findings

The global acceptance and resilience of cryptocurrency exchanges critically depend on the robustness of their cybersecurity infrastructure. This systematic review synthesizes high-impact cybersecurity incidents from 2009 to 2024, analyses attack patterns, and explores the evolving threat landscape in the quantum-computing era. Crucially, this review establishes the largest unified database of 220 exchange-only incidents, which were meticulously extracted from peer-reviewed articles, auditor reports, court records, and technical disclosures. To the best of our knowledge, no prior study has compiled a dataset of this scale and scope across both CEX and DEX. This exclusive focus on exchange breaches, rather than wallets or generalized DeFi hacks, provides regulators, operators, and researchers with a unique evidence base for systemic risk analysis and cross-architecture comparability.

- Cryptocurrency exchanges are susceptible to both classical cyberattacks–such as phishing, API vulnerabilities, and smart contract exploits and emerging quantum-enabled threats that challenge the foundational cryptographic primitives.
- Widely adopted cryptographic algorithms like RSA and elliptic curve cryptography are vulnerable to quantum algorithms, necessitating a transition to post-quantum alternatives such as lattice-based and hash-based cryptography.
- Quantum computing represents both a threat and an opportunity: it enables advanced attacks on existing encryption, yet fosters new cryptographic techniques capable of securing digital assets in the post-quantum era.
- Despite advances in post-quantum cryptography, real-world integration into cryptocurrency platforms remains limited. This highlights the urgent need for collaborative efforts among researchers, developers, and exchange operators to bridge the gap between theory and practice.

10.2 Significance of the study

This review highlights the urgency of transitioning to quantum-resilient cryptographic frameworks to mitigate future threats. As quantum computing matures, the risk of cryptographic failure in virtual asset exchanges increases, thereby threatening the integrity of digital transactions and user trust.

Unlike previous reviews that included wallets or generalized DeFi exploits, this is the first systematic PRISMA-ScR scoping review to assemble and quantitatively analyze the largest unified dataset of CEX and DEX incidents. The novelty lies not only in its exchange-only lens but also in the unprecedented comparability of systemic risks across custodial and non-custodial architectures. By linking 15 years of empirical breach data to emerging quantum risks, this study bridges the gap between retrospective incident analyses and forward-looking post-quantum readiness.

This study contributes to the literature in several ways.

- Providing the first structured classification of major cybersecurity incidents across 15 years of exchange operations in a unified dataset.
- Identifying systemic vulnerabilities linked to repeated attack vectors and connecting them to post-quantum fragilities.
- Offering actionable insights for exchange security evolution in both the classical and quantum threat landscapes.

10.3 Call for action

Considering the increasing sophistication of cyberattacks and the approaching threat of quantum computing, this study advocates coordinated, forward-looking actions. The key recommendations are as follows.

- Urgent adoption of quantum-resistant cryptographic algorithms across all layers of cryptocurrency exchange infrastructure to ensure long-term data and transaction integrity.
- Strengthening of layered defense mechanisms, including MFA, secure APIs, anomaly detection systems, and periodic quantum-readiness audits.
- Development and enforcement of international standards for post-quantum cryptography to promote interoperability, security compliance, and sector-wide resilience.

The forward path requires sustained collaboration among regulators, exchange operators, cybersecurity experts, and cryptographers. Through joint efforts, the digital asset ecosystem can be fortified against emerging threats, enabling secure and trustworthy financial innovations in the quantum era.

Author contributions

AO: Supervision, Writing – review and editing, Methodology, Software, Investigation, Writing – original draft, Conceptualization, Funding acquisition, Visualization, Formal Analysis, Validation, Data curation, Project administration, Resources. SM: Funding acquisition, Visualization, Resources, Validation, Formal Analysis, Project administration, Writing – original draft, Investigation, Writing – review and editing, Data curation, Supervision, Methodology, Conceptualization, Software.

Funding

The authors declare that no financial support was received for the research and/or publication of this article.

Acknowledgements

The authors would like to thank the Vellore Institute of Technology (VIT) for the open-access funding.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that Generative AI was used in the creation of this manuscript. The authors declare that Generative AI was used to prepare this manuscript. During the preparation of this study, we used ChatGPT to improve the readability and language of the manuscript. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the content of the publication.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fbloc.2025.1713637/full#supplementary-material

References

Abhishta, A., Joosten, R., and Nieuwenhuis, L. J. M. (2019). "Impact of successful ddos attacks on a major crypto-currency exchange," in *2019 international conference on information and communication technology convergence (ICTC)* (Jeju, Korea (South): IEEE), 973–978. doi:10.1109/ICTC46691.2019.8939862

Adamik, F., and Kosta, S. (2019). "Smartexchange: decentralised trustless cryptocurrency exchange," in *Business information systems workshops (BIS 2018), revised papers* (Springer International Publishing), 356–367. doi:10.1007/978-3-030-04849-5_31

Agarwal, U., Rishiwal, V., Tanwar, S., and Yadav, M. (2023). Blockchain and crypto forensics: investigating crypto frauds. *Int. J. Netw. Manag.* 34, e2255. doi:10.1002/nem.2255

Ahuja, P. (2023). Cryptocurrency: a new millennium currency (problem and prospects in India). *Int. J. Res. Appl. Sci. and Eng. Technol. (IJRASET)* 11, 1514–1518. doi:10.22214/ijraset.2023.54567

Al-Amri, R., Zakaria, N. H., Habbal, A., and Hassan, S. (2019). Cryptocurrency adoption: current stage, opportunities, and open challenges. *Int. J. Adv. Comput. Res.* 9, 293–307. Identifies current adoption barriers and research gaps. doi:10.19101/IJACR.PID43

AL-Mubayedh, D., AL-Khalis, M., AL-Azman, G., AL-Abdali, M., Al Fosail, M., and Nagy, N. (2019). "Quantum cryptography on ibm qx," in *2019 2nd international conference on computer applications and information security (ICCAIS)*, 1–6. doi:10.1109/CAIS.2019.8769567

Alauthman, M., Al-Qerem, A., Alkasassbeh, M., Aslam, N., and Aldweesh, A. (2024). "Malware threats targeting cryptocurrency: a comparative study," in *2024 2nd international conference on cyber resilience (ICCR)* (IEEE), 1–8.

Alfieri, C. (2022). Cryptocurrency and national security. *Int. J. Criminol.* 9. doi:10.18278/ijc.9.1.3

Algazy, K., Sakan, K., Nyssanbayeva, S., and Lizunov, O. (2024). Syrga2: post-quantum hash-based signature scheme. *Computation* 12, 125. doi:10.3390/computation12060125

Alghamdi, S. M., Kammoun Jarraya, S., and Kateb, F. A. (2024). Enhancing security in multimodal biometric fusion: analyzing adversarial attacks. *IEEE Access* 12, 106133–106145. doi:10.1109/ACCESS.2024.3435527

Alia, M. A. (2014). Cryptography-based authentication methods. *Proc. World Congr. Eng. Comput. Sci. (WCECS 2014) San Francisco, U. S. A Int. Assoc. Eng.* 2, 468–473.

Alzaabi, F., and Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access* 12, 30907–30927. doi:10.1109/access.2024.3369906

Amirthalingam, G., and Radhamani, G. (2014). Multimodal biometric cryptosystem for face and ear recognition based on fuzzy vault. *Res. J. Appl. Sci. Eng. Technol.* 7, 4211–4219. doi:10.19026/rjaset.7.791

Anita, N. (2019). "Blockchain security attack: a brief survey," in 2019 10th international conference on computing, communication and networking technologies (ICCCNT) *(IEEE)* (Piscataway, NJ: Survey of attack vectors–useful for summarizing security vulnerabilities), 1–7. doi:10.1109/ICCCNT45670.2019.8944599

Antony, B., and Revathy, S. (2024). A novel model for sybil attack detection in online social network using optimal three-stream double attention network. *J. Supercomput.* 80, 7433–7482. doi:10.1007/s11227-023-05677-3

Arias-Oliva, M., Pelegrín-Borondo, J., and Matías-Clavero, G. (2019). "Variables influencing cryptocurrency use: a technology acceptance model in Spain," in Frontiers in psychology *examines psychological and behavioral factors influencing adoption. Useful for evaluating user awareness and behavioral risk.*

Arli, D., van Esch, P., Bakpayev, M., and Laurence, A. (2021). Do consumers really trust cryptocurrencies? *Mark. Intell. and Plan.* 39, 74–90. Addresses the issue of consumer trust in cryptocurrency ecosystems. Useful for regulatory and perception analysis. doi:10.1108/MIP-01-2020-0036

Arunachalam, M., and Subramanian, K. (2015). Aes based multimodal biometric authentication using cryptographic level fusion with fingerprint and finger knuckle print. *Int. Arab J. Inf. Technol.*

Asare, B. (2024). "Blockchain technology and vulnerability exploits on smart contracts," in *Blockchain technology and vulnerability exploits on smart contracts.*

Aspris, A., Foley, S., Svec, J., and Wang, L. (2021). Decentralized exchanges: the "wild west" of cryptocurrency trading. *Int. Rev. Financial Analysis* 76, 101845. doi:10.1016/j.irfa.2021.101845

Astrakhantseva, I., Astrakhantsev, R., and Los, A. (2021). Cryptocurrency fraud schemes analysis. *SHS Web Conf.* 106, 02001. doi:10.1051/shsconf/202110602001

Ayeni, R., Adebiyi, A., Okesola, J., and Igbekele, E. (2024). "Phishing attacks and detection techniques: a systematic review," in *2024 international conference on science, engineering and business for driving sustainable development goals (SEB4SDG)* (IEEE), 1–17.

Badaw, E., and Jourdan, G. V. (2020). Cryptocurrencies emerging threats and defensive mechanisms: a systematic literature review. *IEEE Access* 8, 200021–200037. doi:10.1109/ACCESS.2020.3034816

Bandara, H., Herath, Y., Weerasundara, T., and Alawatugoda, J. (2022). On advances of lattice-based cryptographic schemes and their implementations. *Cryptography* 6, 56. doi:10.3390/cryptography6040056

Banoth, R., and Regar, R. (2023). "An introduction to classical and modern cryptography," in *Classical and modern cryptography for beginners* (Cham: Springer), 1–12. doi:10.1007/978-3-031-32959-3_1

Barbon, A., King, T. H. D., and Wang, C. W. (2021). On the quality of cryptocurrency markets: centralized *versus* decentralized. *J. Corp. Finance* 70, 102049. doi:10.1016/j.jcorpfin.2021.102049

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., and Serusi, S. (2021). "Cryptocurrency scams: analysis and perspectives," in *Empirical analysis of scams–vital for fraud typology and risk quantification*. IEEE Access. doi:10.1109/ACCESS.2021.3123894

Bashir, I. (2020). "*Mastering blockchain: a deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, ethereum, and more* (packt publishing)," in *Comprehensive overview including consensus, tokenization, ethereum 2.0, enterprise blockchain, DeFi, scalability, and DApps*. 3rd edn.

Basilan, M. (2024). Bitcoin tops $107,000, inching closer to google, amazon in market cap ranks. Available online at: https://www.ibtimes.com/bitcoin-tops-107000-inching-closer-google-amazon-market-cap-ranks-3755778.IBTimesUS (Accessed 16 August 2025)

Behzadi, L., and Joseph, J. (2024). "Blockchain security considerations," in *Leveraging blockchain technology* (Boca Raton, FL: CRC Press), 73–92.

Bentov, I., Kumaresan, R., Miller, A., and McCorry, P. (2019). "Tesseract: real-time cryptocurrency exchange using trusted hardware," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security (CCS '19)* (London, UK: Association for Computing Machinery), 1521–1538. doi:10.1145/3319535.3355511

Bergstrom, J. (2024). A looming threat to bitcoin: the risk of a quantum hack. Available online at: https://johnlothiannews.com/a-looming-threat-to-bitcoin-the-risk-of-a-quantum-hack/.JohnLothianNews (Accessed 16 August 2025)

Berry, H. S. (2022). The evolution of cryptocurrency and cyber attacks. *IEEE Xplore*, 1–7. doi:10.1109/icca56443.2022.10039632

Bhaskar, N., and Chuen, D. (2024). "Bitcoin exchanges," in *Handbook of digital currency* (Academic Press), 537–551.

Bhatt, A., and Sisodia, K. (2024). "Operational risks in blockchain technology," in *Leveraging blockchain technology* (Boca Raton, FL: CRC Press), 41–56.

Bhusal, C. S. (2021). Systematic review on social engineering: hacking by manipulating humans. *J. Inf. Secur.* 12, 104–114. doi:10.4236/jis.2021.121005

Birthriya, S., Ahlawat, P., and Jain, A. (2024). A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies. *J. Appl. Secur. Res.* 20, 244–292. doi:10.1080/19361610.2024.2372986

Bit2Me Academy (2016). Historia de los exchanges y el trading de bitcoin. Available online at: https://academy.bit2me.com/en/historia-exchanges-trading-bitcoin/ (Accessed August 16, 2025).

Blockchain, C. (2022). Crypto and defi hacks, fraud and scams report. Available online at: https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/.

Brown, R., Bendiab, G., Shiaeles, S., and Ghita, B. (2020). "A novel multimodal biometric authentication system using machine learning and blockchain," in *Proceedings of the 12th international network conference (INC 2020)* (Rhodes, Greece), 19–21. doi:10.1007/978-3-030-64758-2_3

Bucko, J., Palová, D., and Vejačka, M. (2015). "Security and trust in cryptocurrencies," in Proceedings of the central European conference in finance and economics (CEFE 2015) *Košice, Slovakia:* Technical University of Košice (Full text available via ResearchGate), 14–24.

Caliskan, K. (2021). Platform works as stack economization: cryptocurrency markets and exchanges in perspective. *Tecnoscienza Italian J. Sci. and Technol. Stud.* doi:10.6092/issn.1971-8853/11746

Caliskan, K. (2022). The elephant in the dark: a new framework for cryptocurrency taxation and exchange platform regulation in the us. *J. Risk Financial Manag.* 15, 118. doi:10.3390/jrfm15030118

Cambridge Centre for Alternative Finance (2017a). Global cryptocurrency benchmarking study. Available online at: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-04-20-global-cryptocurrency-benchmarking-study.pdf. Oneoftheearliestcomprehensivebenchmarkingstudies–setsabaseline.

Cambridge Centre for Alternative Finance (2017b). *Global cryptocurrency benchmarking study. Tech. Rep., Cambridge centre for alternative finance*. Cambridge Judge Business School. Asia-Pacific: 36 via Cambridge University.

CCData (2025). "2024 annual exchange review: spot trading volumes," *Tech. Rep.* London, United Kingdom: VVData.

Chainalysis (2022). "The 2022 crypto crime report," in *Industry report detailing types and trends in crypto-related crime. Central to evidencing real-world threat models*. Available online at: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

Chainalysis (2023a). 2023 global crypto adoption index. Available online at: https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/.Breaksdownadoption acrossregions–centralforsociotechnicalanalysis.

Chainalysis (2023b). The chainalysis 2023 crypto crime report. Available online at: https://go.chainalysis.com/2023-crypto-Crime-Report.html.Extendsb9withnewercrime trends–vitalforcontemporarycybercrimelandscape.

Chainalysis Team (2024). 2024 crypto crime trends: illicit activity down as scamming and stolen funds fall, but ransomware and darknet markets see growth. Available online at: https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (Accessed August 16, 2025).

Charoenwong, B. (2022). A decade of cryptocurrency "hacks": 2011–2021. *SSRN Prepr.* doi:10.2139/ssrn.3944435

Chen, A. C. H. (2024). The security performance analysis of blockchain systems based on post-quantum cryptography: a case study of cryptocurrency exchanges. *Inf. and Commun. Secur. J.* 15, 34–50. doi:10.48550/arXiv.2404.16837

Chenchev, I., Aleksieva-Petrova, A., and Petrov, M. (2021). Authentication mechanisms and classification: a literature survey. *Intelligent Comput. Proc. 2021 Comput. Conf.* 285, 1051–1070. doi:10.1007/978-3-030-80129-8_69

Cherkaoui, I., Ali, O., and Horgan, J. (2024). "Novel hybrid post-quantum encryption design on embedded devices," in *2024 IEEE 29th international conference on emerging technologies and factory automation (ETFA)* (IEEE), 1–8. doi:10.1109/ETFA61755.2024.10794230

Cherniei, V., Cherniavskyi, S., Babanina, V., and Tykho, O. (2021). Criminal liability for cryptocurrency transactions: global experience. *Eur. J. Sustain. Dev.* 10, 304. doi:10.14207/ejsd.2021.v10n4p304

Chohan, U. W. (2022). "The problems of cryptocurrency thefts and exchange shutdowns," in Social science research network (SSRN) *discusses exchange shutdowns and thefts–critical for the section on operational risk*.

Chutipat, V., Kasemrat, R., Kraiwanit, T., and Phaksipaeng, I. (2023). Selection of cryptocurrency exchange platforms in a developing economy. *Corp. and Bus. Strategy Rev.* 4, 344–350. Discusses platform selection in developing markets–relevant to adoption and decision factors. doi:10.22495/cbsrv4i2siart14

CoinDesk (2023). Mt. gox pushes repayments by a year. Available online at: https://www.coindesk.com/business/2023/09/21/mt-gox-pushes-repayments-by-a-year/ (Accessed August 16, 2025).

CoinMarketCap (2023). Binance exchange information. Available online at: https://coinmarketcap.com/exchanges/binance/.ProvidescurrentmetricsforBinance–usefulfor exchangeprofiling.

CoinMarketCap (2025). Top cryptocurrency spot exchanges. Available online at: https://coinmarketcap.com/rankings/exchanges/ (Accessed August 16, 2025).

Coinpedia (2023). "Global crypto adoption report," in *Adoption statistics globally–useful for user trends section*. Available online at: https://coinpedia.org/research-report/global-crypto-adoption-report/.

Coinweb (2023). How many crypto wallets are there?. Available online at: https://coinweb.com/trends/how-many-crypto-wallets-are-there/ (Accessed August 16, 2025).

Collins, J. (2022). Crypto crime and control: cryptocurrencies as an enabler of organized crime. Available online at: https://globalinitiative.net/wp-content/uploads/2022/06/GITOC-Crypto-crime-and-control-Cryptocurrencies-as-an-enabler-of-organized-crime.pdf.

Connolly, L. Y., and Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: taxonomising countermeasures. *Comput. and Secur.* 87, 101568. Analyzes the evolution of crypto-ransomware and corresponding defensive strategies. Essential for the cybersecurity threats section. doi:10.1016/j.cose.2019.101568

Conti, M., Kumar, S., Lal, C., and Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE Commun. Surv. and Tutorials* 20, 3416–3452. doi:10.1109/COMST.2018.2842460

Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., and Vigne, S. A. (2019a). The destabilising effects of cryptocurrency cybercriminality. *Econ. Lett.* 178, 108741. doi:10.1016/j.econlet.2019.108741

Corbet, S., Lucey, B., Urquhart, A., and Yarovaya, L. (2019b). Cryptocurrencies as a financial asset: a systematic analysis. *Int. Rev. Financial Analysis* 62, 182–199. doi:10.1016/j.irfa.2018.09.003

Cryptohopper (2023). What was the first crypto exchange?. Available online at: https://www.cryptohopper.com/blog/what-was-the-first-crypto-exchange-449 (Accessed August 16, 2025).

Crystal Blockchain (2024a). The 10 biggest crypto exchange hacks in history. Published by Crystal Blockchain B.V. Available online at: https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/.

Crystal Blockchain (2024b). Security breaches and fraud involving crypto. *Ongoing registry breaches–useful industry-wide data points*. Available online at: https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/.

Crystal Intelligence (2024). Expert analysis: wazirx hack. Available online at: https://crystalintelligence.com/investigations/expert-analysis-wazirx-hack/.

Czapliński, T., and Nazmutdinova, E. (2019). Using fiat currencies to arbitrage on cryptocurrency exchanges. *J. Int. Stud.* 12, 184–192. doi:10.14254/2071-8330.2019/12-1/12

de Saint Guilhem, C. D., Fischlin, M., and Warinschi, B. (2020). "Authentication in key-exchange: definitions, relations and composition," in *2020 IEEE 33rd computer security foundations symposium (CSF)* (IEEE), 288–303. doi:10.1109/CSF49147.2020.00028

DefiLlama (2025a). 2024 DEX spot trading volume report. *Tech. Rep.* DefiLlama.

DefiLlama (2025b). "2024 perpetual futures volume – centralized exchanges," *Tech. Rep.* DefiLlama.

DefiLlama (2025c). "2024 perpetual futures volume – decentralized exchanges," *Tech. Rep.* DefiLlama.

Dey, J., and Dutta, R. (2023). Progress in multivariate cryptography: systematic review, challenges, and research directions. *ACM Comput. Surv.* 55, 1–34. doi:10.1145/3571071

Dey, K., Debnath, S. K., Stănică, P., and Srivastava, V. (2022). A post-quantum signcryption scheme using isogeny-based cryptography. *J. Inf. Secur. Appl.* 69, 103280. doi:10.1016/j.jisa.2022.103280

Dharminder, D., Reddy, C. B., Das, A. K., Park, Y., and Jamal, S. S. (2023). Post-quantum lattice-based secure reconciliation enabled key agreement protocol for iot. *IEEE Internet Things J.* 10, 2680–2692. doi:10.1109/JIOT.2022.3213990

Dimpfl, T., and Flad, M. (2020). Nothing but noise? Price discovery across cryptocurrency exchanges. *J. Financial Mark.* 52, 100565. doi:10.1016/j.finmar.2020.100565

Drzazga, B., and Krzywiecki, L. (2022). Review of chosen isogeny-based cryptographic schemes. *Cryptography* 6, 27. doi:10.3390/cryptography6020027

Easa, R. J., Yahya, A. S., and Ahmad, E. K. (2023). Protection from a quantum computer cyber-attack: survey. *Technium* 5, 1–12. doi:10.47577/technium.v5i.8293

Edwards, D. (2024). "Malware defenses," in *Critical security controls for effective cyber defense: a comprehensive guide to CIS 18 controls* (Berkeley, CA: Apress), 277–308. doi:10.1007/978-1-4842-9738-9_14

Eigelshoven, F., Adam, M. T. P., and Benlian, A. (2021). "Cryptocurrency market manipulation: a systematic literature review," in *Proceedings of the forty-second international conference on information systems (ICIS 2021)* (Austin, TX, USA: Association for Information Systems).

Erinle, Y., Kethepalli, Y., Feng, Y., and Xu, J. (2023). Sok: Design, vulnerabilities, and defense of cryptocurrency wallets. Available online at: https://arxiv.org/abs/2307.12874.

Falowo, O., Ozer, M., Li, C., and Abdo, J. (2024). Evolving malware and ddos attacks: decadal longitudinal study. *IEEE Access*. doi:10.1109/ACCESS.2024.3376682

Fang, F., Ventre, C., Basios, M., Kanthan, L., Martinez-Rego, D., Wu, F., et al. (2022). Cryptocurrency trading: a comprehensive survey. *Financ. Innov.* 8, 13. doi:10.1186/s40854-021-00321-6

Faruk, M. J. H., Rahman, M. A., Alharbi, F., Alharbi, A., and Saad, M. A. (2022). "A review of quantum cybersecurity: threats, risks and opportunities," in Proceedings of the 2022 1st international conference on AI in cybersecurity (ICAIC) *(IEEE)*, 1–7. doi:10.1109/ICAIC53980.2022.9896970

Fathalla, E., and Azab, M. (2024). Beyond classical cryptography: a systematic review of post-quantum hash-based signature schemes, security, and optimizations. *IEEE Access* 12, 175969–175987. doi:10.1109/access.2024.3485602

Feder, A., Gandal, N., Hamrick, J. T., and Moore, T. (2017). The impact of ddos and other security shocks on bitcoin currency exchanges: evidence from mt. gox. *J. Cybersecurity* 3, 137–144. doi:10.1093/cybsec/tyx012

Feng, Y., Zhou, J., Li, J., Zhao, W., Shi, J., Shi, R., et al. (2022). Skc-ccco: an encryption algorithm for quantum group signature. *Quantum Inf. Process.* 21, 328. doi:10.1007/s11128-022-03664-w

Fernández-Caramés, T. M. (2020). Towards post quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*. doi:10.1109/ACCESS.2020.2968985

Fu, S., Wang, Q., Yu, J., and Chen, S. (2022). Ftx collapse: a ponzi story. *arXiv Prepr.* doi:10.48550/arXiv.2212.09436

Future Market Insights (2023). Crypto trading platforms market. Relevant for market analysis. Available online at: https://www.futuremarketinsights.com/reports/crypto-trading-platforms-market.Givesindustryforecastandgrowthprojections.

Gangele, S. (2024). Data security system for a bank based on two different asymmetric algorithms cryptography. *Int. J. Multidiscip. Res. (IJFMR)* 6, 11710. doi:10.36948/ijfmr.2024.v06i01.11710

Gayathri, S., and Shanmugam, K. (2023). Giottus story–a case study of india's highly rated crypto exchange. *J. Inf. Technol. Teach. Cases* 14, 282–289. doi:10.1177/20438869231187662

Ghinea, D., Kaczmarczyck, F., Pullman, J., Cretin, J., Kölbl, S., Misoczki, R., et al. (2023). "Hybrid post-quantum signatures in hardware security keys," in Applied cryptography and network security (ACNS 2023) *(springer nature Switzerland), vol. 13907 of* lecture notes in computer science, 480–499. doi:10.1007/978-3-031-33623-2_23

Giechaskiel, I., Cremers, C., and Rasmussen, K. B. (2016). "On bitcoin security in the presence of broken cryptographic primitives," *Lect. Notes Comput. Sci.*, 9558. 201–222. doi:10.1007/978-3-319-45741-3_11

Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., et al. (2022). Quantum computing: a taxonomy, systematic review and future directions. *Softw. Pract. Exp.* 52, 66–114. doi:10.1002/spe.3039

Giron, A. A., Custódio, R., and Rodríguez-Henríquez, F. (2023). Post-quantum hybrid key exchange: a systematic mapping study. *J. Cryptogr. Eng.* 13, 71–88. doi:10.1007/s13389-022-00288-9

Goh, Z. H., Wang, Y., Leng, L., Liang, S.-N., Jin, Z., Lai, Y.-L., et al. (2022). A framework for multimodal biometric authentication systems with template protection. *IEEE Access* 10, 96388–96402. doi:10.1109/ACCESS.2022.3205413

Gong, G. (2024). Uni/multi variate polynomial embeddings for zksnarks. *Cryptogr. Commun.* 16, 1257–1288. doi:10.1007/s12095-024-00723-0

Gorkhali, A., Li, L., and Shrestha, A. (2020). Blockchain: a literature review. *J. Manag. Anal.* 7, 321–343. doi:10.1080/23270012.2020.1801529

Gottipati, H. (2020). A proposed cybersecurity model for cryptocurrency exchanges. *Master's thesis*. Edmonton: Concordia University of.

Gueron, S., Persichetti, E., and Santini, P. (2022). Designing a practical code-based signature scheme from zero-knowledge proofs with trusted setup. *Cryptography* 6, 5. doi:10.3390/cryptography6010005

Gupta, A., Panda, M., and Gupta, A. (2024a). Advancing Api security: a comprehensive evaluation of authentication mechanisms and their implications for cybersecurity. *Int. J. Glob. Innovations Solutions (IJGIS)*. doi:10.21428/e90189c8.406d2328

Gupta, S., Pritwani, M., Shrivastava, A., Moharir, M., and Ar, A. (2024b). "A comprehensive analysis of social engineering attacks: from phishing to prevention-tools, techniques and strategies," in *2024 second international conference on intelligent cyber physical systems and internet of things (ICoICI)* (IEEE), 1–8.

Gyongyosi, L., and Imre, S. (2019). A survey on quantum computing technology. *Comput. Sci. Rev.* 31, 51–71. doi:10.1016/j.cosrev.2018.11.002

Hamrick, J. T., Zhang, Y., Xu, M., Zhang, L., Yang, Y., and Yan, S. (2021). A survey on concept factorization: from shallow to deep representation learning. *Inf. Process. and Manag.* 58, 102534. doi:10.1016/j.ipm.2021.102534

Hasan, M., Rozony, F. Z., Kamruzzaman, M., and Uddin, M. K. S. (2024). Common cybersecurity vulnerabilities: software bugs, weak passwords, misconfigurations, social engineering. *Glob. Mainstream J. Innovation, Eng. and Emerg. Technol.* 3, 42–57. doi:10.62304/jieet.v3i04.193

Hedge with Crypto (2024). Cryptocurrency exchange hacks. Available online at: https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/.Listshistorical exchangehacks–practicalcasereferences.

Hendrix, C., and Lewis, R. (2021). *Survey on blockchain privacy challenges*. USA: University of Colorado, Colorado Springs CO.

Higbee, A. (2018). "The role of crypto-currency in cybercrime," in Computer fraud & security *2018*, 5–8. doi:10.1016/S1361-3723(18)30086-0

Holub, A., Shachtman, A., Kaczmarek, K., Naik, N., and Christin, N. (2018). "Coinhoarder: tracking a Ukrainian bitcoin phishing ring dns style," in *2018 APWG symposium on electronic crime research (eCrime)* (IEEE), 1–10. doi:10.1109/ECRIME.2018.8376208

Homoliak, I., and Perešíni, M. (2024). Sok: cryptocurrency wallets – a security review and classification based on authentication factors. 1–8. doi:10.1109/icbc59979.2024.10634439

Hong, S. (2019). Survey on analysis and countermeasure for hacking attacks to cryptocurrency exchange. *J. Korea Convergence Soc.* 10, 1–6. doi:10.15207/JKCS.2019.10.10.001

Horch, A., Sittig, D., and Posegga, J. (2022). "Adversary tactics and techniques specific to cryptocurrency scams," in Proceedings of Open Identity Summit 2022 (OID 2022) *(Gesellschaft für Informatik)*, 111–122. doi:10.18420/OID2022-10

Horlemann, A. L. (2023). "An introduction to code-based cryptography," in *Proceedings of the summer school on finite geometry and friends*, 35. Lecture notes/summer school contribution.

Hussain, H. S. (2023). "Cryptocurrency methodologies and techniques," in *The data-driven blockchain ecosystem: fundamentals, applications, and emerging technologies*. Editors A. Khang, S. Chowdhury, and S. Sharma (Boca Raton, FL: CRC Press), CRC Press Information Science and Statistics), 21–29. doi:10.1201/9781003269281-2

Ikematsu, Y., Nakamura, S., and Takagi, T. (2023). Recent progress in the security evaluation of multivariate public-key cryptography. *IET Inf. Secur.* 17, 210–226. doi:10.1049/ise2.12092

Illia, A., Lawson-Body, A., Lee, S., and Akalin, G. I. (2023). Determinants of cryptocurrency exchange adoption: a conceptual model. *Int. J. Technol. Hum. Interact.* 19, 1–14. doi:10.4018/IJTHI.326760

IMARC Group (2023). Cryptocurrency market forecast. Available online at: https://www.imarcgroup.com/cryptocurrency-market.Marketvaluationforecast; strengthenseconomicandadoptionnarrative.

Inayat, U., Farzan, M., Mahmood, S., Zia, M., Hussain, S., and Pallonetto, F. (2024). Insider threat mitigation: systematic literature review. *Ain Shams Eng. J.* 103068. doi:10.1016/j.asej.2023.103068

Islam, M. R., Khan, F., and Al Mahmud, A. (2018). "Cryptocurrency vs fiat currency: architecture, algorithm, cashflow and ledger technology on emerging economy," in 2018 international conference on information and communication technology for the

Muslim world (ICT4M) *(kuala lumpur, Malaysia: IEEE)*, 64–69. doi:10.1109/ICT4M.2018.00020

Jain, V., Goyal, A., and Kumar, R. (2021). "Coin drop—a decentralised exchange platform," in *Data engineering and communication technology* (Springer), 37 379–388. Singapore, vol. 73 of *Lecture Notes on Data Engineering and Communications Technologies*. doi:10.1007/978-981-16-3961-6_33

Jani, S. (2018). "The growth of cryptocurrency in India: its challenges and potential impacts on legislation," in ResearchGate *analyzes India's regulatory and societal responses–useful in regional policy comparison*.

Jiao, T., Xu, Z., Qi, M., Wen, S., Xiang, Y., and Nan, G. (2024). A survey of ethereum smart contract security: attacks and detection. *Distributed Ledger Technol. Res. Pract.* 3, 1–28. doi:10.1145/3643895

John, M., Ozioma, O., Ngozi, O., and Egbogho, H. (2023). *Lattices in quantum-era cryptography*, 3.*Int. J. Res. Publ. Rev.* doi:10.5281/zenodo.10207209

Johnson, K. (2020). Decentralized finance: regulating cryptocurrency exchanges. *Wm. and Mary Law Rev.* 62, 1911.

Kamruzzaman, A., Thakur, K., and Ali, M. (2024). "Cybersecurity threats using application programming interface (api)," in *2024 international conference on Computing, internet of things and microwave systems (ICCIMS)* (IEEE), 1–6.

Kapoor, J., and Thakur, D. (2022). "Analysis of symmetric and asymmetric key algorithms," in *ICT analysis and applications* (Springer Singapore), 133–143. doi:10.1007/978-981-16-2377-6_11

Kasera, A. (2020). Cryptocurrency frauds. *Int. J. Eng. Adv. Technol. (IJEAT)* 9, 261–268. doi:10.35940/ijeat.f1391.089620

Kathed, A., Yadav, A., and Singh, D. (2019). "An enhanced 3-tier multimodal biometric authentication," in *2019 international conference on intelligent computing and control systems (ICCS)* (Madurai, India: IEEE), 1243–1248. doi:10.1109/ICCS45141.2019.9065742

Kawai, D., Tanaka, Y., Maehira, T., and Orihara, R. (2023). User participation in cryptocurrency derivative markets. 5th Conf. Adv. Financial Technol. (AFT 2023) *Schloss Dagstuhl – Leibniz-Zentrum für Inf. vol. 282* Leibniz Int. Proc. Inf. (LIPIcs) 8, 1–8:20. Explores behavioral trends in crypto derivatives trading. doi:10.4230/LIPIcs.AFT.2023.8

Keller, A., and Scholz, M. (2019). "Trading on cryptocurrency markets: analyzing the behavior of bitcoin investors," in *Proceedings of the 40th international conference on information systems (ICIS 2019)* (Munich, Germany: Association for Information Systems).

Khosravi, A., and Eghlidos, T. (2023). Quantum cryptanalysis of symmetric primitives by improving relaxed variants of simon's algorithm. *ISeCure* 15. doi:10.22042/ISECURE.2023.198343

Kim, C. Y., and Lee, K. (2018). "Risk management to cryptocurrency exchange and investors guidelines to prevent potential threats," in *2018 international conference on platform technology and service (PlatCon)*, 1–6. doi:10.1109/PlatCon.2018.8472760

Kiraz, M. (2016). A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing. *J. Ambient Intell. Humaniz. Comput.* 7, 731–760. doi:10.1007/s12652-016-0385-0

Krafft, P. M., Pentland, A., and Shmueli, E. (2018). "An experimental study of cryptocurrency market dynamics," in *Proceedings of the 2018 ACM conference on economics and computation (EC '18)* (Ithaca, NY, USA: Association for Computing Machinery), 531–548. doi:10.1145/3219166.3219239

Ku-Mahamud, K. R., Omar, M., Abu Bakar, N. A., and Muraina, I. D. (2019). Awareness, trust, and adoption of blockchain technology and cryptocurrency among blockchain communities in Malaysia. *Int. J. Adv. Sci. Eng. Inf. Technol.* 9, 1217–1222. Regional case study–important for comparative user adoption discussion. doi:10.18517/ijaseit.9.4.6280

Kuang, R., Perepechaenko, M., and Barbeau, M. (2022). A new post-quantum multivariate polynomial public key encapsulation algorithm. *Quantum Inf. Process.* 21, 360. doi:10.1007/s11128-022-03712-5

Kumar, S., Dwivedi, M., Kumar, M., and Gill, S. (2024). A comprehensive review of vulnerabilities and ai-enabled defense against ddos attacks for securing cloud services. *Comput. Sci. Rev.* 53, 100661. doi:10.1016/j.cosrev.2024.100661

Leroux, A. (2022a). "A new isogeny representation and applications to cryptography," in Advances in cryptology – ASIACRYPT 2022 *(springer nature Switzerland), vol. 13793 of* lecture notes in computer science, 3–35. doi:10.1007/978-3-031-22966-4_1

Leroux, A. (2022b). *Quaternion algebra and Isogeny-Based cryptography*. Paris: Institut Polytechnique de. Ph.D. thesis.

Li, W., Bu, J., Li, X., Peng, H., Niu, Y., and Zhang, Y. (2022). A survey of defi security: challenges and opportunities. 34, 10378–10404. doi:10.1016/j.jksuci.2022.10.028

Limdrian, J., Thorif, M., Fredyan, R., and Ibrahim, M. (2024). "Exploring security in cryptocurrency: challenges, solutions, and implications–a systematic literature review," in 2024 international conference on ICT for smart Society (ICISS) *(IEEE)*, 1–9. doi:10.1109/ICISS61969.2024.10699164

Magizov, R., Shamin, A., and Ponomarev, E. (2019). "Problems of criminal responsibility for illegal circulation of cryptocurrency," in *2019 12th international conference on developments in eSystems engineering (DeSE)* (IEEE), 633–638. doi:10.1109/DeSE.2019.00185

Makridis, C. A., Fröwis, M., Sridhar, K., and Böhme, R. (2023). The rise of decentralized cryptocurrency exchanges: evaluating the role of airdrops and governance tokens. *J. Corp. Finance* 79, 102358. doi:10.1016/j.jcorpfin.2023.102358

Malviya, A. K., Tiwari, N., and Chawla, M. (2022). Quantum cryptanalytic attacks of symmetric ciphers: a review. *Comput. Electr. Eng.* 101, 108122. doi:10.1016/j.compeleceng.2022.108122

Mamatha, G. S., Dimri, N., and Sinha, R. (2024). Post-quantum cryptography: securing digital communication in the quantum era. *arXiv Prepr. arXiv:2403*. doi:10.48550/arXiv.2403.11741

Manimuthu, A., Sreedharan, V. R., Rejikumar, G., and Marwaha, D. (2019). "A literature review on bitcoin: transformation of crypto currency into a global phenomenon," in *Relevant for the historical background*. IEEE Engineering Management Review Reviews Bitcoin's emergence and its implications for global economic systems.

Manthovani, R. (2023). A comparative analysis of money laundering crimes in Indonesia through cryptocurrency. *Int. J. Cyber Criminol.* doi:10.5281/zenodo.4766612

Marchsreiter, D., and Sepúlveda, J. (2023). "A pqc and qkd hybridization for quantum-secure communications," in *2023 26th euromicro conference on digital system design (DSD)* (IEEE), 545–552. doi:10.1109/DSD60801.2023.00079

Marella, V., Zeng, D., and Wang, H. (2021). "Rebuilding trust in cryptocurrency exchanges after cyber-attacks," in Proceedings of the 54th Hawaii international conference on system sciences (HICSS 2021) *(hawaii, USA: hawaii international conference on system sciences)*, 6314–6323. Focuses on post-attack strategies for trust restoration. doi:10.24251/HICSS.2021.758

María, N. P. (2024). "Post-quantum symmetric cryptography," in *Symmetric cryptography, volume 2: cryptanalysis and future directions* (Springer), 203. doi:10.1007/978-3-031-23304-3_9

Mateen, M. (2023). *Regulation in the cryptocurrency industry*. Thesis: University of Missouri-Kansas City.

Mattos, S. M., Cestari, V. R. F., and Moreira, T. M. M. (2023). Scoping protocol review: prisma-scr guide refinement. *Rev. Enferm. UFPI* 12. doi:10.26694/reufpi.v12i1.3062

McCorry, P., Möser, M., and Ali, S. T. (2018). "Why preventing a cryptocurrency exchange heist isn't good enough," in *Security protocols XXVI* (Cham: Springer), 150–158. 11286 of *Lecture Notes in Computer Science*. doi:10.1007/978-3-030-03251-7_12

Minto, A. (2022). The legal characterization of crypto-exchange platforms. *Glob. Jurist* 22, 137–156. doi:10.1515/gj-2020-0085

Mohammadi, R., Hosseini, M., and Bahrami, R. (2024). "Uncovering security vulnerabilities through multiplatform malware analysis," in Security and privacy, e455. doi:10.1002/spy2.455

Mohsin, K. (2022). Cryptocurrency legality and regulations – an international scenario. *Int. J. Cryptocurrency Res.* 2, 19–29. doi:10.51483/IJCCR.2.1.2022.19-29

Monrat, A. A., Schelen, O., and Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE ACCESS* 7, 117134–117151. doi:10.1109/ACCESS.2019.2936094

Morin, A., Dandekar, V., and Smarandache, A. (2023). "How cryptocurrency exchange interruptions create arbitrage opportunities," in *2023 IEEE European symposium on security and privacy workshops (EuroS&PW)* (IEEE), 33–40. doi:10.1109/EuroSPW59978.2023.00028

Mosca, M. (2018). Cybersecurity in an era with quantum computers: will we be ready? *Tech. Rep. Glob. Risk Inst.* 16, 38–41. doi:10.1109/msp.2018.3761723

Mosca, M., and Piani, M. (2024). "Quantum threat timeline report 2024," *Tech. Rep.* Toronto, Canada: Global Risk Institute.

Moussa, W., Nadia, B., and Ines, G. (2020). Asymmetric effect and dynamic relationships over the cryptocurrencies market. *Comput. and Secur.* 96, 101860. doi:10.1016/j.cose.2020.101860

Munn, Z., Peters, M. D. J., Stern, C., Tufanaru, C., McArthur, A., and Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review. *BMC Med. Res. Methodol.* 18, 1–7. doi:10.1186/s12874-018-0611-x

Munn, Z., Pollock, D., Khalil, H., Alexander, L., Mclnerney, P., Godfrey, C. M., et al. (2022). What are scoping reviews? Providing a formal definition of scoping reviews as a type of evidence synthesis. *JBI Evid. Synth.* 20, 950–952. doi:10.11124/JBIES-21-00483

Murugappan, M., Nair, R., and Krishnan, S. (2023). Global market perceptions of cryptocurrency and the use of cryptocurrency by consumers: a pilot study. *J. Theor. Appl. Electron. Commer. Res.* 18, 1955–1970. doi:10.3390/jtaer18040098

Nabilou, H. (2020). The dark side of licensing cryptocurrency exchanges as payment institutions. *Law Financial Mark. Rev.* 14, 39–47. doi:10.1080/17521440.2019.1626545

Nagarajan, G., Gopi, R. M., and Sanjai, R. (2024). "Role of hash-based signatures in quantum cryptography," in AIP conference proceedings *(AIP publishing)*, 3075 020007. doi:10.1063/5.0212709

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *SSRN 3440802*

Nakamoto, S. (2009). Bitcoin: a peer-to-peer electronic cash system. Available online at: https://bitcoin.org/bitcoin.pdf.

National Institute of Standards and Technology (2024). Nist releases first 3 finalized post-quantum encryption standards. NIST News. *Online*

Navamani, T. M. (2021). *A review on cryptocurrencies security*. Journal of Applied Security Research. Oxfordshire, United Kingdom: Taylor & Francis. doi:10.1080/19361610.2021.1933322

Navarro, R. R. (2019). Preventative fraud measures for cryptocurrency exchanges: mitigating the risk of cryptocurrency scams. *Utica Coll. Thesis*.

Nosouhi, M. R., Sood, K., Chamola, V., Jeong, J. J., and Gaddam, A. (2024). Towards quantum-secure software defined networks. *IET Quantum Commun.* 5, 66–71. doi:10.1049/qtc2.12073

Olaiya, O. P., Adesoga, T. O., Adebayo, A. A., Sotomi, F. M., Adigun, O. A., and Ezeliora, P. M. (2024). Encryption techniques for financial data security in fintech applications. *Int. J. Sci. Res. Archive* 12, 2942–2949. doi:10.30574/ijsra.2024.12.1.1210

Olaniyan, J., and Ogunola, A. A. (2024). Protecting small businesses from social engineering attacks in the digital era. *World J. Adv. Res. Rev.* 24, 834–853. doi:10.30574/wjarr.2024.24.3.3745

Oosthoek, K. (2021). "Cyber security threats to bitcoin exchanges: adversary exploitation and laundering techniques," in *Covers cyber-attack strategies and laundering–technical depth for risk section*. IEEE Transactions on Network and Service Management. doi:10.1109/TNSM.2020.3046145

Oosthoek, K., Bowen, B. M., and Hutchison, D. (2020). "From hodl to heist: analysis of cyber security threats to bitcoin exchanges," in *2020 IEEE international conference on blockchain and cryptocurrency (ICBC)* (IEEE), 1–8. doi:10.1109/ICBC48266.2020.9169412

Padhiar, S., and Mori, K. H. (2022). A comparative study on symmetric and asymmetric key encryption techniques. Implement. Data Anal. Archit. Next Generation Wirel. Commun. *IGI Glob.*, 132–144. doi:10.4018/978-1-7998-6988-7.ch008

Paganini, P. (2018). Group-ib: 14 cyber attacks on crypto exchanges resulted in a loss of $882 million. Available online at: https://securityaffairs.co/77213/hacking/cyber-attacks-crypto-exchanges.html. Security Affairs (Accessed 16 August 2025)

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The prisma 2020 statement: an updated guideline for reporting systematic reviews. *BMJ* 372, n71. doi:10.1136/bmj.n71

Pan, D., Long, G-L, Yin, L., Sheng, Y-B, Ruan, D., and Xin Ng, S. (2024). The evolution of quantum secure direct communication: on the road to the qinternet. *IEEE Commun. Surv. and Tutorials*. doi:10.1109/COMST.2024.3372208

Pandya, S., Mittapalli, M., Gulla, S. V. T., and Landau, O. (2019). Cryptocurrency: adoption efforts and security challenges in different countries. *HOLISTICA* 10, 167–186. doi:10.2478/hjbpa-2019-0024

Panjwani, P. (2023). S Korean crypto exchange gdac hacked for nearly $13m. Available online at: https://www.coindesk.com/tech/2023/04/10/s-korean-crypto-exchange-gdac-hacked-for-nearly-13m/.CoinDesk (Accessed 16 August 2025)

Panthi, S., and Bhuyan, B. (2023). "Quantum-resistant hash-based digital signature schemes: a review," in *Frontiers in computing and systems* (Springer Nature Singapore), 637–655. doi:10.1007/978-981-99-8147-8_46

Patashkova, Y., Niyazbekova, S., Kerimkhulle, S., Serikova, M., and Troyanskaya, M. (2021). Dynamics of bitcoin trading on the binance cryptocurrency exchange. *Econ. Annals-XXI* 187, 177–188. doi:10.21003/ea.V187-17

Patel, S. M. (2022). Fraud on the crypto market. *Harv. J. Law Technol.* doi:10.2139/ssrn.4278973

Patel, S., Singh, H., Chatterjee, P., and Saxena, A. (2019). "Dauth: a decentralized web authentication system using ethereum based blockchain," in 2019 IEEE international conference on blockchain (Blockchain-2019) *(IEEE)*, 208–215. doi:10.1109/Blockchain.2019.00033

Poonia, L., and Tinker, S. (2024). A comprehensive analysis of the types, impacts, prevention, and mitigation of ddos attacks. *Recent Patents on Engineering*

Prabakaran, D., and Ramachandran, S. (2022). Multi-factor authentication for secured financial transactions in cloud environment. *CMC-Computers, Mater. and Continua* 70, 1781–1798. doi:10.32604/cmc.2022.019846

Prendi, L., Borakaj, D., and Prendi, K. (2023). The new money laundering machine through cryptocurrency: current and future public governance challenges. *Corp. Law and Gov. Rev.* 5, 84–91. doi:10.22495/clgrv5i2p9

Preskill, J. (2018). Quantum computing in the nisq era and beyond. *Quantum* 2, 79. doi:10.22331/q-2018-08-06-79

Purohit, H., Dadhich, M., and Ajmera, P. K. (2023). Analytical study on users' awareness and acceptability towards adoption of multimodal biometrics (mmb) mechanism in online transactions: a two-stage sem-ann approach. *Multimedia Tools Appl.* 82, 14239–14263. doi:10.1007/s11042-022-13786-z

Rani, S., and S. Vennila Fathima Rani, (2024). Securing digital wallets: threats and countermeasures. *mLAC J. Arts, Commer. Sci. (m-JACS)* 2, 25–32. doi:10.59415/mjacs.v2i4.185

Reijnders, K. (2023). "Effective pairings in isogeny-based cryptography," in Progress in cryptology – LATINCRYPT 2023 *(springer nature Switzerland), vol. 14203 of* lecture notes in computer science, 109–128. doi:10.1007/978-3-031-47637-2_6

Rejeb, A., Rejeb, K., and Keogh, J. G. (2021). Cryptocurrencies in modern finance: a literature review. *Etikonomi* 20, 93–118. Literature review summarizing cryptocurrency's financial impact. Good overview source. doi:10.15408/etk.v20i1.16911

Ren, L., and Zhang, D. (2022). A qr code-based user-friendly visual cryptography scheme. *Sci. Rep.* 12, 7667. doi:10.1038/s41598-022-11871-9

Reynolds, M. (2025). Q-day is coming: the apocalypse of encryption. *Wired*.

Rezaeighaleh, H., and Zou, C. C. (2020). "Multilayered defense-in-depth architecture for cryptocurrency wallet," in *2020 IEEE 6th international conference on computer and communications (ICCC)* (IEEE), 2212–2217. doi:10.1109/ICCC51575.2020.9345013

Ricci, S., Dobias, P., Malina, L., Hajny, J., and Jedlicka, P. (2024). Hybrid keys in practice: combining classical, quantum and post-quantum cryptography. *IEEE Access* 12, 23206–23219. doi:10.1109/access.2024.3364520

Rosch-Grace, D., and Straub, J. (2021). "Analysis of the necessity of quantum computing capacity development for national defense and homeland security," in *2021 IEEE international symposium on technologies for homeland security (HST)*, 1–8. doi:10.1109/HST53381.2021.9619831

Rot, A., and Blaicke, B. (2019). "Blockchain's future role in cybersecurity: analysis of defensive and offensive potential," in *2019 9th international conference on advanced computer information technologies (ACIT)* (IEEE), 447–451. doi:10.1109/ACITT.2019.8779860

Roy, K. S. (2019). *A survey on post-quantum cryptography for constrained devices*. International Journal of Applied Engineering Research. (India: Research India Publications)

Ruiz, E. P., and Angelis, J. (2022). Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges. *J. Money Laund. Control* 25, 766–778. doi:10.1108/jmlc-09-2021-0106

Ruoti, S., Kaiser, B., Yerukhimovich, A., Clark, J., and Cunningham, R. (2020). Blockchain technology: what is it good for? *Commun. ACM* 63, 46–53. doi:10.1145/3369752

Saha, R., Kumar, G., Devgun, T., Buchanan, W. J., Thomas, R., Alazab, M., et al. (2023). A blockchain framework in post-quantum decentralization. *IEEE Trans. Serv. Comput.* 16, 1–12. doi:10.1109/TSC.2021.3116896

Santhosh, A., and Subramanian, N. (2024a). "Classify attacks based on blockchain components," in *2024 12th international symposium on digital forensics and security (ISDFS)* (IEEE), 1–6.

Santhosh, A., and Subramanian, N. (2024b). "Classify attacks based on blockchain components," in *2024 12th international symposium on digital forensics and security (ISDFS)* (IEEE), 1–6. doi:10.1109/ISDFS60427.2024.10663992

Sarkis-Onofre, R., Catalá-López, F., Aromataris, E., and Lockwood, C. (2021). How to properly use the prisma statement. *Syst. Rev.* 10, 117. doi:10.1186/s13643-021-01671-z

Scharfman, J. (2023). *The cryptocurrency and digital asset fraud casebook*. Springer Nature Switzerland AG. doi:10.1007/978-3-031-23679-2

Sengupta, J., Ruj, S., and Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. *J. Netw. Comput. Appl.* 149, 102481. doi:10.1016/j.jnca.2019.102481

Shaji, N. A., Basheer, M., and Ramya, R. S. (2022). "Geofencing and cryptocurrency exchange platforms with blockchain anonymity," in *2022 IEEE 7th international conference on recent advances and innovations in engineering (ICRAIE)* (IEEE), 1–6. doi:10.1109/ICRAIE56454.2022.10054294

Shalini, S., and Santhi, H. (2019). "A survey on various attacks in bitcoin and cryptocurrency," in 2019 international conference on communication and signal processing (ICCSP) *(IEEE)*, 0329–0333. doi:10.1109/ICCSP.2019.8698003

Shandilya, S., Datta, A., Kartik, Y., and Nagar, A. (2024). "A study in attack and breaches," in *Digital resilience: navigating disruption and safeguarding data privacy* (Boca Raton, FL: CRC Press), 279–309.

Sharma, D. K., Singh, N. C., Noola, D. A., Doss, A. N., and Sivakumar, J. (2022). A review on various cryptographic techniques and algorithms. *Mater. Today Proc.* 51, 104–109. doi:10.1016/j.matpr.2021.05.483

Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., and Trück, S. (2022). The illogic of plausible deniability: why proxy conflict in cyberspace May no longer pay. *J. Cybersecurity* 8, tyac007. doi:10.1093/cybsec/tyac007

Shou, C., Ke, Y., Yang, Y., Su, Q., Dadosh, O., Eli, A., et al. (2024). Backrunner: mitigating smart contract attacks in the real world. ArXiv preprint arXiv:2409.06213. Available online at: https://arxiv.org/abs/2409.06213.

Sigalos, M. (2023). Sam bankman-fried found guilty on all seven criminal fraud counts. Available online at: https://www.cnbc.com/2023/11/02/sam-bankman-fried-found-guilty-on-all-seven-criminal-fraud-counts.html.CNBC (Accessed 16 August 2025)

Sigurdsson, G., Petursson, A., and Kristjansson, K. (2020). "Vulnerabilities and security breaches in cryptocurrencies," in *Blockchain and cryptocurrency: legal and security considerations* (Springer Nature Switzerland), 87–102. doi:10.1007/978-3-030-56784-5_6

Singamaneni, K. K., and Muhammad, G. (2024). A novel integrated quantum-resistant cryptography for secure scientific data exchange in ad hoc networks. *Ad Hoc Netw.* 164, 103607. doi:10.1016/j.adhoc.2024.103607

Singh, M. K. (2022). "Code-based cryptography: a comparative study of key sizes," in *Advanced communication and intelligent systems* (Springer Nature Switzerland), 359–368. doi:10.1007/978-3-031-21407-3_32

Soana, G. (2024). *The anti-money laundering regulation of crypto-assets in Europe: a critical analysis*, 13. of *Giustizia penale europea* (CEDAM).

Sobral, J. (2022). On the security of multivariate encryption schemes. *J. Inf. Secur.*

Soska, K., Christin, N., and Eskandari, S. (2021). "Towards understanding cryptocurrency derivatives: a case study of bitmex," in Proceedings of the 2021 ACM SIGSAC conference on computer and communications security (CCS) *(ACM)*, 1736–1753. doi:10.1145/3460120.3484592

Souza, O. T., and Carvalho, J. V. F. (2022). Market efficiency assessment for multiple exchanges of cryptocurrencies. *Rev. Gestão (REGE)* 31, 137–151. doi:10.1108/REGE-05-2022-0070

Srivastava, V., Baksi, A., and Debnath, S. K. (2023). An overview of hash-based signatures. Cryptol. ePrint Arch. *Rep. 2023/639*. Available online at: https://eprint.iacr.org/2023/639.

Stovold, E., Beecher, D., Foxlee, R., and Noel-Storr, A. (2014). Study flow diagrams in cochrane systematic review updates: an adapted prisma flow diagram. *Syst. Rev.* 3, 54. doi:10.1186/2046-4053-3-54

Subramani, S., Selvi, M., Kannan, A., and Santhosh Kumar, S. V. N. (2023). "Review of security methods based on classical cryptography and quantum cryptography," in *Cybernetics and systems*. doi:10.1080/01969722.2023.2166261

Suga, Y., Shimaoka, M., Sato, M., and Nakajima, H. (2020). "Securing cryptocurrency exchange: building up standard from huge failures," in *Financial cryptography and data security: FC 2020 international workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC* (Springer International Publishing), 254–270. doi:10.1007/978-3-030-54455-3_19

Sumalatha, U., Prakasha, K. K., Prabhu, S., and Nayak, V. C. (2024). A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: fusion, attacks, and template protection. *IEEE Access* 12, 64300–64334. doi:10.1109/ACCESS.2024.3395417

Szymanski, T. H. (2022). The cyber security *via* determinism' paradigm for a quantum-safe zero trust deterministic internet of things (iot). *IEEE Access* 10, 45893–45930. doi:10.1109/ACCESS.2022.3169137

Takahashi, H., Sato, H., and Kono, K. (2019). "Multiple layered security analyses method for cryptocurrency exchange servicers," in *2019 IEEE 8th global conference on consumer electronics (GCCE)* (IEEE), 775–779. doi:10.1109/GCCE46687.2019.9015207

Tandon, A., and Nayyar, A. (2019). "A comprehensive survey on ransomware attack: a growing havoc cyberthreat," in *Cybersecurity issues in emerging technologies* (Singapore: Springer), 1–27. doi:10.1007/978-981-13-8775-3_1

Thanalakshmi, P., Rishikhesh, A., Marion Marceline, J., Joshi, G., and Cho, W. (2023). A quantum-resistant blockchain system: a comparative analysis. *Mathematics* 11, 3947. doi:10.3390/math11183947

Tom, J. J., P. Anebo, D. N., Onyekwelu, D. B. A., Wilfred, A., and E. Eyo, R. (2023). Quantum computers and algorithms: a threat to classical cryptographic systems. *Int. J. Eng. Adv. Technol. (IJEAT)* 12, 25–38. doi:10.35940/ijeat.E4153.0612523

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K., Colquhoun, H., Kastner, M., et al. (2016). A scoping review on the conduct and reporting of scoping reviews. *BMC Med. Res. Methodol.* 16, 15. doi:10.1186/s12874-016-0116-4

Tripathi, S., Gupta, A., Kumar, R., and Aggarwal, S. (2023). *Tex – true exchange: decentralized cryptocurrency exchange for indian markets* Les Ulis, France: EDP Sciences. 01158, 430. doi:10.1051/e3sconf/202343001158

Triple-A Technologies Pte. Ltd (2024). The state of global cryptocurrency ownership in 2024. Available online at: https://www.triple-a.io/cryptocurrency-ownership-data/. Foreword by Eric Barbier (Accessed 16 August 2025)

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., et al. (2022). Cryptocurrencies and future financial crime. *Crime Sci.* 11, 1. doi:10.1186/s40163-021-00163-8

Vasavi, K., and Latha, Y. (2019). Rsa cryptography based multi-modal biometric identification system for high-security application. *Int. J. Intelligent Eng. Syst.* 12, 10–21. doi:10.22266/ijies2019.0228.02

Vasek, M., and Moore, T. (2018). "Analyzing the bitcoin ponzi scheme ecosystem," *Proc. Bitcoin Workshop, Lect. Notes Comput. Sci.*, 10958. 101–112. doi:10.1007/978-3-662-58820-8_8

Vasek, M., Thornton, M., and Moore, T. (2014). "Empirical analysis of denial-of-service attacks in the bitcoin ecosystem," in *Financial cryptography and data security (FC 2014), Lect. Notes Comput. Sci.* 8438. 57–71. doi:10.1007/978-3-662-44774-1_5

Vergara-Merino, B., Vargas-Peirano, L., Silva-Dreyer, A. M., Vergara-Merino, L., and Vargas-Peirano, M. (2021). What you need to know about scoping reviews. *Medwave* 21, e8144. doi:10.5867/medwave.2021.02.8144

Veroni, M. (2023). A study on tighter and more efficient isogeny-based cryptographic protocols

Victor, F., and Weintraud, B. (2021). "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges," in Proceedings of the web conference 2021 (WWW '21) *(ACM)*, 23–32. doi:10.1145/3442381.3449824

Vidal-Tomás, D. (2021). An investigation of cryptocurrency data: the market that never sleeps. *Quant. Finance* 21, 2007–2024. doi:10.1080/14697688.2021.1930124

Vidal-Tomás, D. (2022). Which cryptocurrency data sources should scholars use? *Int. Rev. Financial Analysis* 81, 102061. doi:10.1016/j.irfa.2022.102061

Vital, L. C. (2022). *Crypto-crime: the evolution of criminal finances using digital assets.* Utica, NY: Utica University Thesis.

Wachter-Zeh, A., Bartz, H., and Liva, G. (2022). Code-based cryptography. *IEEE Access* 10, 118876–118911. doi:10.1109/ACCESS.2022.3218765

Wang, X., Xu, G., and Yu, Y. (2023). Lattice-based cryptography: a survey. *Chin. Ann. Math. Ser. B* 44, 945–960. doi:10.1007/s11401-023-0053-6

Wang, Y., Sheng, S., and Wang, Y. (2024a). "A systematic literature review on smart contract vulnerability detection by symbolic execution," in *Blockchain and trustworthy systems* (Singapore: Springer), 226–241. doi:10.1007/978-981-97-2257-9_17

Wang, Y., Lu, W., Lin, M. B., Ren, R., and Härdle, W. K. (2024b). Cross-exchange crypto risk: a high-frequency dynamic network perspective. *Int. Rev. Financial Analysis* 94, 103246. doi:10.1016/j.irfa.2024.103246

Wątorek, M., Drożdż, S., Kwapień, J., Minati, L., Oświęcimka, P., and Stanuszek, M. (2020). Multiscale characteristics of the emerging global cryptocurrency market. *Chaos, Solit. and Fractals* 136, 110037. doi:10.1016/j.chaos.2020.110037

Weger, V., Gassner, N., and Rosenthal, J. (2022). A survey on code-based cryptography. *arXiv Prepr. arXiv:2201.07119*. doi:10.48550/arXiv.2201.07119

Weichbroth, P., Wereszko, K., Anacka, H., and Kowal, J. (2023). Security of cryptocurrencies: a view on the state-of-the-art research and current developments. *Sensors* 23, 3155. doi:10.3390/s23063155

World.org (2023). History of cryptocurrency: the idea, journey, and evolution. *World.org Learn Cent. Crypto 101. 8-minute Read.*

Xia, P., Sun, X., Shi, L., Wu, L., and Du, X. (2020). A differentially private greedy decision forest classification algorithm with high utility. *Comput. and Secur.* 96, 101930. doi:10.1016/j.cose.2020.101930

Xiong, X., and Luo, J. (2024). Global trends in cryptocurrency regulation: an overview. 71, 92. doi:10.1007/978-3-031-68974-1_4

Xu, J., Paruch, K., Cousaert, S., and Feng, Y. (2023). Sok: decentralized exchanges (dex) with automated market maker (amm) protocols. *ACM Comput. Surv.* 55, 1–50. doi:10.1145/3570639

Yang, Y., Yuan, H., Yan, L., and Ruan, Y. (2023). Post-quantum identity-based authenticated multiple key agreement protocol. *ETRI J.* 45, 1090–1102. doi:10.4218/etrij.2022-0320

Yi, H. (2022). Secure social internet of things based on post-quantum blockchain. *IEEE Trans. Netw. Sci. Eng.* 9, 950–957. doi:10.1109/TNSE.2021.3095192

Zaoui, M., Yousra, B., Yassine, S., Yassine, M., and Karim, O. (2024). A comprehensive taxonomy of social engineering attacks and defense mechanisms: toward effective mitigation strategies. *IEEE Access* 12, 72224–72241. doi:10.1109/ACCESS.2024.3403197

Zeng, P., Bandyopadhyay, D., Méndez Méndez, J. A., Bitner, N., Kolar, A., and Solomon, M. T. (2024). Practical hybrid pqc-qkd protocols with enhanced security and performance. *arXiv Prepr. arXiv:2411*, 01086. doi:10.48550/arXiv.2411.01086

Zewdie, M., Girma, A., and Sitote, T. (2024). A comprehensive review of insider threats and social engineering attacks detection: challenges, gaps, and a deep learning-based solution. Available online at: https://ssrn.com/abstract=4731400. SSRNPreprint.

Zhang, R., Xue, R., and Liu, L. (2019). Security and privacy on blockchain. *ACM Comput. Surv.* 52, 1–34. doi:10.1145/3316481

Zhang, Z., Xu, C., and Han, Y. (2024). Privacy-preserving cryptocurrency with threshold authentication and regulation. *IEEE Trans. Inf. Forensics Secur.* 19, 6620–6635. doi:10.1109/TIFS.2024.3419694

Zheng, Z. (2022). "Lattice-based cryptography," in *Modern cryptography volume 1: a classical introduction to informational and mathematical principles* (Singapore: Springer), 253–351. doi:10.1007/978-981-16-5047-5_6

Zhou, Z., and Shen, B. (2022). Toward understanding the use of centralized exchanges for decentralized cryptocurrency. Available online at: https://arxiv.org/ftp/arxiv/papers/2204/2204.08664.pdf.

Zhou, F., Chen, Y., Zhu, C., Jiang, L., Liao, X., Zhong, Z., et al. (2023). Visual analysis of money laundering in cryptocurrency exchange. *IEEE Trans. Comput. Soc. Syst.* 11, 731–745. doi:10.1109/tcss.2022.3231687