Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Blockchain Analysis, Challenges and Applications: A Review

Sara Mohammed Younis [a], ***Haider Mohammed Abdulnabi*** [b]

[a] *Basra University Collage,Basra, postal code 61015, Iraq, Email: pgs.sara.mohamad@uobasrah.edu.iq*

[b] *Basra University Collage,Basra, postal code 61001, Iraq, Email: mashhad01@gmail.com*

ARTICLE INFO

Article history:
Received: 26 /7/2024
Rrevised form: 15 /9/2024
Accepted : 15 /1/2025
Available online: 30 /30/2025

Keywords:

Keywords: Blockchain,

proof of work (POW),

IoT, cryptography, ATM.

ABSTRACT

The most dependable service on the planet is blockchain. It functions like a ledger to enable distributed transaction processing. The internet of things (IoT), financial services, non-financial services, and a plethora of other sectors are only a few of the domains in which blockchain technology finds application. Without the requirement for central authority verification, blockchain combines a distributed ledger and a distributed database. The many consensus methods, blockchain challenges, and their extent are covered in this study. This technology is still facing numerous obstacles that need to be resolved, like scalability. The ripple protocol consensus algorithm (RPCA), delegated proof of stake (dPOS), proof of work (POW), proof of stake (POS), stellar consensus protocol (SCP), and proof of importance (POI) are the consensus algorithms behind the technology known as blockchain. This Review discusses the fundamental idea behind blockchain technology as well as different mining techniques, consensus problem algorithms for consensus, and performance-based comparison algorithms, blockchain's benefits, the architecture of Blockchain and applications of blockchain such as ATM.

https://doi.org/10.29304/jqcsm.2025.17.11962

1. Introduction

Blockchain technology has emerged as a groundbreaking innovation, fundamentally transforming the way transactions are conducted and recorded across various sectors. At its core, blockchain is a decentralized ledger that organizes transactions into "blocks," which are then linked in a sequential chain [1], [2]. This structure not only enhances security through cryptographic hash functions but also ensures that each block is inherently tied to the previous one, creating a robust and tamper-resistant record. The decentralization characteristic of blockchain eliminates the need for central authorities, such as banks or governments, allowing for peer-to-peer transactions that reduce costs and enhance trust among participants [3]. Centralisation, untrustworthiness, and illegal access to data [2],[3], and [4].

The blockchain is the biggest distributor and open digital record that enables simultaneous ownership transfers between parties without the need for a middleman while achieving a high level of security for the transfer process

∗Corresponding author

Email addresses: *pgs.sara.mohamad@uobasrah.edu.iq*

Communicated by 'sub etitor'

against attempts at fraud and manipulation. Anyone can participate in this record, regardless of location. With this technology [5], Since the blockchain system was first used in 2008 as the primary platform for the bitcoin currency, which gained its strength from this technology, many people mistakenly believe that bitcoin and the blockchain are one and the same, but this is untrue; the blockchain is what sets bitcoin apart from other virtual currencies [6]. It is important to remember that every action that occurs on the blockchain is recorded in an unchangeable record. The nine fundamental parts of the blockchain are as follows [7]:

1- The nodes that It is represented the users,
2- The transaction, which is the smallest part of the blockchain, such as records, information, etc.,
3- The block is the unit of data building used to store a set of transactions that are distributed to nodes,
4- The chain, which represents a chain of blocks,
5- The miners, which are nodes that operate on to verify the blocks before adding and distributing them to the nodes,
6- The protocol that represents the rules and data for the implementation of the blockchain,
7- The entry process, which is the sub-process that takes place within a single block,
8- The hash represents the distinctive DNA of the block and the digital signature of the block may be forgotten,
9- And finally, the time imprint, which is the time when the operation was performed within the chain.

Despite its potential, blockchain technology faces several challenges, including scalability, interoperability, and regulatory concerns. Understanding these challenges is crucial for leveraging blockchain's full potential while ensuring its responsible application across different domains. This review paper aims to provide a comprehensive analysis of blockchain technology, exploring its foundational principles, current challenges, and diverse applications. By examining existing literature and case studies, we seek to identify key trends and insights that can inform future developments in blockchain technology. Ultimately, our objective is to contribute to a deeper understanding of how blockchain can be effectively utilized to overcome existing obstacles and maximize its benefits across various industries. The next section is divided into the following parts: section 2 discusses all concepts behind the term blockchain. Blockchain architecture is shown in section 3, while section 4 illustrated the algorithm used. A comprehensive analysis of these algorithm is in section 5 with a case study distributed in section 6.

2. The Fundamental Idea of Blockchain

Peer-to-peer networks and distributed consensus algorithms are combined in blockchain technology, an integrated multi-field infrastructure development, to address classic distributed database synchronized issues. It involves economic models, math, encryption, and algorithms [8].

2.1 Blockchain's Benefits:

2.1.1 Decentralization

The primary advantage of the blockchain is that, because of this feature, data is not recorded, held, or updated by a central authority. The necessity for a central authority or mediator to verify or authenticate transactions is eliminated by the automatic sharing and distribution of information across network nodes. A single node's failure has no effect on the blockchain network's availability or security, which is a very useful feature in preventing malicious attacks or technological faults and eliminating a single point of failure [9][10].

2.1.2 Networks that are peer-to-peer (P2P)

A peer-to-peer (P2P) network's decentralization enables those who use it to conduct transactions without the need for a central server. Peers, or nodes—usually computers—contain freely and without the assistance of a third party on the network. As opposed to the conventional client-server model, where a request is made by a client and then achieved by a server, the P2P network paradigm allows nodes to act as both clients and servers, offering them equal power and enabling them to perform the same tasks in a network. Blockchain is a peer-to-peer network that functions as the distributed ledger for digital assets [11].P2P networks are not managed by a central server; instead, the network's nodes, or users, are in charge of keeping them up to date. Each node in the network functions as a server, capable of file uploading, downloading, and sharing files with other nodes. The nodes use their hard discs

instead of a central server to store this data. The P2P network is faster, more secure, and more effective since each node has the ability to send, receive, and store files. It is significant to note that the P2P design works best when there are a large number of active nodes in the blockchain network, which enables peer nodes to be quickly located by new peers who join the network. Make sure there are enough nodes remaining in the network to cover any gap in case a large number of them leave [12].

2.1.3 Open and Transparency:

The blockchain makes all transaction data from the scattered network nodes available and transparent. Since blockchain technology is decentralized, all nodes are guaranteed to exchange records and data. Every node within the network is endowed with equal access rights and responsibilities to authorized information that is shared with other nodes within the same network. It enhances the blockchain's consistency and accuracy throughout the whole network [13].

2.1.4 Anonymity:

Data transmission and transactions can now be anonymous thanks to blockchain technologies, which remove the need to reveal the true identity of the node connected to the user. Rather, the only thing needed is for the node to be aware of the user's blockchain address. Users can communicate with the blockchain network by using an address that is generated at random [14]. Due to the decentralized nature of the blockchain network topology, there is no central body that oversees or maintains track of users' private information. The blockchain's trustless ecosystem allows for some degree of anonymity. This function ensures the confidentiality and privacy of the participants [15].

2.1.5 Traceable and Immutable:

The blockchain updates the distributed ledger with transactions in a sequential time-order. Every transaction is time- and date-stamped in order to preserve the transaction sequence and enable data traceability [16]. The timestamp supports the accuracy of the data in addition to ensuring real-time transaction tracking, the timestamp supports the data's accuracy. However, it encourages permanent alterations to data or records. Once the transaction has been confirmed and added to the block via a consensus procedure, it cannot be altered. It is challenging to circumvent the system and alter the record, even for an attacker with extremely powerful computing skills. This can only happen if the attacker controls a minimum of 50% of the nodes. This function ensures the blockchain system's dependability and durability while preventing double spending [17].

2.1.6 Trust and Secure:

New transactions cannot be added to the distributed ledger until the majority of network nodes concur through consensus procedures to confirm the veracity of the data transmitted via encryption. Once the data has been validated, put into the distributed ledger, and verified, it is made available to all participating network peers. Consequently, the blockchain acquires confidence and transparency [18]. Symmetric encryption techniques guarantee the security of blockchain technology. The reliable cryptocurrency hashing chain is an additional element that enhances blockchain security. Since the hash value of the previous block must be included when a new block is generated along with other elements through consensus methods, it is extremely difficult to alter any information in the hash value [19].

3. Architecture of Blockchain

Fig. 2 – Proof of Work (POW)Blockchain is a decentralized, immutable database that simplifies tracking of assets and recording of transactions within a corporate network [20], [21]. Assets that are tangible include things like real estate, vehicles, cash, and homes. Trademarks, intellectual property, patents, and copyrights are some instances of intangible assets [22]. A hash function joins the blocks to create an unbreakable chain [23], [24].

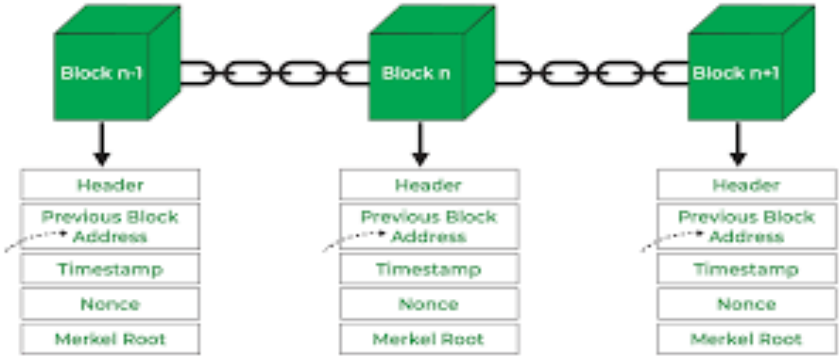

Fig. 1 – Blockchain Architecture

A block is composed of multiple transactions that are logically arranged and grouped together [12]. An event that occurs specifically, such as moving money from one account to another, is documented by a transaction [13], [15]. The size of the transactions that make up a block varies depending on the blockchain's kind and design [16]. The genesis block is the first block in the blockchain; nevertheless, Figure 1 depicts the general structure of a block in the blockchain, which includes the following properties:

- A nonce: is a figure that was chosen at random. A nonce is used to provide replay security, encryption, and authentication in a number of cryptographic procedures. It is utilized in blockchain transaction replay defence and proof-of-work (Pow) consensus algorithms [17], [18].
- A Merkle root: is a hash of every node in the Merkle tree. Massive data structures can be efficiently and reliably verified with Merkle trees [19]. In the context of blockchain technology, Merkle trees are frequently employed to facilitate effective transaction verification [20]. The block creation time is represented by the timestamp. The time when the mining nodes started mining is recorded because it is Unix time [21]. The value exceeds the timestamp of the preceding blocks [22].
- The timestamp: is the block's creation time. The time when the mining nodes started mining is recorded because it is Unix time [21]. The value exceeds the timestamp of the preceding blocks [22].
- A hash function: A function known as a hash function is able to reduce a message of any length to a message description of a predetermined length. The hash process can be used on blockchains because of two features [10]. Hashing, first of all, yields the irreversible result B, but it is unable to identify the pre-hash structure A [23].
  Block body: It has transactional data on it [24].

4. THE CONSENSUS ALGORITHM

Over 1500 cryptocurrency tokens are in circulation right now. Here are a few well-known consensus algorithms:

4.1 Proof of Work (Pow)

The most popular algorithm is the proof-of-work algorithm. Cryptocurrencies like bitcoin and Ethereum, each with unique characteristics, employ this algorithm [25]. Fig 2 The blockchain's proof of work (PoW) mechanism is used to validate transactions and create new blocks. Miners compete with one another using proof of work to finish the network transaction and receive payment. This algorithm's main objective is to resolve the mathematical puzzle. Right now, what is a mathematical puzzle? The problem is one that will need a lot of processing power to resolve. After figuring out the puzzle, miners validate the transaction and create a new block. Only a block is permanently added to the chain when additional nodes have verified the transaction's validity. If the problem is too complicated to solve, a lot of time will be needed to generate the blocks. However, if the issue is too simple in another case, spam and DOS attacks are more likely to occur. Other nodes must be able to quickly verify the solution; otherwise, not all nodes will be able to determine whether the computation is accurate. As a result, it will need to trust other nodes, which goes against one of the key characteristics of blockchain technology: transparency. The puzzle's complexity is contingent upon the quantity of users, network load, and power availability. Each block's hash value includes the

hash value of the previous block, enhancing security. Since the genesis block has no parent block, it is an exception and has a hash value of zero [26]. This type of consensus is based on Bitcoin. This puzzle is known as hash cash. The Proof of Work algorithm permits adjusting a puzzle's complexity in accordance with the network's overall power. Any block may be formed in roughly ten minutes on average. The primary drawbacks of this algorithm are its enormous cost, computations that are pointless, and 51 percent attack [27].

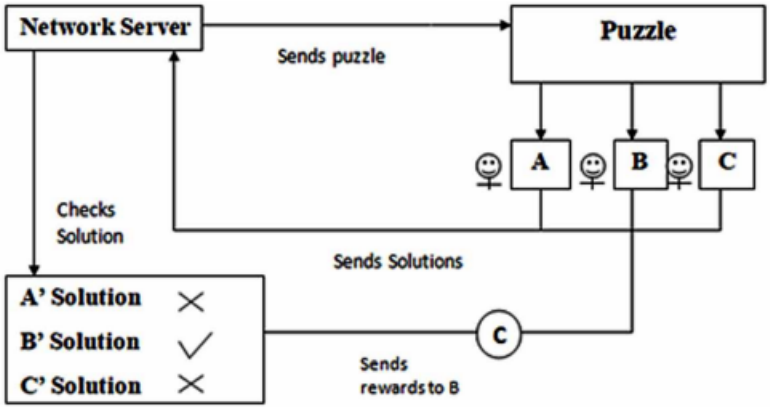

Fig. 2 – Proof of Work (POW)

4.2 Proof of stake

Even though proof of stake was included in the original Bitcoin project, its use was not carried out for a variety of reasons, including its resilience [26]. This is a different algorithm than the Proof of Work algorithm, which verifies the transaction using a cryptographic technique. For peer coin, proof of stake is typically used instead of proof of work. Traditionally, the account balance was used to pick miners in this process; the higher the account balance, the higher the chance of becoming a miner. Because of his large account balance and subsequent inequity towards others, the richest individual is therefore more likely to become a permanent miner. Because of the centralization that results from this process, other alternative selection procedures have been developed. Proof of Stake in peer coin cryptocurrency blends the notion of "coin age" with randomization. According to [26], the equation is as follows: proof hash * coin age * target. Coins that have not been spent for at least 30 days are eligible to compete for the next block. The likelihood of a larger, older collection of coins signing the following block is increased. The stake in currency must start with zero "coin age" after being selected to sign a block and must wait at least 30 days before signing another block. As a result, this technique secures the network and produces new coins without using a lot of computing power. Compared to Proof of Work, which mostly depends on energy consumption, Proof of Stake is more effective [28].

4.3 Delegated Proof of Stake

When Satoshi Nakamoto first launched the project, he envisioned a scenario where anyone could mine using their CPU. Each node had the potential to participate in the blockchain, and their hashing powers could align. However, as time progressed, specialized mining equipment was developed. In delegated proof of stake (dPOS) systems, stakeholders can designate a variable number of witnesses to produce blocks. Witnesses can be added or removed from the list during each maintenance interval. At a set rate of one block every n seconds, each witness takes turns producing a block. They receive rewards for each block they create. If an elected witness fails to present a block after being chosen, they risk being voted out in the next election. Once new blocks are generated based on the designated number of witnesses, a predefined online time must be maintained. BitShares serves as an example of a dPOS system. Blockchains that utilize dPOS are generally more efficient in terms of productivity and energy consumption compared to proof of stake (PoS) and proof of work (PoW) systems.

4.4 Proof of Importance

POI clusters data and gives the most significant nodes a priority utilizing hash calculations by utilizing transaction graph analysis and indications like transaction amounts and node balances [30], [28]. Certain nodes are more significant than others. NEM introduces the importance of the notion of proof. PoI uses a mechanism that NEM calls "harvesting," which selects the network users (nodes) permitted to add a block to the blockchain. Nodes retain the transaction fees in exchange for harvesting blocks. An account with a higher importance rating has a better chance of being selected to harvest a fresh block.. XEM is the main cryptocurrency that Proof of Importance uses. Every account on the NEM network has access to the XEM balance. PoI takes advantage of a process that NEM refers to as "harvesting," which chooses which nodes—network users—are allowed to contribute a new block to the blockchain. Nodes that harvest a block are granted the right to retain the transaction fees. An account with a higher importance rating has a better chance of being selected to harvest a fresh block. XEM is the main cryptocurrency that Proof of Importance uses. Every account on the NEM network has access to the XEM balance.

4.5 Practical Byzantine Fault Tolerance

In distributed systems, byzantine fault tolerance may be a useful technique for resolving transmission faults [31]. However, the Byzantine system from before required exponential operations. The 1999 introduction of the PBFT system resulted in a reduction of algorithm complexity to a polynomial level and an increase in efficiency [28].

4.6 Ripple Transaction Protocol

The core of ripple technology is the XRP ledger, a shared public ledger that facilitates distributed payments, exchanges, and remittances. It was generated by a consensus process. Ryan Fugger created the ripple payment system for the first time in 2004. Open Coin developed the ripple transaction protocol (RTP) based on an idea by Ryan Fugger. The direct transfer of funds between two parties is made possible by the Ripple Transaction Protocol. Ripple is quick and provides security. It was a distributed public ledger framework that allowed for payments, exchanges, and remittances by using consensus mechanisms [28].

5. A Comparative Analysis of Algorithms

Blockchain consensus methods vary in their benefits and downsides. Table 1 presents a comparison of different algorithms for certain important properties of the blockchain.

1. Energy Saving: Mining nodes in Proof of Work must constantly solve a mathematical challenge, which requires a lot of processing power. It follows that there is a tremendous amount of energy [32]. On the other hand, with PoS and DPoS, miners' workload diminishes since the search space becomes more constrained. In terms of consensus strategy, mining does not exist for PBFT or Ripple. It conserves energy as a result

2. Data Model: A data model is an asset-focused transaction. Networks can be created by many businesses to trade assets with one another, but specific configurations are needed for every system [33]. These organizations are known as ledger owners. Ripple makes its ledger public and issues its own token assets as a means of exchange.

3. Application: Certain ledgers enable the execution of extensive computations that are specified by the user. Users can use Ethereum and its derivatives, including Hyper chain, Quorum, Monax, Parity, and Definitely, to programmed any kind of business logic to be executed on top of the ledger [28].

Examples: The Proof of Work algorithm is used by Ethereum and Bitcoin. While Ripple employs the Ripple Transaction Protocol and features an account-based data format, Peercoin solely concentrates on proof of stake

Table 1 - Blockchain algorithms are compared for a set of blockchain features.

Characteristics/ Processes	Prof of work	Proof of Stake	Proof of Importance	Practical Byzantine Fault	Practical Byzantine Fault	Ripple Transaction

				Tolerance	**Tolerance**	**Protocol**
Creator	Ari Joels and Markus Jakobsson	The coin Peer Coin	NEM	Danial Larimer	Castro and liskov	Jed McCaleb and Chris larsen
The year	the year 1999	6. -	The year 2015	The year 2014	The year 1999	The year 2012
Identity of nodes	Public	Public	Public, Private	Public	Private	Public
Processing Capacity	7. High	Comparatively inexpensive	Low	Low	Low	Low
Efficiency in Energy Use	No	Partially	Yes	partially	Yes	yes
Information model	Transaction-oriented	Account-based	Transaction-Based, Account-Based	Transaction-based, Account based	Essential: valued	Account-based
Language	C++, Golang, Solidity, LLL	Michaleson	Java	No scripting	GoLang, java	Java, Go, c++
Uses	Crypto-currency, General application	Michaleson Application	Blockchain Platform	Decentralized Exchange	Generally Used	Digital Resources, money
As an example	Bitcoin, Ethereum, ZCash, and Litecoin	Tezos, Peercoin, and Mint	XEM	Cryptocurrences	Hyperledger	Spiral

6. ATM (Automated Teller Machine)

Bank users can access their accounts without needing to do so by using an ATM. Visit the bank. The only way to do this is to create the application utilizing online ideas. When the product is put into operation, the user will be able to view all of the data and services that the ATM offers after entering the required options and arguments. In addition, the software offers advanced user-required services like depositing money and obtaining checks. The information is kept in the database and is accessible whenever needed. The implementation must operate on ATM hardware or a comparable emulation. It is also possible to use requirements for effectively utilizing the generated product.

The following steps were taken in order to construct this ATM system:

1. The verification procedure.
2. Select the account, service, and language.
3. Services provided by banks.

4. Deals.
5. Unique services.

The card number and PIN can be obtained by the user thanks to the program's architecture. After verification, a menu is given to it, and the / option is there. For instance, the user can adjust the size of the Payment History option in the main menu when wishing to display a list of past payments. The payment history appears on the screen when the The General Assembly option is chosen .user ought to peruse other pages as well, such as the prior and following ones. When retrieving or presenting a large amount of data, the user can encounter delays if they are not logged into the same bank branch system.

6.1 How an ATM Operates:

The data terminal functioned as an ATM. ATMs require a host computer to connect to or communicate with as described in fig. 3

1. The host computer might be thought of as an ISP, or Internet service provider.
2. The host computer serves as the user's portal to access all of the different ATM networks.
3. Customers use an "ATM CARD," a plastic card with a magnetic stripe, to authenticate themselves when using an ATM system.
4. The magnetic stripe stores the customer's account number and PIN (personal identification number), a numeric password.
5. The consumer is prompted to insert their card at the ATM.
6. The customer's personal identification number (PIN) is prompted when the card is entered.
7. The consumer enters their PIN.
8. In the event that the card is legitimate and the computer can handle it, control moves on to the next step and asks the user to deposit, withdraw, or transfer money.
9. Most ATMs will keep the card if the number is input incorrectly multiple times in succession as a security measure to stop unauthorised users.
10. A smart card is used by ATMs to read and save consumer data.

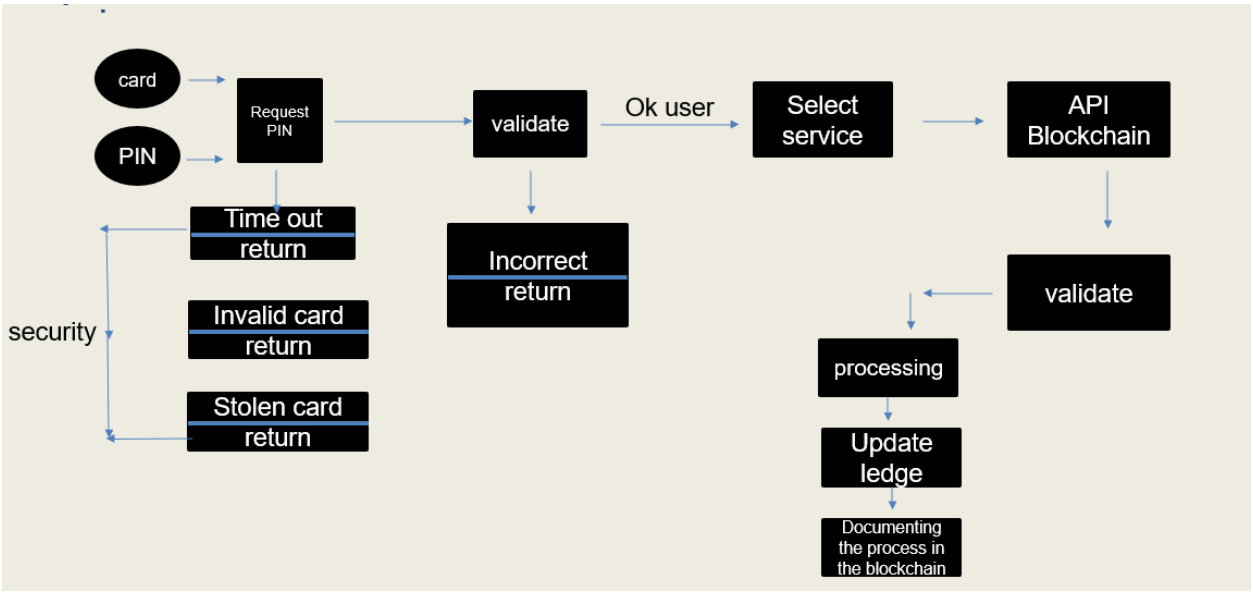

Fig. 3 – ATM Structure.

6.2 ATM Security and Safety

The security services that users require to safeguard their ATM cards from fraudulent use are included in the security standard. The primary goals of ATMs are access control, correct functionality, availability, data integrity, confidentiality, and accountability. It is possible to identify the primary functional security requirements to address common threats. They are as follows [28]:

1: Identity verification.

2: Authorization and Access Control.

3: Confidentiality Protection.

4: Data Integrity Protection.

5: Strong Accountability.

6 Activity Logging.

7: Alarm Reporting.

8: Audit.

9: Security Recovery.

10: Security Management.

6.3 Threats to an ATM Network

There will be numerous risks to the ATM network. A small percentage of network threats are:

1. Eavesdropping: By connecting to the transmission medium, an attacker may be able to eavesdrop on data and gain unauthorized access. This is one of the network's most common attacks.
2. A masquerade: When someone impersonates someone else in an effort to get information, it might be dangerous.
3. Service Denial: Provision of Services When one entity neglects to complete its task and keeps other entities from completing theirs, this is known as denial.
4. Traffic Analysis: The term "traffic analysis" describes the possibility that a hacker could obtain information by gathering and examining data such as a virtual channel's (VC) volume, timing, and communication parties. Even though the data is encrypted, volume and timing can still provide a hacker with a wealth of information because encryption has no effect on these factors.
5. Information corruption: occurs when someone with the right authorization manipulates, delays, erases, or changes data that has been communicated.
6. Forgery: The term used to describe the sending and reporting of fraudulent information is forgery. In order to actually accomplish this, some data that belongs to the verified person must be changed.

7. Conclusion

In recent years, there has been a notable surge in the field of blockchain analysis. Blockchain analysis has applications and limitations, much like any other developing technology. We shall examine the conclusion derived from the examination of various applications and problems in this review. In conclusion, blockchain analysis offers a wide range of applications, even though it has issues with data integrity, pseudonymity, scalability, and privacy. Blockchain research has shown its worth in a number of fields, including finance, supply chain management, and forensic investigations. It has also helped prevent money laundering. For blockchain analysis to be widely adopted and effective as the technology develops, it will be essential to solve its problems and fully utilize its potential.

References

1. Majid M, Habib S, Javed AR, Rizwan M, Srivastava G, Gadekallu TR, Lin JC. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors. 2022 Mar 8;22(6):2087.
2. ALahmed S. Internet of Things Based Blockchain Technology for Gas Station. Iraqi Journal of Intelligent Computing and Informatics (IJICI). 2022 Dec 1;1(2):86-96.

3. Ma M, Shi G, Li F. Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario. IEEE access. 2019 Mar 10;7:34045-59.
4. Sultana T, Almogren A, Akbar M, Zuair M, Ullah I, Javaid N. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. Applied Sciences. 2020 Jan 9;10(2):488.
5. Lewis A. Blockchain technology explained. Blockchain Technologies. 2015:1-27.
6. Scholer K. An introduction to Bitcoin and Blockchain technology. Kaye Scholer LLP. 2016 Feb:3-22..
7. Banerjee M, Lee J, Choo KK. A blockchain future for internet of things security: a position paper. Digital Communications and Networks. 2018 Aug 1;4(3):149-60.
8. Lin IC, Liao TC. A survey of blockchain security issues and challenges. Int. J. Netw. Secur.. 2017 Sep 1;19(5):653-9.
9. Hamza NM, Ouf S, El-Henawy IM. A Proposed Technique for Enhancing the Mining Process in Blockchain Architecture. In2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) 2020 Mar 11 (pp. 7-12). IEEE.
10. Huynh TT, Nguyen TD, Tan H. A survey on security and privacy issues of blockchain technology. In2019 international conference on system science and engineering (ICSSE) 2019 Jul 20 (pp. 362-367). IEEE.
11. Hao W, Zeng J, Dai X, Xiao J, Hua Q, Chen H, Li KC, Jin H. BlockP2P: Enabling fast blockchain broadcast with scalable peer-to-peer network topology. In Green, Pervasive, and Cloud Computing: 14th International Conference, GPC 2019, Uberlandia, Brazil, May 26–28, 2019, Proceedings 14 2019 (pp. 223-237). Springer International Publishing.
12. Puthal D, Malik N, Mohanty SP, Kougianos E, Das G. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. IEEE Consumer Electronics Magazine. 2018 Jun 15;7(4):6-14.
13. Li S, Xiao H, Wang H, Wang T, Qiao J, Liu S. Blockchain dividing based on node community clustering in intelligent manufacturing cps. In2019 IEEE International Conference on Blockchain (Blockchain) 2019 Jul 14 (pp. 124-131). IEEE.
14. Sahoo S, Fajge AM, Halder R, Cortesi A. A hierarchical and abstraction-based blockchain model. Applied Sciences. 2019 Jun 7;9(11):2343.
15. Ma Y, Sun Y, Lei Y, Qin N, Lu J. A survey of blockchain technology on security, privacy, and trust in crowdsourcing services. World Wide Web. 2020 Jan;23:393-419.
16. Yang X, Liu J, Li X. Research and analysis of blockchain data. InJournal of Physics: Conference Series 2019 Jun 1 (Vol. 1237, No. 2, p. 022084). IOP Publishing.
17. Golosova J, Romanovs A. The advantages and disadvantages of the blockchain technology. In2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE) 2018 Nov 8 (pp. 1-6). IEEE.
18. Ling X, Wang J, Le Y, Ding Z, Gao X. Blockchain radio access network beyond 5G. IEEE Wireless Communications. 2020 Oct 20;27(6):160-8.
19. Sankar LS, Sindhu M, Sethumadhavan M. Survey of consensus protocols on blockchain applications. In2017 4th international conference on advanced computing and communication systems (ICACCS) 2017 Jan 6 (pp. 1-5). IEEE.
20. Banerjee M, Lee J, Choo KK. A blockchain future for internet of things security: a position paper. Digital Communications and Networks. 2018 Aug 1;4(3):149-60.
21. Li S, Xiao H, Wang H, Wang T, Qiao J, Liu S. Blockchain dividing based on node community clustering in intelligent manufacturing cps. In2019 IEEE International Conference on Blockchain (Blockchain) 2019 Jul 14 (pp. 124-131). IEEE.
22. Hughes L, Dwivedi YK, Misra SK, Rana NP, Raghavan V, Akella V. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. International journal of information management. 2019 Dec 1;49:114-29.
23. Lin IC, Liao TC. A survey of blockchain security issues and challenges. Int. J. Netw. Secur.. 2017 Sep 1;19(5):653-9.
24. Yang X, Liu J, Li X. Research and analysis of blockchain data. InJournal of Physics: Conference Series 2019 Jun 1 (Vol. 1237, No. 2, p. 022084). IOP Publishing.
25. Ogiela MR, Majcher M. Security of distributed ledger solutions based on blockchain technologies. In2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA) 2018 May 16 (pp. 1089-1095). IEEE.
26. Mingxiao D, Xiaofeng M, Zhe Z, Xiangwei W, Qijun C. A review on consensus algorithm of blockchain. In2017 IEEE international conference on systems, man, and cybernetics (SMC) 2017 Oct 5 (pp. 2567-2572). IEEE.
27. Tosh DK, Shetty S, Liang X, Kamhoua C, Njilla L. Consensus protocols for blockchain-based data provenance: Challenges and opportunities. In2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) 2017 Oct 19 (pp. 469-474). IEEE.
28. Krishnamurthi R, Shree T. A Brief Analysis of Blockchain Algorithms and Its Challenges. Architectures and frameworks for developing and applying blockchain technology. 2019:69-85.
29. ALahmed S. Internet of Things Based Blockchain Technology for Gas Station. Iraqi Journal of Intelligent Computing and Informatics (IJICI). 2022 Dec 1;1(2):86-96.
30. Tasatanattakool P, Techapanupreeda C. Blockchain: Challenges and applications. In2018 International Conference on Information Networking (ICOIN) 2018 Jan 10 (pp. 473-475). IEEE.
31. Sultana T, Almogren A, Akbar M, Zuair M, Ullah I, Javaid N. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. Applied Sciences. 2020 Jan 9;10(2):488.
32. Ogiela MR, Majcher M. Security of distributed ledger solutions based on blockchain technologies. In2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA) 2018 May 16 (pp. 1089-1095). IEEE.
33. Dinh TT, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering. 2018 Jan 4;30(7):1366-85.