Analysis of Blockchain Security: Classic attacks, Cybercrime and Penetration Testing

Shreshta Kaushik, Nour El Madhoun

Analysis of Blockchain Security: Classic attacks, Cybercrime and Penetration Testing

Shreshta Kaushik*, Nour El Madhoun* † ‡
* LISITE Laboratory, ISEP, 10 Rue de Vanves, Issy-les-Moulineaux, 92130, France
† Université Paris-Saclay, CNRS, Laboratoire Interdisciplinaire des Sciences du Numérique, 91190, Gif-sur-Yvette, France
‡ Sorbonne Université, CNRS, LIP6, 4 place Jussieu 75005 Paris, France
E-mails: shreshta.kaushik@eleve.isep.fr; nour.el-madhoun@isep.fr
nour.el-madhoun@universite-paris-saclay.fr; nour.el_madhoun@sorbonne-universite.fr

***Abstract*—Blockchain is an innovative technology that gives built-in security to any software or application. There is a wide range of applications for blockchain, from risk management to financial services, crypto-currencies and the Internet of Things (IoT). This innovation is based on transparency, immutability, security, efficiency and decentralization. It is a trending topic since cryptocurrencies are a hot topic in the market. Blockchain is a combination of mathematics, cryptography, algorithms and models. In this paper, we present a general overview of the security aspects of blockchain technology.**

***Index Terms*—Attack, Authentication, Blockchain, Confidentiality, Integrity, Pentest, Privacy, Security.**

I. Introduction

Blockchain technology is considered as one of the most promising innovations of the past few years, with potential applications in many areas such as finance, trade, the Internet of Things, supply chain management and many others. This technology is based on a distributed data management system that allows transactions to be recorded and validated in a seamless, secure and reliable manner. Since the creation of the first bitcoin cryptocurrency in 2008, blockchain technology has grown rapidly. Blockchain-based cryptocurrencies have revolutionized financial markets by offering alternatives to traditional systems, while businesses and governments around the world are beginning to explore the different applications of blockchain technology to improve the efficiency and transparency of their operations [1].

The security of blockchain systems is a major concern due to the decentralized and open nature of the technology. Not only are blockchain systems subject to various technical threats such as denial of service attacks, 51% attacks, and smart contract vulnerabilities, but they also attract the attention of cybercriminals who seek to exploit these weaknesses for illegal activities. Cybercrime in blockchain includes, but is not limited to, money laundering, fraud and the sale of illegal goods and services. These illegal activities can result in significant financial losses to users and businesses, as well as a loss of trust in the technology [2]. In addition, the transparency of transactions on blockchain can also present privacy risks to users who may be exposed to phishing attacks and cyberbullying. In order to counter these risks, solutions such as anonymous transactions and privacy protocols have been developed to preserve users' anonymity on the blockchain [3].

The objective of this paper is to provide a general analysis of blockchain security by examining traditional attacks, cybercrime and penetration testing.

This paper is organized as follows. Section II explains the principle of blockchain technology, including its features and consensus algorithms. Section III discusses classic attacks on blockchain, while section IV examines the most well-known methods of cybercrime in the field of blockchain. Section V describes the blockchain penetration testing process. The last section concludes the paper.

II. Blockchain Technology: Overview

A. What is a Blockchain ?

A blockchain is a series of blocks that hold data. This concept was first introduced in 1991 by a group of researchers and was initially designed to timestamp digital documents to prevent them from being backdated or tampered with. A blockchain is a publicly accessible distributed ledger that has a unique characteristic: once data has been recorded on the blockchain, it becomes challenging to alter it [4]. Each block in a blockchain contains specific information, such as the hash of the block and the hash of the previous block (see Fig. 1 and Fig. 2). It also stores other data that depends on the type of blockchain. For example, the Bitcoin blockchain stores data about transactions, including the sender, receiver and transaction amount. The hash of a block can be compared to a fingerprint because it identifies the block and all its contents and it is always unique, just like a fingerprint. Once a block is created, its hash is calculated. Therefore, any change in the block causes a change in the hash. In other words, hashes are dedicated to detect changes in blocks. The hash of the previous block creates a series (chain) of blocks, which makes a blockchain secure. As shown in Fig 2, block number 3 points to block number 2 and number 2 points to number 1. Indeed, the block number 1 in Fig. 2 (or block 0 in Fig. 1) cannot point to the previous blocks because it is the first one. We call it the Genesis block. If an attacker is going to try to change the content of block 2 in Fig. 2, it causes the hash of block 2 to change and this will automatically make block 3 and all subsequent blocks invalid because they no longer store a valid hash of the previous block.

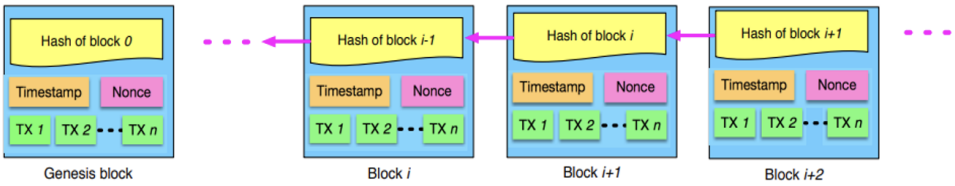

Fig. 1. Example 1 of blockchain [4]

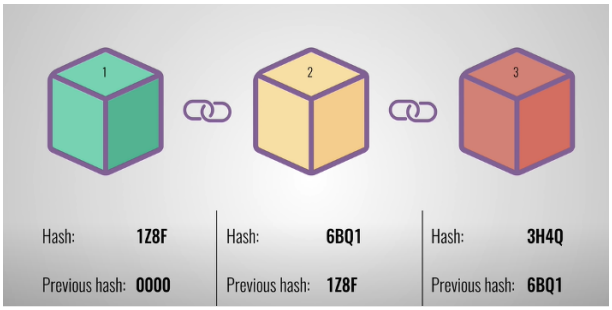

Fig. 2. Example 2 of blockchain [5]

However, the use of hashes does not suffice to prevent falsification. Today's computers are fast and can calculate hundreds of thousands of hashes per second. Attackers can effectively forge a block and recalculate all the hashes of other blocks to make a blockchain valid again. Therefore, to mitigate this problem, there is a set of consensus algorithms that aim to slow down the creation of new blocks but also to validate them (see section II-B). For example, in the case of the Bitcoin blockchain: it takes about 10 minutes to run the consensus algorithm to create a new block, validate it and add it to the chain. This mechanism makes it very difficult to forge blocks, because if an attacker modifies a block, he needs to rerun the consensus algorithm for all the following blocks but also in all the other nodes since each node has a copy of the blockchain [6].

The main characteristics of a blockchain are [7] [8] [9]:

- Distribution and decentralization: they are similar but have slightly different meanings. The distribution property focuses on the distribution of data, while the decentralization property focuses on the distribution of decision-making and power control. Both characteristics are often used interchangeably, as they are closely related and present in most blockchain systems.
  - Distribution: the blockchain is a distributed ledger where data is stored on a network of nodes rather than on a centralized server. This means that no individual node controls all of the data, but rather all nodes have a copy of it.
  - Decentralization: the blockchain is decentralized, meaning that there is no central authority that controls the network. This means that there is no single point of failure or governance. All nodes are involved in making decisions about the evolution of the network.
- Immutability: once a transaction is recorded on the blockchain, it cannot be modified or deleted, which guarantees the integrity of the data (transactions and blocks).
- Transparency: all users of the network can see all the transactions that have been made on the blockchain.
- Replication: all users of the blockchain have the same copy of the ledger, then the data is duplicated throughout the system.
- Cryptography: the blockchain uses cryptography to ensure user authentication and data integrity. For authentication, each user of the blockchain has its own key pair (public/private) that is generated using the Elliptic Curve Digital Signature Algorithm (ECDSA). For the integrity of the data (transactions and blocks), hash functions are used.

B. Consensus Algorithms

A consensus algorithm is a crucial mechanism in the operation of blockchains, enabling participants to reach agreement on the state of the decentralized ledger without depending on a central authority. It determines how transactions are validated, added to the blockchain and guaranteed to be immutable. Different types of consensus algorithms have been developed, each with their own characteristics, advantages and disadvantages. These algorithms play a key role in establishing trust and security within blockchains, enabling decentralized and reliable consensus. The following is an overview of the three main algorithms:

1) Proof of Work (PoW): it is used by the Bitcoin blockchain. In this algorithm, miners must solve complex mathematical problems to add blocks to the chain. Solving these problems requires considerable computing power and is energy-intensive. However, once the problem has been solved, it is easy to verify the solution.

Thus, the PoW algorithm offers high security by making modification of the blockchain history extremely costly. However, this approach is energy-intensive and can lead to centralized mining [10].

2) Proof of Stake (PoS): it is used by the Ethereum blockchain (in transition to Ethereum 2.0). In this algorithm, validators are selected according to their financial participation, i.e. the amount of tokens they own. Unlike the PoW algorithm, there is no complex problem solving or competition between miners. validators are randomly chosen according to their financial participation, and are responsible for validating transactions and adding blocks to the chain. PoS is less energy-intensive than the PoW, but it does present the potential risk of centralizing power among holders of large quantities of tokens [11].
3) Delegated Proof of Stake (DPoS): it is used by the EOS and Tron blockchains. In this algorithm, token holders elect delegates, also known as "witnesses", who are responsible for validating transactions and creating blocks. Unlike other consensus algorithms, not all token holders participate directly in the consensus process. Instead, they delegate their validation power to these elected delegates. This improves network scalability by avoiding direct participation by all token holders. However, there is a risk of centralization of power if a small number of delegates is chosen on a permanent basis [12].
4) Proof of Authority (PoA): it is mainly used in private blockchains and consortia. The validators are predetermined trusted entities. Unlike PoW and PoS, there is no competition or problem solving to choose validators, but they are selected on the basis of their reputation and status as trusted entities within the network. The PoA relies on a pre-established trust in the validators, which can lead to a centralization of power and challenge the decentralization inherent in blockchain technology [13].

III. Classic Attacks on a Blockchain

Blockchains are considered reliable and secure data storage systems, but that doesn't mean they are immune to attack. Attackers are always looking for ways to infiltrate networks to steal funds or disrupt their normal operation. In this section, we present the most common attacks in blockchains:

1) 51% Attack: it can be applied to any blockchain based on the PoW consensus algorithm (see section II-B), where computing power is used to solve complex problems and validate transactions. It occurs when an attacker or a group of attackers control 51% or more of the computing power of the blockchain network and therefore he will be able to influence the consensus of the blockchain, cancel previous transactions, mine blocks and spend the same funds several times. Indeed, 51% attacks have been observed on several blockchains, especially on small networks and altcoins that have low participation and low hashing power. Protection against this type of attack is achieved by promoting decentralization, encouraging the participation of numerous miners and diversifying computing power on the network [14].
2) Replication attack: it is a threat where copies of the legitimate blockchain are created to introduce fraudulent transactions or alter the transaction history. This can compromise the integrity of the blockchain. Users can prevent this type of attack by ensuring they use robust consensus algorithms that guarantee the validity of blocks, and by verifying the integrity of the chain by comparing versions between network nodes [15].
3) Selfish mining: it is an attack where a malicious miner keeps newly mined blocks for itself instead of sharing them with the rest of the network. This gives it an unfair advantage in terms of mining rewards and upsets the balance of the system. Indeed, to avoid this attack, it is important to use fair consensus protocols that reward honest participation, and to carefully monitor miners' activity for suspicious behavior [16].
4) Sybil attack: it involves the creation of multiple identities or nodes by an attacker to gain disproportionate control over the network. This can enable the attacker to distort consensus results or disrupt normal blockchain operations. Indeed, the implementation of identification and verification mechanisms for network participants, such as reputation systems or reputation-based consensus mechanisms, is essential to avoid this type of attack [17].
5) Replay attack: it occurs when a valid transaction or message is reproduced in another blockchain, which can lead to double spending or undesirable effects. Protective algorithms must be implemented against this type of attack, such as digital signature mechanisms to guarantee the authenticity of transactions, and appropriate verification mechanisms to prevent transactions from being repeated [18].
6) Routing attack: attackers can manipulate the routing of transactions to redirect them to malicious nodes or prevent them from reaching their intended destination. In a blockchain, transactions are propagated through the peer-to-peer network, where each node forwards them to other nodes until they reach the miners for inclusion in a block. However, in a routing attack, attackers seek to manipulate routing mechanisms to influence the path of transactions. To avoid this type of attack, it is important to use attack-resistant routing protocols that can help mask the identity of nodes and make it more difficult for attackers to target transactions. In addition, the use of network monitoring mechanisms can help detect anomalies in transaction routing. By monitoring traffic, communication patterns and latency variations, users can identify suspicious behavior and take steps to counter the routing attack [19] [20].
7) Man-in-the-middle attack: it occurs when third parties intercept communications between blockchain participants, modify the data or messages exchanged, and impersonate the parties involved. The use of secure connections and encryption protocols to protect communications between

blockchain nodes is a way of being protected against this type of attack [21] [22].

8) Denial-of-Service (DoS) attack: it aims to disrupt or block access to the blockchain network by flooding the network with malicious traffic, thereby overloading nodes and network resources. This type of attack can be prevented by implementing mechanisms to detect anomalous behavior, bandwidth limits and systems to protect against DoS attacks [23].

IV. Cybercrime and Blockchain

Blockchain technology, like any technological innovation, presents opportunities for cyber criminals. Cybercrime in the blockchain space can take many forms, ranging from attacks to steal funds to market manipulation techniques aiming to gain financial advantage. In this section, we examine the most well-known cybercrime methods used in the blockchain world, as well as recommended preventative measures to protect users and their investments.

1) Fraud and scams: cybercriminals can create fraudulent blockchain projects, fictitious ICOs (Initial Coin Offerings) [24] or worthless tokens to cheat investors out of their money. Users can protect themselves by thoroughly researching blockchain projects, checking the credibility of the team behind the project and reading the opinions of other investors [25].
2) Phishing: phishing attacks aim to steal blockchain users' personal information and private keys. Cybercriminals send misleading e-mails or messages claiming to come from legitimate blockchain platforms to trick users into divulging their confidential information. Users can protect themselves by carefully checking website URLs, never clicking on suspicious links and using hardware wallets or trusted wallets to store their cryptocurrencies [2] [26].
3) Illegal markets: often known as "darknet markets". They use cryptocurrencies and blockchain technology to facilitate the sale of illicit products, such as drugs, weapons and stolen data. These markets take advantage of the anonymity and resistance to censorship offered by blockchain to evade detection and repression [26]. In order to combat illegal markets in the context of blockchain, the collaboration between regulators, law enforcement authorities and industry players must be strengthened to detect and dismantle illegal markets. It is also important to raise users' awareness of the risks associated with transactions on illegal markets and to encourage them to use blockchain technology in a legal and ethical manner [27].
4) Market manipulation: indeed, there are malicious actors who can use market manipulation techniques, such as wash trading (fictitious transactions to inflate volume) or pump and dump (mass buying to artificially increase the price before selling quickly), to manipulate cryptocurrency prices. Users must be cautious when investing, diversify investments and consult reliable sources of information [28] [29].
5) Money laundering: the pseudonymous nature of some blockchains enables criminals to launder money using cryptocurrency transactions as they can be difficult to trace or associate with a real person, facilitating the money laundering process and complicating the task of law enforcement agencies. Therefore, in order to prevent money laundering in the blockchain field, it is essential to implement strict regulations and rigorous identity verification procedures within cryptocurrency exchange platforms. This reduces the risk of these platforms being used for illicit purposes. In addition, collaboration with regulators is crucial in identifying suspicious activity and reporting transactions linked to money laundering. Finally, raising user awareness is essential to educate them on the risks associated with money laundering and encourage them to maintain transparency and compliance in their cryptocurrency transactions [30] [31].

V. Blockchain Penetration Testing

Blockchain penetration testing is a systematic method for assessing the resistance of blockchain systems to malicious attacks. They involve simulating real-world attacks on the blockchain system using specific techniques such as system reconnaissance, data injection, denial of service, and account hacking. The goal of these tests is to discover vulnerabilities in the system and allow developers to fix these weaknesses before an attacker can exploit them. Penetration testing can also be used to assess regulatory and security compliance. The results of these tests can be used to improve the overall security of the blockchain system by identifying and fixing potential vulnerabilities [32] [33]. The steps in the penetration testing process are:

1) Discovery: the first step in blockchain penetration testing is to thoroughly understand the architecture and functioning of the blockchain in order to enhance its security. This involves analyzing the blockchain's capabilities in preserving integrity, storing data, ensuring confidentiality, and maintaining availability. During this phase, it is crucial to pay attention to the following aspects: understanding the blockchain architecture and how it is implemented, ensuring compliance with governance and standard requirements, and conducting a readiness assessment to evaluate the technological capabilities and security practices of the blockchain.
2) Evaluation: it aims to identify potential vulnerabilities or loopholes that may present risks to the blockchain application. Various tests are conducted, including network penetration testing, static and dynamic application testing, testing of wallets, GUI, databases, application logic, and blockchain integrity testing. Each attack vector mentioned is thoroughly analyzed to ensure that security controls are capable of detecting, mitigating, and investigating any unauthorized access. The evaluation provides practical insights into the blockchain application, assessing its level of penetration based on industry methods and standards.

These comprehensive tests and analysis help validate the effectiveness of security controls.

3) Functional testing: it focuses on ensuring that all services utilized within the blockchain are functioning as intended. Testers examine various components, such as the blockchain size, that requires regular monitoring to verify its functionality and performance as the chain grows over time without size limits. Testers also validate the proper addition of blocks to the chain after transaction verification, verify data transmission through peer-to-peer architecture, conduct API testing to ensure the validity of requests and responses, perform integration testing to ensure seamless communication within the blockchain network, conduct performance testing to assess readiness for production, and execute security testing to identify and address potential vulnerabilities. This comprehensive functional testing ensures the blockchain application operates smoothly and securely.
4) Reporting: a detailed report is generated, outlining each vulnerability identified during the blockchain application's penetration testing. This comprehensive and well-explained report helps security experts understand the identified loopholes and enables them to implement necessary security practices and measures accordingly.
5) Remediation: the final step in blockchain penetration testing is to remediate the vulnerabilities reported by the security expert and request a re-scan. By addressing the identified vulnerabilities and making the necessary improvements, organizations can present users with a secure and reliable blockchain application, fostering user confidence and loyalty. This process contributes to an organization's future endeavors and establishes a strong foundation for secure blockchain implementations.

VI. Conclusion

Blockchain technology has significant potential in many areas, including finance, commerce, the Internet of Things and supply chain management. However, it is essential to recognize that security remains a major concern for blockchain systems due to their decentralized and open nature. Conventional attacks such as the 51% attack, replication attack and other types of cybercrime can compromise the integrity and the trust in the technology. To mitigate these risks, it is crucial to adopt robust security measures, such as robust consensus algorithms, implementing confidentiality and authentication protocols, and carrying out regular penetration tests to identify and correct potential vulnerabilities. In addition, close collaboration between regulators, law enforcement authorities and industry players is required to detect and combat blockchain-related criminal activity.

References

[1] N. El Madhoun, J. Hatin, and E. Bertin, "A decision tree for building it applications," *Annals of Telecommunications*, vol. 76, no. 3, pp. 131–144, 2021.

[2] E. Reddy and A. Minnaar, "Cryptocurrency: A tool and target for cybercrime," *Acta Criminologica: African Journal of Criminology & Victimology*, vol. 31, no. 3, pp. 71–92, 2018.

[3] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[4] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[5] K. Ahmadi, "Learning blockchain," *https://www.linkedin.com/pulse/learning-blockchain-kiki-ahmadi/*, last connection (03/01/2023).

[6] V. Schlatt, T. Guggenberger, J. Schmid, and N. Urbach, "Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity," *International journal of information management, Elsevier*, p. 102470, 2022.

[7] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019.

[8] N. Fahmi, D. E. Hastasakti, D. Zaspiagi, and R. K. Saputra, "A comparison of blockchain application and security issues from bitcoin to cybersecurity," *Blockchain Frontier Technology*, vol. 3, no. 1, pp. 81–88, 2023.

[9] K. Daimi, I. Dionysiou, and N. El Madhoun, *Principles and Practice of Blockchains*. Springer Nature, 2022.

[10] N. Sapra, I. Shaikh, and A. Dash, "Impact of proof of work (pow)-based blockchain applications on the environment: a systematic review and research agenda," *Journal of Risk and Financial Management*, vol. 16, no. 4, p. 218, 2023.

[11] C. Schwarz-Schilling, J. Neu, B. Monnot, A. Asgaonkar, E. N. Tas, and D. Tse, "Three attacks on proof-of-stake ethereum," *International Conference on Financial Cryptography and Data Security*, pp. 560–576, 2022.

[12] Q. Hu, B. Yan, Y. Han, and J. Yu, "An improved delegated proof of stake consensus algorithm," *Procedia Computer Science*, vol. 187, pp. 341–346, 2021.

[13] J. Yang, J. Dai, H. B. Gooi, H. D. Nguyen, and A. Paudel, "A proof-of-authority blockchain-based distributed control system for islanded microgrids," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 8287–8297, 2022.

[14] C. Ye, G. Li, H. Cai, Y. Gu, and A. Fukuda, "Analysis of security in blockchain: Case study in 51%-attack detecting," *2018 5th International conference on dependable systems and their applications (DSA), IEEE*, pp. 15–24, 2018.

[15] R. Gupta, A. Kumari, and S. Tanwar, "A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, p. e4009, 2021.

[16] M. Saad, L. Njilla, C. Kamhoua, and A. Mohaisen, "Countering selfish mining in blockchains," *2019 International Conference on Computing, Networking and Communications (ICNC)*, pp. 360–364, 2019.

[17] A. Hafid, A. S. Hafid, and M. Samih, "A tractable probabilistic approach to analyze sybil attacks in sharding-based blockchain protocols," *IEEE Transactions on Emerging Topics in Computing*, vol. 11, no. 1, pp. 126–136, 2022.

[18] I. A. R. Djinko, T. Kacem, and A. Girma, "Blockchain-based approach to thwart replay attacks targeting remote keyless entry systems," *2022 International Conference on Engineering and Emerging Technologies (ICEET)*, pp. 1–6, 2022.

[19] R. Chaganti, R. V. Boppana, V. Ravi, K. Munir, M. Almutairi, F. Rustam, E. Lee, and I. Ashraf, "A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges," *IEEE Access*, 2022.

[20] M. Ali, A. El-Moghith, A. Ibrahim, M. N. El-Derini, and S. M. Darwish, "Wireless sensor networks routing attacks prevention with blockchain and deep neural network." *Computers, Materials & Continua*, vol. 70, no. 3, 2022.

[21] I. Riadi, R. Umar, I. Busthomi, and A. W. Muhammad, "Block-hash of blockchain framework against man-in-the-middle attacks," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 8, no. 1, pp. 1–9, 2022.

[22] P. Ekparinya, V. Gramoli, and G. Jourjon, "Impact of man-in-the-middle attacks on ethereum," *2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS)*, pp. 11–20, 2018.

[23] M. Mirkin, Y. Ji, J. Pang, A. Klages-Mundt, I. Eyal, and A. Juels, "Bdos: Blockchain denial-of-service," *Proceedings of the 2020 ACM SIGSAC conference on Computer and Communications Security*, pp. 601–619, 2020.

[24] N. Essaghoolian, "Initial coin offerings: Emerging technology's fundraising innovation," *UCLA l. Rev.*, vol. 66, p. 294, 2019.
[25] G. A. Siu, A. Hutchings, M. Vasek, and T. Moore, ""invest in crypto!": An analysis of investment scam advertisements found in bitcointalk," *2022 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–12, 2022.
[26] M. Chawki, "Cybercrime and the regulation of cryptocurrencies," *Future of Information and Communication Conference*, pp. 694–713, 2022.
[27] R. Broadhurst, D. Lord, D. Maxim, H. Woodford-Smith, C. Johnston, H. W. Chung, S. Carroll, H. Trivedi, and B. Sabol, "Malware trends on 'darknet'crypto-markets: Research review," *Available at SSRN 3226758*, 2018.
[28] J. Hamrick, F. Rouhi, A. Mukherjee, A. Feder, N. Gandal, T. Moore, and M. Vasek, "An examination of the cryptocurrency pump-and-dump ecosystem," *Information Processing & Management*, vol. 58, no. 4, p. 102506, 2021.
[29] J. Nicholls, A. Kuppa, and N.-A. Le-Khac, "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape," *Ieee Access*, vol. 9, pp. 163 965–163 986, 2021.
[30] D. Dupuis and K. Gleason, "Money laundering with cryptocurrency: open doors and the regulatory dialectic," *Journal of Financial Crime*, vol. 28, no. 1, pp. 60–74, 2020.
[31] M. W. Calafos and G. Dimitoglou, "Cyber laundering: Money laundering from fiat money to cryptocurrency," *Principles and Practice of Blockchains*, pp. 271–300, 2022.
[32] A. Bhardwaj, S. B. H. Shah, A. Shankar, M. Alazab, M. Kumar, and T. R. Gadekallu, "Penetration testing framework for smart contract blockchain," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 2635–2650, 2021.
[33] S. Emery, C. E. Chow, and R. White, "Penetration testing a us election blockchain prototype," *Electronic Voting (E-Vote-ID)*, pp. 82–97, 2021.