International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cybersecurity in Blockchain and Potential Risk of Undressed Fraud in Crypto

Ayotunde O Oyatomi

B.S in Computer Science and associate degree in Elect/Elect

Abstract

The cybersecurity area encompassing blockchain technology and cryptocurrency reflects concerns regarding defense mechanisms and transparent regulatory frameworks. Centralized crypto services, such as exchanges and bridges, remain vulnerable to fraud, posing a threat to the security of the entire blockchain ecosystem. This work explores the crypto frauds that have remained undetected for an extended period, provided the technology is transparent. The research is an in-depth comparative case study, relying on secondary information about five well-known blockchain crypto fraud cases (Mt. Gox, Ronin Bridge, FTX, and the Ponzi schemes CBEX and PCEX). The way the research results are framed highlights the vulnerability of the system. The results reveal that security failures are not frequent at the core level of protocols, but rather in the centralized components and even fraudulent structures surrounding them, including exchanges, bridges, and Ponzi schemes. These strata foster individual cases of information asymmetry and failure, which enable cyberattacks, national malpractices, and planned frauds. The research has found that the safety of the blockchain ecosystem requires a fundamental shift to verifiable operations and robust regulatory oversight of intermediaries.

Keywords: Blockchain Security, Centralized Exchanges, Fraud, Cryptocurrency bridges, regulatory Supervision

INTRODUCTION

The emergence of blockchain technology ensures that trust is designed and managed in the digital system [1]. Since its inception as the technology upon which Bitcoin was built, the central innovation of blockchain is that any decentralized, immutable, and transparent ledger can be created without the involvement of a central authority [2]. Cryptographic hashing, distributed consensus, and cryptographic proofs theoretically result in a system where transactions are verifiable and irreversible, and where trusted intermediaries are unnecessary**.** The deeper meaning of this architecture is that it may produce a system that is so trustless that players can engage with each other safely based on mathematical certitude and not institutional credibility. The growing cryptocurrency economy based on this technology, however, has an intense and disturbing contradiction [3]. Security breaches, complex cyberattacks, and undetected fraudulent schemes often exploit vulnerabilities in the blockchain protocol layer. The term 'undetected fraud' refers to a specific category of malfeasance that is not an overt assault, but rather a subtle, systemic manipulation and misappropriation that remains uncovered over extended periods [4]. This is predatory, as it undermines the blockchain's promises of transparency and verifiable security. Although the blockchain register itself is immutable and transparent, the numerous layers of applications, smart contracts, and centralized services built on top of it create veils of darkness where fraud can thrive

undetected [5]. This study aims to critically explore the dissonance between theoretical blockchain security and actual fraud in the cryptocurrency space. Using a comparative case study approach and relying on secondary data, this study will examine the presentation of cybersecurity risks and undetected fraud at various organizational levels. The key research questions are: "How do the hypothetical blockchain security models fail in practice, and become vulnerable to fraud that can be committed without being detected? What are the typical socio-technical high-risk points that facilitate external attacks and internal, hidden fraud in the various forms of crypto business? And what can we learn through historical failures to inform a more resilient and secure future of the ecosystem? These questions remain unanswered so far. In responding to these questions, this paper examines critically a superficial explanation of hacks and the systemic risks that persist in paraciting this space.

Theoretical Framework and Analytical Review

To continue with the systematic assessment of the cybersecurity and fraud situation around the blockchain, the present study employs several levels of theoretical modeling to integrate the aspects of technology, economy, and organization [6]. The main explanatory analytical model employed is the Layered Blockchain Security Model [7]**. A**ccording to it, the total security that a user will encounter when operating in the crypto ecosystem will eventually collapse at the base of the adding stack. These models include: The Protocol Layer- i.e.- the base blockchain- such as Bitcoin and Ethereum and its consensus mechanism [8]; the Application Layer- applications such as smart contracts and Dapps; the Bridge and Interoperability Layer- referring to assets and data transfer protocols across multiple blockchains [9]; the Access and Custodial Layer- wallets and centralized exchanges- CEX and decentralized exchanges- DEX; and the Governance and Human Layer- entities, management structures, and the users themselves [10]. This model is useful because it shows how the protocol layer with high-grade cryptography security can be broken in case the layers above have vulnerabilities [6]-[10]. This model of layering is also informed by theories that have been developed in other fields.

Economics Principal- Agent Theory [11] is highly applicable when examining risks to the centralized custodial activities of exchanges (Access Layer) and corporate entities (Governance Layer) [12]. It has to do with the possible conflict that can exist between the agent (say, a cryptocurrency exchange) being able and having opportunity to act contrary to the interests of its principal (say, a user who has deposited funds) in the case of information asymmetry [10]-[12]. The total absence of transparency about the inner accounting of an exchange gives rise to an extreme type of information asymmetry, which is exactly the state of affairs that allows undiscovered fraud to take place [13], as Mt. Gox and FTX [14] have shown. Thus, it does not matter whether the underlying blockchain will be immutable when the balance of assets available to the user is just the record in the internal mutable database of a cryptocurrency exchange [6]-[12].

Socio-Technical Systems [15] reminds us that technical examination of such complex systems is not enough; social, organizational and human factors have equally decisive parts to play. The smart contract might have sound mathematical implementation, but centralized control or user vulnerability to phishing might create an overall threat to the system. This is consistent with the Routine Activity Theory of criminology [16], which argues that crime happens when motivated criminals, the presence of appropriate targets, and the inability to protect them come together. The pseudo-anonymity and vast value of such ecosystems in the crypto-space [17] provide an excess of motivated criminals and adequate targets. The capable guardian is then often not found at the Protocol Layer, but instead at the Application, Bridge, and

Governance layers, where the oversight of regulators is lax; code is not audited, and internal controls are weak or non-existent [18].

The literature available presents a solid base of knowledge, yet tends to dwell on individual aspects. Considerable work has studied Protocol-Level Security [19], and the game-theoretic incentives of consensus mechanisms, including Proof-of-Work and Proof-of-Stake [20], have been systematically shown to be resistant to large-scale attacks, including 51 percent attacks, on established networks. A second main line of research has been working on Smart Contract Vulnerabilities, listing technical vulnerabilities, including re-entrancy attacks, integer overflows, and logic errors, and proposing redress, such as formal verification and thorough auditing. The third one is centered around the Economics of Crypto Exchanges, which makes them centralized honeypots, which are easy to manipulate and may fail in operation. By contrast, analysis integrating these threads into a multi-layered socio-technical perspective to offer a straightforward, explicit commentary on the phenomenon of unnoticed long-term fraud in the background of the transparent ledger has been meager. This manuscript, therefore, seeks to fill this gap by using this combined theoretical framework to compare some of the seminal cases [15]-[20].

Method

This study employs the qualitative comparative 'Case Study' design, as it merits examining complex modern phenomena 'in situ', especially when delineation between research paradigms and blockchain ecosystems is not conveniently accomplished [21]. It is a secondary data analysis method that allows for studying past events when collecting primary data. The multi- and triangulated sources available for use would make the results more valid and reliable, for the incidence or defect of one source would be mitigated [22].

A multi-faceted collection of data was rigorously carried out in various combinations, affording total reliance on multiple sources to construct a single significant basis. There were Official Forensic and Post-Mortem Reports, published by companies in question, court-appointed examiners, and bankruptcy trustees [9]-[10], [18]-[22]. These reports provide firsthand, critical, and often technical insights into the chronology of events and their causes. Second, it added Chainalysis, Cipher Trace, and Elliptic, specialized companies that provide Blockchain Forensic Analysis [23]. These analyses utilize on-chain data provided by public blockchain explorers (e.g., Etherscan) to track the flow of stolen funds, the wallet addresses used, and the timing of transactions, thereby creating a non-biased, evidence-driven layer [24]. Third, Legal and Regulatory Filings played an important role, including indictments and complaints, as well as discoveries by agencies such as the U.S. Securities and Exchange Commission (SEC) [25] and the Commodity Futures Trading Commission (CFTC) [26]. These documents present legally screened though accounts and observations of governance failure and fraud. Finally, reputable sources, such as investigative journalism outlets like Reuters, The Wall Street Journal, and CoinDesk [27], provided the narrative background, as well as human interest and insight into inner corporate cultures that are not typically featured in formal reporting.

This study is purposively sampled to examine failures of the blockchain stack at which they occur. The five cases, therefore, chosen are: Mt. Gox (2014): The Grounds for External Penetration, Deep Internal Operational Failures, and Collapse at the Access and Custodial Layer (Centralized Exchange). Axie Infinity/Ronin Bridge (2022): More recently, that is how the Application Layer (DeFi) and the Bridge and Interoperability Layer were made subject to a socio-technical assault (social engineering) against a

centralized set of validators. FTX (2022): This is a transforming failing case, as it is considered a Governance and Human Layer failure. Where systemic, undetected, internal fraud by the top corporate leadership was completely independent of blockchain security [23]-[27].

To further demonstrate the constant and dynamic nature of the unidentified fraud, this study includes two recent case studies of Ponzi schemes that exploit the frenzy surrounding AI and cryptocurrency. These cases are:

CBEX Crypto Scam (2024) is a purported AI-trading platform that offered high returns, but was actually a Ponzi scheme, primarily targeting customers in African countries. It is a perfect example of fraud in the Governance and Human Layer, where a facade of legitimacy is created by the hype surrounding technology. Since its inception, this case was supposed to conduct fraudulent activities [28].

PCEX Exchange (2025) employs advanced scam schemes, including fabricated testimonials and non-existent regulatory licenses, to defraud users worldwide. This scenario illustrates how malevolent actors can establish fake intermediaries without any legitimate operational infrastructure by exploiting a failure at the Access and Custodial Layer [29].

The data were then synthesized systematically across cases in each instance. In every case, the data were coded and analyzed based on a pre-decided list of analytical themes that would match with the theoretical framework: (a) Primary Attack Vector or Failure Mechanism; (b) Primary and Secondary Layers of the Blockchain Stack Affected; (c) Duration of Undetected Activity; (d) Total Financial Impact; and (e) Identified Root Causes in categories of Technical, Operational, or Governance-related [30]. This comparative analysis made it possible to reveal trends, dissimilarities, and even general themes in the different incidents.

Results

A comparative analysis of five failures in the blockchain ecosystem reveals several architectural gaps, including instances of Ponzi schemes. The characteristics of each instance are summarized in the table below

Table 1: Comparative Analysis of Major Blockchain Security Incidents

Case Study	Primary Layer Affected	Financial Impact	Duration Undetected	Primary Attack/Failure Vector	Root Cause Category
Mt. Gox (2014)	Custodial (Centralized Exchange)	850,000 BTC (~$450M)	Several Years	Protracted drain of funds; poor key management	Operational Failure & Gross Negligence
Ronin Bridge (2022)	Interoperability (Cross-Chain Bridge)	$625 Million	6 Days	Compromise of 5/9 validator keys via spear-phishing	Socio-Technical (Social Engineering &

Case Study	Primary Layer Affected	Financial Impact	Duration Undetected	Primary Attack/Failure Vector	Root Cause Category
					Centralization)
FTX (2022)	Governance (Corporate Entity)	~$8 Billion	Over 1 Year	Systemic misappropriation of customer assets to affiliated hedge fund	Deliberate Internal Fraud & Governance Failure
CBEX Scam (2024)	Governance/Human (Ponzi Scheme)	Undisclosed (Significant)	Several Months	AI-hyped marketing for a non-existent investment product; classic Ponzi structure	Deliberate Ponzi Scheme & Deceptive Marketing
PCEX Exchange (2025)	Custodial (Fake Exchange)	Undisclosed (Significant)	Several Months	Fabricated exchange platform; fake liquidity and regulatory claims to lure deposits	Deliberate Scam & Fake Infrastructure

The details of the outlined failure are provided below, explaining the particular mechanisms of failure through the lens of Principal-Agent problems and the lack of competent guardians. CBEX Crypto Scam: The Ponzi Scheme with AI hype

Table 2: Analysis of Failure Mechanisms and Guardian Absence

Case Study	Manifestation of Principal-Agent Problem	Absence of "Capable Guardian"	Information Asymmetry
Mt. Gox	Agent (Exchange) failed to safeguard principal's (User) assets.	No internal financial controls; no external audit or regulation; users could not verify reserves.	Total; internal ledger was fictional and not reconciled with blockchain.

Case Study	Manifestation of Principal-Agent Problem	Absence of "Capable Guardian"	Information Asymmetry
Ronin Bridge	Agent (Validator Set) was compromised, violating its duty to secure the bridge.	Inadequate security protocols against social engineering; over-reliance on a small, known validator set.	Partial; the bridge operated normally, hiding the fact its security model was breached.
FTX	Agents (Executives) systematically looted principals' (Customers) funds.	No board oversight, risk management, or regulatory scrutiny; complicit or ineffective auditors.	Total; deliberate concealment and misrepresentation of financial health.
CBEX Scam	Agents (Operators) promised AI-driven returns but ran a Ponzi scheme, betraying investor trust.	No legitimate product or regulatory oversight; reliance on hype over substance.	Total; the entire operation was a facade with no real underlying investment activity.
PCEX Exchange	Agent (Fake Exchange) claimed to be a legitimate custodian but was designed solely to steal deposits.	No genuine regulatory license, operational infrastructure, or third-party verification.	Total; the platform was a complete fabrication from inception.

Mt. Gox Collapse

Down the Custodial Layer. For almost an exemplary case of a Principal-Agent problem, Mt. Gox demonstrated a complete absence of socio-technical security principles. The exchange, allegedly acting as an agent for hundreds of thousands of users, had breached the very minimum custodial responsibility. While the initial conception was that this could have been one hack, on the contrary, secondary insights into the investigation by the trustee suggest a long-term, perhaps several years, undetected siphoning of approximately 850,000 BTC. The causes were multifactorial. Technically, the exchange was subject to transaction malleability attacks from the get-go, but the far more compelling case was made with the catastrophic failures in operations, which included gross negligence in the safeguarding of private keys and, more seriously, a catastrophic failure to reconcile internally mutable accounts with the immutable Bitcoin blockchain. This created a major information asymmetry- users saw balances on the Mt. Gox website, unaware these entries were fictions with no bearing on real on chain assets. At every level, a "capable guardian" was missing, such as an internal audit, external regulatory oversight, and the lack of users to verify. Thus, the opacity of the system allowed the user, as principal, to be kept blind to the employee's incompetence and wrongdoing [26].

Axie Infinity/Ronin Bridge Hack

Interoperability Layer Failure. The Ronin Bridge incident constitutes a case study on how decentralization can be an illusion and how socio-technical attacks can leverage robust technical defenses. Through blockchain forensics, consistent with in-depth preliminary investigations by Sky Mavis and Chainalysis, a forensic analysis confirmed that the assailants stole $625 million by compromising the cryptographic private keys of five out of nine validator nodes needed to authorize bridge transactions. This was accomplished not through the bridge's cryptography but, rather, through a well-crafted social engineering operation-a fake job offer that successfully phished an Axie Decentralized Autonomous Organization (DAO) employee into granting access to the validator nodes. This attack vector is an ideal example of the convergence of Routine Activity Theory elements: a motivated offender, a highly suitable target (the bridge holding hundreds of millions of dollars), and a missing capable guardian. Packaged as decentralized, the validator set was small, controlled by known entities, thereby creating a centralized attack surface. The six days during which the fraud went undetected was possible because the bridge operated normally; though compromised, the validators' day-to-day functionality offered insulation against scrutiny of the breach, definitely demonstrating that liveness is not a guarantee of security [27].

A disintegration of FTX

Failure of the Governance Layer. FTX is the cruelest example, showing undetected fraud mainly within the Governance and Human Layer, totally dissociated from the security of underlying blockchain technology [14]. The SEC complaint and the CEO's criminal trial elaborated that the core of the failures consisted of inevitable, long-standing breaches of the principal-agent relationship. Hundreds of millions of dollars in customer deposits on the Access Layer at FTX were never supposed to be put into regular accounts, separate and protected from FTX's owners. Instead, in a systematic and obviously secretive manner, the customer funds were transferred to Alameda Research, the FTX trading entity, to cover some very risky investments, extravagant execution costs, and trading losses. The above lapse was assisted by a complete absence of corporate governance, internal controls, and financial transparency. There were no boards providing oversight-a risk management committee was non-existent with the ungainly separation of duties. The information asymmetry classified as extraordinary: customers, regulators, and investors-maintained faith in the public orientation of FTX when, internally, it was staging fraud. The "capable guardian," represented by auditors and regulators, was absent, misled, or incompetent. This was no matrix failure of blocks but was a classical corporate fraud targeting crypto assets, amply demonstrating that the Protocol Layer loses meaning should the operators at the access layer and governance be corrupt or incompetent [28].

CBEX Crypto Scam

The Ponzi Scheme with AI hype. The case of CBEX is a prime case of a Governance and Human Layer failure wherein the promise of state-of-the-art business (AI) was a red herring in an archetypal Ponzi scheme. Compared to FTX, which was a legitimate business that spiraled into a fraudulent business, CBEX was a fraudulent business. It was using the black box character of AI hype to have unsustainable returns, mainly appealing to African investors. The plan was solely based on the information asymmetry because investors could not do anything to confirm the presence of the alleged AI trading algorithms. The lack of an effective guardian was complete: there was no corporate organization that could be audited, no actual product that could be reviewed, and the regulators were either absent or were slow to respond. As this case shows, the simplest type of unnoticed fraud the Ponzi scheme has acquired a new powerful mask in the crypto and AI sector, flourishing in areas with low financial literacy and close supervision [29].

PCEX Exchange

The Counfeit Custodian. The case of PCEX highlights the weakness at the Access and Custodial Layer, and how the bad actors can easily develop fully fictional intermediaries. PCEX was positioning itself as a legitimate cryptocurrency exchange that has an easy to use interface, false trading volume and counterfeit regulatory licenses. Its business model was not facilitation, but to hoard user deposits and vanish - a "rug pull" on the exchange level. This is the worst case of the Principal-Agencies problem when the will of the agent was to harm the principal. The so-called competent guardian did not exist; the user could not figure out the advanced fake appearance of the platform and a real exchange. The case points to the fact that low barriers to entry to the crypto ecosystem to establish centralized services are a two-sided sword, which allows not only negligence but also premeditated large-scale theft by actors who never had an intention to act in good faith in the first place [27]-[29].

Discussion

The five-case study analysis reveals intricate situations in cybersecurity within the blockchain ecosystem. To begin with, it has demonstrated deficiencies that are always layered over the core protocol. The unchanging but open nature of base-layer blockchains could not prevent these disasters; it is the fraud that occurred in black box, off-chain, or centralized services. This leads to an inherent "Trust Transfer Paradox" in evading trust in traditional banks; users must, in turn, place even more trust, and eventually misplaced trust, in unregulated exchanges, bridge validators, corporate officers, and, as the new cases demonstrate, outright fraudsters [30].

The trends in Table 2 are a significant and compelling factor in the application of Principal-Agent Theory. In both instances, the agents of Mt. Gox, Ronin validators, FTX leadership, CBEX operators, and PCEX creators had the incentive and opportunity to act against the interests of their principals (the consumers). The facilitating situation was the organized lack of a capable guardian as stipulated by the Routine Activity Theory. This protector was either not implemented at the working level at Mt. Gox, or was not part of the organizational security culture at Ronin, or was not addressed in the corporate law and financial regulation at FTX, or was simply non-existent in the total framework of CBEX and PCEX [31]-[33]. Such a five-fold breakdown of the guardianship in the technical, organizational, and legal spheres proves the multidimensionality of the problem.

In addition, the presence of CBEX and PCEX expands the concept of undetected fraud. Whereas Mt. Gox and FTX were cases of corruption within initially legitimate organizations, CBEX and PCEX were set up as fraudulent entities. This means that the ecosystem is susceptible not just to the breakdown of good actors but also to predation by pure malicious actors, who may also take advantage of the same information asymmetries and guardianship. The fact that their activities took several months to unfold indicates that the combination of technological hype and global presence enables even current Ponzi schemes and counterfeit exchanges to exist undetected for long enough to cause significant financial harm.

The political implications are not hard to realize. Even solutions such as auditing smart contracts, though required, are utterly inadequate to mitigate threats on the Custodial and Governance layers and will be useless against planned scams. The existence of the ecosystem relies on the obligatory presentation of competent guardians. This involves:

1. Regulatory Guardianship: Imposing a set of standards of corporate governance, segregation of consumer assets, and on-chain verifiable evidence-of-reserves of any centralized custodian. This would help bring to the forefront entities like FTX and avoid those of a fraudulent nature, such as

PCEX.

2. Architectural Guardianship: Enhancing practices to ensure that there is indeed decentralization of validator sets and more transparent mechanisms of governance to minimize the risk of centralization, as would have been experienced in the Ronin Bridge hack.
3. Individual and Collective Guardianship: Building on-chain analytics user culture, where all services are held to the can't be evil standard, high-reward AI-driven offerings like CBEX are embraced with skepticism, and the user culture is encouraged to be more skeptical.

The key to achieving this is to strengthen the upper layers of the stack as a system, which will eliminate the undetected cycle of fraud that feeds on the promise on which blockchain technology was built.

Conclusion

To support the argument, the study suggested that the cybersecurity of the blockchain ecosystem can be determined as a layered challenge, whereby the strong clarity of lower-level protocols is routinely negated by upper-level layers that are more vulnerable to critical vulnerabilities. Following comparative studies of events at Mt. Gox, Ronin Bridge, FTX, and the Ponzi scheme CBEX and PCEX, undetected fraud is an architectural feature that systems with a centralized policy or mobile fraudulent scams of its own possess to become transparent [31]-[33]. Theoretical perspectives including Principal-Agency Theory and Routine Activities Theory also had a similar story to tell; undetected fraud flourishes when information asymmetries are enormous and no one is capable of acting as the guardian, such as internal controls, transparent auditing, and other effective controls. Its core conclusion is, therefore, that the so-called trustless principle of blockchain is more of a myth in actuality; rather, the trust is relocated to new, unregulated and unaccountable participants of the game, code governors, and Ponzi schemes of all sorts. Thus, until a paradigm shift that would shake the roots, the cycle of decline and plundering will continue to be repeated in a number of decades to come. The change will not be limited to the enhancement of the security of the smart contracts, but will entail a monumental adoption of systemic reforms to bring an element of transparency, the ability to verify, not trust, as the only way to counter the complex Ponzi schemes. Strengthening of such human and institutional layers is more important to the well-being of the ecosystem than tightening of cryptographic layers.

Future Research Directions

This study has opened up several of potential research avenues. Firstly, quantified metrics with benchmarks for assessing decentralization and custodial risk should be developed and standardized for CeFi and DeFi protocols indeed, beyond mere qualitative assessment. Second, the techno legal research agenda could explore real-time privacy-preserving Proof of Reserves and Proof of Liabilities audits using a technical solution that is blockchain-ready. Third, research should look at the effectiveness of decentralized insurance and on-chain forensic tools that serve as automated "guardians" to mitigate fraud-induced losses. Also, there is a pressing need for socio-technical research in which the lawmakers might understand behavioral economics vis-à-vis user trust on the Cryptocurrency platforms and design more effective educational interventions. Finally, the comparative legal analysis of the regulatory-this global framework for Cryptocurrency will provide the best practice to govern centralized intermediaries in a way that does not kill the installation and leaves significant points toward a more secure and trustful ecosystem.

References

1. L. S. F. Lin, "Cryptocurrencies and AI-enabled organised fraud: Emerging risks and countermeasures," Charles Sturt University Research Output, Jun. 18, 2025. https://researchoutput.csu.edu.au/en/publications/cryptocurrencies-and-ai-enabled-organised-fraud-emerging-risks-an
2. L. D. Christensen, "Preventing Fraud in Crypto Payments," Journal of Economic Criminology, vol. 7, p. 100124, Jan. 2025, doi: 10.1016/j.jeconc.2024.100124
3. K. B. Yahia, "The dark side of cryptocurrency adoption in an emerging market: perspectives of Tunisian users vs. professionals," International Journal of Emerging Markets, pp. 1–24, Sep. 2025, doi: 10.1108/ijoem-04-2024-0687
4. Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," Electronics, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.
5. "A Systematic Literature Review on Tackling Cyber Threats for Cyber Logistic Chain and Conceptual Frameworks for Robust Detection Mechanisms," IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/10933978
6. A. Bayramova, D. J. Edwards, and C. Roberts, "The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime," Buildings, vol. 11, no. 7, p. 283, Jun. 2021, doi: 10.3390/buildings11070283.
7. Z. Mahmood and V. Jusas, "Blockchain-Enabled: Multi-Layered Security Federated Learning Platform for Preserving Data Privacy," Electronics, vol. 11, no. 10, p. 1624, May 2022, doi: 10.3390/electronics11101624.
8. "Deep Learning, Blockchain based Multi-layered Authentication and Security Architectures," IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9793179
9. "Towards Interoperable Blockchains: A Survey on the Role of Smart Contracts in Blockchain Interoperability," IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9519640
10. D. Ciesielska-Maciągowska, "Cryptocurrency exchanges in the decentralized finance system," Questa Soft, 2025. https://www.ceeol.com/search/article-detail?id=1363307
11. D. Braun and D. H. Guston, "Principal-agent theory and research policy: An introduction," RERO DOC, 2003, [Online]. Available: https://doc.rero.ch/record/299898
12. B. Steil, "Changes in the Ownership and Governance of Securities Exchanges: Causes and Consequences," Brookings-Wharton Papers on Financial Services, vol. 2002, no. 1, pp. 61–91, Jan. 2002, doi: 10.1353/pfs.2002.0021.
13. P. Fay, "Price Dynamics of Cryptocurrency and its Determinants," Sep. 03, 2025. https://theses.hal.science/tel-05293348/
14. S. Fu, Q. Wang, J. Yu, and S. Chen, "FTX Collapse: A Ponzi Story," in Lecture notes in computer science, 2023, pp. 208–215. doi: 10.1007/978-3-031-48806-1_14.
15. S. H. Appelbaum, "Socio-technical systems theory: an intervention strategy for organizational development," Management Decision, vol. 35, no. 6, pp. 452–463, Aug. 1997, doi: 10.1108/00251749710173823.
16. F. Miró, "Routine Activity Theory," The Encyclopedia of Theoretical Criminology, pp. 1–7, Jan. 2014, doi: 10.1002/9781118517390.wbetc198.

17. O. A. S. Al-Azri, "Exploiting Social Media Analytics to Identify Critical Factors Affecting Cryptocurrencies Adoption and Utilization - ProQuest." https://www.proquest.com/openview/ff45bf5201fcc6a0c660d5d5c1f07a1c/1?pq-origsite=gscholar&cbl=2026366&diss=y
18. E. Danter, "Responsibilities, Regulations, Control Frameworks," in Palgrave studies in accounting and finance practice, 2022, pp. 9–30. doi: 10.1007/978-3-030-92466-9_2.
19. A. Sundararajan, A. Chavan, D. Saleem, and A. I. Sarwat, "A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security," Energies, vol. 11, no. 9, p. 2360, Sep. 2018, doi: 10.3390/en11092360.
20. B. Sriman, S. G. Kumar, and P. Shamili, "Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake," in Advances in intelligent systems and computing, 2020, pp. 395–406. doi: 10.1007/978-981-15-5566-4_34.
21. L. McLeod, S. G. MacDonell, and B. Doolin, "Qualitative research on software development: a longitudinal case study methodology," Empirical Software Engineering, vol. 16, no. 4, pp. 430–459, Jan. 2011, doi: 10.1007/s10664-010-9153-5.
22. K. Da Silva Santos, M. C. Ribeiro, D. E. U. De Queiroga, I. A. P. Da Silva, and S. M. S. Ferreira, "O uso de triangulação múltipla como estratégia de validação em um estudo qualitativo," Ciência & Saúde Coletiva, vol. 25, no. 2, pp. 655–664, Feb. 2020, doi: 10.1590/1413-81232020252.12302018
23. N. Kumar and A. Vaish, "Use of Blockchain Technology in Digital Forensics," in CRC Press eBooks, 2024, pp. 1–16. doi: 10.1201/9781003449515-1.
24. Y. Marchenko, W. J. Knottenbelt, and K. Wolter, "EthExplorer: A Tool for Forensic Analysis of the Ethereum Blockchain," in Lecture notes in computer science, 2020, pp. 100–117. doi: 10.1007/978-3-030-44411-2_7.
25. S. Gadinis, "The SEC and the Financial Industry: Evidence from Enforcement Against Broker-Dealers," The Business Lawyer, vol. 67, no. 3, pp. 679–728, 2012, [Online]. Available: https://www.jstor.org/stable/23240011
26. "Commodity Futures Trading Commission," CFTC. https://www.cftc.gov/
27. A. Carson and K. Farhall, "Understanding Collaborative Investigative Journalism in a 'Post-Truth' Age," Journalism Studies, vol. 19, no. 13, pp. 1899–1911, Jul. 2018, doi: 10.1080/1461670x.2018.1494515.
28. "CBEX crypto scam: AI-hyped Ponzi scheme defrauds African investors," France 24, July 1, 2025. [Online]. Available: https://www.france24.com/en/live-news/20250701-cbex-crypto-scam-ai-hyped-ponzi-scheme-defrauds-african-investors
29. "A Deep Dive into the Crypto Scam Tactics You Need to Know," BTCC, A5setGuruMax, Sept. 10, 2025. [Online]. Available: https://www.btcc.com/en-CA/square/A5setGuruMax/927534
30. A. E. Muhammad, K. C. Yow, J. Baili, Y. Cho, and Y. Nam, "CORTEX: Composite Overlay for Risk Tiering and Exposure in Operational AI Systems," arXiv.org, Aug. 24, 2025. https://arxiv.org/abs/2508.19281
31. A. Collomb, P. De Filippi, and K. Sok, "Blockchain Technology and Financial Regulation: A Risk-Based Approach to the Regulation of ICOs," European Journal of Risk Regulation, vol. 10, no. 2, pp. 263–314, Jun. 2019, doi: 10.1017/err.2019.41.
32. N. Belenkov et al., "SoK: A Review of Cross-Chain Bridge Hacks in 2023," arXiv.org, Jan. 06, 2025. https://arxiv.org/abs/2501.03423

33. A. Aibai, J. Julaiti, and S. Gou, "The Asymmetric Effects of Upside and Downside Risks in Cryptocurrency Markets: Insights from the LUNA and FTX Crises," Finance Research Letters, vol. 67, p. 105750, Sep. 2024, doi: 10.1016/j.frl.2024.105750.