Computer Systems Science & Engineering
DOI:10.32604/csse.2022.017941
Review

Tech Science Press

Intrusion Detection Systems Using Blockchain Technology: A Review, Issues and Challenges

Salam Al-E'mari[1], Mohammed Anbar[1,*], Yousef Sanjalawe[1,2], Selvakumar Manickam[1] and Iznan Hasbullah[1]

[1]National Advanced IPv6 Centre of Excellence (NAv6), Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
[2]Computer Sciences Department, Northern Border University (NBU), 9280 NBU, Ar'ar, the Kingdom of Saudi Arabia
[*]Corresponding Author: Mohammed Anbar. Email: Anbar@usm.my
Received: 18 February 2021; Accepted: 18 April 2021

Abstract: Intrusion detection systems that have emerged in recent decades can identify a variety of malicious attacks that target networks by employing several detection approaches. However, the current approaches have challenges in detecting intrusions, which may affect the performance of the overall detection system as well as network performance. For the time being, one of the most important creative technological advancements that plays a significant role in the professional world today is blockchain technology. Blockchain technology moves in the direction of persistent revolution and change. It is a chain of blocks that covers information and maintains trust between individuals no matter how far apart they are. Recently, blockchain was integrated into intrusion detection systems to enhance their overall performance. Blockchain has also been adopted in healthcare, supply chain management, and the Internet of Things. Blockchain uses robust cryptography with private and public keys, and it has numerous properties that have leveraged security's performance over peer-to-peer networks without the need for a third party. To explore and highlight the importance of integrating blockchain with intrusion detection systems, this paper provides a comprehensive background of intrusion detection systems and blockchain technology. Furthermore, a comprehensive review of emerging intrusion detection systems based on blockchain technology is presented. Finally, this paper suggests important future research directions and trending topics in intrusion detection systems based on blockchain technology.

Keywords: Blockchain; intrusion detection system; network security; malicious attacks

1 Introduction

Blockchain is an emerging technology that underlies the infrastructure of Bitcoin. In 2008, Nakamoto discovered blockchain's potential to be used in other domains, thus making Bitcoin the first of blockchain's many implementations. Blockchain technology has been increasingly used in different fields, especially in the security field, which has an important presence in different network environments, such as traditional networks, the Internet of Things (IoT), and cloud computing. Blockchain technology has many features

that may enhance network security. Its most important feature is that it works with decentralized and distributed environments; therefore, it does not need a trusted third party to manage the network. Blockchain technology has been applied to cryptocurrency networks, wherein the blockchain provides cryptocurrency its basic infrastructure, which allows financial operations to be performed in a secure manner and be distributed within networks.

Currently, there are many different types of digital currencies, such as Bitcoin, Litecoin, Ethereum, and Ripple, which have been built into a new durable ecosystem and may be integrated with different network types. Recently, these network environments have been suffering from a critical challenge related to detecting attacks because different types of cyberattacks rely on the complexity of the networks' infrastructure. Therefore, traditional intrusion detection systems (IDSs) are unable to detect blockchain-related attacks. Researchers thus intend to use blockchain technology to enhance IDSs and improve attack detection.

The main contribution of this paper is to provide a comprehensive analysis of blockchain-based IDSs. This review will accomplish the following:

- Present an overview of blockchain technology and its importance, and introduce the advantages of and threats to blockchain;
- Discuss and analyze existing blockchain-based IDSs to provide a clear analysis of the current works conducted in this field;
- Compare and analyze the proposed techniques to highlight current research gaps;
- Provide future research directions and open research issues concerning IDSs based on blockchain.

This review is scientifically significant because it allows researchers to analyze blockchain's role in IDSs by providing them with a clear view of the advantages, threats, and opportunities that result from using blockchain in IDSs.

This review is organized as follows. Section 2 provides a comparison with existing reviews in the same field, Section 3 presents an overview of the structure, basic applications, and characteristics of blockchain, Section 4 presents an overview of IDS types, techniques, performance measurements of IDS, Related models of IDSs based on blockchain are discussed in Section 5; Future research directions are presented in Section 6, and Section 7 concludes this review.

2 Comparison with Exiting Reviews

Some reviews have been conducted to address security issues in IDSs using blockchain technology. For instance, Kolekar et al. [1] conducted an overview of blockchain technology and IDS showing the integration between blockchain and IDS. Meanwhile, Shreevyas et al. [2] discussed the usage of blockchain in IDSs as a trusted technique used to detect cyberattacks. In addition, Meng et al. [3] discussed the usage of blockchain technology in a collaborative IDS. This review presented a general background of blockchain technology and IDSs and discussed the challenges of using blockchain-based IDS. Lastly, this review concluded that blockchain technology cannot handle all IDS issues.

Furthermore, Wang et al. [4] conducted a review to discuss the role of blockchain technology in IoT applications; they focused on blockchain-based IoT applications, and compared them. Khan et al. [5] reviewed IoT security limitations and discussed blockchain technology as a potential emerging for solving security issues in IoT architecture. Other similar surveys have investigated the impact of using blockchain-based IDS in the IoT [6,7]; they summarized existing research security challenges that IoT architecture and blockchain-based Internet services suffer from. A more elaborate survey was presented by Sengupta et al. [8] to determine how blockchain technology handles security challenges effectively in

the IoT and Industrial Internet of Things. Ultimately, the majority of existing reviews focus on the challenges or advantages of using blockchain technology in the security field [9].

To summarize and illustrate how the present review is different from the existing reviews, Tab. 1 presents a comparison of discussed topics. At the time of writing this review and according to the comparative analysis conducted in Tab. 1, there is no comprehensive review highlighting a taxonomy of blockchain-based IDS, challenges, results, applications, and research trends. We can also find that the present review is more universal than former related reviews conducted in the same area.

Table 1: Comparison with several existing reviews

Ref. of review	Blockchain review	IDS review	Criteria-based taxonomy	Analysis of models	Research issues	Comparison with prior reviews
[2]	✓	✓	×	×	✓	×
[3]	✓	✓	×	×	✓	×
[4]	✓	×	×	×	✓	×
[5]	✓	×	×	×	✓	×
[6]	✓	×	×	×	✓	×
[7]	✓	×	×	×	×	✓
[8]	✓	×	×	×	✓	✓
[9]	✓	×	×	×	×	×
Proposed review	✓	✓	✓	✓	✓	✓

3 Overview of Blockchain

As aforementioned, blockchain technology was introduced by Nakamoto in 2008 as an underlying technology for Bitcoin to record all transactions of Bitcoin and to create security against potential attacks [10]. Fig. 1 presents blockchain's roadmap from 2008 to 2019. Bitcoin's initial infrastructure based on blockchain technology appeared in 2009 over a peer-to-peer (P2P) network, which is called the Bitcoin network. Since then, cryptocurrencies have gained worldwide attention, and researchers have harnessed and applied blockchain technology to domains, such as smart contracts and supply chain management. This evolution has occurred because blockchain is autonomous, distributed, immutable, and contractual [11,12].

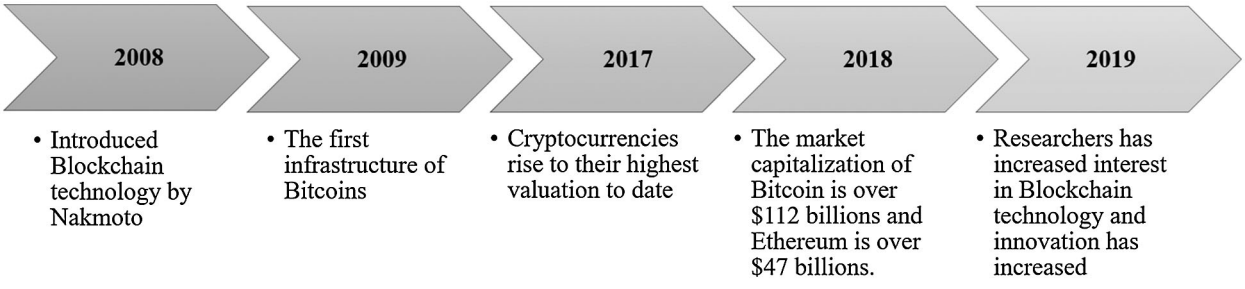

Figure 1: Roadmap of blockchain technology

3.1 Blockchain Structure

A blockchain is a linked-data structure wherein each block has two main sections: a header and body. The header section consists of a nonce, a previous hash, a Merkle root hash, a timestamp, and a difficulty target. The body section contains a list of transactions. Fig. 2 presents the structure of a blockchain. The first block is always called a genesis, all blocks are linked together via cryptography, and blocks are distributed between nodes over a network [12].

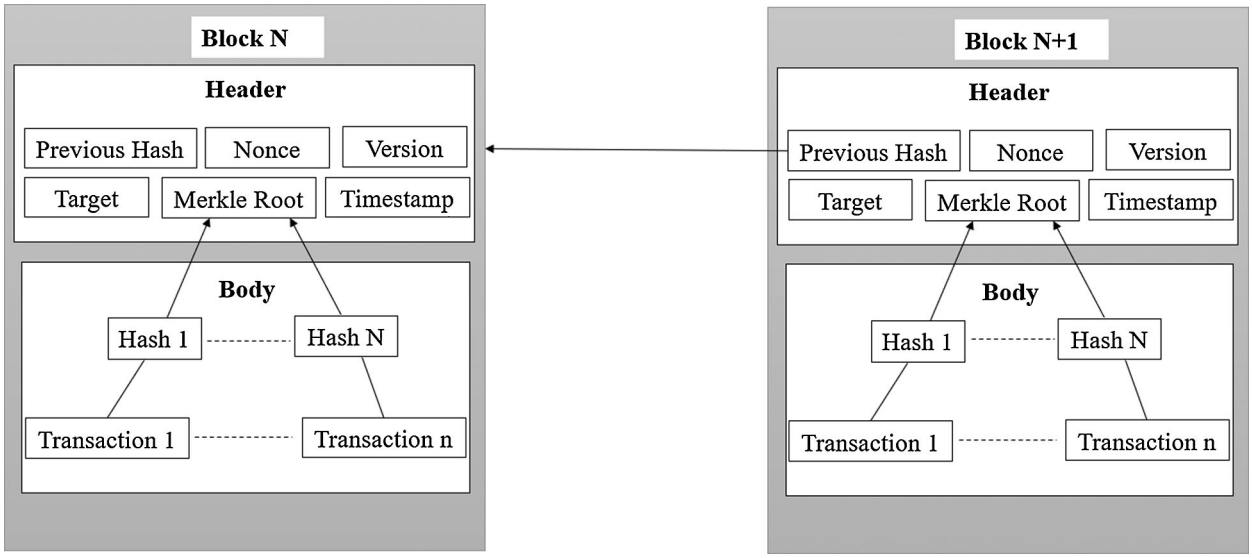

Figure 2: Blockchain structure

Furthermore, to adhere to the rules of blockchain technology, all nodes in the blockchain network must have the same block list, which is presented in Fig. 3. When a new block is added, it broadcasts to all nodes in the network. Each node verifies the new block through a consensus mechanism that confirms a transaction in the block. There are various consensus algorithms to ensure that all nodes have the same blockchain list, such as proof of work and proof of stake [13,14].

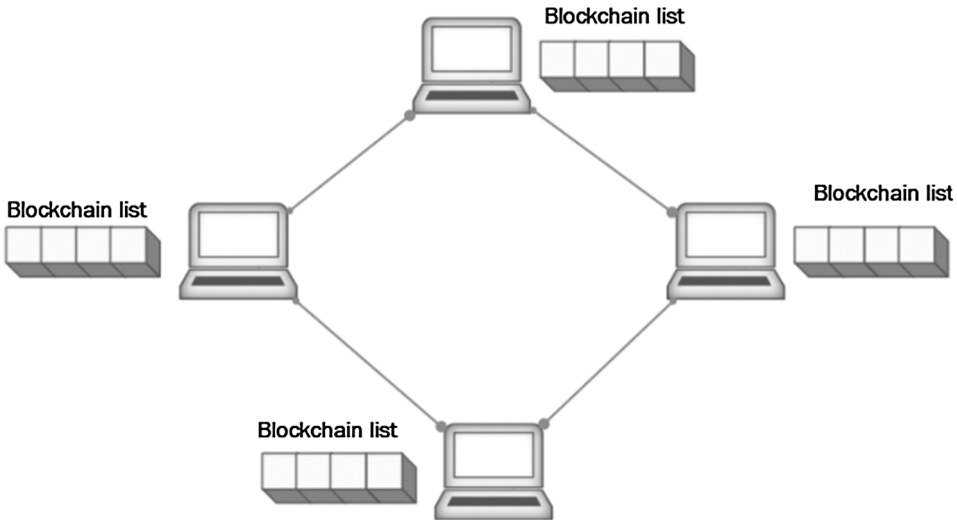

Figure 3: Over P2P network

3.2 Basic Principles of Blockchain Technology

There are many principles of blockchain technology that are applied to three main layers: the network, data, and application layers. First, the network layer is compatible with the P2P network architecture, which supports decentralized connections and distributed network mechanisms. The network layer is responsible for forwarding and verifying data between nodes. In addition, blockchain technology stores the same chain in all nodes over a network; thus, all nodes are synchronized. Therefore, when a new block is generated, it is then verified by a consensus algorithm. If the new block is valid, then it broadcasts to all other nodes. Otherwise, it is discarded. In addition, there are several types of consensus algorithms that all operate on two principles: (i) the freshness principle achieves fair competition through fresh resources for each new block that is added, and (ii) the unpredictability principle prevents any participant from predicting which node will create a new block. Tab. 2 illustrates some of the consensus algorithms that are used in blockchain networks [15,16].

Table 2: Examples of consensus algorithms

Algorithm	Description	Advantage	Disadvantage
Proof-of-Work (PoW)	PoW is widely used in blockchain verification to validate data in complex mathematical computation. The first node solves the crypto puzzle, then it adds a new block that will be verified later, by using existing-verified nodes in the network.	Verification technique for PoW is extremely efficient	High power consumption
Proof-of-Stake(PoS)	PoS selects participants based on their stake cryptocurrency	It reduces energy consumption in PoW, and it is efficient for large-scale networks.	It suffers from DoS attack, and there is a lack of synchronization between participants.
Proof-of-Elapsed time (PoET)	Randomly, it generates waiting time slots for each participant, while user who has a less waiting time will be added into a new block.	It consumes less energy than PoW. Also, it ensures freshness and unpredictability principles.	It does not indicate how the algorithm can solve the conflict. Also, its voting approach is very complicated.
Proof-of-Space (PoSp)	A verifier requests from the prover to reserves a disk-space to store necessary information, then a prover sends to the verifier to ensure reserving that disk-space.	It reduces power consumption, which makes it more difficult for malicious participants to join network.	Producing a new block is difficult; therefore, it is challenging in solving the distributed consensus problem.
Practical Byzantine Fault	There are three sequential steps required to add a new block to chain successfully, namely: (i) new round, (ii)	It can handle a third pernicious network. No need for the miner; thus,	The node cannot join network before verifying it by the whole network.

(Continued)

Table 2 (continued).

Algorithm	Description	Advantage	Disadvantage
Tolerance (PBFT)	prepare, and (iii) commit, where each step is executed after getting two- thirds voting from nodes in the network.	it reduces energy consumption efficiently.	
Ripple	Participants either server or clients in the network. Client transfers transaction, where the server has a unique node list that calculates the percentage of agreement, if it reaches 80% then the transaction will be added into a ledger.	If value of unique node list is less than 20%, then it maintains the network from invalid nodes. It has no miner; therefore, it reduces energy consumption efficiently.	It does not deal with transactional anonymity.

Second, the data layer presents the data structure of the block. Blocks contain data or transactions that do not exceed several megabytes in size. Each block is linked together by a previous hash field through a miner. When a block solves a cryptographic puzzle and obtains the previous hash, a new block is appended to the end of the chain. Furthermore, each block has several fields, which are described in Tab. 3. The data layer also concerns user authentication and transaction encryption. Each user has a public key to validate authentications, and this key is visible to anyone in the blockchain network. Digital signatures are used to verify miners' transactions, and all validated transactions are kept in a public ledger [12,17].

Table 3: Fields of block structure in blockchain

Field	Description
Version	It is the identification rules used by the protocol.
Timestamp	It records the time required for creating a block, and it is used for ensuring the traceability.
Previous Hash	It indicates the previous block used for linking the current block with the chain.
Target (nBit)	It is used by consensus algorithms to define the difficulty level of their mechanism.
Nonce	It is calculated by the miner to generate a hash block, while it should be a unique number and leading by zeros.
Merkle Root	It includes all hashes values of legitimate transactions.
Hash	Hashing transaction occurs by Merkel tree, where each node is related with its parent node; therefore, if the transaction is modified, then it will affect all hash tree from the leaf node to the Merkle root, respectively.

Finally, the application layer is responsible for interacting with users, whether they are programmers or end-users. The application layer can be classified into two different layers. The first layer is meant for developers to build and test the application's code and is called the fabric layer. The second layer is the application layer, which allows end-users who use applications as a black box to perform specific tasks without knowing the details of the code [18].

3.3 Blockchain's Applications

As shown in Fig. 4, numerous industry sectors have used blockchain technology: the financial, healthcare, and cybersecurity sectors, and more [19,20]. Blockchain's features are what make blockchain a charming technology for industries and researchers. Initially, blockchain was applied in the financial field to manage transactions directly between financial institutions without any intermediaries. Therefore, blockchain can enhance business interactions and operational procedures.

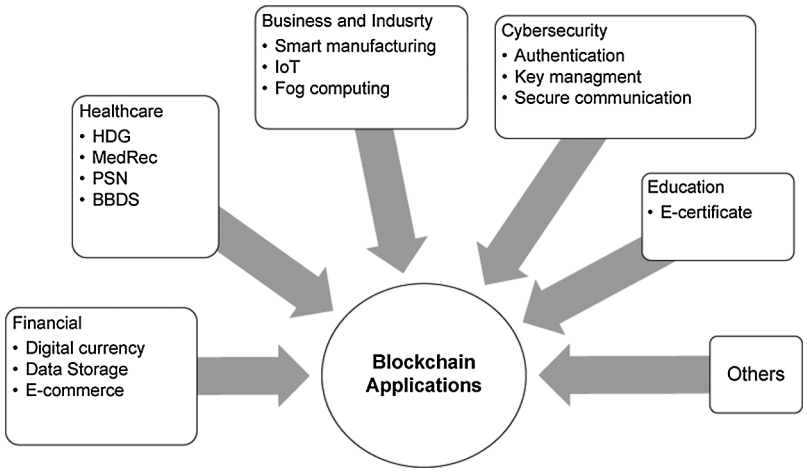

Figure 4: Blockchain applications[1]

Financial Applications: The initial use for blockchain was in cryptocurrency to provide cheaper, faster, more flexible, and more secure payment services than existing international payment methods [21]. In 2016, Bitcoin's capital market reached 10 billion dollars without the need for third parties, and all of its transactions were stored in a secure manner [15]. Therefore, there are several applications for blockchain to develop financial services and support digital currency investments.

Healthcare Applications: Blockchain technology offers the healthcare management system a way to store and process medical records over a network without disclosing patients' privacy or being modified by cyberattacks. Furthermore, it ensures data integrity and medical record accountability [22]. Blockchain technology provides several other potential benefits for healthcare systems, such as decentralization, health data ownership, and robustness. However, a blockchain-based healthcare management system would need to be developed. For instance, developing blockchain-based electronic medical records means that health or personal records would need to be shared over a network. Smart contracts have been found to be suitable for storing and managing medical records as they ensure security and privacy features. Other challenges include the fact that electronic medical records have no standards, and that the healthcare system has an enormous volume of data [23].

[1] HDG: healthcare data gateway. PSN: application of pervasive social network, MedRec: is a distributed ledger protocol. BBSD: blockchain-based data sharing for electronic medical records in cloud environments.

Business and Industry Applications: Blockchain technology has been applied to the business and industry sectors, which has led to the term "smart manufacturing." This means that industries can share goods over a network in a secure, decentralized, and self-regulating way [19]. Moreover, IoT ecosystem-based blockchain technology has been applied to IoT devices (smartphones, vehicular networks, smart cities, and so forth), and has led users to solve issues such as managing data and keeping it private [24].

Cybersecurity Applications: Cybersecurity encompasses various aspects of online security, such as applications, networks, and information. In addition, cybersecurity deals with different architectures, such as the IoT and cloud. The main goal of cybersecurity is to detect and protect systems from cyber-attacks. Blockchain's characteristics allow the implementation of cybersecurity systems, thus solving key issues such as decentralized distributed domain name services, keyless signature infrastructure, and secure data storage. Recently, numerous applications have begun to adopt and rely on blockchain-based cybersecurity [20].

Education Applications: Blockchain technology has been applied to online education, which has several advantages for teachers, students, and institutions. A teacher can add a block of student information to the chain, or institutions can manage certification in a secure way through digital infrastructures. Furthermore, blockchain technology offers features that can collect and analyze data and generate reports about all entities in a given institution. Blockchain technology provides security in education because it achieves confidentiality, integrity, and availability, and it enables controlled access to students' information. In addition, it has enhanced accountability, authentication, performance, trust, and interoperability. However, it suffers from several limitations, such as scalability, type of security, and privacy issues [25,26].

Other Fields: Several additional fields have integrated blockchain technology into their systems. For instance, e-governments allow governments and citizens to interact, and smart contracts implemented on blockchain infrastructure can increase level of Quality-of-Services (QoS). Moreover, these fields established a decentralization-based blockchain database to ensure transparency, accessibility, and other important QoS features. Blockchain technology has also been applied to the energy field. There are many applications for blockchain technology that support energy management, such as increasing the security of the energy grid and supporting the energy trade [27].

In summary, blockchain is useful for decentralized applications in P2P networks. Furthermore, the trust and security that blockchain technology solves some main problems of cybersecurity. However, blockchain technology is not an optimal solution for all industries because it still has some challenges. For instance, traditional databases are at the core of some industries and provide fast and robust tools for many applications [28]. Therefore, the next section discusses the benefits of blockchain as well as the main challenges and threats it faces. Fig. 5 presents the percentage of the use of blockchain technology in different sectors' operations.

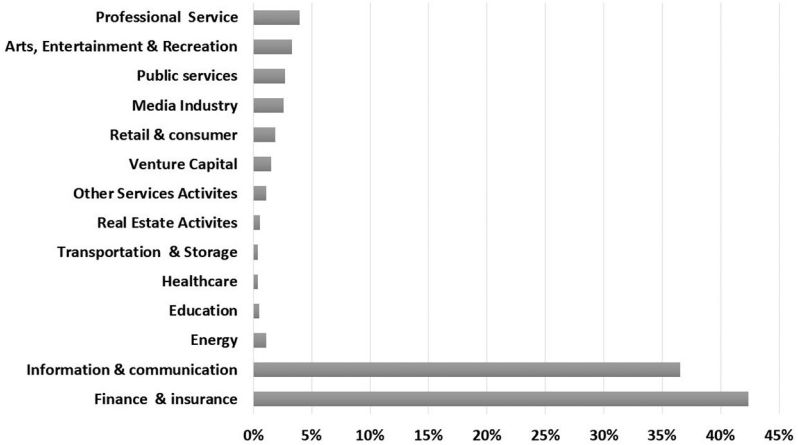

Figure 5: Percentage of different domains using blockchain

3.4 Blockchain's Benefits, Challenges, and Threats

Blockchain technology provides several benefits to its users. Some of these benefits are summarized below in Tab. 4. The main advantage of blockchain is its decentralization feature. Decentralization means that there is no need for third parties and that all participants make decisions about the information contained in a network [29].

Table 4: Benefits of blockchain

Benefit	Description
Decentralization	The nodes might share transactions between themselves without the need for central point.
Empowered Users	Users have a full privilege and permission to manage their transactions before adding them into a blockchain list, while those users can only read their transactions after adding them into a blockchain list.
High-quality data	Data in a blockchain is available over different nodes consistently. It is characterized by its accurateness and freshness.
Reliability and Robustness	Blockchain's nodes resist against any malicious attack since it is a decentralized network.
Trust	No need for a third-party in blockchain to allow users to share their transactions in a trusted manner.
Immutable	No one can modify transactions in a blockchain once they were added into a blockchain list.
Simple Ecosystem	Only one ledger is required for each blockchain network.
Availability	The user can create transactions anytime.
Few Fees	Blockchain reduces the cost of transactions by avoiding third parties.
Efficiency	Transactions occur quickly and automatically.
Auditability	Authorized participants can audit transactions in a blockchain.
Traceability	Authorized participants can track any transaction easily.
Transparency	Blockchain provides transparent transactions to ensure a consistent relationship between parties instead of doing a negotiation.
Security	Blockchain uses a complex cryptographic for each transaction and block.

Despite the benefits gained from using blockchain technology, it still suffers from several challenges. Some of these challenges are presented below in Tab. 5 [30].

Although blockchain technology provides reliable and comfortable services for transactions executed over a network, the blockchain list itself faces different security issues. Therefore, it is important to take these issues into consideration. Tab. 6 outlines the main threats that blockchains may face [31–33].

This comprehensive overview of blockchain technology shows that it will revolutionize numerous fields in the future. Although it has some challenges, blockchain has various advantages, such as enhancing IDS performance.

Table 5: Fields of block structure in blockchain

Challenge	Description
Energy Consumption	The miner is responsible for adding any new block in a blockchain; thus, it consumes power to validate the expanding volume of transactions.
Signature Verification	Signature transaction requires a complex cryptographic calculation in a blockchain.
Slow	Any Blockchain's block must be encrypted and verified, then it should be broadcasted over networks.
High Cost	While the cost of initial capital in Blockchain is extremely high, holding a huge volume of transactions also consumes energy; therefore, the overall cost of maintaining each transaction will be increased.
Scalability	Because of the Blockchain has an immutable nature, nodes cannot delete any block from the chain; therefore, the blockchain size is increased over time incrementally.

Table 6: Main threats in Blockchain

Threat	Description
51% Attack	One or group of miners consumes more than the half of available computational power.
Fork Problem	Multiple new blocks are added to the old blocks in the chain; therefore, transactions processing capability might be affected negatively.
Consensus Delay	Inserting false block or DDoS attacks into a blockchain to make a consensus delay.
Identity Theft	Unauthorized participant stoles the private key, while no third-party can recover it. As a result, blockchain network goes down.
Selsh Mining	Attacker generates invalid block, then a miner cannot publish a valid block into the rest of network.

4 Intrusion Detection System

The IDS is a device or software that, through the use of different detection approaches, can detect an attack on a system and then send a notification or report to the system's administrator when it detects such an attack. The IDS may be a single device that observes a stand-alone system or a network system that performs local analysis to detect attacks. Furthermore, IDSs provide the three most important security services: (i) data confidentiality, which checks if the data is stored in a secure place in the system; (ii) data availability, which checks if data are available for an authorized user; and (iii) data integrity, which checks if data are correct and consistent with other data in the system [34].

4.1 IDS Types

Network-based intrusion detection system (NIDS) and the host-based intrusion detection system (HIDS) are stand-alone IDSs. To enhance the performance of IDSs in large IT ecosystems, multiple detectors have been used to correlate alerts and exchange knowledge; these detectors are called collaborative intrusion detection systems (CIDSs). CIDSs come in three different network architectures: centralized, hierarchical, and distributed [35]. Fig. 4 presents the IDS classifications. A centralized CIDS uses several IDSs to monitor the network, wherein each IDS connects and shares data with a single analysis unit. Hierarchical

and decentralized CIDSs also use several IDSs, but analysis units connect in a heretical structure to monitor multiple points in the network. A decentralized CIDS can overcome the single point of failure problem. Meanwhile, a distributed CIDS is a P2P network architecture in which each participant has an analysis unit and shares information with others in a distributed manner [36,37].

4.2 IDS Detection Techniques

The most well-known IDS approaches are signature and anomaly. The signature approach tries to detect attacks through the mapping between signatures (i.e., patterns or rules) in the database. Although it can detect known attacks easily, this approach suffers because it cannot detect a new attack with no known patterns or rules. Conversely, the anomaly approach can detect unknown attacks by monitoring the system's behavior. The anomaly approach finds abnormal activities and generates an alarm for the network administrator. Although this approach can detect unknown attacks, it may send false positive alarms. Each approach employs several techniques, as shown in Fig. 5.

Pattern Matching: Pattern matching compares new strings that enter the system with strings in the system's database to verify that there is no malicious attack occurring. If there is any matching pattern, then the system detects an attack and will generate an alarm; if there is no matching pattern, then no attack is detected. There are two kinds of pattern matching algorithms: single and multiple. Single pattern matching algorithms are simple because they search for one pattern at a time. Multiple pattern matching algorithms search for all patterns at the same time, require more time and resources [38,39]. A popular pattern matching algorithm applied to IDSs is the Boyer–Moore single pattern algorithm compares strings from the rightmost character. Although it has achieved the best performance in searching operations, the Boyer–Moore algorithm does not have feature scalability. Meanwhile, the Aho–Corasick and Wu–Manber algorithms are multiple pattern matching algorithms that search for more than one pattern simultaneously; however, the Aho–Corasick algorithm requires more memory than the Wu–Manber algorithm [40]. Pattern matching algorithms have a trade-off between their search speed and consumed memory. Some researchers have proposed ways to optimize these algorithms, while others have proposed new algorithms to enhance the performance of detection techniques in IDSs [38–40].

Rule-based: This technique is used in both signature and anomaly approaches. Signature detection diagnoses packets and detects malicious attacks through rules that are predefined in the system, whereas anomaly detection diagnoses the behavior of the system and detects differences between normal and abnormal behavior depending on predefined rules in the system, such as programmers' sequence of system calls. Both detection methods must update a network's rules to acquire more security. Updating the rules using the signature approach is simple, easy, and automatic; updating the rules using anomaly detection, however, is more complex because it needs time to record new training rules [41,42].

State-based: Signature detection uses the state transition analysis technique to describe attack scenarios. This technique contains two main elements, namely, state, and arc. The state represents the user or process, and the arc represents an action; if the user or process reaches the final state, then an attack occurs and the system detects it. The first tool to implement the state transition analysis technique was the Unix State Transition Analysis Tool, which executes host-based intrusion detection. The Unix State Transition Analysis Tool is a rule-based expert system that looks for known attacks in the audit traces of multi-user computer systems. However, it suffers from some limitations, such as its features being difficult to extend or adapt to different operating systems [43].

Data Mining: The signature detection approach can use data mining techniques to discover new patterns for IDSs and to overcome its main disadvantage. Although data mining is used mainly in the signature approach, much research has also applied data mining to anomaly detection. However, data mining requires data from various machine learning techniques, such as rule-based, classification, and clustering,

to gather knowledge for network intrusion detection [44,45]. Some of the existing data mining algorithms are shown in Tab. 7 [46,47].

Table 7: Data mining techniques

Methodology	Algorithm
Classification	Decision tree (DT), Support Vector Machin (SVM), Bayesian Networks (BN) K-Nearest Neighbors (K-NN), Artificial Neural Network (ANN) and Kstar.
Clustering	K-Means, Expectation Maximization (EM) and Hierarchical Clustering (HC).
Rule System	OneR, RIPPER Rule (RR), Association Rule (AR), Conjunctive Rule (CR) and Fuzzy.
Optimization	Linear Programming (LP) and Genetic Algorithm (GA).
Regression	Regression Trees (RT) Reinforcement Learning Automata (LA).
Ensemble	AdaBoost.

Statistical-based Intrusion Detection: This technique deals with two profiles in anomaly detection: one for observing current network traffic, and the other for statistical training. When an event occurs, the anomaly detection system evaluates it by comparing two behaviors. If the anomaly score exceeds the threshold, then the intrusion detection system generates an alarm [48]. Most model-based statistics assume multivariate statistical techniques, such as the chi-square statistic, Canberra technique, and Hotelling's T-squared distribution. Numerous anomaly detection mechanisms find outliers in the dataset by analyzing behavior, as each element in the dataset has specific features and a local outlier factor that could be used to detect the abnormal behavior [49,50].

Biological Models: Prior works have proven that the human immune system and computer network security are similar in nature. Both systems have a complex network and aim to protect its nodes from any malicious attack. In addition, both systems have security policies and security levels. The human immune system sets its policies to depend on natural selection phenomena, and its security levels should meet disposability, correction, integrity, and accountability requirements. Meanwhile, computer network systems establish a set of rules to defend against attacks and detect illegal actions that may occur in the network that break specific security levels [51–53]. In recent years, several algorithms inspired by biological processes, such as genetic algorithms and artificial neural network algorithms [54,55], have been widely applied to the anomaly detection approach to enhance the performance of intrusion detection.

Learning Models: Artificial learning techniques have increased the effectiveness of the anomaly detection approach. Anomaly detection can be supervised or unsupervised. Supervised anomaly detection is taught by a labelled dataset that distinguishes between normal and abnormal behavior. Supervised learning algorithms include support vector machines and the k-nearest neighbor. Unsupervised anomaly detection is taught by unlabeled training data; therefore, it uses several techniques to distinguish between normal and abnormal behavior in the system. One of these techniques is clustering, which has been used in anomaly intrusion detection to find outliers exhibiting anomalous behavior. The k-mean clustering algorithm is the most popular such algorithm, and has been applied to intrusion detection [56–58].

4.3 IDS Performance Measures

To ensure that an IDS's security service works efficiently, there are several evaluation metrics that might be used to measure the performance of any IDS. Researchers often use accuracy, false positive rates, and false negative rates. The equations below are used to measure the performance of IDSs [34].

Accuracy (AC) measures the IDS's accuracy in detecting an attack [59,60]:

$$AC = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

The *detection rate (DR)* is the ratio between intrusions detected to total attacks on the system [61]:

$$DR = \frac{TP}{TP + TN} \tag{2}$$

Precision (P) measures the ratio of attacks that were predicted correctly to the total attacks in the system, and is calculated as follows [62]:

$$P = \frac{TP}{TP + FP} \tag{3}$$

The *true negative rate (or specification) (TNR)* measures the ratio of normal values to the values that were successfully detected as legitimate in the system [63]:

$$TNR = \frac{TN}{TN + FP} \tag{4}$$

The *false positive rate (FPR)* measures the ratio of normal points that were detected as attacks and is calculated by Eq. (5) [64]. If the FPR is high, then the performance of the IDS is low.

$$FPR = \frac{FP}{FP + TN} \tag{5}$$

The *false negative rate (FNR)* measures the ratio of attacks that were not detected in the system [64]:

$$FNR = \frac{FN}{FN + TP} \tag{6}$$

The *true positive rate (or recall) (TPR)* measures the ratio of predicted attacks to the actual number of attacks on the system, and is determined by the following equation [62]:

$$TPR = \frac{TP}{TP + FN} \tag{7}$$

In the above equations, TP denotes the number of true positives, FN denotes the number of false negatives, TN denotes the number of true negatives, and FP denotes the number of false negatives. Tab. 8 presents the related confusion matrix [65,66].

Table 8: Confusion matrix

	Positive	Negative
True	Attack present Alarms are generated	No attack No alarms
False	No Attack Alarms are generated	Attack present No alarms

5 IDSs based on Blockchain Technology

Several works have used blockchain technology in IDSs to detect malicious attacks. These works can mainly be classified into two main categories: those that rely on the anomaly detection approach, and those that rely on the signature approach. Fig. 6, Fig. 7 and Fig. 8 illustrate different taxonomies of IDSs based on blockchain models for the detection approach. The following subsections discuss in detail IDSs based on blockchain models that use anomaly and signature detection techniques. Note that blockchain technology is more commonly adopted for anomaly detection than for signature detection.

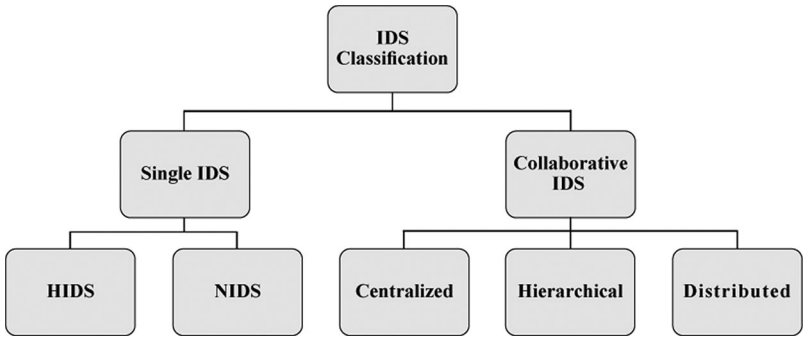

Figure 6: IDS classification-based location

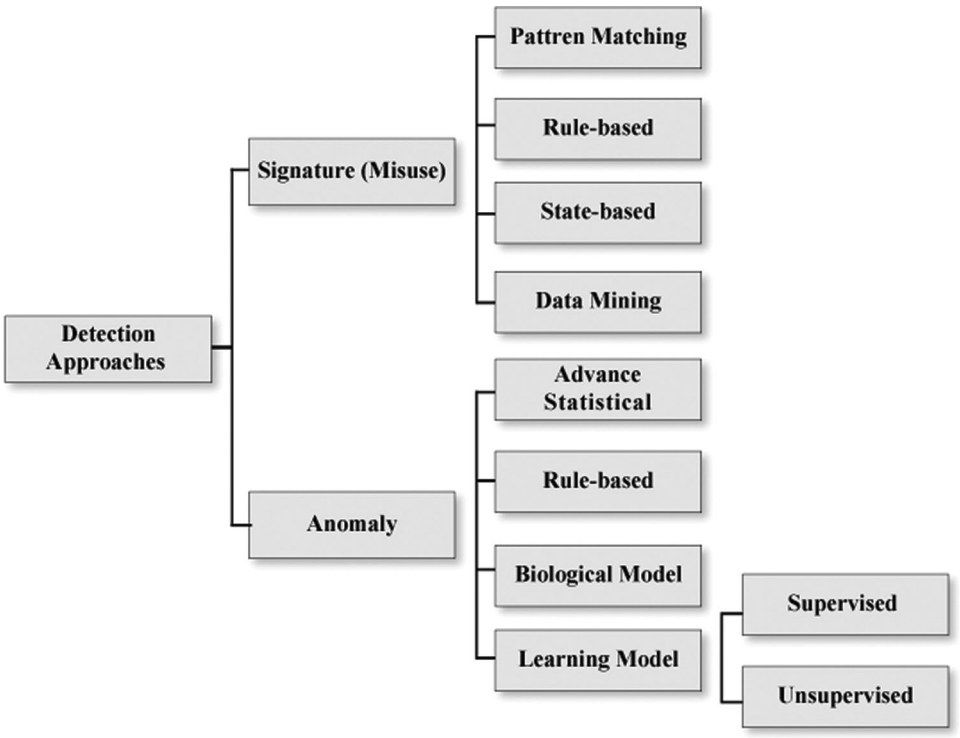

Figure 7: Detection approaches

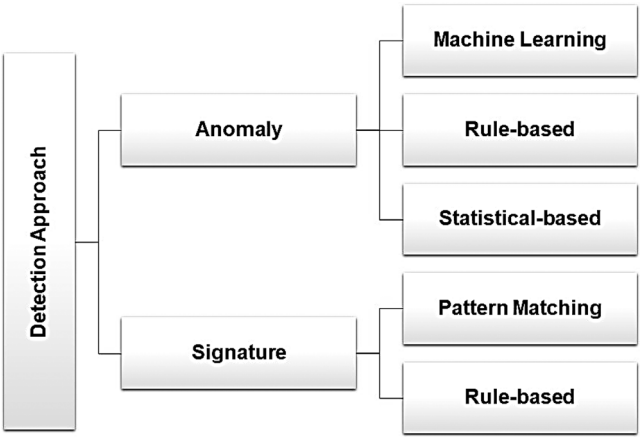

Figure 8: Taxonomy of IDS based on Blockchain models

5.1 Anomaly Detection Approach

The anomaly detection technique monitors a system's behavior by constructing a profile over a given period of time; this profile contains all activities of the system. However, there are different models for creating a profile file for the system, such as time series and threshold models [67]. The present review discusses three models that researchers have used to adopt blockchain technology, namely, machine learning, rule-based, and statistical models. Details about each model are presented in the following subsections.

5.1.1 Machine Learning Models

Machine learning can assist IDSs in detecting new and current attacks automatically and without human intervention by optimizing the system's feature selection. Recently, there have been many machine learning algorithms adopted into IDSs to enhance system security, such as support vector machines, artificial neural networks, and genetic algorithms [67]. This subsection presents the related works on IDS-based machine learning and how blockchain has been integrated into such learning.

Golomb et al. [68] introduced a blockchain protocol (called CIoTA) based on a distributed and collaborative anomaly detection framework used in the IoT. Each device contains a local model to detect malicious behavior, and new detection frameworks are shared by adding new blocks to the chain that are then propagated to all neighboring nodes. Experimental results revealed that CIoTA improves device and network security by detecting different types of attacks in the network. However, because CIoTA is designed for limited resources, it may increase overhead when many devices are available in the network.

Moreover, Idé [69] introduced a novel blockchain protocol, called CollabDict, for collaborative anomaly detection in the IoT network; this protocol learns collaboratively in blockchain platforms. CollabDict addresses three issues commonly faced by statistical machine learning algorithms: consensus-building, data privacy, and validation. CollabDict accomplishes consensus building by using a proof-of-vote mechanism-based statistical generalization and realizes data privacy by only sharing the client's aggregated statistics. However, validation remains a challenge for the CollabDict protocol. Thus, validation and its consequences need to be reviewed carefully in future research. Kumari et al. [70] protected blockchain networks from attacks using a modified k-means algorithm, which detects malicious nodes by classifying the nodes in the network based on their behavior patterns. Each pattern is built based on two parameters: (i) the time consumed for one transaction and (ii) the number of transactions from one node to another.

Finally, Dey [71] introduced an intelligent software agent based on game theory algorithms and machine learning techniques. This agent runs on an application layer and has two objectives: (i) determining old

transactions of participants that are likely to be malicious and (ii) calculating the value of current transactions and their probability of attacking.

5.1.2 Rule-based Models

Rule-based models observe the events of a system that has rules stored in a database to determine if an event is normal or abnormal. The model has one drawback: its failure to detect abnormal events if there are not many rules in the database.

Signoriniet et al. [72] proposed a model called BAD, which is a blockchain anomaly detection approach for the Bitcoin network. This model saves malicious transactions in an attack log at the first injection in the network; it then uses this log to prevent the attacks from spreading throughout the network. The BAD model takes blockchain's features (i.e., distributed, decentralized, and no need for third parties) to manage sensitive information. In addition, the BAD model is trusted because data behavior is verified by all of the nodes in the network, and it has a tamperproof feature that prevents malicious software from modifying the blockchain. However, the BAD model only works efficiently if the attacker repeats the same malicious transaction every time.

Signorini et al. [73] also proposed the ADvISE anomaly detection tool for blockchain systems; it collects and analyses blockchains' meta-data (forks), and then records malicious forks at the first attack in the database. Afterward, all peers in the blockchain network share the database to prevent attacks from being executed, thus protecting the network. Despite ADvISE being a tool designed for any type of attack, it works efficiently only when the attack has replicated itself more than once. Kanth et al. [74] presented a blockchain-based CIDS to detect doorknob rattling attacks through pluggable authentication modules (PAM) based on the private Ethereum blockchain. This PAM model can detect doorknob-rattling attacks more rapidly than previous models, but it lacks scalability.

Steichen et al. [75] introduced the ChainGuard model based on software-defined networking to detect and prevent abnormal behavior. The ChainGuard model uses software-defined networking functions to filter the traffic of the network through a firewall of blockchain applications. As a result, it minimizes denial-of-service and distributed denial-of-service attacks on the network because it prevents malicious packets from influencing the blockchain.

Moreover, Zhu et al. [76] proposed a novel model for managing storage in cloud computing based on blockchain technology. Their model reduces the risk of attacks on the blockchain and is called controllable blockchain data management. This model increases a network's security level by submitting trusted authority nodes, which have higher voting authorization compared to other nodes in the network. The model also has the authority to terminate any malicious node, and thus it has controllability. In addition, controllable blockchain data management provides a privacy-preserving feature because it grants public keys, private keys, and permissions to each user who joins a network in which users are unknown to each other. Furthermore, users' votes are signed, and users must pay fees to vote, which decreases the risk of malicious voting. This model also has openness and transparency because it publishes modifications and voting records over the network; moreover, the network is not affected if a single node crashes.

5.1.3 Statistical Models

A statistical model-based IDS relies on analyzing and correlating data, then applying statistical theories on such data to detect attacks. Users also define the threshold for each statistical variable. However, current statistical models suffer from insufficiency in genetic architecture because confidentiality, integrity, and availability have not been considered within the current statistical models' principles. At the time of the present review, there is no literature on adopting a blockchain technology-based statistical model [77].

Pham et al. [78] proposed an anomaly detection technique in the Bitcoin network that uses two approaches, namely, the LOF and the densification power law. Their findings showed that the proposed technique achieves

high anomaly detection rates, and that the technique can be applied in different networks. However, the main challenge of this technique is that it is has difficulty measuring the accuracy of the LOF method.

5.2 Signature Detection Approach

There have been several works conducted to detect attacks using blockchain technology based on the signature detection approach. This section presents two signature models based on blockchain.

5.2.1 Pattern Matching Models

Although the pattern matching model is the most widely used model by the signature detection approach, limited research has been conducted on it regarding blockchain technology. Pattern or string-matching models use single or multiple patterns matching algorithms to detect malware. The single pattern approach compares only one pattern at a time to detect malware, whereas the multiple-patterns approach compares more than one pattern at a time [39].

Hu et al. [79] presented an approach to collaborative intrusion detection based on blockchain for multi-microgrid systems. The approach has three aspects: (i) it integrates the consensus mechanisms of blockchain with multi-microgrid systems to enhance the accuracy of CIDSs; (ii) it uses periodic and time-triggered patterns to reduce false positive rates; and (iii) it enhances delegated proof of stake (DPoS) consensus algorithms to solve the single richest member problem.

5.2.2 Rule-based Models

Rule-based models have a set of rules that match against network traffic or audit data. They can detect any attack if the rules match. However, since using a rule-based model alone is insufficient for malware detection, it needs to be integrated with another technique [80]. This subsection discusses how researchers have started to integrate the rule-based model with blockchain technology.

Alexopoulos et al. [81] proposed a blockchain framework based on CIDSs to enhance malicious detection. The proposed framework tries to archive accountability, integrity, resilience, consensus, scalability, and privacy, while reducing overhead requirements by exchanging alerts between nodes based on secure ledger distribution. The framework considers each alert message as a transaction produced by an IDS node, and then all collaborating nodes utilize consensus mechanisms to validate the alert. Thus, it prevents storing malicious alert. However, Alexopoulos' proposed framework has not been implemented or evaluated in a real or virtual environment.

Li et al. [82] extended a generic framework to improve the signature detection approach based on blockchain technology and thus increase the IoT network's security level. The improved framework is called CBSigIDS. It builds a trusted signature database and shares it between all nodes in the network; moreover, each record is signed by a private key. CBSigIDS is effective and robust in detection because a malicious node cannot add a signature to the database; however, this approach faces the limitations of blockchain technology, such as energy, cost, and scalability.

The database, but it faces the limitations of blockchain technology, such as energy, cost, and scalability.

5.3 Analysis of Blockchain-IDS Models

As mentioned earlier, blockchain-based IDS models are based on anomaly and signature approaches, both of which have various challenges that may be solved via blockchain technology. This subsection presents the challenges of IDS in both approaches. In addition, it provides an analysis of and comparisons between the existing blockchain-based IDS models.

The anomaly detection approach suffers from a high number of false alarms, and it is unable to detect encrypted packet that occurs by cyberattacks. Moreover, it has difficulty constructing a normal profile for

dynamic systems, its alarms are not classified, and initial training is required. In contrast, the main limitation in the signature detection approach is that it is unable to detect a new cyberattack in the system. Therefore, this approach needs to be updated frequently, and it is an inappropriate choice for detecting a multi-step attack [83].

The existing blockchain-based IDS models also suffer from different issues. Tab. 9 provides a description of each model along with their strengths and weaknesses. As aforementioned, the common challenge between all models is that they have no standard design.

Table 9: Summary of the blockchain-based IDS models

Ref	Description	Strengths	Weaknesses
[68]	It proposes blockchain protocol (CIoTA) based on a distributed and collaborative mechanism for anomaly detection in IoT network.	It improves security of IoT devices and the whole network as well.	It is not efficient security protocol for many IoT devices.
[69]	It proposes a protocol (CollabDict) for a collaborative anomaly detection based on blockchain and Gaussian mixture learning algorithm.	Performance of CollabDict is better than fuses multitask learning algorithm.	Collaborative learning has three main challenges, namely: (i) validation, (ii) consensus building, and (iii) data security.
[70]	It relies on the use of the k-means algorithm to distinguish between malicious nodes and normal nodes through the analysis of pattern behavior for each node in a blockchain network.	It manages nodes and transactions in the network efficiently, also, it classifies nodes correctly.	It uses mean value for each cluster; thus, inaccurate cluster head might be selected, besides, it uses a static distance measure rather than a dynamic one.
[71]	It detects anomaly behaviours of participates in a blockchain network based on a game theory and a supervised machine learning algorithms.	It provides probability for each attack based on value of the transaction.	It requires improvements to strengthen its defense mechanism.
[72]	It builds BAD model to detect malicious transactions and prevent spreading them over the network.	It prevents malicious software from modifying the transactions' trace. Furthermore, data behavior should be verified from all participants in the network; thus, network security is increased.	It cannot detect the malicious transactions efficiently.
[73]	It provides a tool used to detect anomaly behaviours in a blockchain network.	It is a flexible tool that can detect several types of malicious transactions in a blockchain network.	It works efficiently in case of having repeating attacks in the network.

Table 9 (continued).

Ref	Description	Strengths	Weaknesses
[74]	It proposes PAM model for addressing two challenges are trusting participants and aggregating data in CIDS.	It prevents doorknob rattling attacks from modifying records in the system instantly before occurring any activity.	PAM model detects one type of attack, and there is no scalability feature.
[75]	It is used for securing Software Defined Network (SDN), by detecting and preventing abnormal behaviors at network level through a firewall of blockchain applications.	ChainGuard reduces the effect of DoS and DDoS attacks on SDN network.	The effectiveness of the proposed model is not evaluated in the real environment.
[76]	It introduces Controllable Blockchain Data Management (CBDM) model, it is a novel model-based blockchain used to obtain storage efficiency in the cloud computing network and minimize risk resulting from malicious attacks in blockchain.	It ensures providing a sufficient storage in cloud computing, and it increases the security level in the whole network.	It is not evaluated in real environment.
[78]	It utilized LOF method and densification power law to detect malicious users and transactions in a Bitcoin network.	It achieves high anomaly detection rate, and it can be adapted in different networks types.	It is difficult to measure accuracy of LOF method; so, it is not efficient in detecting anomaly behaviours.
[79]	It produces a collaborative intrusion detection (CID) model-based on blockchain technology for Multi-microgrid system. It records the target of CID in a blockchain and builds a correlation model of Multi- microgrid system, by a consensus algorithm.	It reduces the false-negative rate by using multiple patterns, and it improves DPoS consensus algorithm. Also, no need for a trusted authority in MMGs.	It is limited to few types of attacks. Also, it does not provide a high level of true positive rate compared to other approaches.
[81]	It uses a blockchain technology to improve CIDS. In addition, it provides a combined architecture based on blockchain and CIDs.	It reduces the overhead and volume of the blockchain construct considerably.	The approach is not assessed in the real environment, and it is not sup- porting scalability feature.

(Continued)

Table 9 (continued).

Ref	Description	Strengths	Weaknesses
[82]	It introduces a generic framework (CBSigIDS) to enhance signature IDS based on a blockchain technology in IoT environment, where it uses consortium blockchain to build trusted rules (signature) database and share it with other nodes in network.	It improves effectiveness and robustness of signature based IDSs.	It suffers from some of challenges such as: vulnerability to the advanced attacks' types and the need for verification and the frequent update in blockchain, which, in result causes a delay and diminishes the overall network performance.

Most existing models leverage the anomaly technique instead of the signature technique due to its benefits. Besides, machine learning methods are receiving more attention from researchers because they have proven their worthiness in detection tasks.

As shown in Fig. 6, IDSs have different architectures. Among them, the CIDS architecture is appropriate for blockchain. The distributed IDS is the most compatible because the blockchain technology builds over a P2P architecture and it is a distributed model. Therefore, the existing models have been proposed for various network architectures. Lastly, we note that the distributed system has four main architectures: (i) client–server, (ii) three-tier, (iii) n-tier, and (iv) peer-to-peer [83–85].

Tab. 10 compares between related works categories based on approach detection, network type, attack type detection and type of blockchain, as well as the simulation and platform that was used in each model. While most IDS models were proposed for different networks architectures, which adopted blockchain technology are assessed in a virtual environment by different simulators. However, there was one real model (CIoTA) applied in the IoT environment, but it also has its own limitations.

6 Future Research Directions

Prior research has focused on constructing models to enhance the performance of IDSs by adopting blockchain technology over several network environments. However, most of these models suffer from issues related to the blockchain technique, IDS approach, or network environment. Therefore, the present paper notes a few issues that require consideration in future research concerning performance improvements for IDSs based on blockchain technology.

No Application in Real Environment: Most IDS models proposed for different network architectures that have adopted blockchain technology were applied in a virtual environment, but not in a real environment. In addition, each model suffers from its own limitations, such as lacking a framework of blockchain-based intrusion detection techniques (either an anomaly or signature).

Increased Accuracy in IDSs Based on Blockchain Technology: An IDS can send false alarms, which means that it can detect an attack when there is none. [81] suggested that these false alarms can be prevented by using the signature detection blockchain nodes to verify alarms, but this has not been implemented. To verify whether an alarm is true, an approach must be designed based on blockchain technology that receives and verifies an alarm before exchanging it over a network.

Table 10: A Summary of the blockchain-based IDS models

Detection Approach	Network Type	Model Name	Attack Type	Simulator	Platform	Ref
Anomaly	Blockchain network	NA*	Trojan keylogger	BTC	CS 224W course website	[78]
		BAD	Eclipse	Bitcoin Testnet	Virtual Machine	[72]
		PAM	Doorknob rattling	Go-Ethereum	Ubuntu	[74]
	IoT	CIoTA	All attacks	IoT simulation testbed consisting of 48 Raspberry Pis	Emulation	[68]
		CollabDict	NA	Gaussian Graphic Model	NC*	[69]
	P2P	ADvISE	Eclipse	NA	NA	[73]
		NA	NA	NS3	Ubuntu	[70]
		NA	NA	NA	NA	[71]
	SDN	ChainGuard	DoS DDoS	SYN flood	Virtual Machine	[75]
	Cloud Computing	CBDM	User Collusion Attack Model (UCAM).	Ethereum client Geth and Wallet	NC	[76]
Signature	IoT	CBSigIDS	Flooding Worm	Snort	Simulated and real CIDN environment.	[82]
	P2P	Generic architecture	NC	NA	NA	[81]
	Multi-microgrid (MMG)	NA	Tampering, Man-in-the-Middle Replay & DoS	Co-simulation	NC	[79]

Data Management in CIDSs Based on Blockchain Technology: The nodes in CIDSs communicate and share data between each other to detect attacks. Blockchain technology emphasizes trust and privacy for sharing data over P2P networks. A mechanism should be proposed to reduce communication overhead by storing alarms and data efficiently. Another issue in data management is accountability in tracing data between nodes over a distributed network.

Build a Hybrid Model Using Blockchain Technology and Other Models to Enhance Detection in IDSs: Anomaly and signature approaches utilize different techniques to detect attacks in a system. As aforementioned, there are a few techniques for adapting blockchain technology with IDSs. Therefore, other techniques can improve the performance of IDSs based on blockchain. For instance, researchers can design a hybrid model using blockchain and biological models to enhance detection with the anomaly approach; they can also employ a hybrid model using blockchain and data mining to enhance detection with the signature approach.

Design Proof-of-Concepts for CIDS: Researchers must demonstrate the probability and effectiveness on CIDSs based on blockchain regarding different issues, such as energy, cost, complexity, speed, and scalability.

7 Conclusion

Recently, blockchain technology has emerged within several fields to ensure high level of security. This paper discussed the structure of blockchain, presented an overview of IDSs, and compared between existing blockchain-based IDS models. However, few research has been conducted on this topic, and no standard approaches or real applications have been demonstrated. In addition, this paper identified future directions that need to be addressed and investigated by researchers to improve the performance of IDSs based on blockchain technology. From the authors' perspectives, the CIDS architecture is the most proper architecture for building general architecture for IDSs based on blockchain technology because CIDSs can share data between nodes over a P2P network, which is considered an important feature in a blockchain structure.

Acknowledgement: I express my gratitude to Universiti Sains Malaysia, Malaysia and Northern Border University, Saudi Arabia, for administrative and technical support.

Funding Statement: This work was supported by Universiti Sains Malaysia under external grant (Grant number 304/PNAV/650958/U154).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. M. Kolekar, R. P. More, S. S. Bachal and A. V. Yenkikar, "Review paper on untwist Blockchain: A data handling process of Blockchain systems," in *2018 Int. Conf. on Information, Communication, Engineering and Technology (ICICET)*, pp. 1–4, 2018.

[2] H. M. Shreevyas, C. S. Kumar, P. Diat-Drdo, R. A. Shaikh, B. Acu *et al.,* "Can Blockchain technology be the future of network intrusion detection system: A review," *International Journal of Applied Engineering Research*, vol. 14, no. 15, pp. 10179–10187, 2019.

[3] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When intrusion detection meets Blockchain Technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.

[4] X. Wang, X. Zha, W. Ni, R. Liu, Y. Guo *et al.,* "Survey on blockchain for Internet of Things," *Computer Communications*, vol. 136, no. 7, pp. 10–29, 2019.

[5] M. A. Khan and K. Salah, "IoT security: Review, Blockchain solutions, and open challenges," *Future Generation of Computer Systems*, vol. 82, no. 15, pp. 395–411, 2018.

[6] H. Hui, X. An, H. Wang, W. Ju, H. Yang *et al.,* "Survey on Blockchain for Internet of Things," *Journal of Internet Services and Information Security*, vol. 9, no. 2, pp. 1–30, 2019.

[7] W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta *et al.,* "A survey on Blockchain-based internet service architecture: Requirements, challenges, trends, and future," *IEEE Access*, vol. 7, pp. 75845–75872, 2019.

[8] J. Sengupta, S. Ruj and S. D. Bit, "A comprehensive survey on attacks, security issues and Blockchain solutions for IoT and IIoT," *Journal of Network and Computing Applications*, vol. 149, no. 6, pp. 102481, 2020.

[9] I. Islam, K. M. Munim, S. J. Oishwee, A. N. Islam and M. N. Islam, "A critical review of concepts, benefits, and Pitfalls of Blockchain technology using concept map," *IEEE Access*, vol. 8, pp. 68333–68341, 2020.

[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available at: https://www.klausnordby.com/bitcoin/Bitcoin_Whitepaper_Document_HD.pdf.

[11] Q. Feng, D. He, S. Zeadally, M. K. Khan and N. Kumar, "A survey on privacy protection in Blockchain system," *Journal of Network and Computer Applications*, vol. 126, no. 2, pp. 45–58, 2019.

[12] W. Gao, W. G. Hatcher and W. Yu, "A survey of Blockchain: techniques, applications, and challenges," in *2018 27th Int. Conf. on Computer Communication and Networks (ICCCN)*, pp. 1–11, 2018.

[13] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat *et al.,* "Provchain: A Blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. of the 17th IEEE/ACM Int. sym. on cluster, cloud and grid computing*, pp. 468–477, 2017.

[14] M. Muzammal, Q. Qu and B. Nasrulin, "Renovating Blockchain with distributed databases: An open-source system," *Future Generation Computer Systems*, vol. 90, no. Supplement C, pp. 105–117, 2019.

[15] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An overview of Blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564, 2017.

[16] Y. Yuan and F. Y. Wang, "Blockchain and cryptocurrencies: model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, 2018.

[17] L. Ismail, H. Hameed, M. AlShamsi, M. AlHammadi and N. AlDhanhani, "Towards a Blockchain deployment at UAE university: Performance evaluation and Blockchain taxonomy," in *Proc. of the 2019 Int. Conf. on Blockchain Technology*, pp. 30–38, 2019.

[18] F. Glaser, "Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis," in *Proc. of the 50th Hawaii Int. Conf. on System Sciences*, 2017.

[19] B. A. Tama, B. J. Kweka, Y. Park and K. Rhee, "A critical review of Blockchain and its current applications," in *2017 Int. Conf. on Electrical Engineering and Computer Science (ICECOS)*, pp. 109–113, 2017.

[20] F. Dai, Y. Shi, N. Meng, L. Wei and Z. Ye, "From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues," in *2017 4th Int. Conf. on Systems and Informatics (ICSAI)*, pp. 975–979, 2017.

[21] C. Elsden, A. Manohar, J. Briggs, M. Harding, C. Speed *et al.,* "Making sense of Blockchain applications: A typology for HCI," in *Proc. of the 2018 CHI Conf. on Human Factors in Computing Systems*, pp. 458, 2018.

[22] A. Al Omar, M. S. Rahman, A. Basu and S. Kiyomoto, "Medibchain: A Blockchain based privacy preserving platform for healthcare data," in *Int. conf. on security, privacy and anonymity in computation, communication and storage*, pp. 534–543, 2017.

[23] C. C. Agbo, Q. H. Mahmoud and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, pp. 56, 2019.

[24] A. Mohsin, A. Zaidan, A. Zaidan, B. Albahri, O. Albahri *et al.,* "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," *Computer Standards & Interfaces*, vol. 1, no. 64, pp. 41–60, 2018.

[25] A. Alammary, S. Alhazmi, M. Almasri and S. Gillani, "Blockchain-based applications in education: A systematic review," *Application Science*, vol. 9, no. 12, pp. 2400, 2019.

[26] N. O. Nawari and S. Ravindran, "Blockchain technology and BIM process: Review and potential applications," *Journal of Information Technology and Constraint Information Technology*, vol. 24, no. 12, pp. 209–238, 2019.

[27] J. A. Jaoude and R. G. Saade, "Blockchain applications-usage in different domains," *IEEE Access*, vol. 7, pp. 45360–45381, 2019.

[28] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the application of Blockchain for the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45201–45218, 2019.

[29] M. Niranjanamurthy, B. N. Nithya and S. Jagannatha, "Analysis of Blockchain technology: Pros, cons and SWOT," *Cluster Computing*, vol. 22, no. 6, pp. 14743–14757, 2019.

[30] J. Golosova and A. Romanovs, "The advantages and disadvantages of the Blockchain technology," in *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, pp. 1–6, 2018.

[31] J. J. Xu, "Are blockchains immune to all malicious attacks?," *Financial Innovation*, vol. 2, no. 1, pp. 2, 2016.

[32] I.-C. Lin and T. C. Liao, "A survey of Blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[33] H. Wang, Y. Wang, Z. Cao, Z. Li and G. Xiong, "An overview of Blockchain security analysis," in *China Cyber Security Annual Conf.*, pp. 55–72, 2018.

[34] G. Agrawal, S. K. Soni and C. Agrawal, "A survey on attacks and approaches of intrusion detection systems," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 8, pp. 231–253, 2017.

[35] S. Tug, W. Meng and Y. Wang, "CBSigIDS: towards collaborative Blockchained signature-based intrusion detection," in *2018 IEEE Int. Conf. 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)*, Halifax, NS, Canada, pp. 1228–1235, 2018.

[36] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," *ACM Computing Surveys CSUR*, vol. 47, no. 4, pp. 55, 2015.

[37] T. A. Alamiedy, M. Anbar, A. K. Al-Ani, B. N. Al-Tamimi and N. Faleh, "Review on feature selection algorithms for anomaly-based intrusion detection system," in *Int. Conf. of Reliable Information and Communication Technology*, pp. 605–619, 2018.

[38] S. Dharmapurikar and J. W. Lockwood, "Fast and scalable pattern matching for network intrusion detection systems," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 10, pp. 1781–1792, 2006.

[39] M. Aldwairi, A. M. Abu-Dalo and M. Jarrah, "Pattern matching of signature-based IDS using Myers algorithm under MapReduce framework," *EURASIP Journal on Information Security*, vol. 2017, no. 1, pp. 2730, 2017.

[40] M. Naik and N. Geethanjali, "A multi-fusion pattern matching algorithm for signature-based network intrusion detection system," *International Journal of Research in Engineering, IT and Social Sciences*, vol. 23, no. 8, pp. 36–41, 2016.

[41] S. Souissi, L. Sliman and B. Charroux, "A novel security architecture based on multi-level rule expression language," in *Int. Conf. on Hybrid Intelligent Systems*, pp. 259–269, 2016.

[42] S. Geetha, U. N. Dulhare and S. S. S. Sindhu, "Intrusion detection using NBHoeffding rule-based decision tree for wireless sensor networks," in *2018 Second Int. Conf. on Advances in Electronics, Computers and Communications (ICAECC)*, pp. 1–5, 2018.

[43] S. Eckmann, G. Vigna and R. Kemmerer, "An attack language for state-based intrusion detection," in *Proc. of the 2000 ACM Workshop on Intrusion Detection*, ACM, 2000.

[44] C.-T. Lu, A. P. Boedihardjo and P. Manalwar, "Exploiting efficient data mining techniques to enhance intrusion detection systems," in *IRI-2005 IEEE Int. Conf. on Information Reuse and Integration, Conf.*, pp. 512–517, 2005.

[45] R. Sahani, C. Rout, J. C. Badajena, A. K. Jena, H. Das *et al.,* "Classification of intrusion detection using data mining techniques," in *Progress in Computing, Analytics and Networking, Springer*, pp. 753–764, 2018.

[46] F. Salo, M. Injadat, A. B. Nassif, A. Shami and A. Essex, "Data Mining techniques in intrusion detection systems: A systematic literature review," *IEEE Access*, vol. 6, pp. 56046–56058, 2018.

[47] M. Anbar, R. Abdullah, I. H. Hasbullah, Y. W. Chong and O. E. Elejla, "Comparative performance analysis of classification algorithms for intrusion detection system," in *2016 14th Annual Conf. on Privacy, Security and Trust (PST)*, pp. 282–288, 2016.

[48] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1–2, pp. 18–28, 2009.

[49] M.-L. Shyu, S. C. Chen, K. Sarinnapakorn and L. Chang, *A novel anomaly detection scheme based on principal component classifier*. Miami Univ Coral Gables Fl Dept of Electrical and Computer Engineering, 2003.

[50] N. Ye and Q. Chen, "An anomaly detection technique based on a chi-square statistic for detecting intrusions into information systems," *Quality and Reliability Engineering International*, vol. 17, no. 2, pp. 105–112, 2001.

[51] A. Boukerche, R. B. Machado, K. R. Jucá, J. B. M. Sobral and M. S. Notare, "An agent based and biological inspired real-time intrusion detection and security model for computer network operations," *Computer Communications*, vol. 30, no. 13, pp. 2649–2660, 2007.

[52] E. A. E. R. Abas, H. Abdelkader and A. Keshk, "Artificial immune system-based intrusion detection," in *2015 IEEE Seventh Int. Conf. on Intelligent Computing and Information Systems (ICICIS)*, pp. 542–546, 2015.

[53] P. Saurabh and B. Verma, "Immunity inspired cooperative agent-based security system," *International Arab Journal of Information Technology*, vol. 15, no. 2, pp. 289–295, 2018.

[54] M. Jha and R. Acharya, "An immune inspired unsupervised intrusion detection system for detection of novel attacks," in *2016 IEEE Conf. on Intelligence and Security Informatics (ISI)*, pp. 292–297, 2016.

[55] M. H. Chen, P. C. Chang and J. L. Wu, "A population-based incremental learning approach with artificial immune system for network intrusion detection," *Engineering Applications of Artificial Intelligence*, vol. 51, no. 1, pp. 171–181, 2016.

[56] M. Zamani and M. Movahedi, "Machine learning techniques for intrusion detection," 2013. [Online]. Available at: https://arxiv.org/abs/1312.2177.

[57] F. Hosseinpour, P. V. Amoli, F. Farahnakian, J. Plosila and T. Hämäläinen, "Artificial immune system based intrusion detection: Innate immunity using an unsupervised learning approach," *International Journal of Digital Content Technology and its Applications*, vol. 8, no. 5, pp. 1, 2014.

[58] H. H. Pajouh, G. Dastghaibyfard and S. Hashemi, "Two-tier network anomaly detection model: A machine learning approach," *Journal of Intelligent Information Systems*, vol. 48, no. 1, pp. 61–74, 2017.

[59] N. Farnaaz and M. Jabbar, "Random forest modeling for network intrusion detection system," *Procedia Computer Science*, vol. 89, no. 1, pp. 213–217, 2016.

[60] I. Iervolino, D. Accardo, A. E. Tirri, G. Pio and E. Salzano, "Quantitative risk analysis for the Amerigo Vespucci (Florence, Italy) airport including domino effects," *Safety Science*, vol. 113, no. 4, pp. 472–489, 2019.

[61] M. Anbar, R. Abdullah, B. N. Al-Tamimi and A. Hussain, "A machine learning approach to detect router advertisement flooding attacks in next-generation IPv6 networks," *Cognitive Computation*, vol. 10, no. 2, pp. 201–214, 2018.

[62] M. Elhamahmy, H. N. Elmahdy and I. A. Saroit, "A new approach for evaluating intrusion detection system," *International Journal of Artificial Intelligent Systems and Machine Learning*, vol. 2, no. 11, pp. 290–298, 2010.

[63] B. Abdullah, I. Abd-Alghafar, G. I. Salama and A. Abd-Alhafez, "Performance evaluation of a genetic algorithm based approach to network intrusion detection system," in *Int. Conf. on Aerospace Sciences and Aviation Technology, vol. 13, no. aerospace sciences & aviation technology, ASAT-13*. The Military Technical College, pp. 1–17, May 26–28, 2009.

[64] N. Gupta, K. Srivastava and A. Sharma, "Reducing false positive in intrusion detection system: a survey," *International Journal of Computer Science and Information Technologies*, vol. 7, no. 3, pp. 1600–1603, 2016.

[65] A. A. Ghorbani, W. Lu and M. Tavallaee, *Network Intrusion Detection and Prevention*. Vol. 47. Boston, MA: Springer US, 2010.

[66] N. Sultana, N. Chilamkurti, W. Peng and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 493–501, 2019.

[67] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," 2017. [Online]. Available at: https://arxiv.org/abs/1701.02145.

[68] T. Golomb, Y. Mirsky and Y. Elovici, "CIoTA: Collaborative IoT anomaly detection via Blockchain," 2018. [Online]. Available at: https://arxiv.org/abs/1803.03807.

[69] T. Idé, "Collaborative Anomaly Detection on Blockchain from Noisy Sensor Data," in *2018 IEEE Int. Conf. on Data Mining Workshops (ICDMW)*, pp. 120–127, 2018.

[70] R. Kumari and M. Catherine, "Anomaly detection in Blockchain using clustering protocol," *International Journal of Pure and Applied Mathematics*, vol. 118, no. 20, pp. 391–396, 2018.

[71] S. Dey, "Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work," in *2018 10th Computer Science and Electronic Engineering (CEEC)*, pp. 7–10, 2018.

[72] M. Signorini, M. Pontecorvi, W. Kanoun and R. Di-Pietro, "BAD: Blockchain anomaly detection," *IEEE Access*, vol. 8, pp. 173481–173490, 2020.

[73] M. Signorini, M. Pontecorvi, W. Kanoun and R. Di-Pietro, "ADvISE: Anomaly Detection tool for Blockchain SystEms," in *2018 IEEE World Congress on Services (SERVICES)*, pp. 65–66, 2018.

[74] V. Kanth, A. Mcabee, M. Tummala and J. Mceachen, "Collaborative Intrusion Detection leveraging Blockchain and Pluggable Authentication Modules," in *Proc. of the 53rd Hawaii Int. Conf. on System Sciences*, 2020.

[75] M. Steichen, S. Homme and R. State, "ChainGuard — a firewall for blockchain applications using SDN with OpenFlow," in *2017 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, pp. 1–8, Sep. 2017.

[76] L. Zhu, Y. Wu, K. Gai and K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Future Generation Computer Systems*, vol. 91, no. 99, pp. 527–535, 2019.

[77] N. Moustafa, K. K. R. Choo, I. Radwan and S. Camtepe, "Outlier dirichlet mixture mechanism: Adversarial statistical learning for anomaly detection in the fog," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 1975–1987, 2019.

[78] T. Pham and S. Lee, "Anomaly detection in the Bitcoin system-a network perspective," 2016. [Online]. Available at: https://arxiv.org/abs/1611.03942.

[79] B. Hu, C. Zhou, Y. C. Tian, Y. Qin and X. Junping, "A collaborative intrusion detection approach using Blockchain for multimicrogrid systems," *EEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1–11, 2019.

[80] C. Turner, R. Jeremiah, D. Richards and A. Joseph, "A rule status monitoring algorithm for rule-based intrusion detection and prevention systems," *Procedia Computer Science*, vol. 95, pp. 361–368, 2016.

[81] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivánkó and M. Mühlhäuser, "Towards Blockchain-based collaborative intrusion detection systems," in *Critical Information Infrastructures Security*, G. D'Agostino, A. Scala, 10707. Cham: Springer International Publishing, pp. 107–118, 2018.

[82] W. Li, S. Tug, W. Meng and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," *Future Generation Computer Systems*, vol. 96, no. 3, pp. 481–489, 2019.

[83] A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 384, 2019.

[84] What is a Distributed System? How a Distributed System Works, "Articles for Developers Building High Performance Systems," 2019. [Online]. Available at: https://blog.stackpath.com/distributed-system/.

[85] S. Al-E'mari, M. Anbar, Y. Sanjalawe and S. Manickam, "A labeled transactions-based dataset on the Ethereum network," in *Int. Conf. on Advances in Cyber Security, Communications in Computer and Information Science*, Singapore: Springer, 1347, pp. 61–79, 2021.