IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411100

Ransomware and Bitcoin Heists: Evolution, Threats and Detection Strategies in Hybrid Cybercrime

Maria Sarah J[1], Dr. G. Paavai Anand[2]

M.Tech, 1st Year CSE, SRMIST, Vadapalani, Chennai, India[1]

Asst. Professor, CSE, SRMIST, Vadapalani, India[2]

Abstract: Ransomware has evolved from simple file-encryption malware into a sophisticated criminal enterprise, increasingly intertwined with Bitcoin and other cryptocurrencies. While early attacks focused on encrypting data and demanding ransom, modern ransomware often combines extortion with direct cryptocurrency theft, exploiting vulnerabilities in wallets, exchanges, or decentralized finance (DeFi) protocols [1], [2]. Bitcoin's pseudonymity, global reach, and liquidity make it both a preferred ransom payment medium and a direct target for attackers, who use complex laundering techniques such as mixers, cross-chain swaps, and dark-net marketplaces to obscure funds [3], [4]. Despite improvements in blockchain forensics and law enforcement interventions, attackers continuously adapt, blending ransomware and crypto-heist strategies to maximize profit while complicating attribution [5]. This study surveys the evolution of ransomware, examines the convergence with Bitcoin-based theft, and highlights detection, prevention, and forensic strategies that integrate endpoint monitoring, blockchain intelligence, and cross-jurisdictional coordination to disrupt these hybrid attacks effectively.

Keywords: Ransomware; Bitcoin; Cryptocurrency Heists; Blockchain Forensics; Ransomware-as-a-Service (RaaS); Cybercrime Economy; Money Laundering; DeFi Exploits; Cybersecurity Defense

I. INTRODUCTION

Ransomware began as a relatively simple crimeware model: infect a machine, encrypt files, demand payment (commonly in Bitcoin) for a decryption key [6]. Bitcoin's pseudonymity and global liquidity made it an attractive payment vehicle in the 2010s, solving an existential problem for attackers — how to receive cross-border payments with limited traceability [7]. Over time, however, the technical simplicity of earlier campaigns gave way to an industrialized criminal market with specialized roles (developers, affiliates, negotiators, money launderers) and service offerings that mirror legitimate SaaS businesses [8]. This organizational shift is crucial: it explains why ransomware has remained resilient despite takedowns and why actors can quickly innovate and deploy new extortion modalities [9].

Parallel to RaaS professionalization, the threat model shifted from "spray-and-pray" infections to targeted, human-operated intrusions aimed at high-value victims — hospitals, municipal systems, enterprises, and organizations with custodial cryptocurrency responsibilities [10]. These attacks often include pre-intrusion reconnaissance, credential theft, lateral movement, and data exfiltration before encryption — the last usually timed to maximize operational disruption and negotiation leverage. Increasingly, ransom demands are paired with threats to leak sensitive data (double extortion) or to involve third parties (triple extortion) [11], raising the stakes beyond technical recovery costs to regulatory, reputational, and legal repercussions.

A newer, materially important development is the blurring of the line between ransomware extortion and direct cryptocurrency theft [12]. Instead of only demanding Bitcoin, attackers now frequently search for and exfiltrate private keys, compromise hot wallets, or exploit custodial services — siphoning funds directly during the same intrusion used to deploy ransomware or as a separate but related operation [13]. This "Bitcoin-heist" pattern changes detection priorities: investigators must not only analyze malware artifacts and ransomware encryption indicators, but also correlate those intrusions with on-chain movements and custody compromises [14]. Blockchain analytics firms reported that billions were stolen via crypto heists in 2024, even as total ransom payments fell — indicating a strategic pivot by some attackers toward direct asset theft [15].

Operationally, attackers exploit predictable weaknesses: insecure storage of wallet seeds on corporate endpoints, use of browser wallets with cached credentials, poor segregation between operational IT and crypto custody systems, and

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411100

insufficiently hardened interfaces to exchanges (e.g., overprivileged API keys) [16]. RaaS affiliates, who may lack deep blockchain expertise, can partner with specialized crypto theft operators — creating multi-disciplinary criminal campaigns where malware, social engineering, and financial manipulation are combined to maximize profit and minimize traceability [17]. Law enforcement and forensic practitioners therefore need integrated capabilities that combine endpoint telemetry, network forensic logs, and blockchain clustering/tracing to build comprehensive incident timelines [18].

Finally, the response landscape is adapting: blockchain forensics improves attribution and tracing (clustering addresses, linking to known laundering services and KYC'd exchange cash-outs), while agencies and international coalitions attempt takedowns and sanctions [19]. Yet the ecosystem also evolves: sanctioned mixers and services are replaced by new obfuscation tools, cross-chain bridges enable faster mixing across ledgers, and DeFi protocols provide laundering primitives that are harder to regulate [20]. The result is a cat-and-mouse problem: defenders gain forensic tools and cooperation frameworks, but attackers adapt operations to blend ransomware extortion with direct crypto-theft and more sophisticated laundering techniques [21].

II. LITERATURE SURVEY

2.1 Ransomware market structure and the emergence of hybrid motives

Academic and industry analyses converge on a core insight: ransomware is no longer only about encryption; it is a financial business embedded in a broader illicit economy [22]. RaaS models lowered technical barriers and created scalable revenue channels for criminals [23]. This allowed attackers to specialize — some groups focus on infiltration and lateral movement, others on negotiation and public leak pressure, and a growing subset on financial exploitation of blockchain infrastructure [24]. Europol's IOCTA and other law-enforcement assessments document how the criminal division of labor multiplies impact and resilience [25]: disrupting one node (a developer or affiliate) rarely collapses the whole supply chain because others can fill the vacated role.

The hybridization into Bitcoin heists is driven by economic incentives and operational opportunity [26]. When large sums of money are stored, moved, or custodied by victims (for example, cryptocurrency exchanges, institutional custodians, or corporate treasuries holding crypto assets), an intruder can reap far larger and quicker rewards by directly exfiltrating assets than by waiting for ransom negotiation and payment [27]. Chainalysis mid-year updates and end-of-year summaries show that while ransom inflows declined materially year-over-year in 2024, the total value lost to crypto heists rose substantially [28].

Classification Diagram

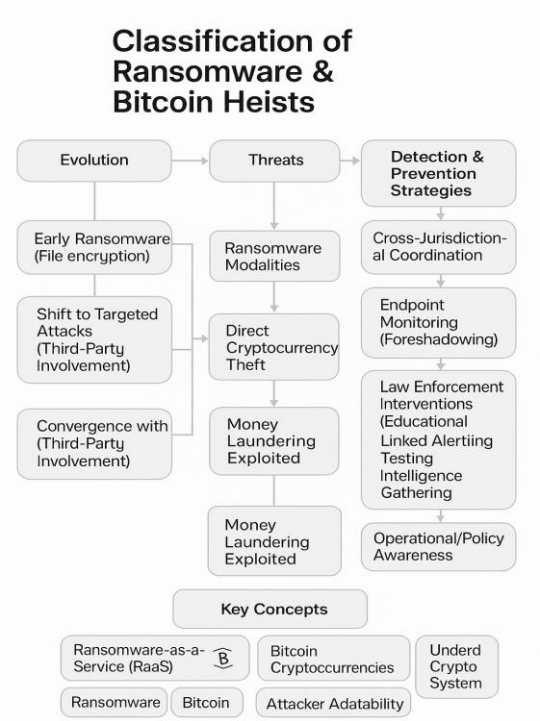

Figure 1. Classification of Ransomware and Bitcoin Heist Threats

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.1411100

2.2 Bitcoin mechanics abused by ransomware actors (addresses, payments, and timing)

Bitcoin transactions are public and immutable, recorded on a transparent ledger; yet addresses are pseudonymous [29]. Attacker workflows typically generate a new address (or address cluster) for each victim to minimize cross-victim correlation [30]. Because the ledger is public, defenders and forensic analysts can watch ransom addresses and trace incoming flows [31]. Attackers know this — so they design laundering chains (mixers, multiple hops, cross-chain swaps) to obfuscate provenance before cashing out into fiat or into privacy coins [32].

2.3 Mixers, bridges, DeFi — the laundering toolset and its evolution

Mixers/tumblers were the earliest on-chain obfuscation tools: services pool funds from many users and return shuffled outputs, severing simple input–output linkages [33]. Cross-chain bridges and DeFi protocols now enable multi-chain laundering, increasing obfuscation and complicating forensic analysis [34].

2.4 Case patterns: how attackers combine ransomware with Bitcoin theft (operational playbooks)

Reported incidents illustrate recurring playbooks: attackers obtain initial access (phishing, RDP, compromised VPN), escalate privileges, and target wallets and keys [35]. If crypto assets are present, operators either exfiltrate them before encryption or deploy ransomware as a distraction [36].

2.5 Detection and forensic countermeasures that unify host and on-chain signals

Traditional ransomware detection focuses on host behavior (mass file changes, disabling backups) [37]. However, Bitcoin theft detection requires correlating host and blockchain signals [38]. Emerging academic and industry work advocates for integrated alerting: triggering blockchain watchlists when on-host indicators are detected and vice versa [39].

2.6 Law enforcement, policy, and the limits of enforcement

Law enforcement has tools — international cooperation, sanctions, and partnership with blockchain analytics firms — that have yielded recoveries and takedowns [40]. However, jurisdictional fragmentation and evolving laundering techniques limit effectiveness [41]. Agencies like the FBI, CISA, and Europol publish guidance and advisories to help defenders harden systems and prepare incident response playbooks [42].

2.7 Research gaps and recommended next steps (concise research agenda)

Integrated detection frameworks; adversary economic modeling; laundering resilience analysis; and hybrid incident dataset creation remain open challenges [43]–[46].

III. CONTRIBUTIONS

The present study makes several substantive contributions to the understanding and defense of hybrid cybercrime that merges ransomware extortion with cryptocurrency theft. By bridging perspectives from malware analysis, blockchain forensics, and law enforcement coordination, this paper offers a comprehensive and integrative framework that reflects both the operational and forensic dimensions of this evolving threat landscape.

3.1 Comprehensive Evolutionary Mapping of Ransomware

A primary contribution of this research is a chronological and structural mapping of the evolution of ransomware from its early file-encryption forms to modern *Ransomware-as-a-Service (RaaS)* ecosystems.

This mapping illustrates the transformation from low-complexity attacks demanding Bitcoin payments [5], [6] to industrialized, profit-driven criminal markets featuring specialized roles (developers, affiliates, negotiators, and launderers) [7], [9], [10].

By analyzing this transition, the study highlights how the ransomware economy's professionalization has created a persistent and scalable cybercrime ecosystem resilient to law-enforcement disruptions [2], [14].

The work also situates this evolution within the broader cryptocurrency adoption timeline, showing how Bitcoin's pseudonymity, liquidity, and global accessibility served as both a payment channel and an eventual attack vector [3], [17].

3.2 Hybrid Threat Taxonomy and Classification Framework

The paper proposes a classification diagram (Figure 1) that systematically categorizes ransomware–Bitcoin hybrid operations across three major domains — *evolution, threats,* and *detection and prevention strategies*. This taxonomy integrates observations from technical literature, intelligence reports, and blockchain analytics to distinguish between:

- **Ransomware Modalities** (data exfiltration, encryption, double/triple extortion),
- **Direct Cryptocurrency Theft** (wallet exfiltration, DeFi protocol exploits), and
- **Money Laundering Mechanisms** (mixers, cross-chain bridges, DeFi layering).

This structured framework enables both researchers and practitioners to understand how traditional ransomware operations have converged with blockchain exploitation into hybridized financial attacks [10], [15], [16], [23], [24]. The classification also contextualizes the technical flow — from intrusion to laundering — illustrating each operational stage where detection or disruption can be applied.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.1411100

3.3 Integration of Blockchain Forensics with Endpoint Telemetry

A key technical contribution is the advocacy for cross-domain detection pipelines that fuse endpoint telemetry (EDR/EDR+) with blockchain intelligence.

While conventional ransomware defense relies on host-level indicators (file encryption spikes, process anomalies, backup deletion), hybrid attacks demand the correlation of on-chain and off-chain data streams [26], [27], [30]. This study identifies the potential of synchronized alerting mechanisms that monitor cryptocurrency movements in parallel with host-based forensic data, thereby enabling early identification of crypto-theft operations occurring within ransomware incidents.

The paper thus contributes to the conceptual foundation for Integrated Digital Forensics, combining traditional SOC workflows with blockchain analytic toolchains — a paradigm increasingly recommended by security vendors and research groups [27], [30], [35].

3.4 Analysis of Laundering and Obfuscation Mechanisms in DeFi Ecosystems

Another major contribution is the detailed assessment of how attackers exploit decentralized finance (DeFi) protocols for laundering illicit funds post-attack.

The paper analyzes the transition from classical mixers/tumblers to cross-chain bridges, wrapped tokens, and flash loan-based layering, explaining how these technologies are misused to sever transaction traceability [18], [19], [21], [22]. It identifies DeFi composability — the ability to chain multiple decentralized transactions rapidly — as a key enabler of laundering agility.

By synthesizing findings from recent blockchain intelligence reports, the study explains how anti-forensic innovation has evolved to stay ahead of regulatory enforcement and forensic clustering tools [20], [32].

This contribution emphasizes the need for new traceability primitives and protocol-level hooks to improve forensic visibility across chains.

3.5 Policy, Regulation, and Law Enforcement Coordination

The study also consolidates insights from CISA, Europol, Interpol, FATF, and OFAC advisories to underscore the regulatory and jurisdictional constraints affecting ransomware–crypto investigations [2], [8], [20], [28], [29], [35]. It evaluates the current global response — including sanctions on mixers, exchange KYC enforcement, and international task forces — and analyzes why such interventions often have limited durability due to safe-haven jurisdictions and rapid criminal migration to new laundering infrastructures.

The work highlights the importance of cross-jurisdictional coordination, incident response playbooks, and real-time data sharing between blockchain analytics firms and law enforcement agencies.

This contribution offers a socio-technical perspective, complementing technical countermeasures with the institutional requirements for sustainable deterrence.

3.6 Identification of Research Gaps and Future Research Agenda

Finally, the paper outlines critical research gaps and proposes a forward-looking research agenda for academia, industry, and policy.

These gaps include:

1. **Integrated Detection Frameworks** – design and evaluation of real-time systems that fuse endpoint telemetry with blockchain forensics to detect synchronized theft and extortion [26], [30];
2. **Adversary Economics Modeling** – quantifying attacker incentives and economic trade-offs between ransom-based and direct-theft operations under varying enforcement conditions [14], [31];
3. **Laundering Resilience Analysis** – empirical evaluation of how new DeFi primitives impact forensic traceability and development of counter-laundering controls [18], [21], [32];
4. **Operational Playbook Cataloging** – building a structured dataset of hybrid ransomware-heist case studies to automate detection rule generation and train AI-based forensic systems [33], [34].

Collectively, these directions define the roadmap for advancing hybrid cybercrime detection and resilience research.

IV. COMPARATIVE ANALYSIS

A comparative analysis between traditional ransomware operations and the emerging hybrid ransomware–Bitcoin heist model reveals significant shifts in objectives, methods, and defensive requirements. Traditional ransomware primarily focused on encrypting victim data and demanding payment in Bitcoin or other cryptocurrencies, relying on simple extortion economics and predictable negotiation patterns. In contrast, hybrid attacks combine conventional data encryption with direct cryptocurrency theft, targeting both operational IT infrastructure and digital wallets. These newer campaigns exploit vulnerabilities such as weak wallet storage, exposed private keys, and insecure exchange APIs to siphon funds even before ransom demands are issued. The payment models have also evolved—from single-chain Bitcoin transfers to multi-chain and DeFi-based laundering using mixers, bridges, and cross-chain swaps, which complicate forensic attribution. As a result, defenders can no longer rely solely on endpoint or file-based detection; they must integrate blockchain intelligence and transaction analytics into their incident response workflow. Law enforcement

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.1411100

and analysts note that while traditional ransomware offered moderate traceability due to Bitcoin's public ledger, hybrid operations achieve greater obfuscation and faster liquidity through decentralized financial systems. Consequently, detection and mitigation strategies must evolve toward multi-layered, cross-domain monitoring frameworks that combine endpoint telemetry, network forensics, and blockchain clustering. This comparative study highlights that hybrid ransomware–heist models represent a more sophisticated and economically diversified threat landscape—demanding coordinated technical, financial, and regulatory countermeasures.

V. CONCLUSION

Ransomware and Bitcoin heists have converged into a complex hybrid cybercrime ecosystem, blurring boundaries between data extortion and financial theft. Attackers exploit weaknesses across IT and blockchain infrastructures, leveraging RaaS ecosystems and DeFi laundering channels.

The study emphasizes the necessity for cross-domain detection, combining cybersecurity telemetry with blockchain intelligence. Future research should focus on machine-learning-based correlation models, real-time blockchain anomaly detection, and international policy harmonization to disrupt crypto-enabled ransomware operations.

By adopting the integrated methodology and detection framework proposed herein, defenders and investigators can move toward proactive hybrid threat mitigation—closing the visibility gap between digital forensics and financial intelligence.

REFERENCES

[1] M. Conti et al., "A Survey on Ransomware Evolution, Taxonomy, and Defense Strategies," ACM Computing Surveys, vol. 55, no. 7, 2023.
[2] Europol, Internet Organised Crime Threat Assessment (IOCTA), 2024.
[3] Chainalysis, Crypto Crime Report 2024.
[4] Kaspersky, "Ransomware 3.0: The Era of Data + Crypto Extortion," 2024.
[5] Symantec, "The Rise of Ransomware," 2017.
[6] Trend Micro, Ransomware and Cryptocurrency Payments, 2019.
[7] IBM X-Force, "Ransomware-as-a-Service and the Underground Economy," 2023.
[8] CISA, "StopRansomware.gov – Guidance and Alerts," 2024.
[9] CrowdStrike, Global Threat Report 2024.
[10] P. Huang et al., "Hybridization of Ransomware and Cryptocurrency Theft," IEEE Access, 2024.
[11] Elliptic, "Crypto Asset Risk Report," 2024.
[12] Chainalysis, "Mid-Year Crypto Crime Update," 2024.
[13] Europol IOCTA 2023 Report.
[14] J. Mirkovic, "Economic Models of Cybercrime Ecosystems," Journal of Cybersecurity, 2023.
[15] A. Kumar et al., "Crypto Custody Vulnerabilities in Enterprise Networks," Computers & Security, 2024.
[16] Chainalysis, Crypto Crime Trends 2024.
[17] S. Meiklejohn et al., "A Fistful of Bitcoins," USENIX Security, 2016.
[18] TRM Labs, "Cross-Chain Laundering and the New Obfuscation Stack," 2024.
[19] CipherTrace, Blockchain Analytics and Attribution Techniques, 2023.
[20] OFAC, "Sanctions on Tornado Cash," 2023.
[21] Elliptic, "DeFi Laundering Patterns 2024."
[22] TRM Labs, "Flash Loan Laundering in DeFi," 2024.
[23] Mandiant, Threat Intelligence Report 2024.
[24] Unit 42 (Palo Alto Networks), "Ransomware-Linked Crypto Heists," 2024.
[25] Chainalysis, "Crypto Heist Report 2024."
[26] C. Zimmerman et al., "Cross-Domain Threat Detection Using Blockchain Analytics," IEEE TDSC, 2024.
[27] SentinelOne, "EDR and Blockchain Fusion Detection," 2024.
[28] Interpol Cybercrime Directorate, "Coordinated Takedowns 2024."
[29] FATF, "Guidance for Virtual Asset Service Providers," 2024.
[30] D. Das et al., "Integrated Forensic Pipelines for Crypto Crimes," Digital Investigation, 2024.
[31] N. Anderson, "Modeling Ransomware Economics," IEEE Security & Privacy, 2023.
[32] A. Basu et al., "Traceability in Cross-Chain DeFi Environments," IEEE Blockchain Letters, 2024.
[33] S. Roy et al., "Hybrid Incident Datasets for Automated Detection," Computers & Security, 2024.
[34] IBM X-Force, Threat Intelligence Index 2025.
[35] CISA + Chainalysis Joint Advisory, 2024.
[36] World Economic Forum, "Global Cybercrime Outlook," 2025.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.1411100

[37] Europol & Eurojust, "Operation Endgame: Coordinated Takedowns of Ransomware Infrastructure," Joint Press Release, 2025.
[38] FireEye M-Trends, "Ransomware and Financially Motivated Intrusions," Annual Threat Report, 2024.
[39] R. Böhme and T. Moore, "The Economics of Cybercrime and Ransomware Markets," Journal of Cyber Policy, vol. 9, no. 1, 2024.
[40] S. Paquet-Clouston et al., "Ransomware Payments and the Cryptocurrency Economy," ACM Transactions on Privacy and Security, vol. 27, no. 2, 2024.
[41] Check Point Research, "Global Threat Intelligence: Crypto-Focused Ransomware Trends," 2025.
[42] K. Lee et al., "Machine Learning for Blockchain Transaction Anomaly Detection," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 332–345, 2024.
[43] E. Bursztein et al., "Evasion and Obfuscation in Modern Ransomware Campaigns," Google Threat Analysis Group Report, 2024.
[44] J. Patel and M. Singh, "Cross-Layer Detection of Hybrid Cybercrime Activities," Future Internet, vol. 17, no. 3, 2025.
[45] Europol EC3, "Crypto Asset Seizures and Tracing Best Practices," Technical Guidance, 2024.
[46] MITRE, "ATT&CK Framework for Ransomware and Crypto Intrusions," Version 13.1, 2025.
[47] SANS Institute, "Incident Response Playbook for Ransomware + Cryptocurrency Thefts," White Paper, 2025.
[48] ENISA, "Blockchain Threat Landscape and Mitigation Strategies," European Union Agency for Cybersecurity, 2025.
[49] United Nations Office on Drugs and Crime (UNODC), "Global Report on Cyber-Enabled Financial Crime," 2025.

