Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
e-ISSN: 2790-4822p-ISSN: 2958-0862

Blockchain technology, methodology behind it, and its most extensively used encryption techniques.

Marwa Sami Mohammed [1*], Asaad N. Hashim [1]

[1] Department of computer science, University Of Kufa, Najaf, IRAQ.

*Corresponding Author: Marwa Sami Mohammed

DOI: https://doi.org/10.55145/ajest.2023.02.02.017
Received February 2023; Accepted April 2023; Available online May 2023

ABSTRACT: Blockchain is an innovative type of information technology (IT). It has the potential to revolutionize various sectors. Since its inception, Blockchain technology(BC) has been a novel technique in IT. Blockchains are public ledger of chronologically-connected transactions or occurrences. Blocks retain their hash code. Due to distributed consensus, it records cryptographic transactions in a public ledger. Thus, Blockchain may resist fraud and hacking, and the secure transmission of information has been provided using these cutting-edge encryption technologies, contributing to Blockchain's rising popularity and demand. Blockchain employs encryption at multiple points throughout the process. Blockchain technology resists various harmful attacks and eliminates many associated dangers, but not all.Distributed consensus, cryptography, and anonymity these mechanisims , in some cases, which may weaken its resilience to various frauds and maliciousness. This research aims to provide a comprehensive study of Blockchain technology, its architecture definition, its most important components, elements, and types, and to clarify the technologies that are considered the basis of its work and integration. Among these techniques is encryption; then, we discuss the most important encryption algorithms (Aes, Des, and Bluefish) currently used with Blockchain to solve the security problems they are exposed to and provide full protection for their data.

Keyword: - Blockchain technology, Cryptography, Hash algorithm, Consensus Mechanism

1. INTRODUCTION

As outlined in its white paper from 2008, bitcoin is a decentralized digital currency (Nakamoto 2008). There would be no bank or governing body in charge of the monetary system. It would instead be managed by a collection of autonomous workers. This article used public and private key cryptography to generate anonymous and secure identifiers. With the use of existing cryptographic time stamps based on hash methods, previous transactions became irreversible. Because of these features, digital cash may be (pseudo)anonymous and difficult to counterfeit. The objective was to provide a system for recording past deals that didn't require a reliable go-between. Even if some nodes in the network sent out false signals, an automated system might nevertheless get the vast majority of nodes to agree on the whole audit trail of financial activity. In order to resolve this distributed consensus problem, participants fought for the right to add new transactions to the decentralized database. An intricate job is taken up by computers. It is only via trial and error that the proof-of-work solution may be found. To update their own blockchains, users wait for the first person to solve the problem to broadcast the latest block of transactions to the network. and here come The term "blockchain" refer to the chain of currently active transactions; therefore, A first person to resolve the problem could affix a block of new transactions to the series of currently active transactions, after which the new block is distributed to the network so that all participants can renew their individual blockchains[1]. the blockchain is a distributed ledger, anybody with the appropriate credentials may access and make changes to the ledger's contents[2]. Blockchain uses several techniques to achieve integration, starting with consensus techniques that ensure that transactions are completed correctly and verified, and they have a significant impact on the effectiveness of the blockchain and its scalability[3, 4]. It was also characterized by decentralization, which is the feature provided by the peer-to-peer network, and it is considered an essential feature in the Blockchain, as it enabled it to transfer valuable assets and digital currencies

*Corresponding author:- marwa.mawash@student.uokufa.edu.iq without the need for an intermediary or central server.[btc network].and the most important techniqusing in blockchain is the cryptography that provide the security on it, and Due to the distributed consensus, it records cryptographic transactions in a public ledger that is impossible to modify or hack. Consequently, blockchain is supposed to be resistant to fraud and hacking. Although blockchain technology is resistant to a variety of destructive attacks and decreases several related risks, it does not prevent all assaults. Its protective methods (such as distributed consensus, cryptography, and anonymity) may compromise its resilience to some sorts of fraud and malice. when the file transmission system employs blockchain technology. Since blockchain merely enables authentication, an encryption mechanism was used to secure the data's privacy[5].Consequently provided the safety of the procedure[4]. In this paper, we will give a general overview of Blockchain technology, including its definition, elements, and components, the most important types, the differences between them, the protocols that govern how they work, how they work, where they are used today in society. We will then explain how Blockchain technology works and explain the main technologies behind its integration and The most important encryption algorithms used in the Blockchain were mentioned, as well as the encryption algorithms that were added to it to increase security during storage and transmission operations.

2. Definition of Blockchain

The blockchain is a series of blocks containing information[6].The BC is a stable digital ledger of business transactions that may be configured to register anything of value. A blockchain is, at its most fundamental level, a time-stamped set of fixed data entries controlled by a group of computers not owned by a single company. Using cryptographic techniques[7].each of these data blocks (blocks) is safeguarded and connected to the others. Additionally, Blockchains are defined as a digital system that employs encryption, networking, incentives structures, and distributed ledger technology to streamline the processes of verifying, executing, and recording transactions amongst a large number of parties. In essence BC systems are decentralized databases with highly desirable qualities. The inalterability of previously completed transactions is one of these benefits, as is the facilitation of the development of trust between participants in the absence of a middleman or third-party[8].At first, it was used mainly for storing exchanges of digital currencies, but now it serves many more purposes, including those unrelated to finance[9].

2.1 Blockchain Architecture: -

The BC is a distributed ledger that is organized as a chain of blocks, each of one of them save an entire record of a transaction. Each block has a pointer to the block that came immediately before it. This pointer serves as a hash value of the prior block, which can be called as the parent block. The hashes of uncle blocks, which are blocks that are offspring of the block's predecessors, would also be saved on the Ethereum BC. The initial block added to the BC is known as the genesis block, and as can be seen in figure(1), it does not have any blocks that it is connected to as its parents[10].

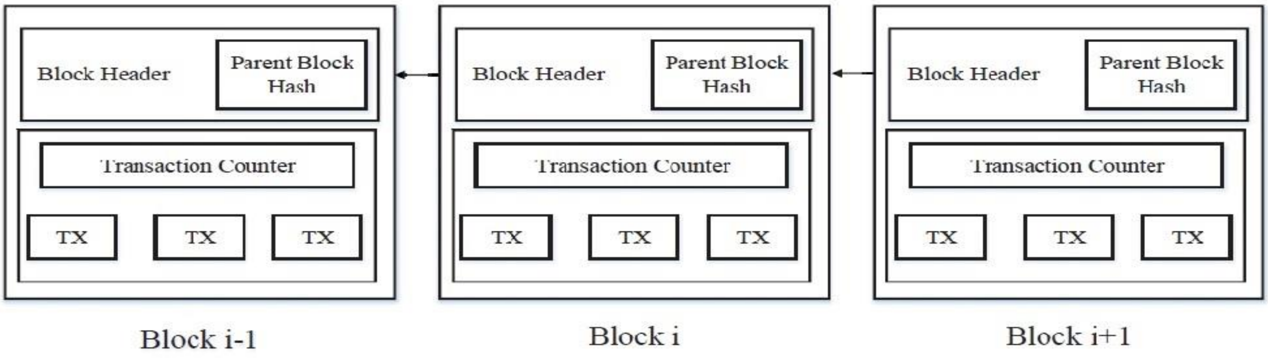

FIGURE 1. - Blockchain composed up of a series of connecting blocks [11]

2.2 Genesis block in BC

It is the initial block, and it is the common origin parent of all blocks that have recently been formed. If we go back in time, we will finally arrive at the genesis block. which first began in the year 2009. Due to the fact that it is encrypted within the bitcoin client program, it is not susceptible to manipulation. The hash and the structure of the encrypted genesis block, which consists of a message, are always available to every node in the network[12].

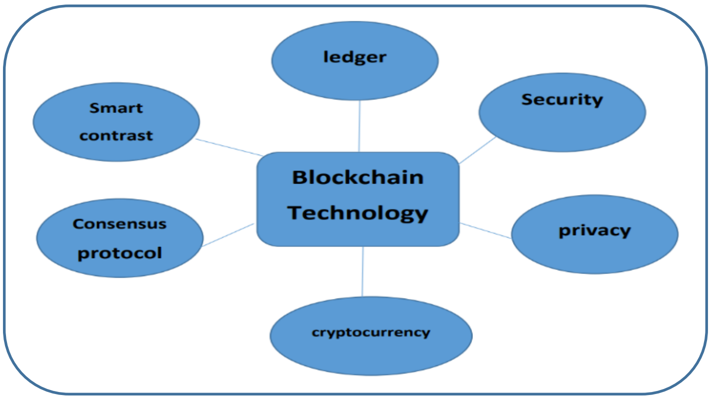

FIGURE 2. - General Architecture of Blockchain Technology[13]

2.3 Elements of Blockchain

The blockchain consist of several element as following: -

1-Ledger: The technology behind BC is a form of distributed ledger. Indicates that everyone on the network has the duplicate copy of the record. In the BC, there is neither a central authority nor a reliable third party. It is nothing more than a mining process[13]

Mining :-is the process by which nodes carry out rigorous computations and dedicate their resources (such as CPU, power, etc.) to locate the nonce(a one-time, unique) number[14].

2-Consensus Protocols: A consensus mechanism is used by the blockchain network to obtain an agreement on the sequencing of transactions in the network, the updating of the ledger, and the selection of a miner for the next block generation[15].

3-Security :- Blockchain makes use of public key cryptography and digital signatures to confirm the authenticity of network transactions[13].

4- Cryptocurrency :- is the process of securing data by converting it (i.e., encrypting it) into a format that can only be decoded (or decrypted) by a person who has a secret key[16].

5-Privacy: - The blockchain allows for the storage of any kind of data. If sensitive data is being processed, for example, the privacy regulations apply. health information or a citizen service[13].

6-Smart contract: - are more potent uses of blockchain technology that monitor every stage of any deal from beginning to finish. When the condition has been met, The smart contracts can be self-enforcing and self-executing[17]. Simple functions can also be written into smart contracts[7]. These contracts serve as commitments with the company[13].

2.4 Components of Blockchain

The blockchain is constructed of the following two components: -

transaction:- represent The activity is initiated by the participant[18]. A blockchain's current state is reflected by the transactions that are continually generated by nodes then aggregated into blocks Every second, a large number of transactions are produced. It is important to verify the original transactions, and to ignore any bogus transactions[14].

Block: - is the Blockchain data structure used to save transaction records. The block is composed of a header and a body. As the figure (3) shows[9].

- **Block header component**

The header is the first part of the block, and it is composed of the following components

- Block version:- includes a list of block verification Bases that must follow[10].
- Merkle tree root hash:- includes a hash value for each transaction in the block[11].
- Timestamp:- provides a timestamp for the present time in seconds using the universal time(UTC) since the first of January 1907[9].
- N bits:- current threshold of hashing target in a compact format for valid block[10, 11].
- Nonce:-a four byte field that typically starts at 0 and increases by 1 for each hash [10].

- Parent block hash: - refer to the prior block.

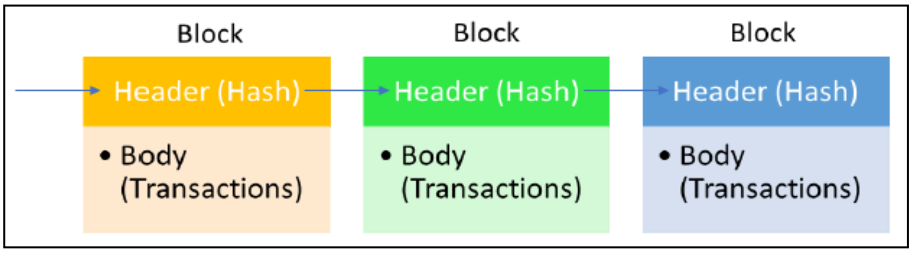

FIGURE 3. - **block in the BC architecture [9]**

- **Body of the block**

It consists of both transactions and a transaction counter in its entirety. The volume of the block as well as the size of each individual transaction, both have a role in determining the maximum number of transactions that may be preserved in the block. In order to verify the authenticity of transactions, BC employs An asymmetrically encrypted digital signature utilized in such an untrustworthy environment [11].

2.5 The mechanism of using a digital signature.

Are utilized as a means of authorship verification concerning the contents. Combining public key encryption with digital signatures is used in conjunction. In order to validate the signature, a receiver utilizes the signer's public key to verifying the signature. In this scenario, a signer's private key utilizes for signing a document. Digital signatures are considered authentic, as they cannot be faked, can only be used once, and cannot be revoked. It means that a digital signature cannot be changed to apply to any other document or content, that only the original signer can consciously claim the signature, and that even the original signer cannot revoke it[9].

2.6 Categories of the Blockchains [13].

Blockchain may be divided into three categories: -

1-public blockchain: - Everyone has access to it. Access to it is unrestricted. Exchanges can be sent for om anybody having an internet connection and a web link. However, because the public chain needs to pay for the transaction, execution, and storage costs, the exchanges are expensive because there is no precise point of attack for the hacker to assault one data center to bring the chain down. The most popular types of public chains are Blockchain and Ethereum[6].

2-**private blockchain:-** Only those invited by one organization are allowed to join and administer the network[9]. Blockchains used privately are authorized. Only if the network administrator accepts him may someone join. It is comparable to a conventional database and is also known as a shared distributed database. In this network, well-known entities are dealt with. The member has control over who may access the chain, whereas the member and validator have limited access to the network since the infrastructure controls it. It has a lower number of attack points[6].

3- **Hybrids (Consortium): -** The technique for determining consensus can only accommodate a particular set number of nodes simultaneously. In this scenario, the read permission may be public, or it could be limited. This lowers the network's level of security and makes it more susceptible to being tampered with in public networks. There is some centralization[19]. Each participant can select his or her consensus node within certain bounds. This kind is appropriate for a network made up of many institutions that are semi-closed[13].

Table 1. - **the difference between blockchains types[19]**

Characteristics	**Public BC**	**Private BC**	**Hybrid BC**
Efficiency	Low	High	High
license of read	Public Could	be public or bounded	Could be bounded or public
Consensus mechanism	Permission less	Permission needed	Permission needed
Consensus Selection	All miners	determined collection of nodes	single organization
Centralization	No	Partial	Yes

2.7 Mechanism of the blockchain working.

Each block contains information shared as feasible, encryption hash estimation of the prior block and a date (or hash respect). Once data has been stored in the blockchain, it cannot be manipulated or changed. As a result, it is an open, dispersed record that may constructively and indefinitely capture communications between two parties. Affirmation of work is a tool that prevents the generation of additional blocks in the blockchain. In the case of BTC, it takes about ten min. to compute work confirmation and include the new block. Because BC uses a peer-to-peer structure, anybody may participate. When an individual joins this framework, they receive a complete copy of the blockchain. The center point might make utilization of this copy of the block to demonstrate that everything is being examined jointly. In case some individual needs to make another block, this block is distributed to each and every participant on the framework, and every center point at that time affirms the block. If everything appears good at every hub, upload this block to the blockchain. This system's hubs all reach an accord. They agree on which blocks are genuine and which are not. Squares are prepared to be rejected by many hubs. So, in order to successfully access the blockchain, you must execute proof of work (pow) for each and every block and control more than fifty percentage of the peer-to-peer network; otherwise, only the temporary block may be accepted by all A (BC) can reach decentralized consensus as a result. As a result, some applications, such as event recording, conciliation records, and other records administration duties, such as character administration, sustenance traceability, reporting provenance, voting, or exchange planning, may be suitable for blockchain. Strong Byzantine fault tolerance and more secure architecture are made possible by BC technology enables more secure architecture and strong Byzantine fault tolerance[6].

2.8 Technologies behind BC.

There are leading three most essential technologies have been combined to make the integration of blockchain

- Consensus mechanism
- p2p network
- Cryptographic[20].

2.8.1 Consensus Mechanism

Consensus is used to verify the transaction and agree on how the ledger should be updated as a consequence of the transaction. Numerous Blockchain implementations use a diverse set of consensus mechanisms[9].Using a consensus process, all financial dealings will be finalized properly, additionally to verify the entire block of transactions. In the context of the applications of BC technology, two problems need fixing.

1-the Inconsistent Expenditures problem: - At the same time, making use of the currency in two different transactions

2-The Byzantine Generals' Trouble: - data is sent between nodes via p2p communication. In a distributed system, nevertheless, It is possible that particular nodes in the system will come under attack, resulting in modifications to the communication contents, necessitating the determination of the normal nodes[13]. The network's many processes need to reach a consensus. Without access constraints, The Sybil assault is a risk for networks, in which harmful programs can establish numerous fraudulent identities[3].The consensus algorithm is the most significant technical part of the BC and has a direct impact on its effectiveness and scalability, and as well as number of resources that are used by the BC system. The currently used consensus algorithms may be broken down into the five categories below.

1-Proof consensus: - In each round of consensus, the miner nodes must demonstrate that they possess a particular competence. In most cases, the technique of evidence involves completing a task in a race against other people. This job should be tough to accomplish yet simple to verify. Proof of Work (Pow) and Proof of Stake (PoS) accounting rights shall be awarded to the mining node that emerges victorious from the tournament.

2-Election consensus: - During each round of consensus, the miners vote for which node should serve as the next leader. The mining node that initially receives more than half of the votes is given the opportunity to construct the next block. This privilege is not given to any miner node, however. The vast majority of existing distributed consensus methods fall within this category. Paxos and Raft are two examples of such conventional distributed consensus algorithms.

3-Random consensus.: -Using a particular random mechanism, a miner node is chosen immediately as the round's leader node.

4-Consortium consensus: -First, the mining nodes use a predetermined technique to choose a group of representative nodes. Next, the representative nodes gain accounting rights either one at a time or by voting for them.

5-Mixed consensus:-In order to choose the leader node, the miner nodes use various consensus techniques in combination with one another. There are a variety of consensus algorithms in BC, as shown in figure (4). An agreement is reached during a round to begin a transaction on the blockchain, and the nodes will be responsible for approving it will first bundle the build the block and then send it out to the network. Furthermore, all the nodes in the Network nodes in a blockchain check each new block for legitimacy before it is added. In keeping with the consensus algorithm. If the obstructing is allowed, it will be added to the existing blockchain as an appendix to carry out an update procedure on data[4].

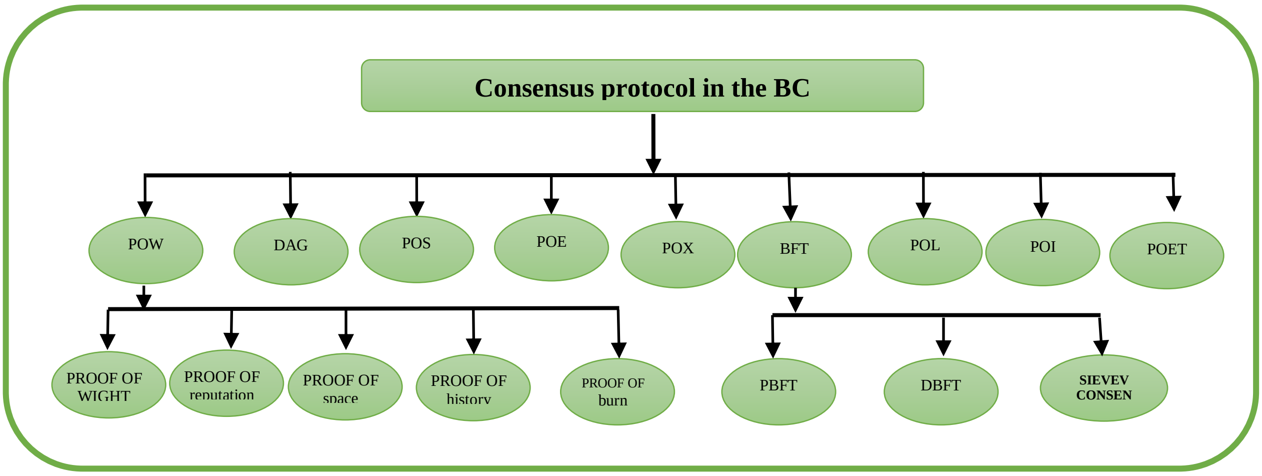

FIGURE 4. - **consensus algorithms in BC[9]**

2.8.2 P2P Network

The blockchain is administered by a decentralized network of computers known as peers. P2P networks are virtual networks constructed on top of the Internet. This peer to peer blockchain network may be represented as structured, unstructured, or hybrid based on numerous characteristics, including the consensus process and blockchain type[21]. Peers build and maintain this P2P network through peer discovery, neighbor selection, and managing inbound/outbound connections. Each node in a blockchain P2P network chooses a small subset of its neighbours randomly from the other nodes' lists to build and maintain outbound connections. Some bootstrap nodes complete the otherwise empty peers' lists. The remainder is progressively filled by peers identified using a distributed peer discovery method, such as Peers' list Exchange Protocol (PEX) and a modified Kademlia DHT protocol[22].A blockchain system must quickly distribute freshly created blocks to maintain a consistent global picture independent of the network's representation. A routing protocol may not be needed, but a synchronization protocol. This is not the case. In peer-to-peer networks, data is directed across the multiple hops using a routing protocol; however, this is not the case in blockchains (e.g., Bitcoin, Ethereum, and Litecoin). exploit unstructured P2P networks to establish an egalitarian network with equal rights for all nodes. P2P networks can have flat or hierarchical random graphs. Each node in the network keeps a directory of other nodes' addresses so that the distributed ledger can be updated in real-time. When one peer sends a network message, it is received by all peers via their connections. A peer of an unstructured network is free to leave and join at any time. An opponent who joins and observes network messages can source fake, rearrange, or insert messages. A blockchain network may also use a prearranged peer-to-peer Because the network's nodes are structured according to a particular topology, it is much simpler to locate a particular resource or piece of data. For better message delivery, each P2P node has a unique identifier. An organized peer-to-peer system keeps track of information via a DHT (distributed hash table) (key, value). Pairs of peers are kept in order to facilitate resource discovery. Using the Kademlia protocol, Ethereum has begun implementing a structured P2P network. Most blockchain networks, however, need more organization. If the (BC)is public, where no limitation to joining or leaving the network is imposed, then many different types of assaults are feasible. Therefore, the blockchain's security relies significantly on the design of the underlying network[21].

2.8.3 Cryptographic

The word "cryptography" comes from the Greek words "Kryptos," meaning "hidden or secret," and "graphein," meaning "to comproof of stack," respectively. The science or method of secret coding, particularly the use of cipher systems or coding. Cryptography is essential for maintaining secure communication between various entities[20]. Data protection against intrusion attempts relies heavily on security measures. Cryptography is one of the most vital tools for protecting sensitive information. In simple words, it can be defined as the practice of secret writing to safeguard information, an example of this Cryptography safeguards information by transforming it into unintelligible ciphertext that can only be deciphered by authorized recipients, who then translates the unreliable information into the original textual content. Symmetric and asymmetric cryptography are the two basic methods for encrypting data. asymmetric cryptography employs both public and private keys,while Symmetric cryptography encrypts and decrypts information using the same key[23].

The following is a list of common terms used in cryptography and blockchain:

-Plain-text: - This is the first understandable message or data that serves as input for the algorithm. It may be either text or numbers[24].

cipher text: - It is the output, which is a message that has been scrambled. It is contingent on the plaintext as well as the private key. You will get two different ciphertexts if you use two separate keys to encipher the same message. The ciphertext consists of a seemingly random stream of data and is now incomprehensible in its current form[24]. Or The text that no one can understand, sometimes known as ambiguous text[23].

key: - The key is an arbitrary mathematical quantity unrelated to the underlying plaintext or method. The algorithm's output changes based on the key's value. The program can perform accurate changes and replacements because of the key[24].

Encryption :- The plaintext is subjected to a series of substitutions and modifications by the encryption algorithm[24]. Encryption refers to any method used to transform plaintext into unreadable code. An encipherment algorithm and a key are required for the encryption method[23].

Decryption: - This is just the algorithem for encryption reversed. It creates the plaintext from the ciphertext and the private key[24].

Integrity:-Several techniques for checking the consistency of data in transit[25].Only authorized miners may create new blocks on the Blockchain [23].

Authentication:- The action of checking the validity of a system entity's declared identity[24]. In the blockchain, it is defined as the ability of a system to test the identity of a new block added.

Acces control :- New blocks on the blockchain may only be added by verified miners, who are then eligible to collect the reward[23].

Hash: - Numbers are used to linking blocks in a blockchain, much like the links in a linked list. These hash numbers are created using a cryptography method[23].

2.9 BLOCKCHAIN-APPROPRIATE ENCRYPTION ALGORITHM

Many encryption algorithms are used to authenticate transactions on the BC, public-key/asymmetric internet participants rely on cryptography to engage safely with the network, necessary in a blockchain, hash functions are used to create digital signatures and to establish a connection between different blocks[26].

2.9.1 Hash function

It is the function that only works in one direction to check the validity of data. Hash functions accept data of any length as input and produce strings of constant length as output, and it may hash a password or a whole document. The Hash function size is a very crucial thing, and A bigger hash makes the function harder to invert and collision-free. Multiple inputs can give the same hash size since hash functions have a fixed output. With so many different hash values, it is hard to discover two inputs that create matching hashes; for example, the Hashes are like data's fingerprints. If the data changes, the fingerprint will not match, and other valuable data will not give the same fingerprint. You can store these hashes to check data integrity later[27].

2.9.1.1 Type of hash algorithms

There are as many hashing algorithms as encryption techniques, but only a few are commonly employed. MD5, SHA-1, SHA-2 and SHA-256 are a few prevalent hashing algorithms[28].

- MD5

It is edition five of the Message Digest algorithm. MD5 provides 128-bit results. MD5 was a popular hashing algorithm. Nevertheless, that was before algorithmic faults began to appear. The bulk of these defects manifested themselves as collisions. Consequently, MD5 started to be superseded[28]. It is the quickest of the NET hashing algorithms, but it is also the most susceptible to long-term attacks. MD5 is susceptible to partial collisions and is unlikely to be able to survive future assaults as hardware capabilities advance[27]. MD5's plaintext of 512 bits stands out compared to other message digest algorithms. This plaintext consists of four blocks, each one a 32-bit block. The message digest is generated by MD5 using a five-step procedure, including padding, length division, input division into 512-bit blocks, an initial altering variable a process block, and four rounds of iteration, with a new constant used in each iteration[23].

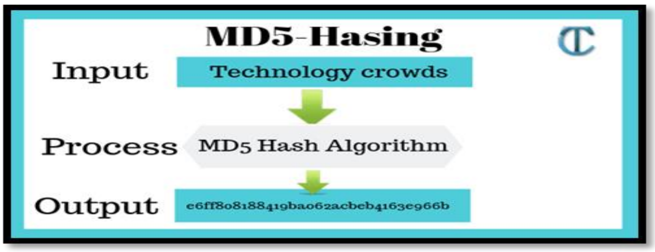

FIGURE 5. - MD5 hash

- SHA-1

It is a second standard version of the Secure Hash Algorithm, the first being SHA-0. SHA-1 produces outputs with 160 bits. After flaws were found in MD5, SHA-1 became one of the main algorithms that replaced it. SHA-1 received widespread adoption and usage. SHA-1 was approved as a conforming (FIPS) 140 methods of hashing[28]. It is a cryptographic hash function that, when given its input, will generate a 160-bit and 20-byte hash output. The Secure Hash Algorithm is its name. Another name for this hash value is a message digest, This message digest is commonly transformed into a hexadecimal number, and these numbers always have 40 digits[23].

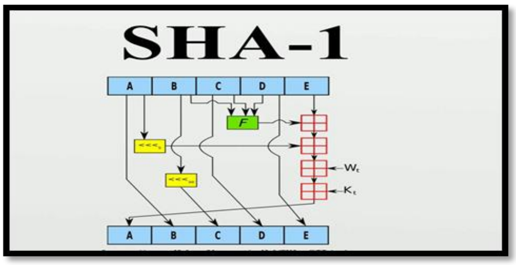

FIGURE 6. - SH1 hash[23]

- SHA-2

The United States's National Security Agency developed and released Secure Hash Algorithm 2 in 2001. There are six possible SHA-2 hashes, each one varying based on the bit amount used to encrypt the data. In order to prevent collisions, SHA-2 ensures that identical input data always generates a unique hash value. SHA-2 employs between 64 to 80 rounds of cryptographic operations, and it is frequently used to validate and sign digital certificates and documents[23].

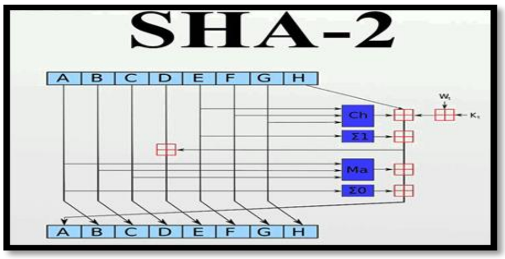

FIGURE 7. - SHA-2[23]

- SHA-256

Cryptographically, one of the most robust hash functions is SHA-256, an enhancement of the earlier SHA-1 method. Up to this point, no one has been able to breach it. It can generate a one-of-a-kind 256-bit hash code, or signature, for every given piece of text or data. A data's veracity may be ascertained by comparing the resultant "hash value" to a standard reference value[5]. SHA-256 is a subset of the SHA-2 family of hashing algorithms (Secure Hash Algorithm 2). The 256-bit output of the Secure Hash Algorithm 256 (SHA-256) is the result of a cryptographic hashing algorithm that has been granted a patent[23].

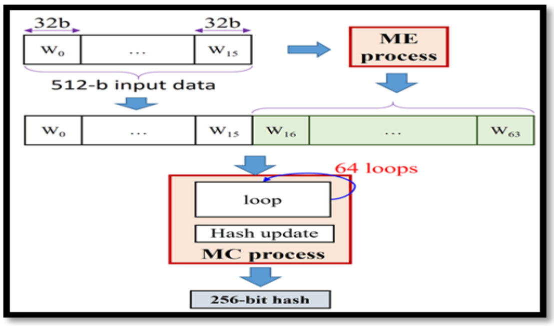

FIGURE 8. - SH256[29]

2.9.2 Other encryption algorithm using in Blockchain

Hash codes are more secure in an extensive network, but in a small network, hackers can always find a way in. For this purpose, the more common and well-known encryption techniques might be employed to protect the data as well as the hash function[5].

2.9.2.1 AES in Blockchain

The AES algorithm is one of the most used ones for secure data storage and transmission. The AES encryption and decryption framework are independent and distinctive. Each of the three key sizes that AES can handle 128, 192, and 256 bits. As the length of the key determines how many rounds are played. AES employs 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys, with the number of rounds determined by the key size. An (AES) encryption technique was applied in Blockchain to provide more security for data during transferring process as the following is first applied AES algorithm to the contents of the specified text file. The encrypted data file is then delivered to a hash function, which uses the SHA-256 hashing technique to generate a hash code. Next, the encrypted file is transferred to the customer.

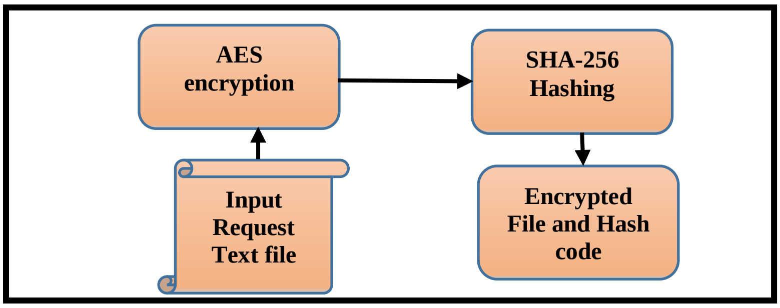

FIGURE 9. - Block diagram of applied AES in blockchain[5]

2.9.2.2 Blowfish in Blockchain

Blowfish can be utilized in place of DES or IDEA because it is also a symmetric block cipher. making it useful both at home and abroad since it supports keys with lengths ranging from 32 to 448 bits. Blowfish was developed in 1993 by Bruce Schneier as a rapid, open-source substitute to current encryption techniques. Since then, its' become the subject of extensive study, and its merits as a secure encryption technique are gradually being recognized. Since Blowfish has never been licensed or patented, it can be used in any way at no cost. The files are stored in the Blockchain after being separated into small parts according to their size, and these pieces are encrypted using the Blockchain's encryption algorithms. In addition, the Blowfish method was used to verify the user in order to get the original content following the acquisition of the private key and information on the parts that were Segmented at each node to be compiled and decoded[30]. In another case, this algorithm is used to secure email data where Block chain may access two sorts of transactions: T(transactions) access for control and management, Email data, data storage, and retrieval. User installs software that leverages the platform to protect her privacy. A new shared (user, service) identity is produced and submitted to the blockchain in a T access transaction. An email transaction's contents are sent to an off-block chain key-value store alongside the blowfish, storing just a pointer to the open email's information (the pointer may be the SHA-256 hash of the information). Both the service and client can now request information by email with a pointer (key) attached. Afterward, the blockchain confirms that the advanced signature belongs to the client or administrator. For the service's permissions to obtain the info, verify, and also well[31].

2.9.2.3 DES in Blockchain

The DES algorithm, a common symmetric encryption system, employs the traditional block cipher form of Encryption. The overall operation of the DES encryption method. The plaintext must be converted, and the block holding the information will be split into two halves before transforming by using competent function. There will be sixteen repetitions. After product transformation, the two-part information components are merged. The combined information will undergo an inverse transformation. The DES encryption process was completed after 16 iterations. The same approach is also utilized for decryption. The only difference between encrypting and decrypting is that the key must be in reverse. DES generates a circular key for every circle. Weak keys are a severe shortcoming of symmetric algorithms. After symmetry drop operation, the weak key is the one that includes all 0's, all 1's, or half 0's and half 1's. The weak key allows the attacker to decrypt the DES encryption in a shorter amount of time[32]. DES is used in blockchain's Message authentication (Hash function with key). This type of Hash function is also referred as the Hash function with the key as its security relies on it. Here is how Encryption works: When a node sends secret information, it uses a mutually predetermined key to construct a message check code. Using the private key, the node obtains the check code after receiving the data. Through the key, the node compares the received and computed check codes. If the two check codes match, communication data integrity is maintained. Method of message authentication:
1) Cryptography. After symmetric or asymmetric encryption, ciphertext is transferred.
2) hash function. Messages of variable length are translated into fixed-length message digests and authenticated.
3) Verification code. An open function generates a fixed identification and authenticates secret messages. There are two primary applications: encrypting the digest value of a message with an encryption technique and employing a specific MAC algorithm[33].

2.10 Application of blockchain technology: -

As the underlying technology for cryptocurrencies and the digital token market, blockchains are acknowledged to have the largest range of applications of any distributed ledger technology. In addition to its broad application, this technology is currently an essential tool for digitizing and decentralizing a variety of other domains, as shown in figure (10). In the not-too-distant future, BC technology will be incorporated into all currently available forms for storing data and verification media of the validity of it. This, in turn, will contribute to the realization of the concept of living in intelligent environments that will be able to respond to our wants and provide us with some ideas. This, in turn, will aid in the achievement of the objective of living in smart settings[19].

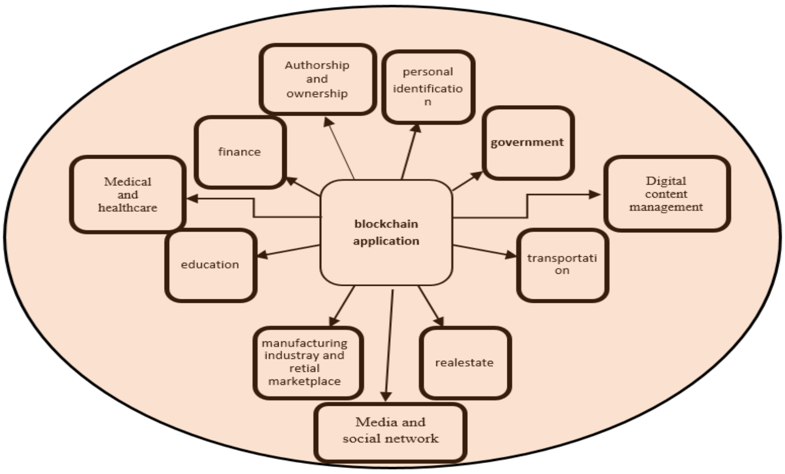

FIGURE 10. - blockchain applications[15]

3. Discussion

In this paper, we discuss blockchain technology and provide an overview of it and its importance at present. It is not limited to the financial industries alone; rather, it can also be found in other fields. It has significant application potential in a wide variety of industries, including logistics, marketing, forecasting, cybersecurity, loT, networking, and more. The Blockchain is going to become a reliable infrastructure for the storing of data. The blockchain integration in storage and transportation and the decentralization that characterized it relied on several techniques. These technologies and protocols that organized its work were clarified, the most important of which is encryption. As a result, the rest of the article explains the various cryptographic approaches utilized by Blockchain and emphasizes the importance of cryptographic ideas to blockchain applications. To sum up, cryptography is essential to the inner workings of blockchain technology. Blockchain transactions and wallets are built on public-key encryption; the immutable nature of Blockchain's enabled by the cryptographic hashing method and Merkle tree principles, as well as using advanced encryption algorithms offering top-tier security.

FUNDING

No funding received for this work

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their efforts.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

[1] W. Bank, "Europe and Central Asia Economic Update, May 2018: Cryptocurrencies and Blockchain," ed: The World Bank, 2018.

[2] A. Jamal, R. A. A. Helmi, A. S. N. Syahirah, and M.-A. Fatima, "Blockchain-based identity verification system," in *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*, 2019, pp. 253-257: IEEE.

[3] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in *2016 2nd international conference on contemporary computing and informatics (IC3I)*, 2016, pp. 463-467: IEEE.

[4] W. Li and M. He, "Comparative analysis of bitcoin, ethereum, and libra," in *2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS)*, 2020, pp. 545-550: IEEE.

[5] P. Nivethini, S. Meena, V. Krithikaa, G. J. I. J. o. A. Prethija, and Applications, "Data security using blockchain technology," pp. 279-282, 2019.

[6] S. Manglekar and H. Dinesha, "Block Chain: An innovative research area," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018, pp. 1-4: IEEE.

[7] S. H. Mehanoor and M. T. Alam, "A Study on Blockchain Technology and Real World Applications."

[8] M. Wohrer and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, 2018, pp. 2-8: IEEE.

[9] M. N. M. Bhutta *et al.*, "A survey on blockchain technology: Evolution, architecture and security," vol. 9, pp. 61048-61073, 2021.

[10] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. J. I. j. o. w. Wang, and g. services, "Blockchain challenges and opportunities: A survey," vol. 14, no. 4, pp. 352-375, 2018.

[11] 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)*, 2017, pp. 557-564: Ieee.

[12] K. Poudel, A. B. Aryal, A. Pokhrel, and P. Upadhyaya, "Photograph ownership and authorization using blockchain," in *2019 Artificial Intelligence for Transforming Business and Society (AITB)*, 2019, vol. 1, pp. 1-5: IEEE.

[13] P. Sri and D. L. J. I. J. E. T. Bhaskari, "A study on blockchain technology," vol. 7, no. 2.7, pp. 418-421, 2018.

[14] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. J. I. C. E. M. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," vol. 7, no. 4, pp. 6-14, 2018.

[15] L. Ismail and H. J. S. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," vol. 11, no. 10, p. 1198, 2019.

[16] R. Houben and A. Snyers, *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. 2018.

[17] S. Anwar, S. Anayat, S. Butt, S. Butt, M. J. I. J. o. I. E. Saad, and E. Business, "Generation analysis of blockchain technology: bitcoin and ethereum," vol. 12, no. 4, pp. 30-39, 2020.

[18] M. H. Miraz and M. J. a. p. a. Ali, "Applications of blockchain technology beyond cryptocurrency," 2018.

[19] A. Priya, A. Khatri, and P. Dixit, "Rise of blockchain technology: beyond cryptocurrency," in *Applications of Computing and Communication Technologies: First International Conference, ICACCT 2018, Delhi, India, March 9, 2018, Revised Selected Papers 1*, 2018, pp. 286-299: Springer.

[20] R. J. J. o. E. T. Banger and I. Research, "A Study On BlockChain And Cryptography," 2019.

[21] M. Raikwar, D. Gligoroski, and K. J. I. A. Kralevska, "SoK of used cryptography in blockchain," vol. 7, pp. 148550-148575, 2019.

[22] V. Deshpande, H. Badis, L. J. P.-t.-P. N. George, and Applications, "Efficient topology control of blockchain peer to peer network based on SDN paradigm," vol. 15, no. 1, pp. 267-289, 2022.

[23] S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, "Research on the Application of Cryptography on the Blockchain," in *Journal of Physics: Conference Series*, 2019, vol. 1168, no. 3, p. 032077: IOP Publishing.

[24] E. EDITION, "THE WILLIAM STALLINGS BOOKS ON COMPUTER."

[25] W. Stallings, "Cryptography and Network Security Principles and Practice Seventh Edition Global Edition British Library Cataloguing-in-Publication Data," 2017.

[26] T. M. Fernandez-Carames and P. J. I. a. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," vol. 8, pp. 21091-21116, 2020.

[27] J. C. Foster, *Hacking the Code: ASP. NET Web Application Security*. Elsevier Science & Technology, 2004.

[28] D. Rountree, *Security for Microsoft Windows system administrators: introduction to key information security concepts*. Elsevier, 2011.

[29] T. H. Tran, H. L. Pham, and Y. J. I. A. Nakashima, "A high-performance multimem SHA-256 accelerator for society 5.0," vol. 9, pp. 39182-39192, 2021.

[30] R. Vasantha and R. S. Prasad, "A Comparative Study on Secured Block chain Technology for K-Nearest Neighbors Algorithm."

[31] R. Vasantha, R. S. Prasad, and A. J. S. T. D. Guntur, "Secured email data based on blowfish with blockchain technology," vol. 8, pp. 456-464, 2019.

[32] A. Sathya and B. G. J. I. J. A. C. S. A. Banik, "A comprehensive study of blockchain services: future of cryptography," vol. 11, no. 10, pp. 279-288, 2020.

[33] F. J. D. Gao and C. D. Systems-S, "Data encryption algorithm for e-commerce platform based on blockchain technology," vol. 12, no. 4&5, pp. 1457-1470, 2019.