

# Survey on cryptocurrency security attacks and detection mechanisms

Amenah Abdulabbas Almamoori<sup>1</sup>, Wesam S. Bhaya<sup>2</sup>

<sup>1</sup>Department of Information Networks, College of Information Technology, University of Babylon, Babylon, Iraq

<sup>2</sup>Department of Information Security, College of Information Technology, University of Babylon, Babylon, Iraq

---

## Article Info

### Article history:

Received Jul 26, 2022

Revised Feb 23, 2023

Accepted Mar 24, 2023

---

### Keywords:

Blockchain

Consensus algorithm

Cryptocurrencies

Cyber-attacks

---

## ABSTRACT

Cryptocurrencies have become extremely popular as a form of payment in recent years. They are supported by blockchain, a cutting-edge advanced technology that makes extensive use of cryptographic mechanisms and other sophisticated distributed computing techniques. On these grounds, cryptocurrencies have been a target of several attacks. Cyber-attacks, for example, are exogenous events that can robustly affect cryptocurrencies by influencing their stabilization of price and market valuation. This study describes an overview of cybercriminals' activities on cryptocurrencies. It provides a detailed discussion on the most popular types of attacks on the cryptocurrency ecosystem. Moreover, it provides possible countermeasures to these attacks. Finally, it produces insights into the most impactful attacks on cryptocurrencies and the best methods that have been proposed for detecting cryptocurrency attacks. The main goal of this survey is to obtain a thorough understanding of cryptocurrency attacks, which have been the subject of major studies concerning financial risks on cryptocurrency. A large number of existing publications have reviewed and assessed various forms of attacks to achieve this goal. However, these works have considerably flawed. To the best of our knowledge, the present survey sheds light on future research directions.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



---

## Corresponding Author:

Amenah Abdulabbas Almamoori

Department of Information Networks, College of Information Technology, University of Babylon

Babylon, Iraq

Email: amenah.net.phd@student.uobabylon.edu.iq

---

## 1. INTRODUCTION

In recent years, cryptocurrencies, such as ethereum, bitcoin, and litecoin, have been widely allowed as a new form of digital currency worldwide. Nowadays, cryptocurrency is used as a payment method of services, such as faucet, gambling, mining pool, marketplace, and mixing; but, it is vulnerable to various threats or cyber-attacks [1]. The recent attack, the bitcoin gold (BTG) attack, was discovered in 2020 by a researcher of the digital currency initiative at Massachusetts Institute of Technology (MIT). BTG attack is one of the newest and most dangerous attacks. An important attribute of cryptocurrency is its capability to act as a decentralized payment system. Nevertheless, the cryptocurrency network has vulnerability to various threats or cyber-attacks.

Blockchain is a distributed ledger technology that allows storing information and exchanges securely. Blockchain technologies aim to provide better trustworthiness, privacy of data, and security of systems, but they are not immune to cyber-attacks [2]. Therefore, most researchers have focused on reducing the risk of attacks or at least to identify and prevent them from affecting transactions and achieve a state of

security during the circulation and use of digital currencies. The cryptocurrency's security is guaranteed by the blockchain consensus mechanism and the public-key cryptography.

Fundamentally, the blockchain is a network of interconnected blocks. The unique block identification is the hash of the block header. Each block is linked to the next in such a way that the previous block's hash is linked to the current block's hash. We can trace it back to the genesis block from any single block in a blockchain because it is linked to the prior block. Tampering with the blocks in a blockchain is impossible because fiddling with one block introduces mistakes in the next, and so on [3].

Bitcoin is the first and most frequently used cryptocurrency based on the blockchain technology. This coin posed a threat to the currency market as a pure alternative that ensured anonymity and was not subject to central government control. Bitcoin continues to have the biggest trading volume of any cryptocurrency. Many vulnerabilities and assaults have been researched as the cryptocurrency market has grown, and these flaws and attacks have been found to affect the cryptocurrency ecosystem. The proof of work (PoW) system in bitcoin ensures transaction security by preventing double spending on the currency.

Data analysis approaches have been widely used in the cyber security field in the past [4]. To that end, having a small number of guiding basics that are easier to adopt in practice might be more valuable. The motivation of the current survey is to serve students and researchers who aim to investigate cryptocurrency security. It also intends to present some types of attacks that strongly impact cryptocurrency users and methods used by researchers to identify most attacks, as well as the results achieved by their research. The significant contributions of this study are presented in the following section.

We divided our work into several parts. First, we reviewed the blockchain network. Then, a taxonomy of several attacks on the cryptocurrency ecosystem was presented. We also compiled a list of several strategies for detecting these assaults and determined the most effective detection methods.

## 2. BLOCKCHAIN NETWORK

The blockchain used to secure digital currencies must be clarified; it does not require a third party, such as a bank or government. Therefore, how the blockchain works and how currencies are traded within this ecosystem should be highlighted. Figure 1 illustrates the journey of the transaction through the various components and participants in the bitcoin network. Each participant, such as the users or miners, has responsibilities and roles. Components, such as the node, wallet, transaction, memory pool, and block, represent the main elements of the transaction lifecycle. A distributed system based on a consensus mechanism is known as a blockchain system that ensures that the states of the specific data are approved by the dispersed nodes. A consensus algorithm is a critical component that determines how the system acts and how well it performs. Evidently, several types of consensus algorithms include PoW, proof of stake, and other algorithms [5].

Furthermore, different types of blockchain systems are entirely dependent on the consensus mechanisms used. Based on different blockchain deployment strategies and the application domains, the two common types of blockchain are public and private blockchain. A public blockchain, also known as the permissionless or unpermissioned, allows anyone to participate to create and validate blocks. Furthermore, it allows adjusting the state of the chain by storing and updating data through transactions between participants. A private blockchain has a restrictive concept compared with a public blockchain. A private blockchain called the permissioned blockchain indicates that only trusted and authorized businesses are allowed to participate in the blockchain operations [6]. Other types of blockchains are consortium and hybrid blockchains. Blockchain technology has progressed through four stages since the inception of the first blockchain system: blockchain 1.0, blockchain 2.0, blockchain 3.0, and blockchain 4.0.

- In the blockchain 1.0 stage, cryptocurrencies, such as bitcoin, litecoin, and dogecoin, employ blockchain technology.
- In the blockchain 2.0 stage, the blockchain technology is used to develop several applications. Ethereum is considered an example of the blockchain 2.0.
- In the blockchain 3.0 stage, the blockchain technology uses decentralized application (DApp).
- In the blockchain 4.0 stage, the blockchain is used in the industry.

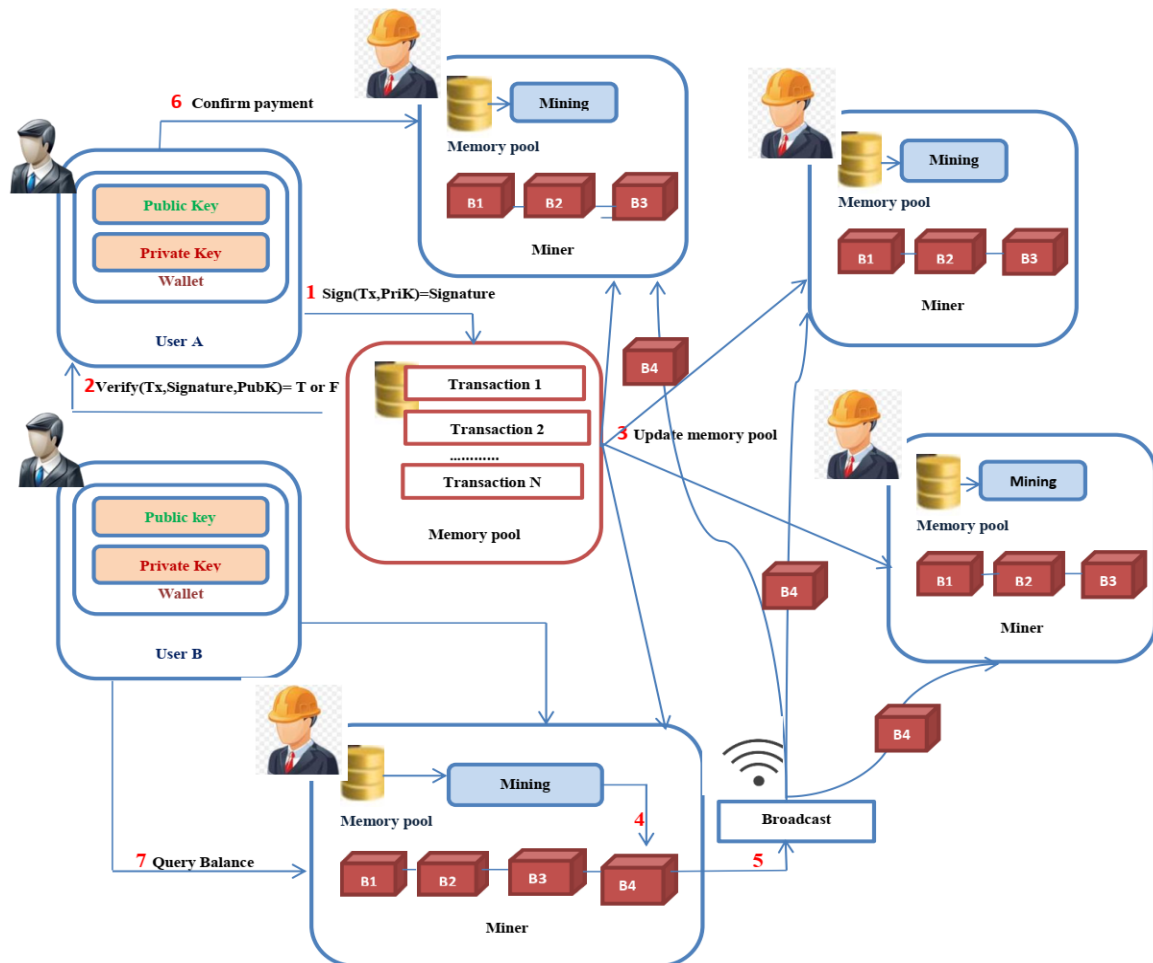


Figure 1. Transaction lifecycle [5]

### 3. RELATED WORK

Over the previous years, several studies on cryptocurrencies have been conducted, specifically with regard to attacks. The most recent methodologies and studies in the cryptocurrency ecosystem are discussed as follows. Scicchitano *et al.* [2] proposed an anomaly detection system based on a deep learning encoder–decoder model. On day 1255, a few days after the current attack, the network identifies a significant anomaly. A detailed examination of the circumstances surrounding the 51% attack reveals that a significant number of organizations, working on ethereum classic network (ETC), discovered the attack and decided to put a halt to their operations. The proposed model also detected the decentralized autonomous organization (DAO) attack.

Baek *et al.* [7] proposed a service-level and network-level model for assessing and identifying distributed denial of service (DDoS) attack of the bitcoin ecosystem. The researchers used principal component analysis (PCA) to perform feature extraction. They also applied multilayer perceptron (MLP). DDoS detection was achieved by dividing the training, validation, and testing sets into 6:2:2 ratios. They gathered statistical information including maximum, minimum, summation, and standard deviation. The accuracy of categorizing regular block data was approximately 70% and the accuracy of detecting DDoS attacks was approximately 50%, according to the findings.

Meanwhile, Iqbal and Matulevičius [8] believed that no mechanisms are currently in place to completely mitigate Sybil attack. However, few preventive measures are in place to focus on this attack. The node's computing power is monitored; thus, the computing power in the blockchain network is increased according to the available nodes in the network [9].

Furthermore, a study examined the use of bio-inspired computing in machine learning models to prevent insider threats and improve the model by automating the feature selection optimization process. They placed various swarm intelligence algorithms to the test, and the results show that they can improve the accuracy and speed of detecting malicious behavior in large data sets [10]. Lai *et al.* [11] presented a complete

overview of the many attack scenarios that the bitcoin network could face, the methods used to carry out the attacks, and reviews of the solutions and countermeasures proposed to combat these attacks. Finally, they summarized other security issues and offered additional improvements to the bitcoin network's security.

We searched through papers detailing various forms of attacks on various cryptocurrencies and did not limit our investigation to a single cryptocurrency. We have classified the attacks into four categories, and each category has been divided into many different types with detailed explanations. Furthermore, we estimated how these attacks were conducted, and presented the detection techniques that produced highly accurate results.

#### 4. CYBER ATTACKS IN CRYPTOCURRENCIES

The various types of attacks have been grouped into four main categories. The four main security concerns to cryptocurrencies are discussed in this section. These cyber-attacks were successful, resulting in substantial losses or the denial of cryptocurrency services. In all cases, the attacker must achieve sufficient utility to justify the essential cost of an attack. Figure 2 illustrates the taxonomy of attacks on the cryptocurrency.

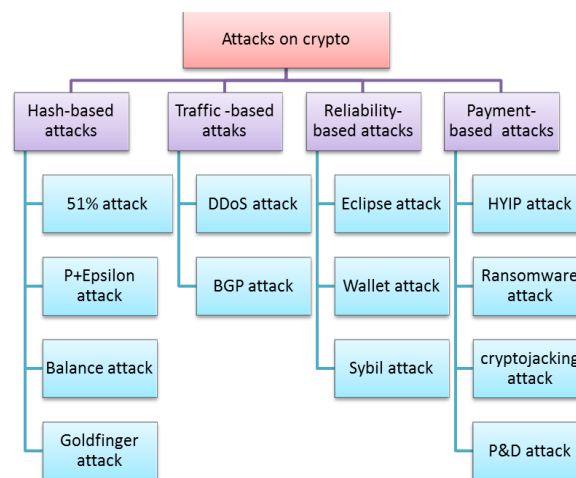


Figure 2. Taxonomy of attacks on cryptocurrency

##### 4.1. Hash-based attack

This attack entails gathering hash values and attempting to find the same hash value for various additional messages sent.

- 51% attack: this type of attack has an entirely negative effect on cryptocurrencies. A 51% attack occurs when a group of miners or an individual miner controls more than 50% of the network's mining hash or devices [12]. This form of threat starts with a private chain of blocks that is completely distinct from the genuine chain. Then, the separated chain is presented to the network to be formed as a genuine chain. By encouraging network nodes to follow their chain, attackers that achieve 51% or more hashing power can drive the longest chain. When mining power is less than 40%, then 51% attack can possibly occur but with a lesser probability, such as BTG [9].
- p+Epsilon attack: this type of attack takes advantage of the network participants' prevailing technique. A blockchain based in facts of PoW is typically vulnerable to this type of attack. When attackers grant participants a payout, a payment matrix is used to obtain an advantage, with the dominant strategy supporting the attacker's aim fulfillment. In light of this, the participants receive no remuneration, whereas the attacker obtains the full amount [13].
- Balance attack: it is a strategy that focuses on nodes with equally distributed mining power [14]. This form of attack can be used to double the amount of money spent on a PoW consensus. An attacker can delay messages on the Ethereum network by using their limited hashing power. This attack may be carried out with 5% of the hashing power accessible [9]. The attacker must initially identify the merchant-involved subgroup before launching transactions to purchase products from them. The attacker should send transactions to this subgroup and mine blocks to the remaining group nodes [15].
- Goldfinger attack: a majority attack, where the attacker is motivated by anything other than the cryptocurrency economy. Purchase of mining equipment, demand for rental (Nice Hash), and other indicators of dominance over the complete network hash rate can be observed. The goal of this attack is to bring down the entire system [16].

#### 4.2. Traffic-based attack

This attack can be classified into two categories, there are:

- DDoS attack: multiple systems overwhelm the resources and bandwidth of the targeted system in a DDoS attack. The target node refuses the transaction because the system is overloaded [12]. Attackers utilize DDoS to prevent authentic transactions from being completed so that invalid transactions can be carried out. On the contrary, DDoS attacks can only significantly limit network activity. DDoS attacks are dangerous because they overload centralized systems with additional traffic. A DDoS attack is supposed to overwhelm centralized servers, although the bandwidth required to overwhelm them are nearly unachievable in most circumstances. According to research, DDoS becomes more prevalent, and each attack costs businesses more than \$2 million.
- Border gateway protocol (BGP) hijacking: BGP hijacking is a technique in which an internet service provider (ISP) sends out bogus routing system announcements to redirect traffic. A routing attack is another name for it. In effect, the ability to undertake a double-spending attack is a conceivable result of this attack. If the attacker wants to hijack all of the traffic for a valid prefix  $p$ , then either: i) announce  $p$  or ii) announce a more specific prefix of  $p$ . In the first status, the attacker receives 50% of the traffic because BGP routers prefer shorter links. The longest-match entry is used by internet routers to forward data, and the attacker engages all traffic destined to the destination in the second status [17].

#### 4.3. Reliability-based attack

This attack can be classified into three categories, there are:

- Eclipse attack: the eclipse attack allows an attacker to control all the target's incoming and outgoing connections, effectively isolating the victim from the rest of the network's peers [18]. On Bitcoin's peer-to-peer network, the two types of eclipse attacks are botnet attack and infrastructure attack. Bots with distinct IP address ranges initiate the botnet attack. The infrastructure attack simulates the threat posed by a company, an ISP, or a nation-state with a large number of contiguous IP addresses [19].
- Wallet attack: a wallet can be controlled by a software application, a hardware device, or an internet service that holds the private and public keys linked with the user's addresses. To transact with a cryptocurrency, users must have control over their cryptocurrency wallets. An attack on a wallet service provider, its users, or wallet software can have a significant impact, culminating in large coin theft and a loss of trust in the entire system. Coinbase is an online cryptocurrency exchange and wallet that, different from single-coin wallets, allows users to possess and trade multiple cryptocurrencies from the same account [16]. Moreover, individual wallet user attacks can be carried out using various harmful techniques to steal user credentials and obtain access to their funds [20].
- Sybil attack: sybil attack is considered a type of reliability threat. It is a system node that manages several identities. Peer-to-peer networks rely on the concept of identity, in which each machine represents a single identity [21]. Douceur [22], a Microsoft researcher, was the first to bring the attack method to the world's attention. The attackers can establish many bogus nodes that look real to their peers. These bogus nodes contribute to network corruption by validating unlawful transactions and modifying valid transactions [9]. Even when the bitcoin blockchain network has a large number of nodes, resulting in a very expensive attack, whereas an opponent has a great number of network nodes, the possibilities of double spending increases.

#### 4.4. Payment-based attack

A number of attacks that use cryptocurrencies as a payment method include the following:

- High yield investment program (HYIP): HYIP is considered a fraudulent activity. Thus, obtaining bitcoin addresses linked to fraud to detect such illegal acts is crucial. Thus far, such actions have been identified by correlating bitcoin addresses with graph mining techniques [23]. According to certain studies, HYIPs account for 0.03 to 0.15% of smart contracts [24]. Other sources believed that HYIP using Ethereum is worth approximately half a million dollars [25].
- Ransomware attack: ransomware is evolving and improving harmful software that takes the shape of Crypto or Locker and is designed to attack and take control of critical infrastructure and computer systems [26]. Some examples include CryptoWall, Cryptolocker, Manamecrypt, and CryptoDefense [27]. A considerable increase is found in crypto-ransomware attacks, which encrypt individual files on a host or network-attached storage and demand a ransom in cryptocurrency [28].
- Cryptojacking attack: in cryptojacking, an attacker executes crypto mining software on the devices of unknown. The two most common attacks in malware code are: web browser-based crypto mining and installable binary crypto mining. Hoya, Japan's largest optical goods producer, shut down its production lines for three days as hackers attempted to set up an illegal cryptocurrency mining operation. A number

of illegal mining operations have already been found. “Bitcoin mining plot” has led to the arrest of Russian nuclear specialists [29].

- Pump & dump attack (P&D): P&D fraud is considered a market manipulation scheme that involves artificially increasing the price of a private security and then selling it to other investors at a much higher price [30]. At present, hundreds of cryptocurrencies occur, the market is unregulated, and prices are easily influenced. Therefore, pump and dumps are extremely typical in these securities. P&Ds are currently led by a significant number of personality internet groups, and the movement has gone viral, despite that it is still relatively unknown [31].

## 5. METHODOLOGIES FOR DETECTING CRYPTOCURRENCY ATTACKS

Cryptocurrency attacks can be detected in various approaches according to the type of attack, its severity, and its impact on the labor market. Table 1 [2], [23], [25], [29], [32]–[45] (in Appendix) highlights most types of attacks against some digital currencies, the detection methods used, the methods applied to evaluate the performance of each model, and the results obtained. This table shows the most common and influential attacks on the cryptocurrency ecosystem.

These techniques can be employed to create a more secure level for cryptocurrency networks with the possibility to detect and prove the specific types of malicious transactions. Importantly, the most common methods used for detecting attacks are machine learning and deep learning. Arguably, in artificial intelligence, machine learning is used to find the best solutions to complicated issues in information science.

## 6. DISCUSSION

In the world of cryptocurrency exchanges and stock trading that provide the speed of implementation to customers and users, any system can suffer from dangerous vulnerabilities related to concerns about security and privacy; thus, using blockchain technology is a robust option to secure services and platforms. However, most digital currencies are exposed to many security threats that cause denial of service or illegal use, such as money laundering. Therefore, these attacks and methods to detect them should be studied. This research presented many types of attacks and the various approaches to detect them.

The four primary attack types were identified, including hash-based, traffic-based, reliability-based, and payment-based attacks; each type comprises many attacks. Therefore, by knowing these types and their impact on digital currencies, we can select the smartest and fastest methods to detect them. One of the greatest challenges the researchers face is the DDoS attack; the methods used to detect it did not achieve high accuracy. Thus, the attack leaves the website inaccessible to the desired users. In practice, the results reached by most researchers show that the most dangerous attack is represented by 51% attack and the DDoS attack. Thus far, several events of 51% attacks have been registered on cryptocurrencies because making considerable amount of money using this method of assault is possible.

In general, all types of legal and illegal digital currencies fall under the umbrella of cryptocurrency. Cryptocurrencies represent danger to the economy, particularly those in the industrialized world, for various reasons. The most important of which is the rise in economic importance of cryptocurrencies to the point where they have become the primary mechanism for settling payments, particularly international exchanges, and the fear of capital flight from them, as well as the possibility of heavy losses. However, in light of the fact that these currencies are not backed by physical assets, they pose a risk.

Although the use of cryptocurrencies in terrorist financing has not grown significantly, anonymity makes them a financial means for people and organizations, as well as criminal and terrorist gangs, who receive payments that may expose them to terrorist financing sanctions. As a result, highlighting the most effective methods for detecting, reducing, and preventing cryptocurrency-related threats is critical. Therefore, our research included a diverse variety of attacks and detection methods. On these grounds, the requirement for cryptocurrency security methods may stimulate the development of better encryption solutions. Despite the current obstacles, the trends indicate a promising future for these currencies.

## 7. CONCLUSION

At present, many cryptocurrencies are vulnerable to cyber-attacks, where platforms of this cryptocurrency face security issues similar to other online businesses. In this study, we provided a thorough survey of the most important cyber-attacks on a cryptocurrency network. As a preliminary study, this research focuses on a summary of key cryptocurrency assaults and the strategies recommended to counter them. Machine learning represents a promising approach to solving complex cybersecurity problems. Therefore, most researchers have used machine learning in their experiments to detect many attacks affecting the cryptocurrency network. Many researchers have presented various approaches that focus on detection,

prevention, and traceback to prevent various attacks. Nonetheless, in detection systems, failure to recognize the limitations of real-time problems, complexity, data integration, and the absence of a regulatory central scope with the traditional cryptocurrencies are key challenges. Ultimately, we aim to expand our survey to include more sorts of cryptocurrency attacks in the future, as well as more detection methods of these attacks, with the aim of proposing new suitable detection mechanisms.

## APPENDIX

Table 1. Methods for detection of cryptocurrency attacks

No	Ref.	Published year	Attack type	Cryptocurrency	Detection or prevention methods	Result and performance measurements
1	[2]	2020	51% attack and DAO attack	ETC	RNNs as a neural encoder-decoder model	Recurrent autoencoder (RAE) model that effectively detect the publicly reported attack
2	[32]	2015	51% attack	Bitcoin	Continuous-time markov chains (CTMCs)	Results obtained are applicable for each state of the Bitcoin network
3	[7]	2019	DDoS attack	Bitcoin	MLP	DDoS attacks were detected with a 50% accuracy, whereas regular block data were identified with a 70% accuracy
4	[33]	2014	DDoS attack	Bitcoin	Word-based classifier	Using a confusion matrix, the accuracy of DDoS attack detection was approximately 75%
5	[34]	2019	Ransomware	Bitcoin	Bayesian belief network (BBN)	The accuracy of ransomware attack detection was approximately 97.5%
6	[35]	2019	P&D	Bitcoin	Random forest	Using LASSO regularized GML and balanced random forests, the likelihood of a currency being pumped with an area under the curve (AUC) of over 90% was predicted
7	[36]	2019	P&D	The model was applied to the full-time series of 172 coins	Extreme gradient boosting	The result was as: 99.5% AUC, 99.7% specificity, and 85.5% sensitivity, using the AUC
8	[37]	2019	Eclipse attack	Ethereum	Random forest	The precision rate is approximately 72%, and the recall rate is approximately 93%
9	[38]	2020	Eclipse attack	Bitcoin	Python-flask web framework and flask's default webserver	The gossip-based protocol provides multiple benefits while introducing a significantly improved detection time and low overheads, using Amazon AWS
10	[39]	2019	Cryptojacking attack	JSECoin and Monero	SVM classification model	97% TPR and 1.1% FPR
11	[40]	2022	Ransomware	Bitcoin	Rule-based algorithms	Accuracy of approximately 96.01%, recall of approximately 96%, precision of approximately 95.9%, and an F-measure of 95.6%, when metrics, accuracy, precision, sensitivity, and F-measure are employed
12	[41]	2019	Cryptojacking attack	Ethereum, Monero, and Zcash	Shared nearest neighbour (SNN) clustering algorithm	Using KNN classifier, 99.7% TPR, 46.1% FPR, 99.9% precision, and 99.7% recall
13	[42]	2019	Cryptojacking attack	Monero	Capsule network (CapsNet) technology	87% of the instances were detected immediately, and 99% of the instances were detected during a window of 11 seconds
14	[29]	2021	Cryptojacking attack	Bitcoin, Monero, and Bytecoin	Random forest	Using the mean square error (MSE) 94.1% TPR, 59% FPR, 99% of AUC for the ROC and 96% of F1-score
15	[43]	2019	HYIP threat	Bitcoin	Random forest	Accuracy of approximately 95% TPR and 4.9 FPR
16	[44]	2018	HYIP threat	Bitcoin	Random forest	Accuracy of approximately 97.9%, 96.8% TPR, 96.9% recall, and 97.9% specificity
17	[23]	2017	HYIP threat	Bitcoin	Random forest	Accuracy of approximately 83% TPR and 4.4% FPR
18	[25]	2018	HYIP threat	Ethereum	Extreme gradient boosting (XGBoost)	94% precision, 81% recall, and 86% F-score
19	[45]	2019	HYIP threat	Ethereum	Random forest	Accuracy of approximately 95% precision and 69% recall

## REFERENCES





- [1] K. Toyoda, T. Ohtsuki, and P. T. Mathiopoulos, "Time Series Analysis for Bitcoin Transactions: The Case of Pirate@40's HYIP Scheme," in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, IEEE, Nov. 2018, doi: 10.1109/icdmw.2018.00028.
- [2] F. Scicchitano, A. Liguori, M. Guarascio, E. Ritacco, and G. Manco, "A Deep Learning Approach for Detecting Security Attacks on Blockchain," in *Fourth Italian Conference on Cyber Security (ITASEC)*, Ancona, Italy: Fourth Italian Conference on Cyber Security (ITASEC), Jun. 2020, pp. 1–11.
- [3] S. Ghimire and H. Selvaraj, "A Survey on Bitcoin Cryptocurrency and its Mining," in *2018 26th International Conference on Systems Engineering (ICSEng)*, IEEE, Dec. 2018, doi: 10.1109/icseng.2018.8638208.
- [4] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/comst.2015.2494502.
- [5] F. Kausar, F. M. Senan, H. M. Asif, and K. Raahemifar, "6G technology and taxonomy of attacks on blockchain technology," *Alexandria Engineering Journal*, vol. 61, no. 6, pp. 4295–4306, Jun. 2022, doi: 10.1016/j.aej.2021.09.051.
- [6] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," *Journal of Network and Computer Applications*, vol. 182, p. 103035, May 2021, doi: 10.1016/j.jnca.2021.103035.
- [7] U.-J. Baek, S.-H. Ji, J. T. Park, M.-S. Lee, J.-S. Park, and M.-S. Kim, "DDoS Attack Detection on Bitcoin Ecosystem using Deep-Learning," in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, IEEE, Sep. 2019, doi: 10.23919/apnoms.2019.8892837.
- [8] M. Iqbal and R. Matulevicius, "Exploring Sybil and Double-Spending Risks in Blockchain Systems," *IEEE Access*, vol. 9, pp. 76153–76177, 2021, doi: 10.1109/access.2021.3081998.
- [9] S. Sayeed and H. M-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack," *Applied Sciences*, vol. 9, no. 9, p. 1788, Apr. 2019, doi: 10.3390/app9091788.
- [10] A. Nicolau, S. Shiaeles, and N. Savage, "Mitigating Insider Threats Using Bio-Inspired Models," *Applied Sciences*, vol. 10, no. 15, p. 5046, Jul. 2020, doi: 10.3390/app10155046.
- [11] L. Lai, T. Zhou, Z. Cai, Z. Liang, and H. Bai, "A Survey on Security Threats and Solutions of Bitcoin," *Journal of Cyber Security*, vol. 3, no. 1, pp. 29–44, 2021, doi: 10.32604/jcs.2021.016349.
- [12] N. Anita and M. Vijayalakshmi, "Blockchain Security Attack: A Brief Survey," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, IEEE, Jul. 2019, doi: 10.1109/iccncnt45670.2019.8944615.
- [13] N. A. Akbar, A. Muneer, N. ElHakim, and S. M. Fati, "Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses," *Future Internet*, vol. 13, no. 11, p. 285, Nov. 2021, doi: 10.3390/fi13110285.
- [14] C. Natoli and V. Gramoli, "The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example," *arXiv*, Dec. 30, 2016, doi: 10.48550/arXiv.1612.09426.
- [15] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.
- [16] S. Ramos, F. Pianese, T. Leach, and E. Oliveras, "A great disturbance in the crypto: Understanding cryptocurrency returns under attacks," *Blockchain: Research and Applications*, vol. 2, no. 3, p. 100021, Sep. 2021, doi: 10.1016/j.bcr.2021.100021.
- [17] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy (SP)*, IEEE, May 2017, doi: 10.1109/sp.2017.29.
- [18] A. Singh, T.-W. Ngan, P. Druschel, and D. S. Wallach, "Eclipse Attacks on Overlay Networks: Threats and Defenses," in *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, IEEE, 2006, doi: 10.1109/infocom.2006.231.
- [19] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse Attacks on Bitcoin's Peer-to-Peer Network," 24th USENIX Security Symposium (USENIX Security 15), 2015, pp. 129–144. Accessed: Apr. 18, 2023. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/heilman>
- [20] M. Guri, "BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, Jul. 2018, doi: 10.1109/cybermatics\_2018.2018.00227.
- [21] S. Shalini and H. Santhi, "A Survey on Various Attacks in Bitcoin and Cryptocurrency," in *2019 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, Apr. 2019, doi: 10.1109/iccsp.2019.8697996.
- [22] J. R. Douceur, "The Sybil Attack," in *Peer-to-Peer Systems*, Springer Berlin Heidelberg, 2002, pp. 251–260, doi: 10.1007/3-540-45748-8\_24.
- [23] K. Toyoda, T. Ohtsuki, and P. T. Mathiopoulos, "Identification of High Yielding Investment Programs in Bitcoin via Transactions Pattern Analysis," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*, IEEE, Dec. 2017, doi: 10.1109/glocom.2017.8254420.
- [24] E. Badawi and G.-V. Jourdan, "Cryptocurrencies Emerging Threats and Defensive Mechanisms: A Systematic Literature Review," *IEEE Access*, vol. 8, pp. 200021–200037, 2020, doi: 10.1109/access.2020.3034816.
- [25] M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, "Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact," *Future Generation Computer Systems*, vol. 102, pp. 259–277, Jan. 2020, doi: 10.1016/j.future.2019.08.014.
- [26] A. M. Maigida, S. M. Abdulhamid, M. Olalere, J. K. Alhassan, H. Chiroma, and E. G. Dada, "Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms," *Journal of Reliable Intelligent Environments*, vol. 5, no. 2, pp. 67–89, May 2019, doi: 10.1007/s40860-019-00080-3.
- [27] A. Zimba, Z. Wang, and H. Chen, "Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems," *ICT Express*, vol. 4, no. 1, pp. 14–18, Mar. 2018, doi: 10.1016/j.icte.2017.12.007.
- [28] S. Maniath, P. Poornachandran, and V. G. Sujadevi, "Survey on Prevention, Mitigation and Containment of Ransomware Attacks," in *Communications in Computer and Information Science*, Springer, Singapore, 2019, pp. 39–52, doi: 10.1007/978-981-13-5826-5\_3.
- [29] M. Caprolu, S. Raponi, G. Oligeri, and R. D. Pietro, "Cryptomining makes noise: Detecting cryptojacking via Machine Learning," *Computer Communications*, vol. 171, pp. 126–139, Apr. 2021, doi: 10.1016/j.comcom.2021.02.016.
- [30] D. Kramer, "The Way It Is and the Way It Should Be: Liability Under §10(b) of the Exchange Act and Rule 10b-5 Thereunder for Making False and Misleading Statements as Part of a Scheme to 'Pump and Dump' a Stock," *University of Miami Business Law Review*, vol. 13, no. 2, p. 243, Jul. 2005.







- [31] M. L. Morgia, A. Mei, F. Sassi, and J. Stefa, "The Doge of Wall Street: Analysis and Detection of Pump and Dump Cryptocurrency Manipulations," *ACM Transactions on Internet Technology*, vol. 23, no. 1, pp. 1–28, Feb. 2023, doi: 10.1145/3561300.
- [32] M. Bastiaan, "Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin," University of Twente, University of Twente: 22 nd Twente Student Conference on IT, 2015, pp. 1–10.
- [33] M. Vasek, M. Thornton, and T. Moore, "Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem," in *Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, 2014, pp. 57–71, doi: 10.1007/978-3-662-44774-1\_5.
- [34] P. S. Goyal, A. Kakkar, G. Vinod, and G. Joseph, "Crypto-Ransomware Detection Using Behavioural Analysis," in *Reliability, Safety and Hazard Assessment for Risk-Based Technologies*, Springer, Singapore, 2019, pp. 239–251, doi: 10.1007/978-981-13-9008-1\_20.
- [35] J. Xu and B. Livshits, "The Anatomy of a Cryptocurrency Pump-and-Dump Scheme." arXiv:1811.10109, Aug. 17, 2019, doi: 10.5555/3361338.3361450.
- [36] F. Victor and T. Hagemann, "Cryptocurrency Pump and Dump Schemes: Quantification and Detection," in *2019 International Conference on Data Mining Workshops (ICDMW)*, IEEE, Nov. 2019, doi: 10.1109/icdmw.2019.00045.
- [37] G. Xu *et al.*, "Am I eclipsed? A smart detector of eclipse attacks for Ethereum," *Computers and Security*, vol. 88, p. 101604, Jan. 2020, doi: 10.1016/j.cose.2019.101604.
- [38] B. Alangot, D. Reijbergen, S. Venugopalan, and P. Szalachowski, "Decentralized Lightweight Detection of Eclipse Attacks on Bitcoin Clients," in *2020 IEEE International Conference on Blockchain (Blockchain)*, IEEE, Nov. 2020, doi: 10.1109/blockchain50366.2020.00049.
- [39] A. Kharraz *et al.*, "Outguard: Detecting In-Browser Covert Cryptocurrency Mining in the Wild," in *The World Wide Web Conference*, ACM, May 2019, doi: 10.1145/3308558.3313665.
- [40] H. S. Talabani and H. M. T. Abdulhadi, "Bitcoin Ransomware Detection Employing Rule-Based Algorithms," *Science Journal of University of Zakho*, vol. 10, no. 1, pp. 5–10, Jan. 2022, doi: 10.25271/sjuoz.2022.10.1.865.
- [41] A. Zimba, C. Ngongola-Reinke, M. Chishimba, and T. F. Mbale, "Demystifying Cryptocurrency Mining Attacks: A Semi-supervised Learning Approach Based on Digital Forensics and Dynamic Network Characteristics," *Zambia ICT Journal*, vol. 5, no. 1, pp. 1–7, May 2021, doi: 10.33260/zictjournal.v5i1.108.
- [42] R. Ning, C. Wang, C. Xin, J. Li, L. Zhu, and H. Wu, "CapJack: Capture In-Browser Crypto-jacking by Deep Capsule Network through Behavioral Analysis," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, IEEE, Apr. 2019, doi: 10.1109/infocom.2019.8737381.
- [43] K. Toyoda, P. T. Mathiopoulos, and T. Ohtsuki, "A Novel Methodology for HYIP Operators' Bitcoin Addresses Identification," *IEEE Access*, vol. 7, pp. 74835–74848, 2019, doi: 10.1109/access.2019.2921087.
- [44] M. Bartoletti, B. Pes, and S. Serusi, "Data Mining for Detecting Bitcoin Ponzi Schemes," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, IEEE, Jun. 2018, doi: 10.1109/cvcbt.2018.00014.
- [45] W. Chen, Z. Zheng, E. C.-H. Ngai, P. Zheng, and Y. Zhou, "Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum," *IEEE Access*, vol. 7, pp. 37575–37586, 2019, doi: 10.1109/access.2019.2905769.

## BIOGRAPHIES OF AUTHORS



**Amenah Abdulabbas Almamoori**     is a Ph.D. student at the College of Information Technology, Department of Information Networks, University of Babylon, Iraq. She received her master's degree in Computer Science (M2R) from the Faculty of Sciences, University of Paris11, France. She also received an internship at Télécom SudParis (TSP) and Laboratoire de Recherche en Informatique (LRI) in France as the graduation requirement for a master's degree. Currently, her research interests are security of cryptocurrency and computer networks. She can be contacted at email: amenah.net.phd@student.uobabylon.edu.iq.



**Wesam S. Bhaya**     received his Ph.D. degree from the Iraqi Commission for Computers and Informatics, Iraq, in 2004. He is a Professor with the Faculty of Information Technology and the Head of the Information Security Department, University of Babylon, Babil, Iraq. His current areas of interest include operating systems, computer networks, SDN, computer security, and wireless communication systems, with an emphasis on network and service management. He participated in different program panels and has contributed to more than 50 articles. He can be contacted at email: wesambhaya@uobabylon.edu.iq.