A Survey of Blockchain from the Viewpoints of Applications, Challenges and Chances

Wageda I. El Sobky[1], Sherif Hamdy Gomaa[2], Ashraf Y.Hassan[3]
Department of Mathematics, Benha Engineering Faculty, Benha University, Egypt[1]
Department of Communication, Benha Engineering Faculty, Benha University, Egypt[2]
Department of Communication, Benha Engineering Faculty, Benha University, Egypt[3]

Abstract - in 2008, the appearance of the Blockchain as the basis of the first decentralized crypto currency not only revolutionized financial commerce but proved a peer-to-peer information exchange in the secure, effective, and transparent method. The Blockchain is a public ledger that works similar to a log by keeping a record of all transactions, secured by a suitable consensus mechanism, and supports an unchallengeable record. Its exceptional features include immutability, irreversibility, decentralization, persistence, and anonymity. With these advantages, it has found applications in almost all fields requiring data sharing among multiple parties but with secure authentication, secrecy, and permanence. Blockchain technology can be used in financial and social facilities, risk management, healthcare. Some of the applications are real-estate, digital identity, and IOT. Despite having many benefits, the Blockchain suffers from numerous difficulties, particularly reaching consensus in a massive network quickly, energy consumption in computation, and requiring storage of the complete chain for verification. This paper discusses the ins and outs of the Blockchain basics, its working, applications, more consensus mechanisms, current trends, and challenges.

Index Terms - distributed ledger, consensus procedures, cryptocurrency, smart contract, selfish mining, energy consumption, Blockchain

1 Introduction

NEW technologies have always been a strong the force with big shifts in the past. By the latest digitalization direction, emerging innovations, as well as enhancements to existing information technology (it) structures are at the forefront of new goods and facilities. The Blockchain has become a key technology for implementing distributed ledgers. New technologies have been a driving major variation in the past. Blockchain has been mostly attracting the attention of performers in the financial sector for its revolutionary enhancements of operations and financials. it allows a group of participating nodes (or parties) that do not trust each other to provide trustworthy and immutable services. Blockchain was a technology initially created to guide the famous cryptocurrency Bitcoin [1]. It allows peer-to-peer transfer of digital resources without any intermediaries. Bitcoin was first projected in 2008 and applied in 2009 by satoshi nakamoto. Then, it has seen enormous growth with the big market, reaching 10 billion dollars in 2016. Bitcoin is the greatest famous application of Blockchain; it can be practical to various applications beyond cryptocurrency. Blockchain can be used in many financial services, such as online payment, remittance, and digital assets. The Blockchain has taken on a range of applications across many industries, including finance, healthcare, government, manufacturing, and distribution. Other applications of Blockchain include distributed resources (power distribution and generation), identity management, crowd funding, governing public records, and electronic voting. The Blockchain is addressed to transform a wide range of applications, including goods transfer, digital media transfer, remote services delivery, moving computing to data sources, and distributed credentialing in Bitcoin. Blockchain is essentially a chain of blocks store all transactions using a public ledger [2] as shown in figure 1. It works in a decentralized situation to comprising many technologies, such as cryptographic hash, digital signatures, and distributed consensus algorithms. The transactions occur in a decentralized way that removes the obligation for any mediators to verify and validate the transactions. Blockchain has many features, such as transparency, decentralization, audibility, and, immutability. the limited frequency and size of the blocks along with the number of transactions the network can process can be considered a scalability problem. The Blockchain became popular because of its success in crypto-currencies, e.g., Bitcoin [3]. The average block creation time in Bitcoin is 10 minutes, and the block size is limited to 1 megabyte which constrains the network's data. The transaction is being effectively limited to 2-4 transactions per second, at present, there are more than 36 million wallet users. Different subjects such as the Blockchain overcrowding problem, increased transaction fees, and transaction delays, will increase concerns. as a result, the technology may not be a supportable approach for private sectors or government to build their business upon the Blockchain stage. Also, maximize block size needs large storage space and because slower broadcast in the Blockchain network [4] so, it has become an excessive challenge to contract with the balance between Blockchain size and trust. Bitcoin works on public key infrastructure (PkI) in the Blockchain for authenticating nameless users and controlling admissions. For identification and authentication, each transaction is digitally signed with the private key. To keep a road of transactions occurring synchronously, many transactions are collected together in a building called a 'block' uniquely known by its timestamp hash. Blockchain has some other subjects about privacy, interoperability, selfish mining, energy consumption, regulation policy, and security. privacy leak may similarly occur within the Blockchain, while the system demand to be widely secured as users make transactions with digital signatures that subordinate private-public key encryption [5]. Also, it is probable to follow the user's actual IP address. The interoperability subject increases due to the absence of a standard protocol for integrating and approving Blockchain grounded solutions among businesses. The additional problem of Blockchain technology is selfish mining, in which miners can improve their better income than their fair by caring for their blocks privately [6]. Consensus mechanisms such as proof-of-stake (pos) and proof-of-work (POW) are also facing serious tasks. For example, in pos, the rich become richer as the opportunity of finding a block depends on how much miners stake have [7]. In POW which is a form of achieving consensus among the distrusted modes is consuming a great amount of electrical energy thus the competitive miners creating blocks by solving hard mathematical equations [8]. Blockchain can also hurt of 51% attacks, where some entity achieves the common in a network and abuses it. Also, the Blockchain may not arrive at its top or expected large-gain approval by stakeholders because of that ascends with actual government regulations [9]. The important reason could be that the Blockchain removes intermediary links to central banks to lead the country's economy. Then, some measures need to be arranged for these subjects in the Blockchain.

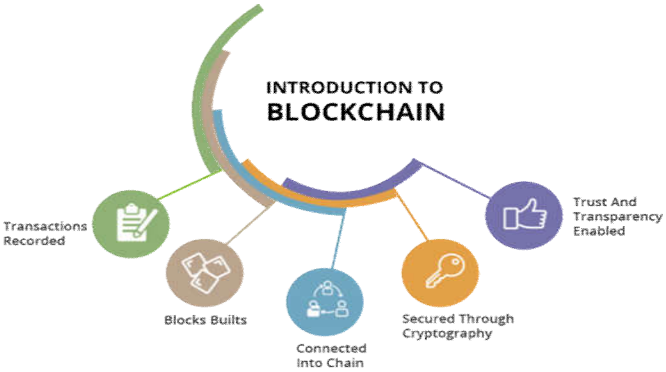

Fig 1 introduction to Blockchain

2 Background

Insurance businesses, banks, and other financial organizations are undergoing a big transformation. The transition involves drivers towards almost full product and facility digitalization, extreme control, destroying sources of income, and rapidly shifting consumer behavior. Specifically, the socio-technical phase of digitalization [10] sparks innovations that impact the whole market site. The new digital technologies introduced could radically change how businesses capture value, and could also redefine what can be considered and what cannot be considered as value-generating activities. Blockchain, which not only attracts the attention of financial institutions but also companies in other industries such as energy, health, entertainment, and manufacturing, is one such digital technology [11]. Due to its potential, heavy investments in many sectors are dedicated to Blockchain growth. Initially, Blockchain was introduced as an approach to cryptography-based payment transactions to provide an alternative confidence mechanism between two transacting parties [12]. Two parties have historically hung on a trusted third party to guarantee confidentiality. This third party is now replaced by Blockchain, which includes the technology's decentralized bookkeeping and faith achieved. In particular, Blockchain allows, through a decentralized ledger, a collective bookkeeping system which by means of a consensus mechanism, allows participants to reach an agreement and therefore by authorize transactions. The details contained in the ledger relating to individual transactions are collected in "blocks." the network checks and verifies these blocks and applies them to the computers of all network members in sequential order. As a result, a long chain of blocks is generated by the chronologically organized blocks, leading to the name "Blockchain." together all blocks represent the distributed ledger of checked transactions and are then delivered to the network. Since the record of all transactions is distributed to the network, intermediaries for verification are not needed by Blockchain. As such, the conventional position of financial institutions has been scrutinized as trusted third parties who verify transactions and mitigate the default risk behind them. The first cryptocurrency [13] was Bitcoin, and it is the most commonly used one to date. Also, it represents one of Blockchain technology's most popular applications. in the financial services sector, Blockchain is proposed as a solution for a wide range of transactions, ranging from real-time payments between two parties (including rapid settlement and without bank account requirements) to transfers of funds through currencies (micropayments, remittances) and digital assets (where records of asset ownership are stored digitally). However, the influence of Blockchain technology could go far beyond some updated procedures and a few new products and services. Several authors expect, because of its disruptive potential that the effects could even go as far as to impact entire business models. The effect of Blockchain on business models in the financial services field, in this context, may be a clear example of its disruptive potential. Blockchain, or the more general word distributed ledger technology (dlt), has also increased interest in the community of information systems (is), e.g. about confidence and cryptographic aspects [14], procedures and implications, and various virtual currency issues. Nevertheless, literature on the subject has yet to provide a concise description of the possible obstacles posed by Blockchain during its breakthrough journey. The payments industry represents a fertile ground for Blockchain research due to a range of initial Blockchain implementations and its immense potential .For banks, payments are often an exciting source of tension. On the one hand, in terms of offering essential and commonly used services to consumers, payments constitute a significant source of income for financial institutions. On the other hand, several developments, such as mobile payments, have become the focus of the payment industry. Also, payments are the anchor commodity for numerous other programs and a crucial factor for consumer data access. Payment information is a source of customer awareness and data and an ability to create reference points in the customer processes of banks, whether private company or institutional. Therefore, it would have catastrophic implications for banks to lose stakes in payment transactions to players using Blockchain. The business models of many financial institutions are under strain, squeezed between the need for investment in enforcement and it is a loss of income from conventional sources, and fierce competition. Further efforts to render the existing payment infrastructure obsolete or to remove payment transactions from financial institutions would also lead to the degradation of the market base of banks. Blockchain technology is a major challenge in this regard, in particular, because it could turn off the third-party role of financial institutions in payments and other fields. At the same time, however, the decrease in costs that could be accomplished by the use of Blockchain is forcing financial institutions to look closely at its creation and even actively drive it forward. Established payment system operators such as fast, international payment transaction providers such as western union and moneygram, as well as regulators, have drawn significant attention to the disruptive potential of Blockchain. Companies from the technology and financial services industries are exploring the introduction of Blockchain-based solution prototypes. In particular, by applying different strategies, from creating in-house platforms to directly investing in Blockchain companies, collaborating with them, or providing accelerator programs to explore Blockchain, incumbent businesses are trying to protect their company. The growth in payments appears to have slowed in terms of speed and intensity, considering the potential and far-reaching effects of Blockchain. Many existing services (e.g., reducing transaction fees and enabling direct transactions by removing intermediaries) may theoretically boost the technology. [15], but the challenges of its growth must be carefully considered and thoroughly understood.

3 Blockchain Architecture

A transaction is a data structure that transfers digital assets between nodes on the Blockchain network. A node establishes a transaction in a decentralized Blockchain network by using a digital signature with private key cryptography. All the transactions are kept in an unverified transaction pool then broadcasted in the network by flooding protocol identified as Gossip protocol. Then, peers have to validate and select the transactions grounded on predetermined standards. For instance, the nodes have to validate and confirm the transactions via testing an initiator has enough balance to generate a transaction or the system fooling in double-spending. Double spending mentions that using the same quantity many times in different transactions [16]. When the transaction is validated and verified by miners, it is comprised of a block. Peers using their computational power to make the blocks are called miners [17]. Miner has to answer a computational puzzle and consumed adequate computing resources to establish a block. The miner who can answer the puzzle first will be a victor and gets the chance to generate a new block. The peers verify the new block by a consensus mechanism, to support a decentralized network derives to a contract on confident matters. Then the new block will be joined to the current chain and written a copy to each peers' immutable ledger in the network. The transaction is validated now, the next block joined with the recent block by a cryptographic hash function. At this moment the block guts first validation while the transaction obtains the second validation. Also, a new block is added to the chain, the transaction will be reconfirmed. At final, the transaction has to get six confirmations from the network to be ended [18].

3.1 Blockchain Transaction procedures

The transaction is a small part that is stored in the records. All records are also known as blocks [19]. The blocks are implemented, performed, and kept in Blockchain to validate by the miners which entries in the network. The earlier transaction cannot be updated but can be reviewed at any time [20]. Blockchain is the original technology of Bitcoin, and it facilitates using a peer to peer universal network in a decentralized way. That makes Bitcoin a trusted and famous digital currency. Mainly, trust has to be the core traditional centralized systems, like the bank, where person’s essential have to put their trust in the network. This is the greatest point on Blockchain technology; it does not need any trust in ownership of the digital assets from any person to another. Blockchain hasn’t trust the system that gives trust by using the functions that broadcast the activities on the network [21]. Security is an additional feature while starting the transactions. Consensus mechanisms and system mining depend on a cryptographic hash function to add security values. For instance, A 256 bits hash algorithm is recognized as SHA-256 [22]. Bitcoin has a different type of input, like a number, text, or computer file of any length, to outcome 64 characters or 256 bits, output called hash [23]. When the input, is the same, the transformed output hash will be accurately similar. But, a small change in the input will totally change the output, so it called a one-way function, meaning it is not possible to obtain the input. Beginning of the transaction procedure we have to verify the identity of the sender, which means the transaction between the sender and the receiver is demanded by the sender, and not by another one else. Figure 2 shows the verification procedure with a simple example, of a transaction between Bob and Alice. Bob and Alice have a balance of Bitcoin, and Alice needs to pay 5 Bitcoin s to Bob. To send the Bitcoin s, Alice will send a message with his data about the transaction in the network. For that, Blockchain uses digital signatures (private and public keys) [24]. Now, Alice brings Bob's data, like transaction amount and his public address, with her digital signature and public key. To make the digital signature, Alice has to use her private key. For checking the validity of the sender, the verifier also needs to check the validity of the sender has enough money to send to the receiver, or not. It could be done by review at the ledger, which reads the information about every past transaction. Transaction validation is accomplished by all miners depend on other criteria. The signature has 256 bits, if someone wants to imitate this signature to make a fake transaction, he has to guess 2256 times, which is impossible, and spend of incomes for a hateful attacker.

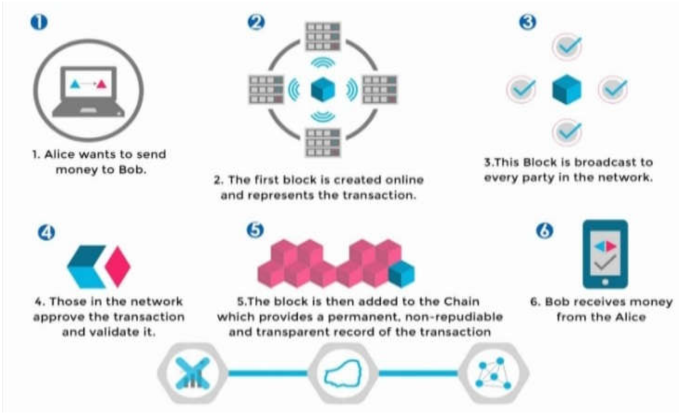
1. Alice wants to send money to Bob.
2. The first block is created online and represents the transaction.
3.This Block is broadcast to every party in the network.
4. Those in the network approve the transaction and validate it.
5.The block is then added to the Chain which provides a permanent, non-repudiable and transparent record of the transaction
6. Bob receives money from the Alice

Fig 2 diagram of a Blockchain network

3.2 Block Structure:

Blockchain includes a chain of blocks, which stores the data about the transactions, as a public ledger. The blocks are connected by a hash that is related to the previous block identified as the *parent* block. The first block is called the *genesis* block, so does not have any parent block. A block involves the block body and the block header [25]. The block header consists of metadata such as parent block hash, block version, timestamp, Merkle tree root hash, nonce, and n Bits as shown in Figure 3 and Table1. The block consists of transactions and a transaction counter. The transaction counter mentions how many transactions to track, and transactions refer to the list of noted transactions in the block. The maximum number of transactions in the block depends on the size of each transaction and the block size. An asymmetric cryptography mechanism is typically used in Blockchain to authenticate the transactions. A digital signature built on asymmetric cryptography is used in an untrusted atmosphere like Blockchain. In this process, each node owns a public and private key in the network. The public key is spread during all nodes and everyone can take it, which assisted in transaction decrypt, but the private key is used for encrypting or signing the transaction.

TABLE 1 BLOCK HEADER ATTRIBUTES

Header Characteristics	Description
Previous Hash Block	A 256-bit hash value that related to the previous block
Block Version	Shows the block rules to track.
Timestamps	Present timestamp as seconds since 2010-07-01T00:00 UTC.
Merkle tree root	The block hash value of all the transactions.
Nonce	A 4-byte area regularly starts with 0 and rises for each hash added.
N Bits	Current hashing goal in a compressed setup.

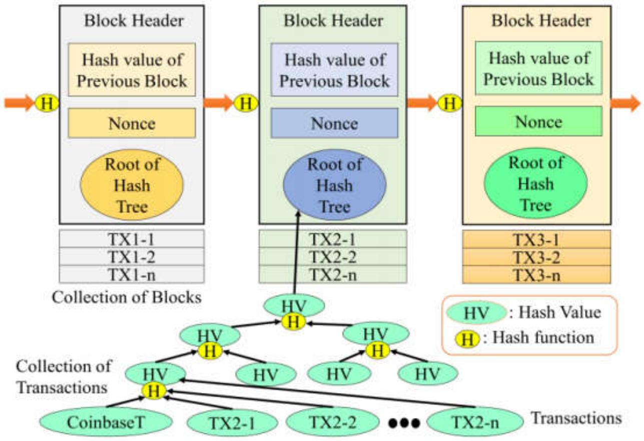

Fig 3 Blocks Structure

3.3 Blockchain Characteristics

The Blockchain characteristics are depicted in Figure 4. With the more characteristics, the Blockchain has created applicability in other divisions as well and not just cryptocurrency.

3.3.1 Decentralization

In a normal centralized organization, each transaction needs to be validated over the central agency as the bank system. Then, trust is needed in the decentralization system, this is the main point. Peer-to-peer Blockchain architecture the system has to be the best way. In the Blockchain network, the transaction has to be connected between two peers (P2P) without authentication by the central node. Then, Blockchain can reduce the trust worry through having several consensus actions. Furthermore, it can reduce the prices (with the operation and development price).

3.3.2 Auditability

All the transactions in the Blockchain are noted in a distributed ledger system.

3.3.3 Anonymity

The user has several addresses in the Blockchain network to reveal his identity. The user can cooperate in the Blockchain network with an arbitrarily created address [26]. In the decentralized system, there is no central authority to controlling or flowing user private information. So, the Blockchain gives a convinced quantity of anonymity through its trustless transactions.

3.3.4 Persistency

In the Blockchain system the truth can be tested [27] and allows the customers to prove their information is reliable and not changed. For instance, if a Blockchain consists of 5 blocks, then the last block holds the hash of the previous one, thus to generate a new block, the data of the recent block is used. So, all blocks are connected with each other in the current chain. All the transactions are linked with the previous transaction. Then, the small change on any transaction will exactly change the block's hash. If anyone wants to change any data, he has to modify all the previous blocks hash data. So, after the miner creates a block, it is confirmed by other nodes in the system. Thus, any spurious data will be noticed by the system. For that, Blockchain is considered and interfere resistant as an absolute distributed ledger.

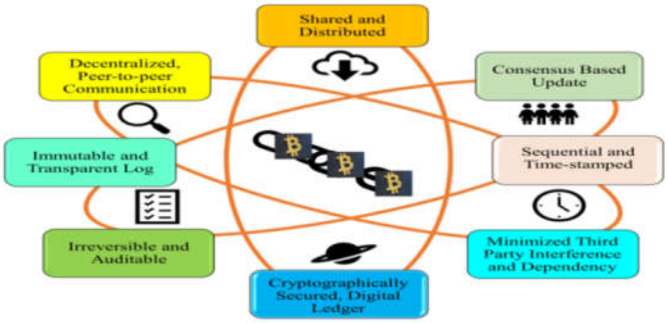
Shared and Distributed
Decentralized, Peer-to-peer Communication
Consensus Based Update
Immutable and Transparent Log
Sequential and Time-stamped
Irreversible and Auditable
Minimized Third Party Interference and Dependency
Cryptographically Secured, Digital Ledger

Fig 4 Blockchain characteristics

4 Classification of Blockchain networks

There are three types of Blockchain, public, private, and consortium. These systems can be compared using different perspectives as described below as shown in Figure 5.

4.1 Public Blockchain

From defiant organizations, a public Blockchain supply an open stand for people and mine and transact. There are no limits to these factors. So, it is called ‘permissionless’ Blockchain. All nodes are given authority to read/write transactions, to review or auditing any part of the Blockchain, all the time. The Blockchain is clear that there are no exact validator nodes. All users can gather transactions and mining to get rewards. With complete decentralization, anyone can join the network; the consensus is realized by any of the decentralized consensus mechanisms. So, the public of the ledger let it to attacks. The strong mechanism of proof of work joint with cryptographic authentication of the Blockchain every time a new block is added balance to this fault.

4.2 Private Blockchain

It is called permission Blockchain then strange users cannot enter it without receiving a request. Nodes are definite either by the network in-charge or a set of the rules, to regulate admission. That levels of the system more centralization, though decreasing the basic Blockchain characteristic of definitely decentralization and openness as defined by Satoshi Nakamoto. This type of Blockchain is to simplify the exchange of information and private sharing among nodes (in the same organization) or multiple organizations with mining controlled by one organization or selective individuals. In the private type, when nodes enter the network, they running as a decentralized system, with each node obtaining a copy of the ledger and cooperating to be a consensus team, but in a different public Blockchain, the writes are forbidden.

4.3 Consortium Blockchain

A consortium Blockchain is considered as permission and private Blockchain, where not a single organization but a set of nodes are in charge of block validation and consensus. These nodes decide who will be a part of the system and who will mine. For validation, they used a multi-signature system, where a block is legal only if the nodes signed it. It is worked by the consortium to either write or read permissions that would be public or private to the network nodes. So, it is an almost centralized system, some validator nodes owing to the control, different from the private Blockchain that is centralized completely, and the public Blockchain that is decentralized completely. Also, the consensus restriction doesn’t promise irreversibility and immutability, then regulate of the consortium by a common can control to interfering of the Blockchain.

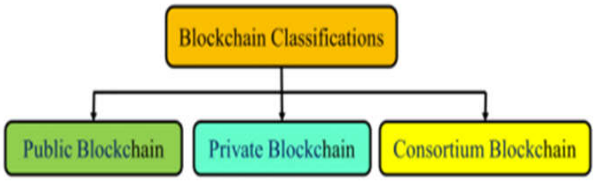

Fig 5 Classification of Blockchain networks

5 Consensus Mechanisms

When nodes initiate sharing information and trading through a Blockchain network, they don’t have a centralized node to control and resolve disputes or protection against violations to keep flowing of assets and ensure an exchange to prevent fraud, like double spending raid [28], [29]. In a distributed system with disbelief users and decentralized, a consensus is the unique and authoritative factor of the next secure update of their distributed case. The next subsets give different types to execute consensus in a Blockchain system shown in figure 6.

5.1 Proof of Work (POW)

It was the original decentralized protocol consensus suggested by Satoshi Nakamoto, to accomplish safety and reliability in the Bitcoin system. The digital currency changes occur in totally decentralized progress, hence, needing a consensus to validate the block and verification. In the Bitcoin field network, the nodes challenge to compute the hash rate of the following block, through imaginary to be less than a dynamically variable target cost, insisted by the consensus regulation. Regulators finding the key, pause for many validations by nodes before attaching the block to the current Blockchain. If multiple nodes find an effective solution that causes a temporary divide (section) in the system, more than one valid block can be created. All of them are appropriate in such situations for nodes closer to the miners to accept the solution they obtain and achieve the similar to other peers. The disagreement at the next step is prevented by embracing at any moment the 'Longest Edition' of the chain acceptable.

5.2 Proof of Stake (POS)

To address the drawbacks of unnecessary power feeding by POW in the Bitcoin application, proof-of-stake has been suggested. To accomplish consensus, Ethereum uses POS. POS recommends buying cryptocurrency and using it by way of a stake in the system instead of investing in resources that can act as healthy computations for hash computation in POW. The stake is straight comparative to the opportunity of being the validator of the block. The block validator is arbitrarily chosen to achieve consensus and is not predetermined. The nodes generating legal blocks get rewards, but the nodes also lose some quantity of their stake if their block is not involved in the current chain. And table 2 shows a comparison between the POW and POS. Based on many issues, numerous consensus styles have been distinguished:

5.2.1 Type of Blockchain

Depend on the Blockchain network is permission or not.

5.2.2 Transaction rate

At the exact point, transactions are validated, which is ultimately determined by the algorithm of consensus. The transaction rate is only7 transactions/sec in Bitcoin, which uses POW since POW needs considerable calculation time and 10 minutes is the block established time.

5.2.3 Scalability

The network of Blockchain is scalable if it can reach consensus on the continuous growth of the number of nodes, particularly in the Blockchain public network.

5.2.4 Participation charges

Initial participation costs are required for some networks. Nodes invest in the cryptocurrency with POS, for instance, to rapid their attention in the block validation and consensus, while POW needs input energy that is not important if you just want to be part of the system and do not need mining.

5.2.5 Trust condition

This decides if, as in consortium and private Blockchain systems or unidentified, as in public and POW-grounded Blockchain, the nodes contributing are to be trusted and predetermined.

TABLE 2
COMPARISON BETWEEN THE POW AND POS

Property	POW	POS
Energy Efficiency	No	Yes
Tolerated Power of Adversary	<25% computing power	<51% stake
Modern Hardware	Very important	No need
Forking	When two nodes find suitable nonce at the same time	Very difficult
Double Spending Attack	Yes	Difficult
Block Creating Speed	Low, depending on the variant	Fast
Pool Mining	Yes, it can be prevented	Yes, difficult to be prevented
Example	Bitcoin	Next coin

5.3 Delegated Proof of Stake (DPOS)

A voting consensus mechanism selected Proof-of-Stake (DPOS) in which each node with a system stake can, through the voting procedure, select the authentication of transactions to another node [30]. Although POS tracks a straight independent strategy, DPOS is an independent process that is illustrative. Representatives are selected by stakeholders to produce and verify a block and are referred to as observers [31]. Then these chosen nodes form a collection that suggests blocks and authenticates information conditions. On behalf of their owners, they toggle on elective for blocks and confirm the last validity blocks. As a result, most applications use an additional lake to fix node disappointments with reserve nodes. There are substantially fewer members for block proofs, different from POS, which enables quicker establish the blocks and easily authorizes transactions [32]. To ensure reliability, the restrictions of the system, like block dimensions and block times, can also be tuned. The key drawback of this consensus process may be its propensity toward control. Bitshare is an instance stage to use the DPOS system. Members in stakes will election for them and use others to the election to become validators.

5.4 Practical Byzantine Fault Tolerance (PBFT)

This algorithm was suggested to be a key to the difficulty of the Byzantine Generals, which is about a strong Byzantine army assault on a rival city [33], [34]. Both loyal generals must work on the same strategy and attack instantaneously for the Byzantine army to succeed. Furthermore, the faithful generals had to stick to the agreed plan don't matter what the defectors do a few defectors should destroy the plan. Likewise, in a

Blockchain, PBFT works among the joining nodes to create consensus. Nodes retain a current position, which is fed along with the message established for calculations upon receipt of a new message, to help the node make a choice. Then this decision is transmitted to the system. For the system, the bulk of the results control consensus. PBFT is used as the underlying consensus framework for hyper ledger [35], which works to build a consortium Blockchain network for companies. It has to remember that several of the latest Blockchain technologies derive from previous work on distributed information. Instances of the previous effort of this kind are.

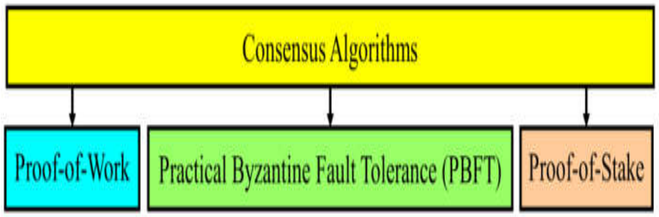

Fig 6 Consensus approaches in the Blockchain

6 Hash Encryption Algorithms

The Blockchain record database is named as blocks that are connected using the techniques of cryptography. The block comprises a hash of prior blocks, time-stamps, and data represented in Merkle Tree [36]. In the Merkle Tree or hash tree, each leaf node is labeled with a data block's cryptographic hash, and each non-node is tagged with its child node's cryptographic hash. Several hash encryption algorithms are usually used in Proof of Work (POW) consensus such as SHA-256, ECDSA, RSA, and ElGamal encryption. Table 3 below shows the comparison of the encryption algorithm used in POW consensus. In early 2001, the United States National Security Agency (NSA) was created by the Secure Hash Algorithm 2 (SHA-2) as a collection of hash functions. The example of the hash tree as in Figure 7:

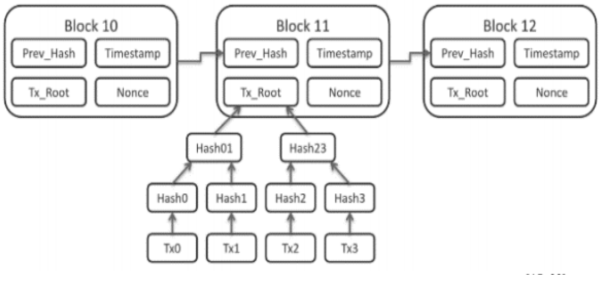

Fig 7 Blockchain Architecture with the Merkle Tree

A classified cipher block through the usage of the one-way compression function develops with the Merkle – Damgard framework using Davies – Meyer structure [37, 38]. The SHA-256, SHA-384, and SHA-512 algorithms are usually recognized as SHA-2, which are modeled after their digest size (bits). Second, the Elliptical Curve Digital Signature Algorithm (ECDSA) offers a variety of Digital Signature Algorithm (DSA) which uses elliptical encryption. This method is designed for the American National Standards Institute by Accredited Standards Committee for Financial Services, X9 [39]. Generally, the size of the public key required for ECDSA is approximates twice the size (bits) of the level of security. Third, Rivest – Shamir – Adleman (RSA) is one of the first cryptosystems that comprise a public key and was broadly utilized for the security of data transfer. The encryption key within the cryptographic hash is public and independent from the preserved, hidden (private) decryption key. The abbreviation of RSA signifies the initial letters for Ron Rivest, Adi Shamir, and Leonard Adleman, that defined the algorithm publicly in 1977 [40]. As the RSA is a relatively slow algorithm, it is less use for encrypting user data. While often it used to perform operations of bulk encryption-decryption at a much higher speed than the symmetric key shared by the process. Lastly, ElGamal encryption is an asymmetric encryption algorithm based on the Diffie – Hellman key exchange for the public-key cryptography. Taher ElGamal defined this algorithm back in 1985 [41]. ElGamal encryption commonly generates a 2:1 scale expansion from plaintext to ciphertext as a result of probabilistic-a single plaintext encoded into several potential ciphertexts.

TABLE 3
COMPARISON OF THE ENCRYPTION ALGORITHM IN POW

Property	SHA256	ECDSA	RSA	ElGamal
Key	Using hash instead of the key	Use the same concept as RSA but much shorter length	The different key used for encryption and decryption purposes	Used the asymmetric key
Scalability	Yes	Yes	No	Yes
Power Consumption	Medium	High	High	Low
Confidentiality	High	Medium	Low	High

7 Blockchain Applications

Blockchain technology has various applications branch. We have to know that Bitcoin is not equivalent to the Blockchain, but it is the most important application of this technology. It is a digital currency, which is managed over an open, anonymous, and public Blockchain system. This technology can be used for discovering solutions for a lot of fields, such as identity management, governance, healthcare, voting, energy resources, supply chain, and more show in figure 7. Also, some prophets expect that Blockchain will affect the digital field like the internet [42].

7.1 Healthcare

Healthcare information exchange is an important research topic, which can benefit both healthcare providers and patients. In healthcare data sharing, many cloud-based solutions have been proposed, but the trustworthiness of a third-party cloud service is questionable. Recently, Blockchain has been introduced in healthcare record sharing, which does not rely on trusting a third party. Electronic health record (EHR) sharing enables to improve the quality and reduce the cost of healthcare, but it is still challenging because of technique issues even though patients and healthcare organizations are willing to share. These technical barriers include confidentiality, privacy, interoperability, integrity and so on. During medical care service, large amount of data is created and need to be stored safely for a long period, often a life time. One major difference between healthcare data and other big data sharing is that electronic health records (EHRs) are normally highly sensitive, which may make patients and medical organizations reluctant to share .A Blockchain created the management of patient's health field [43]. The history of a patient's medical is kept on a decentralized network, reachable to the doctors and medical insurance services.

7.2 Energy Industry

This is one of the important uses of Blockchain applications linked to microgrids. A microgrid is a kind of electric power sources and loads combined and succeeded with Enhancing energy manufacture and consumption reliabilities and efficiencies [44]. These electric power sources distribute power generators, with new energy stations, and the energy can be stored in services owned and created by energy suppliers or individual organizations. Blockchain technology is ready to disrupt nearly every industry and business model, and the energy sector is no exception. Energy businesses across the world have already started exploring the use of Blockchain technology in large-scale energy trading systems, peer-to-peer energy trading, project financing, supply chain tracking, and asset management among other applications. Information and Communication Technologies (ICTs) recently started revolutionizing the energy landscape, and now Blockchain technology is providing an additional opportunity to make the energy system more intelligent, efficient, transparent, and secure in the longer term. The idea of this paper is to examine more closely the use of Blockchain technology for its possible application in the energy efficiency industry and to determine how it could make energy efficiency markets more secure and transparent in the longer term.

7.3 Voting

Blockchain can be used as a solution to the problems in many fields, about controlling the database of the governments. One of the important problems can be discovered in voting. Lately, it was discovered that a main U.S. voting system data had installed control admission software on many networks [45]. When counting the total votes, this software permitted to change it. An example such as this creates confidence in America's voting system, Popular expects foreign meddling in midterms. Blockchain solves this subject by giving a distributed ledger that The most suitable hash encryptions algorithms to implement in e-Voting technology is ElGamal encryption as it has the Homomorphic multiplication property [46], which encoded the transaction data into unreadable cipher text to reducing the risk of data being exposed. The mixing of authority permutes and encrypts are handled as input in the next block. Moreover, the utilization of this encryption method guarantees the confidentiality of the secure Blockchain-Based Transaction Processing System (Bb-TPS) and the consolidated statement automatically delivers in real-time [47].

7.4 Identity Management

Personal identity can be proved using documents such as a national ID card, driver's license, and passport. But actually, it is hard for any effective system for securing online identities. Blockchain technology can be used to generate a stand to protect an identity's data from being robbery or decreases fake actions. Blockchain allows everyone to establish an encrypted identity, without needing any password or username while requested extra security features and lead over entering their personal data. Using identity verification with the Blockchain feature, Blockchain can generate a digital ID. This ID can be used for every online transaction like a watermark. Blockchain supports governments to find and remove fraud by checking the identity of every transaction. Blockchain has a solution in the identity management field, so the consumer can deal with online payments by using an application for authentication instead of using biometric methods or password and username [48].

7.5 Insurance

Blockchain can support the insurance field transactions among customers, policymakers, and the companies of insurance. Blockchain can be used to exchange, sell and buy policies of insurance, acceptance and procedure requests, and also provide reinsurance activities between companies of insurance. Smart contracts can be automated used by insurance policies, which can exactly reduce management budgets [49].

7.6 Stock Market

Blockchain technology could solve the problems that appear in the marketing field, such as trust, interoperability, and clarity [50]. By the role of mediators, the controlling procedure and working being clearance, it takes 3 days or more to finish and confirm all transactions. So, the stock market contributors, for instance, controllers, dealers, brokers, and the stock conversation, are going over a heavy procedure. Blockchain is the solution in that case. It can make the stock conversation more ideal by decentralization system and the automation network [51].

7.7 Trade Finance

It is an important procedure, that becomes very inactive and expensive, due to the occurrence of unimportant traders is helping to deals. This process uses different banks (and funds) before the money can be composed. Facilities like Western Union, it is earlier and saves time but also expensive. Blockchain can rapidly and controlling this procedure, prevent the needless intermediary. At the same time, it lets money transfer cheaper. So far, the budgets for transfer were 5-20%. The Blockchain decreases the budgets to 2-3% of the full quantity and gives guaranteed.

7.8 Blockchain in the IOT

IOT using Blockchain can be constructed to preserve an increasing list of encoded secured information archives protected versus variation and change. For example, IOT linked (e.g. RFID) benefits with a private place and temperature data changes with defiant ideas in a store or a smart house [52], the Blockchain can update this data. This allows all entire nodes to share the information and grade of the set as it changes between parts to guarantee the steps of an arrangement are done [53].

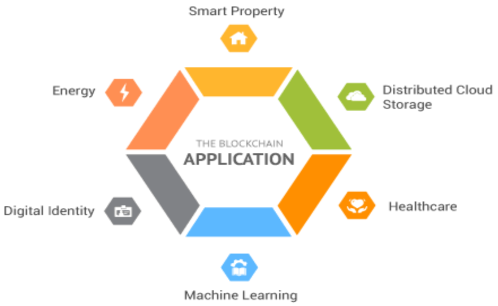

Fig 8 Applications of Blockchain Technology

8 Blockchain challenges

The Blockchain has a few drawbacks regarding its abilities and profits, the greatest thoughtful is the issue of celebration. The block authentication and consensus enable the complete Blockchain, it has always happened, thus requiring a large place. The constraint of block size is a major donor to the problem of celebration. With the 1MB block size range and the later consensus procedure, just 6-7 transactions, increase the transaction fees, and confirmed in a second. By decelerating the block's propagation, increasing the size of the blocks will produce an added delay. An advanced form of the Blockchain called Bitcoin -NG, which splits the block into two sections to decrease the broadcast size, has been proposed to achieve security with reduced block size. In traditional Blockchain systems, forks cause more delays, as the nodes are awaiting the longest version to validate the right Blockchain. One more problem of the Blockchain is the '51% attack' issue. If more than 51 percent of the nodes participate to create fraudulent blocks or inverse verified transactions, this issue occurs. Then higher calculating power principals to faster block creation, honest nodes will not be a challenge for a reasonable form of the Blockchain as only the longest version will be considered by nodes. The power or energy needed is another significant problem for the Blockchain. Mining a 1 Bitcoin is expected to require energy equal to a typical US household's 2 years of feeding. Energy feeding is also calculated to be equal to 80,000X of the energy feeding of credit card procedure for each Bitcoin transaction. Figure 8 demonstrates the above overall challenges.

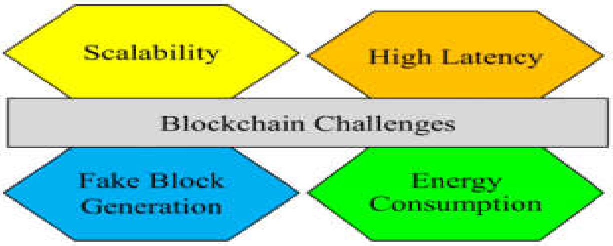

Fig 9 Blockchain challenges

9 Future Scope Of Blockchain Technology

The investigators think that in both business and academia, Blockchain has tremendous possibilities. We have temporarily addressed various potential scopes for Blockchain technique in this part, with properties security, calibration, large information, and intelligent deals. Therefore, to assess its significance as well as the tradeoffs, there should be a common testing procedure for Blockchain-built keys. This approach may be divided into two stages: the testing stage and the standardization. Depend on some basic parameters; beginning with stage will validate the developers' statements about their Blockchain answers. Then evaluate the Blockchain-based answer's efficiency on the testing stage. The online trade company owner, for example, cares about the Blockchain-based solution's results. So, to test the amount, power, and dormancy of the developed solution stage, there should be some standardizing and testing systems. This technology enables enterprises to generate a digital track of their creations records and can produce a certificate by recording new creations, prototypes, and proof of concepts that could show the credibility, life, and possession of the IP asset. Quality and code study are contributed to by assessment. It has been shown that a slight bug in the development of clever contracts may have a devastating effect. The DAO assault, where more than 60 million bucks were taken because of the recursive call bug, is an exact example. So, analyzing the raids on the clever deal is very significant. The act of the clever deal, on the other hand, may become an interesting study subject. Cleverer deal-based implementations will be put into use as Blockchain technology acquires enormous interest from the private and public sections.

10 Conclusion

The Blockchain is used universally for safeguarding peer-to-peer system setup with decentralization. This paper obtained a complete analysis of the Blockchain system by stress on the practical shape of Blockchain then giving the network structures. Consensus algorithms are designated to help in many applications. As the result, this paper is giving dissimilar security challenges.

References

[1] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. https://Bitcoin .org/Bitcoin . pdf

[2] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, “Blockchain for ai: Review and open research challenges,” *IEEE Access*, vol. 7, pp. 10 127–10 149, 2019.

[3] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system.

[4] A. Blundell-Wignall, “The Bitcoin question,” 2014.

[5] A. Biryukov, D. Khovratovich, and I. Pustogarov, “De anonymization of clients in Bitcoin p2p network,” in *Proceedings of the 2014ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 15–29.

[6] E. Heilman, “One weird trick to stop selfish miners: Fresh Bitcoin s, a solution for the honest miner,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 161–162.

[7] S. King and S. Nadal, “Pp coin: Peer-to-peer crypto-currency with proof-of-stake,” *self-published paper, August*, vol. 19, 2012.

[8] E. Heilman, “One weird trick to stop selfish miners: Fresh Bitcoin s, a solution for the honest miner,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 161–162.

[9] T. I. Kiviat, “Beyond Bitcoin: Issues in regulating Blockchain transactions,” *Duke LJ*, vol. 65, p. 569, 2015

[10] Tilson, D., K. Lyytinen, and C. Sørensen, “Digital Infrastructures: The Missing IS Research Agenda”, Information Systems Research 21(4), 2010, pp. 748–759.

[11] Wörner, D., T. von Bomhard, Y.-P. Schreier, and D. Bilgeri, “The Bitcoin Ecosystem: Disruption Beyond Financial Services?”, ECIS 2016 Proceedings, (2016).

[12] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. https://Bitcoin .org/Bitcoin .pdf

[13] Robleh, A., J. Barrdear, R. Clews, and J. Southgate, “Innovations in Payment Technologies and the Emergence of Digital Currencies”, Bank of England, 2014. http://www.bankofengland.co.uk/publications/Documents/quarterlyb ulletin/2014/qb14q3digitalcurrenciesBitcoin 1.pdf

[14] Beck, R., J. Stenum Czespluch, N. Lollike, and S. Malone, “Blockchain – the Gateway to Trust-Free Cryptographic Transactions”, ECIS 2016 Proceedings, (2016).

[15] Holotiuk, F., F. Pisani, and J. Moormann, “The Impact of Blockchain Technology on Business Models in the Payments Industry”, Proceedings of the 13th International Conference on Wirtschafts information,(2017), 912–926.

[16] *G. Karame, E. Androulaki, and S. Capkun, “Two Bitcoin s at the price of one? Double-spending attacks on fast payments in Bitcoin.” IACR Cryptology e Print Archive, vol. 2012, no. 248, 2012.*

[17] J. A. Kroll, I. C. Davey, and E. W. Felten, “The economics of Bitcoin mining, or Bitcoin in the presence of adversaries,” in *Proceedings of WEIS*, vol. 2013, 2013, p. 11.

[18] M. del Castillo, “Chain is now working on six criticized Blockchain networks,” 2017.

[19] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *IEEE Communications Surveys &Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[20] 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*. IEEE, 2017, pp. 557–564.

[21] F. Glaser, “Pervasive decentralization of digital infrastructures: a framework for Blockchain-enabled system and use case analysis,” 2017.

[22] K. J. O’Dwyer and D. Malone, “Bitcoin mining and its energy footprint,” 2014.

[23] A. Manimuthu, R. Sreedharan V., R. G., and D. Marwaha, “A literature review on Bitcoin : Transformation of cryptocurrency into a global phenomenon,” *IEEE Engineering Management Review*, vol. 47, no. 1, pp. 28–35, First quarter 2019.

[24] G. O. Karame and E. Androulaki, *Bitcoin andBlockchain security*. Artech House, 2016

[25] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, “Provchain: A Blockchain-based data provenance architecture in a cloud environment with enhanced privacy and availability,” in *Proceedings of the 17thIEEE/ACM international symposium on cluster, cloud and grid computing*. IEEE Press, 2017, pp. 468–477

[26] Q. Wang, X. Li, and Y. Yu, “Anonymity for Bitcoin from secure escrow address,” *IEEE Access*, vol. 6, pp. 12 336–12 341, 2018.

[27] D. Shrier, W. Wu, and A. Pentland, “Blockchain& infrastructure (identity, data security),” *Massachusetts Institute of Technology-Connection Science*, vol. 1, no. 3, 2016.

[28] G. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in Bitcoin ”, in Proceedings of ACM conference on Computer and communications security, pp. 906-917, 2012.

[29] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, and E. Felten, “Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrency”, in Proceedings of the IEEE Symposium on Security and Privacy, pp. 104-121,2015.

[30] D. Larimer, “Delegated proof-of-stake (dos),” *Bitshare whitepaper*, 2014.

[31] “Delegated proof-of-stake consensus — bit shares 3.0,” https://bitshares.org/technology/delegated-proof-of-stake-consensus/, (Accessed on 05/21/2019).

[32] G.-T. Nguyen and K. Kim, “A survey about consensus algorithms used in Blockchain.” *Journal of Information processing systems*, vol. 14, no. 1, 2018.

[33] M. Castro and B. Liskov.“Practical Byzantine Fault Tolerance”, in Proceedings of the 3rd Symposium on Operating Systems Design and Implementation, pp. 173-186, 1999.

[34] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem”, ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, pp.382-401, 1982.

[35] Hyper ledger project, https://www.hyperledger.org/, 2015, Last Accessed on 4th February 2018.

[36] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.

[37] Penard, W., & van Werkhoven, T. (2008). On the secure hash algorithm family. Cryptography in Context, 1-18.

[38] Brown, K. (2002). Announcing approval of federal information processing standard (fips) 197, advanced encryption standard (AES).National Institute of Standards and Technology, Commerce.

[39] Gallagher, P. (2013). Digital signature standard (DSS).Federal Information Processing Standards Publications, volume FIPS, 186-3.

[40] Marwaha, M., Bedi, R., Singh, A., & Singh, T. (2013). Comparative analysis of cryptographic algorithms. Int. J. Adv. Eng. Tech/IV/III/July-Sept, 16, 18.

[41] ElGamal, T. (1985). A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472.

[42] R. L. Twesige, “A simple explanation of Bitcoin and Blockchain technology,” 2015.

[43] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, “A Case Study for Blockchain in Healthcare: “MedRec” Prototype for Electronic Health Records and Medical Research Data”, Whitepaper, August 2016,http://dci.mit.edu/assets/papers/eckblaw.pdf, Last Accessed 04 Feb 2018.

[44] R. H. Lasseter and P. Biagi, “Microgrid: A conceptual solution,” in *IEEE Power Electronics Specialists Conference*, vol. 6. Citeseer, 2004, pp. 4285–4291.

[45] Fair fight donate via Act Blue,” https://secure.actblue.com/donate/ fair-fight-reproductive-rights, (Accessed on 05/21/2019).

[46] Multiplicative vs. Additive Homomorphic ElGamal 2020 [Online]. Available: https://nvotes.com/multiplicative-vs-additivehomomorphic-elgamal/.

[47] Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving Blockchain based transaction processing systems. International Journal of Accounting Information Systems, 30, 1-18.

[48] O. Jacobovitz, “Blockchain for identity management,” *The Lynne and William Frankel Center for Computer Science Department of Computer Science.Ben- Gurion University, Beer Sheva*, 2016.

[49] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamar´ ıa, “Blockchain and smart contracts for insurance: Is the technology mature enough?” *Future Internet*, vol. 10, no. 2, p. 20, 2018.

[50] L. Lee, “New kids on the Blockchain: How Bitcoin ’s technology could reinvent the stock market,” *Hastings Bus. LJ*, vol. 12, p. 81, 2015.

[51] D. Tapscott and A. Tapscott, “How Blockchain will change organizations,” *MIT Sloan Management Review*, vol. 58, no. 2, p. 10, 2017.

[52] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home”, in Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 618-623, 2017.

[53] D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. Mohanty, and A. Y. Zomaya, “Secure and Sustainable Load Balancing of Edge Datacenters in Fog”, IEEE Communications Magazine, 2017, pp. in Press.

AUTHOR CONTRIBUTIONS

Sherif Hamdy Gomaa was born in Egypt in 1973. He received the B.Sc. degree in Electronics and communications from Air defense college, Alexandria university, Egypt, in 1995. He received the M.Sc. degree in Electronics and Electrical Communications Engineering from faculty of engineering Aswan University, Egypt, in 2017. He is currently a demonstrator at Faculty of Engineering, Benha University, Egypt. his current research interests include data security, and cryptography.

Wageda Ibrahim El Sobky was born in Egypt in 1981. She received the B.Sc. degree in communications and computers from Benha faculty of engineering in 2003. She received the B.Sc. degree in science from Benha faculty of science in 2008. She received the M.Sc. in applied mathematics from Benha University, Cairo, Egypt, in 2012 and the Ph.D. degree in cryptography from Ain Shams University, Cairo, Egypt, in 2017. She is currently a doctor in basic engineering sciences, at Benha Faculty of Engineering, Benha University, Egypt. Her current research interests include data security, and cryptography.

Ashraf Y.Hassan: received the B.Sc. degree (with honors) and the M.S. degree in electrical engineering from, Benha University, Benha, Egypt, in 2000 and 2004, respectively, and the PhD degree in Electronics and Electrical Communications Engineering from Cairo University, Cairo, in2010.From 2000 to 2010, he served as a research and teaching assistant at the electrical technology department in Benha Faculty of Engineering. He works nine years as a researcher in the research and development centre in Egyptian Telephone Company from 2000 to 2009.From 2012 until 2015, he works as a visiting assistant professor at Northern Border University – Faculty of Engineering, Saudi Arabia. In 2017, he has promoted to associate professor degree. Now he was the head of the electrical engineering department from 2017 to 2019 in Benha faculty of engineering – Benha University, Egypt. Now he is the head of a research group working in physical layer researches for new communication standards such as 5G, DVB-S2, and ISDB-S3 standards.