ELMİ TƏDQİQAT Beynəlxalq Elmi Jurnal. İyul 2026, Cild: 6, Sayı: 7, s. 96–102
SCIENTIFIC RESEARCH International Scientific Journal. July 2026, Volume: 6, Issue: 7, pp. 96–102
DOI: https://doi.org/10.36719/2789-6919/61/96-102

Theoretical Foundations of Cryptocurrency-Related Cybercrime: Architecture, Taxonomy, and Threat Vectors

Leyla Shahbalayeva

Abstract. *The rapid integration of cryptocurrencies into the global financial system has transformed the digital economy while simultaneously creating a fundamentally new criminogenic environment in which digital assets function both as valuable targets and as instruments facilitating cybercrime. This article develops a comprehensive theoretical framework for understanding cryptocurrency-related cybercrime through a systematic review and critical synthesis of contemporary academic literature, cybersecurity reports, and regulatory perspectives. The study examines the core architectural characteristics of blockchain-based systems—including decentralisation, pseudonymity, transaction irreversibility, cryptographic security, and smart contract programmability—and explains how these features generate structural opportunities for criminal exploitation while also providing inherent security advantages. Based on the reviewed literature, a six-category taxonomy of cryptocurrency-related cybercrime is proposed, classifying offences according to the primary criminal target and the functional role of digital assets within illicit activities. Furthermore, the cryptocurrency threat landscape is conceptualised across five interconnected attack surface layers encompassing blockchain infrastructure, wallets and private keys, cryptocurrency exchanges, smart contract ecosystems, and user-level vulnerabilities. The paper also analyses the principal categories of malware employed against cryptocurrency environments, including cryptojacking, ransomware, information stealers, clipboard hijackers, and Trojan-based attacks, together with their operational mechanisms. Finally, the study synthesises existing defensive strategies into a multilayered countermeasure framework that integrates cryptographic safeguards, secure software engineering practices, regulatory governance, organisational cybersecurity measures, and user awareness. The findings demonstrate that mitigating cryptocurrency-related cybercrime requires a convergent and interdisciplinary security approach combining technological innovation, legal regulation, and continuous cybersecurity education without undermining the transformative potential of blockchain technology.*

Keywords: *cryptocurrency, blockchain technology, cryptocurrency-related cybercrime, cybercrime taxonomy, threat vectors, blockchain security, malware, cybersecurity*

Azerbaijan State University of Economics, Master's student, Baku, Azerbaijan
E-mail: leylashahbalayeva@gmail.com
Received: 26 March 2026; Accepted: 27 May 2026; Published online: 30 July 2026

Kriptovalyuta ilə əlaqəli kibercinayətlərin nəzəri əsasları: arxitektura, taksonomiya və təhdid vektorları

Leyla Şahbalayeva

Xülasə. *Kriptovalyutaların qlobal maliyyə sisteminə sürətlə inteqrasiyası rəqəmsal iqtisadiyyatı əhəmiyyətli dərəcədə transformasiya etməklə yanaşı, rəqəmsal aktivlərin həm qiymətli hədəf, həm də kibercinayətkarlığı asanlaşdıran vasitə kimi çıxış etdiyi yeni kriminogen mühitin formalaşmasına səbəb olmuşdur. Bu məqalədə kriptovalyuta ilə əlaqəli kibercinayətkarlığın dərk edilməsi üçün müasir elmi ədəbiyyatın, kibertəhlükəsizlik hesabatlarının və normativ-hüquqi yanaşmaların sistematik ədəbiyyat icmalı və tənqidi təhlil əsasında hərtərəfli nəzəri çərçivə təqdim olunur. Tədqiqat blokçeyn əsaslı sistemlərin əsas memarlıq xüsusiyyətlərini, o cümlədən mərkəzsizləşdirmə (decentralisation), psevdonimlik, tranzaksiyaların geri dönməzliyi, kriptoqrafik təhlükəsizlik və ağıllı müqavilələrin proqramlaşdırıla bilməsini təhlil edir, onların cinayətkar istismar üçün yaratdığı struktur imkanları və sistemlərin təhlükəsizlik üstünlüklərini izah edir. Təhlil edilmiş ədəbiyyata əsaslanaraq, cinayətlərin əsas hədəfi və rəqəmsal aktivlərin qanunsuz fəaliyyətlərdə funksional roluna görə təsnif olunduğu altı kateqoriyalı taksonomiya təklif edilir. Bundan əlavə, kriptovalyuta ekosistemindəki təhdid mənzərəsi blokçeyn infrastrukturu, pul kisələri və məxfi açarlar, kriptovalyuta birjaları, ağıllı müqavilə ekosistemləri və istifadəçi səviyyəsində zəifliklərdən ibarət beş qarşılıqlı əlaqəli hücum səthi üzrə konseptuallaşdırılır. Məqalədə həmçinin kriptoqazma (cryptojacking), fidyə proqramları (ransomware), məlumat oğurlayan proqramlar (information stealers), mübadilə buferi oğurlayıcıları (clipboard hijackers) və Trojan tipli hücumların fəaliyyət mexanizmləri sistemli şəkildə təhlil olunur. Nəhayət, mövcud müdafiə strategiyaları kriptoqrafik mühafizə tədbirləri, təhlükəsiz proqram təminatı mühəndisliyi, normativ tənzimləmə, təşkilati kibertəhlükəsizlik tədbirləri və istifadəçi maarifləndirilməsini əhatə edən çoxsəviyyəli əks-tədbirlər çərçivəsində ümumiləşdirilir. Nəticələr göstərir ki, kriptovalyuta ilə əlaqəli kibercinayətkarlığın effektiv azaldılması texnoloji innovasiyaları, hüquqi tənzimləməni və davamlı kibertəhlükəsizlik təhsilini birləşdirən inteqrativ, fənlərarası təhlükəsizlik yanaşmasını tələb edir.*

Açar sözlər: *kriptovalyuta, blokçeyn texnologiyası, kriptovalyuta ilə əlaqəli kibercinayətkarlıq, kibercinayətkarlığın taksonomiyası, təhdid vektorları, blokçeyn təhlükəsizliyi, zərərli proqram təminatı, kibertəhlükəsizlik*

Azərbaycan Dövlət İqtisad Universiteti, magistrant, Bakı, Azərbaycan
E-poçt: leylashahbalayeva@gmail.com
Daxil oldu: 26 Mart 2026; Qəbul edildi: 27 May 2026; Onlayn dərc edildi: 30 İyul 2026

Introduction

Cryptocurrencies have undergone a remarkable transformation over the past decade, evolving from an experimental concept into a structurally significant component of the global financial architecture. The emergence of Bitcoin in 2008, followed by the proliferation of thousands of alternative digital assets and the development of programmable blockchain platforms such as Ethereum, has created an entirely new category of financial instruments with properties that distinguish it categorically from conventional fiat currency systems. Decentralized, cryptographic security, transaction irreversibility, pseudonymity, and smart contract programmability together define a technological paradigm that simultaneously generates substantial economic utility and enables novel forms of criminal exploitation (Nakamoto, 2008; Antonopoulos, 2017).

The convergence of these properties with rapid globalisation of digital asset adoption has produced a structural criminogenic environment in which the same features that attract legitimate users also facilitate criminal actors across a broad spectrum: exchange hacks, smart contract exploits, social engineering, ransomware, money laundering, and illicit mining. Despite growing literature addressing specific attack types, the field lacks a unified theoretical framework connecting blockchain architecture to the crime typologies it enables and the multi-layer threat vectors through which offences are executed. This article addresses that gap through systematic synthesis of academic scholarship, international regulatory reports, and documented incident analyses (FATF, 2021; Europol, 2022).

Methods

This article employs a qualitative systematic literature review drawing on foundational blockchain scholarship (Nakamoto, 2008; Böhme et al., 2015; Narayanan et al., 2016; Antonopoulos, 2017); international regulatory reports from FATF, Europol, UNODC, Chainalysis, ENISA, and Kaspersky; and peer-reviewed research on DeFi security (Gudgeon et al., 2020), blockchain governance (Schär, 2021), and the blockchain-cybercrime nexus (Kshetri, 2019).

The Synthesis Proceeds Through Three Analytical Stages

The first establishes the technological architecture of cryptocurrencies and identifies the specific properties that create structural conditions for criminal exploitation. The second develops a crime taxonomy by integrating and reconciling the classification approaches applied by FATF (2021), Europol (2023), UNODC (2022), and Kshetri (2019), organising crime categories according to the dual criteria of the nature of the criminal target and the functional role of cryptocurrency in the offence. The third maps the threat landscape across the five-layer attack surface model and analyses the malware ecosystem and countermeasure framework at each layer.

Results

Technological Architecture and Criminogenic Properties of Blockchain Systems

A cryptocurrency is a decentralized, cryptographically secured distributed network for executing digital asset transactions without central intermediaries (Böhme et al., 2015). Four structural properties constitute the direct source of their criminogenic potential. Decentralisation eliminates single-point institutional control. Pseudonymity frustrates post-facto attribution of criminal transactions. Transaction irreversibility removes the chargeback mechanisms that remediate payment fraud in banking — confirmed transactions cannot be reversed by any party. Programmability through smart contracts creates immutable deployed code whose vulnerabilities cannot be corrected through standard software update processes (Narayanan et al., 2016; Schär, 2021). These properties are not correctable defects but permanent features: countermeasures must manage permanent residual risk rather than eliminate vulnerabilities inherent to the system's design (Antonopoulos, 2017).

Six-Category Taxonomy of Cryptocurrency-Related Cybercrimes

Synthesising the classification frameworks of FATF (2021), Europol (2023), UNODC (2022), and Kshetri (2019), and grounding the taxonomy in documented international incidents, this article proposes a six-category classification organised by the dual criteria of criminal target and the functional role of cryptocurrency in the offence. This dual-axis structure is more analytically stable across evolving criminal methodologies than purely technique-based classifications, because it locates crime categories at the level of purpose and target rather than at the level of implementation, which changes more rapidly.

Table 1

Six-category taxonomy of cryptocurrency-related cybercrimes

Category	Primary target / role of cryptocurrency	Representative incidents	Key architectural property
I. Infrastructure attacks	Exchange systems, smart contracts, consensus protocols, bridges	Mt. Gox (2014); DAO hack (2016); Ronin Bridge (2022, $615M)	Immutability; composability
II. Criminal instrument use	Cryptocurrency as laundering / payment medium	Tornado Cash (2022); Bitzlato (2023); Silk Road; Hydra Market	Pseudonymity; borderlessness
III. User-targeted fraud	Retail investors; DeFi participants	OneCoin; PlusToken; Squid Game Token (2021)	Irreversibility; info. asymmetry
IV. Ransomware / extortion	Critical infrastructure; enterprises	WannaCry (2017); Colonial Pipeline (2021)	Irreversibility; pseudonymity
V. Illicit mining	Victim computational resources	Smominru campaign (2017-2021)	Pseudonymity (Monero)
VI. State-sponsored / organised actors	Strategic infrastructure; sanctions evasion	Lazarus Group (cumulative >$3B)	All four properties

Source. Developed by the author based on FATF (2021); Europol (2023); UNODC (2022); Kshetri (2019).

Category I — Direct attacks on cryptocurrency infrastructure — encompasses centralised exchange hacks, smart contract exploits, and consensus-layer attacks. Exchange hacks, from the Mt. Gox collapse (2014, ~850,000 BTC) and Coincheck breach (2018, >USD 530 million) to the FTX insolvency (2022), exploit hot wallet custody weaknesses and operational security failures. Smart contract exploits target logical vulnerabilities — reentrancy, access control failures, oracle manipulation, flash loan abuse — in immutable code; the DAO hack (2016, USD 60 million) and Ronin Bridge compromise (2022, USD 615 million) illustrate the systemic risk created when DeFi composability allows vulnerabilities in one protocol to cascade through interconnected systems (Gudgeon et al., 2020; Europol, 2023). Consensus attacks — 51% attacks on proof-of-work and proof-of-stake networks — remain viable against smaller, lower-capitalisation chains as demonstrated by attacks on Ethereum Classic (2019) and Bitcoin Gold (2018) (Narayanan et al., 2016).

Category II exploits pseudonymity and borderlessness for money laundering and sanctions evasion — the Tornado Cash sanctioning (2022) and Bitzlato case (2023) illustrate the scale of mixing-facilitated laundering (FATF, 2021). Category III exploits irreversibility through ICO fraud, Ponzi schemes, rug pulls, and SIM-swapping. Category IV leverages irreversibility to eliminate payment reversal risk, with Colonial Pipeline (2021) demonstrating critical infrastructure consequences. Category V monetises computational resources using Monero for attribution resistance (Kaspersky, 2022). Category VI encompasses state-sponsored operations with strategic objectives, exemplified by the Lazarus Group (Europol, 2023).

Multi-Layer Threat Vector Analysis

Protocol-level threats originate in consensus mechanisms and cryptographic foundations. The principal vector is consensus manipulation — 51% attacks and staking concentration — enabling double-spending, censorship, and network reorganisation. Secondary risks include cryptographic flaws and consensus failures during protocol upgrades. Application-layer vectors target smart contracts and dApps. Dominant vulnerability classes — reentrancy, integer overflow, access control failures, oracle manipulation, and flash loan arbitrage — exploit the gap between developer intent and code specification. DeFi composability compounds these risks, and immutability of deployed code means remediation requires hard forks rather than standard patching (Gudgeon et al., 2020).

Infrastructure-level threats target exchanges, custodial wallets, and cross-chain bridges — centralised aggregation points that recreate concentrated targets despite decentralised protocols. Key management and wallet-layer threats operate where blockchain security meets user practice: private key compromise through clipboard hijackers, information stealers, or trojanised wallets is operationally terminal without recovery mechanisms (Antonopoulos, 2017). Human-behavioural attack vectors exploit the most accessible element of the attack surface — phishing, impersonation, and investment fraud leverage irreversibility to convert brief deception into permanent loss. Economic vectors — pump-and-dump schemes, wash trading, governance manipulation — operate through incentive structures rather than individual deception (Schär, 2021; Kshetri, 2019).

Cryptocurrency-Targeting Malware and Countermeasure Framework

Five functional malware categories target cryptocurrency assets: clipboard hijackers substitute addresses at transaction initiation; information stealers extract credentials and seed phrases; trojanised wallet applications manipulate transactions or exfiltrate cryptographic material; remote access trojans provide persistent system control; and cryptojacking malware covertly mines cryptocurrency — the Smominru campaign (2017-2021) infected over 500,000 systems (Kaspersky, 2022; ENISA, 2021). Distribution relies on phishing infrastructure, compromised software updates, supply-chain attacks on open-source libraries, and social media campaigns combining technical exploits with social engineering (Europol, 2022; Chainalysis, 2023).

The countermeasure framework operates across four interdependent levels: technical (hardware wallet adoption for offline key isolation and hardware-enforced transaction confirmation); organisational (update discipline, extension governance, access control policies); behavioural (seed phrase management, address verification, phishing recognition); and institutional (mandatory operator security standards and international law enforcement cooperation). Their interdependence is critical: failure in any single dimension — most consequentially improper seed phrase management — negates protections implemented across all others (ENISA, 2021; Kaspersky, 2022).

Discussion

The Architectural Foundation of Criminal Exploitation

The central finding of this theoretical analysis is that cryptocurrency-related cybercrime is not primarily a product of implementation failures correctable through better engineering, but a structural consequence of the architectural properties that make cryptocurrencies economically valuable. Pseudonymity, irreversibility, borderlessness, and programmability cannot be removed or substantially weakened without undermining the value proposition of decentralised digital assets. The threat landscape documented above is not a transitional phenomenon that will diminish as the technology matures, but a permanent feature of the ecosystem. The implication is a categorical shift from a correctability model of security — in which the goal is to eliminate vulnerabilities until a secure state is reached — to a resilience model, in which the goal is to limit the consequence of failures that architectural necessity makes impossible to fully prevent.

The human-behavioural layer is the most exploited and most neglected dimension of cryptocurrency security. Irreversibility converts social engineering into permanent financial loss with no conventional analogue, arguing for reorienting security investment toward practical user education. Hardware wallet protections are negated by improper seed phrase management — the technical layer is ineffective without the behavioural layer (Antonopoulos, 2017; Kshetri, 2019).

Conclusion

First, the criminogenic properties of cryptocurrencies are architectural necessities, not correctable defects. Pseudonymity, irreversibility, borderlessness, and smart contract immutability cannot be eliminated without undermining the technology value. Security strategy must therefore build on a resilience model — managing permanent residual risk through layered defences.

Second, the six-category taxonomy proposed here — organised by criminal target and the functional role of cryptocurrency in the offence — provides an analytically stable framework that accommodates the continued evolution of criminal methodologies without requiring continuous structural revision. The explicit mapping of each category to the specific architectural property it exploits makes clear that the cryptocurrency crime landscape requires categorically differentiated responses across technical, regulatory, educational, and law enforcement dimensions.

Third, the multi-layer attack surface analysis demonstrates that the human-behavioural layer is both the most exploited and the most neglected dimension of cryptocurrency security. The irreversibility property converts successful social engineering into permanent financial loss at a rate that has no conventional financial analogue, making the development of practically effective user education programmes the highest-priority intervention in the current threat environment. Future research should build on this theoretical foundation through empirical investigation of user competence and behaviour, experimental evaluation of specific protective technologies, and comparative regulatory analysis across jurisdictions at different stages of cryptocurrency governance development.

References

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open blockchain* (2nd ed.). O'Reilly Media.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Chainalysis. (2023). *The 2023 Crypto Crime Report*. https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/

European Union Agency for Cybersecurity. (2021). *Threat landscape for cryptocurrencies*. https://www.enisa.europa.eu/publications/threat-landscape-for-cryptocurrencies

Europol. (2022). *Cryptocurrencies: Tracing the evolution of criminal finances*. Publications Office of the European Union. https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

Financial Action Task Force. (2021). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Updated-guidance-rba-virtual-assets-vasps.html

Gudgeon, L., Werner, S., Perez, D., & Knottenbelt, W. J. (2020). DeFi protocols for loanable funds: Interest rates, liquidity and market efficiency. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies* (pp. 92–112). Association for Computing Machinery. https://doi.org/10.1145/3419614.3423254

Kaspersky. (2022). *Kaspersky Security Bulletin 2022: Statistics*. https://securelist.com/ksb-2022-statistics/108129/

Kshetri, N. (2019). Blockchain and cybersecurity. *Journal of Cyber Policy, 4*(1), 19–38. https://doi.org/10.1080/23738871.2019.1571736

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E. W., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review, 103*(2), 153–174. https://doi.org/10.20955/r.103.153-74

United Nations Office on Drugs and Crime. (2022). *Global Programme on Cybercrime*. https://www.unodc.org/unodc/en/cybercrime/global-programme-on-cybercrime.html