Blockchain Technology: A Comprehensive Survey

Deepak Sukheja, VNR VJIET, Hyderabad. E-mail: deepaksukheja@yahoo.com

Lingineni Indira, VNR VJIET, Hyderabad. E-mail: indiralingineni@gmail.com

Prteek Sharma, PIMR, Indore. E-mail: prateeksharma14@gmail.com

Sachin Chirgaiya, SVVU, Indore. E-mail: sachin.chirgaiya@gmail.com

Abstract--- Blockchain has various advantages, for example, decentralization, pertinacity, namelessness and audit ability. There are a broad variety of apps in the block chain including cryptocmTenl.1, financial services, risk management, open and community services internet of stuff (loT), despite the fact that the various investigations center for utilizing the blockchain innovation in different application angles, there is no complete review of the block chain technology From the point of perspective of both technology and implementation. To block this vacuous, we lead a far reaching study on the blockchain technology. Specifically, this document provides the taxonomy of the block chain, initiates typical blockchain consensus algorithms and evaluates blockchain apps and discusses technical difficulties in addition to latest developments in addressing problems. In addition, this paper additionally calls attention to the future bearings in the blockchain innovation.

Keywords--- Blockchain, Crypto Currency, Consensus Algorithm, Applications, Smart Contract, Security Challenges, Trust.

I. Introduction

The word ' blockchain technology ' is used by people to mean different things, and it can be confusing. They sometimes talk about the Bitcoin Blockchain, sometimes they're other virtual currencies, sometimes they're intelligent agreements. Most of the moment they talk about distributed ledgers, i.e. a list of transactions shared between several PC's, instead of being stored on a central server. There is absolutely no doubt that the focus that was once only on a single currency is quickly moving towards application that are based on crypto currency and that are build on a blockchain [1]. In the recent computing era, distributed processing and data warehouse is the two important technologies, which are used for both the computer processing, for reporting and data analysis. Both of the technologies have several benefits, but the block-chain technology extends these technologies, i.e. the block-chain technology has high integrity and transparency than the data warehouse and the confidentiality and the performance are greater than the data warehouse. The simplest form of the blockchain act as a join, replicated, added database where access to the record is shared, but verification is performed by all group of participants. The basis of the block chain is a list of documents called blocks that are connected using cryptography to provide safety. As mentioned in [2,3,4,5], blockchain is a sort of distributed, electronic, append-only database (leader) capable of holding any data (e.g. records, occurrences, transactions) and setting guidelines on how this data is updated and also functioning as a distributed ledger in a secure setting. It is an evolving technology that allows the sharing of information in a decentralized and transactional manner that has the capacity to radically change the way companies perform business and the way institutions process transactions. The block chain presents itself in a decentralized transaction setting as an alternative to the platform where all transactions are clearly accessible to all. The block is then broadcast to every node in the network and the nodes approved that the transaction is valid; one of the significant features of blockchain is how many nodes in a distributed block-chain network maintain the consensus, i.e the block can be added to the already available block-chain, which provides a permanent and transparent record of transactions which is well described in [6, 10]. Also the new technology called the Internet of Things (IoT) has been work based on the block-chain technology, in which a large-scale block-chain-based storage system, called Sapphire, has been created for data analytics in the IoT [11,12,13,14].

In this article we are going to review the basic concepts of the blockchain technique along with its algorithms, advantages, characteristics, security issues, as well as the future works. The rest of this paper has clarified as pursues. Section 2 explains fundamental concepts of the blockchain technology along with the characteristics of this technique, key concepts, and advantages. Section 3 illustrates the numerous consensus algorithm employed in the blockchain technology. The assorted application areas of the blockchain concept have clarified in the Section 4. Section 5 explicates the security issues also challenges faced by the blockchain concept.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

Various limitations and vulnerabilities of blockchain are projected in Section 6. The Section 7 comprises future advances of the blockchain technique. At last, Section 8 concludes the paper.

II. Blockchain Taxonomy

A blockchain is a list of transactions or a record that is kept up by a network of clients, instead of a focal specialist. It is a sequentially requested series of blocks ensured by illuminating a Proof-of-Work (PoW) / Proof-of-stack or any other consensus algorithms. It's known as blockchain in light of the fact that new exchanges are packaged into "blocks" of information and composed onto the finish of a "chain" of existing blocks depicting every earlier exchange. The tying is depleted by joining the hash of the earlier block to the recent block, the hash of the recent block to the subsequently block, and so on. Consecutive nested blocks undertaking transactions to come in a sequential order, thus a transaction cannot be changed antedated without changing its block and all the following blocks. At the same time as the majority of decentralized electronic systems suffer from dual-spending assault, the blockchain makes it impractical except if assailant powers more than 51 percent of the entire system computational power. The scheme makes it computationally hard to generate successive nested blocks (block hashes) to prevent double-spending attack. The scheme will therefore continue to operate correctly while the opponent nodes ' collective computational strength does not regulate the computing power of the trusted node [16].

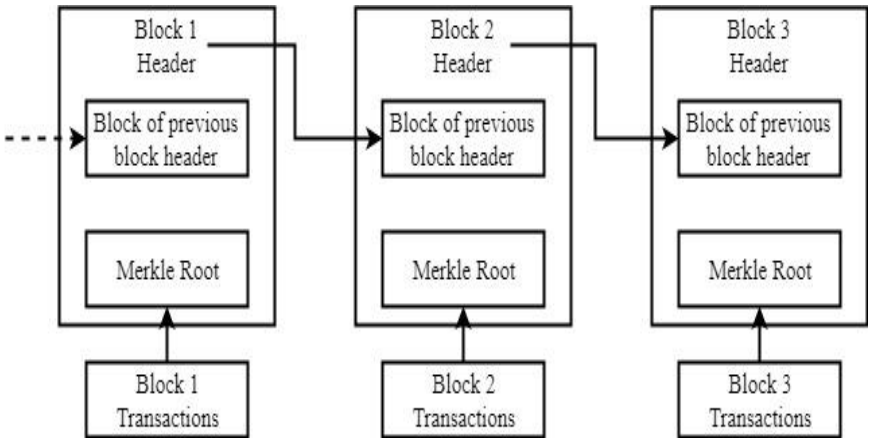

Figure 1: The Structure of the Blockchain

Seeing as a sub-chain is regarded an applicable only if it is longer than a competitor chain, honest nodes should produce fresh blocks quicker than an opponent attempts to close or even better an applied blockchain after modifying an ancient transaction. The scheme delivers this efficiency by implementing a proof-of-work system, which testifies that a node has invested the required funds to do a computationally challenging job. A standard blockchain structure consists of several nodes which don't totally dependence each other. Some nodes display Byzantine behavior [17], but the greater part is honest. The nodes together maintain a set of shared, worldwide states and conduct transactions that alter states. Blockchain is an outstanding structure of information that stores historical statements and transactions. All nodes in the framework are in agreement with the operations and their order. In blockchain, each block is connected by a cryptographic pointer to its predecessor, all the way back to the initial block (genesis). This is why blockchain is called a distributed record.

Component of Block	
Index (Block No.)	(which block has index)
Previous #	Is previous block is validate
Time Stamp	When was created
Data	What information is stored
Nonce	A random unique number to prevent a reply attach on the blockchain
Current #	The hash that generated for current block

Figure 2: The Component of the Blockchain

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

The blockchain consists of blocks, each block has two parts: block header and block body. The block header includes the latest version amount [18], the objective hash estimation of the previous block, the timestamp and the random number resulting from a hash calculation problem. In the current network, the block body includes the deal information that is recorded as Merkle tree. The block header contains the previous block's hash estimate and is associated with the subsequent block. So every block in the blockchain is connected together, forming such a chain of integrity. Transactions in an open blockchain are publicly visible while they depend on a personal blockchain or a blockchain consortium

2.1 Characteristics of Blockchain Technology

The main characteristics of Blockchain Technology at application level: a) Immutability, b) Transparency, c) Identityd) Distributione) Transactions of) Historical recordg) Ecosystem and h) Inefficiency are well describe in [19, 20].Other than these main characteristics additionally there are some technical key characteristics. That has described in the section 2.2.

2.2 Technical Key Characteristics of the Blockchain

Fairley, Peter has mentioned the following Technical key characteristics of blockchain in [21].

a) Digital

Entire information in Blockchain is digitized disposing of requirement for common documentation.

b) Distributed Ledger

The Blockchain shares undefined copies of all data. Participants approve data independently without an authority being integrated. The remaining nodes continue to work, even if one node fails, ensuring no disturbance.

c) Consensus–Based

A transaction on Blockchain can be executed just if every one of the gatherings on the system collectively affirms it. Be that as it may, agreement based principles can be changed to suit different conditions. Each node could be included in the consensus process in the government blockchain. And it's only a preferred set of nodes that validate the block in the blockchain consortium. As for the private chain, one union is fully governed and the union could conclude the final agreement.

d) Cryptographically Sealed

Blocks created are resolved in the chain cryptographically. This means that it is difficult to delete, modify or copy blocks already created and placed them on the network, thus generating real computerized resources and ensuring a high level of robustness and trust. Furthermore, the decentralized storage in a Blockchain is known to be very disappointment-safe. Indeed, even in case of the disappointment of a large number of network participants, the Blockchain stays accessible eliminating the single purpose of disappointment. Data stored in a Blockchain is changeless.

e) Chronological and Time-Stamped

As the name indicates, blockchain is a chain of blocks-each being a storehouse that stores transaction data and also connects to the previous block in the same transaction. These connected blocks form a chronological chain providing a trail of the fundamental transaction.

2.3 Conceptual Structure of Blockchain

The fundamental distinction among the three sorts of block chains is that open blockchain is decentralized; consortium blockchain is mostly brought together and private blockchain is completely unified as it is controlled by a solitary gathering.

It is helpful to arrange blockchain as public or private to distinguish the primary features of various blockchain. Understanding their fine distinctions in any situation requires a finer taxonomy. This segment introduces four supporting ideas which are mentioned in [22], based on which a progressively itemized arrangement of the frameworks can be acquired

a) Distributed Ledger

A record is an information structure consisting of an ordered transaction list. A record may, for instance, record economic transactions between different banks or exchanged products between recognized parties. In blockchain, all nodes recreate the record.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

In addition, transactions are collected into blocks that are then linked together. Along these lines, in essence, the distributed record is an append-only replicated data structure. A blockchain starts with some fundamental states, and the ledger records the entire history of state-made update activities.

b) Consensus

The record's substance represents historical and current statements maintained by the blockchain. As recreated, all sides must grant updates to the record. In other words, a consensus must be reached between various sides.Note; this is not the case in many real-world applications, such as fiat currency, where updates are selected by one substance (e.g. bank or government).

A main feature of a blockchain scheme is that the nodes do not trust each other, suggesting that some people may act in Byzantine ways. The accord convention should along these lines endure Byzantine disappointments. The exploration inscription on conveyed accord is tremendous, and there are numerous variations of recently proposed conventions being created for block chains [25]. Usually they can be ordered along a spectrum. One extreme comprises of protocols based on pure computation that use computation evidence to randomly pick a node that chooses the next procedure on its own.

c) Cryptography

Blockchain systems make overwhelming utilization of cryptographic strategies [23] to ensure reliability of the records. Reliability here refers to the ability to detect tampering of the blockchain data. This property is indispensable in broad daylight settings where there is no pre-built up trust. For instance, open trust in cryptographic forms of money like Bitcoin, which decides estimations of the monetary standards, is predicated upon the respectability of the record; that is the record must have the capacity to distinguish twofold spending. Indeed, even in private block chains, uprightness is similarly fundamental on the grounds that the verified nodes can still act maliciously.

The safety of Blockchain shows that the availability of public key cryptography is expected. Identities are obtained from public key certificates, including user and transaction identities. Therefore, secure key management is crucial for any blockchain. Losing private keys, as in other safety schemes, means losing access. But losing the keys in blockchain apps like crypto currencies has an instant and lasting impact on cash.

d) Smart Contracts

When a transaction is conducted, a smart contract refers to the computation conducted. It can be considered as a stored procedure that is invoked on a transaction. Each node agrees with the inputs, outputs and states that are exaggerated by the smart contract execution. All block chains have worked in keen gets that actualize their transactions rationales. For instance, the integrated smart contract main checks transaction inputs in crypto currencies by checking their signatures. Next, it proves that the output address balance matches the input equilibrium. At last, Changes are applicable to countries. We don't allude to such built-in rationales as smart contracts in whatever remains of the journal. Rather, we are only looking at smart contracts that consumers can define.

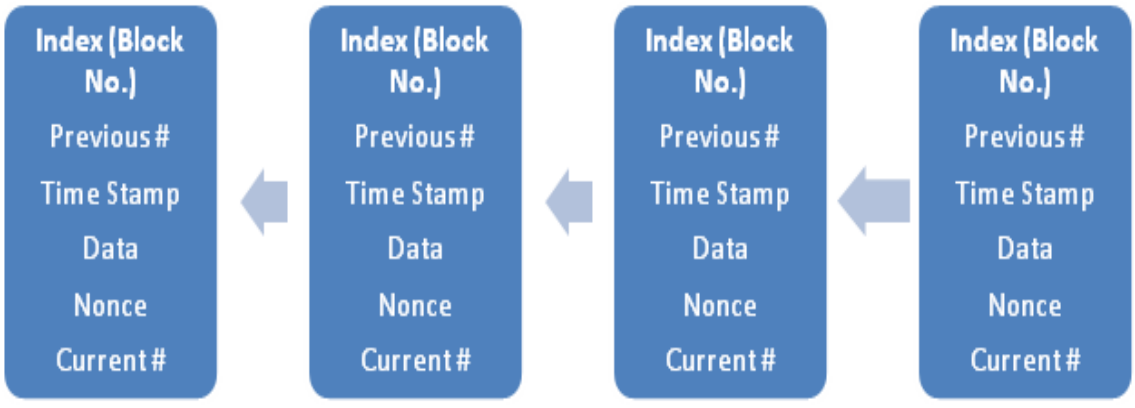

Figure 3: The Structure of the Block Chain

2.5 Advantages of Blockchain Technology

Blockchain could guarantee their accuracy and prevent illegal access through:-

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

a) Reliability

A blockchain network's decentralized nature Change the entire transaction record database from closed and centralized documents Maintained to open distributed documents continued by thousands of nodes by only a few attributed organizations. A single node failure does not influence the entire network's operation. This remains away from the single purpose of deception and ensures the high reliability of apps based on the development of blockchain.

b) Trust

Blockchain network functions as fresh trust bearers with decentralized documents, such as central government issuing currencies and commercial banks. These documents are distributed between a networks of manipulated nodes (Underwood 2016).

c) Security

The blockchain utilizes one-way hash function which has a numerical capacity that takes a variable-length input string and changes over it into a fixed-length binary sequence. The yield bears no apparent relationship to the input. The procedure is difficult to turn around on the grounds. Furthermore, the newly generated block is strictly following the linear sequence of time.

d) Efficiency

All information is consequently gone through pre-set methods. Blockchain technology can therefore not only significantly reduce labor costs, but also enhance effectiveness. For Blockchain 1.0's electronic currency, the mechanization of distributed record is primarily settlement automation. Blockchain technology could speed up the clearing and settlement of certain economic transactions by reducing the number of mediators involved and making the compromise process faster and gradually more efficient.

III. Blockchain Consensus Algorithm

A consensus algorithm [26] is like Bit coin's PoW (Proof-of-Work), which requires miners to solve complex cryptographic mathematical puzzles for which they get rewarded with certain amount of Bit coins. It is important to understand that each block which is added to the network must follow a set of consensus rules.

E.g. Bit coin's consensus rules are no double spending, correct format of blocks, a certain amount of reward for miners etc. Blocks that fail to follow these consensus rules will be rejected. A blend of PoW consensus algorithms and the consensus rules offers a strong and reliable network which is secure and guarantees that every one of the hubs in the system concurs on a standard worldwide condition of the blockchain. The consensus protocol has three essential highlights dependent on which its proficiency can be resolved.

- ***Security***

A consensus protocol has characterized to be protected if every one of the hubs suggests the similar yield then the yields is substantial according to the tenets. This is additionally called as constancy of the common state.

- ***Real-Time Value***

A consensus protocol guarantees the real-time likeness if every right hub taking an interest in consensus, in the long run, harvest esteem.

- ***Fault Resilience***

A consensus protocol suggests the fault resilience in the event that it can recuperate from a disappointment of a hub partaking in the consensus.

A few protocols are expected to guarantee the ledgers in various hubs are reliable. Next we present a few regular methodologies to deal with achieving a consensus in the blockchain.

3.1 Consensus Tactics

Within this subdivision, we fleetingly outline the activities of the distinctive consensus algorithm [27, 28, 29, 30] employed for the blockchain technology. The most broadly utilized consensus algorithms are the Proof of Work (PoW) algorithm in addition to the Proof of Stake (PoS) algorithm; be that as it may, there are likewise different consensus algorithms which use elective executions of PoW and PoS, just as other hybrid employments as well as some innovative consensus systems.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

3.1.1 Proof of Work (PoW)

Consensus Evidence of Work (PoW) is the most comprehensive consensus mechanism transmitted in current block chains. Bitcoin provided PoW and expect every peer to vote with their computing strength by describing PoW instances and developing the suitable blocks. Bitcoin, for instance, hires a hash-based PoW which involves discovering a nonce esteem, to the extent that, if hashed with additional block parameters (e.g. Merkle hash, previous block hash), the hash estimate must be slightly lower than the current objective estimate. PoW was the underlying consensus algorithm for the functioning of Blockchain.

This algorithm has utilized to authenticate the exchange besides to augment new blocks to the prevailing chain. In this algorithm, the excavators in the system contend with one another in so as to comprehends the exchange and get compensated. The PoW algorithm delivers effort to comprehend Numerical condition or confusion that requires a lot of computational energy. One of the associated aspects can be the mathematical equation:

1. Hash function, i.e., when the yield is acknowledged and the contribution is to be establish.
2. Integer factorization, i.e., augmentation of two different numbers to be introduced as a number.

The solution to the mathematical equation or PoW problem remains named as hash. Numerous trial and errors are prerequisite before the valid PoW has generated via the miners as producing a PoW is a random process using little probability.

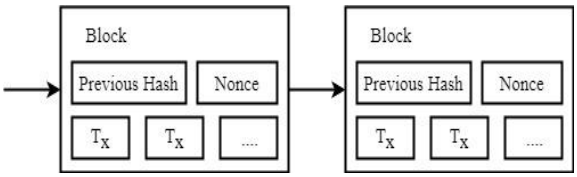

Figure 4: Imagining of two blocks within the PoW block chain

Algorithm 1 Proof-of-Work (PoW)

1. **Function** PoW$(nonce, difficulty)$

   $result \leftarrow$

   $ORIGINAL\ PoW\ (nonce, difficulty)$
2.
3. **assert**$ORIGINAL\ PoWSuccess\ (result)$
4. **return**$TEE.ATTESTATION\ (\langle nonce, difficulty \rangle)$, **null**)
5. **end function**

In contrast with defining an explanation for the numerical condition, it is generally less demanding to authenticate the resolution. When hash esteem has established by a unique excavator, anything left by the miners in the scheme demanded for authenticating this resolution as well as examine for the accompanying circumstances:

1. The former block referenced is substantial.
2. Timestamp of the block is more prominent than the past referenced block and is under15 minutes into the future.
3. Examine that the nonce of the block is substantial.

When a 51% consensus is come to in the system, the block can be acknowledged as well as added to the Blockchain. The most broadly utilized PoW plot depends on SHA-256 and was presented as a piece of Bitcoin. Particular additional hashing algorithms that are utilized for PoW incorporates Crypto Night, Scrypt, Quark, SHA-3, scrypt-n, besides the amalgamations. The hashing algorithm utilized by Ethereum is named Ethash.

3.1.2 Proof-of-Stake (PoS)

Proof of Stake (PoS) algorithm contemplates the number of coins or the stake claimed by an individual. It necessitates the clients to demonstrate the responsibility for a certain stake in the crypto currency, which sets the amount of blocks that can be authenticated by the client. The customers who approve the exchanges within this algorithm and produce the blocks are alluded to as falsifiers and the procedure is labeled forging or minting.

For example, a customer who owns 1% of the accessible crypto currency can possibly forge only 1% of the blocks.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

When a counterfeiter adds a block to the blockchain, he is paid with exchange fees instead of crypto currency units. Subsequently, it implies that no new crypto currency has engendered. The exchange expense stands an intrigue acquired on the stake of the client.

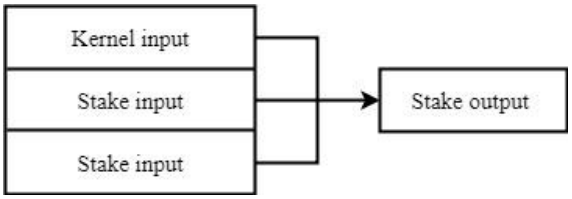

Figure 5: Structure of PoS Transaction

The PoS algorithm has simpler riddles and thus proceeds less time to generate a block when contrasted with the PoW mechanism. They are likewise greater condition neighborly as they necessitate less equipment as well as the electricity cost. The rudimentary crypto currency to approve the PoS method was Peer coin. Later it was trailed by Nxt, Black coin, in addition to the Shadow Coin.

3.1.3 Proof-of-Probability (PoP)

The PoW technique consumes a big quantity of electricity as a result of overheated mining, just as the cost of buying mining equipment. The PoS technique solved the financial disadvantage of the PoW technique to deal with this problem, but members are difficult to get into the scheme and can readily be monopolized by a big share holder. Only the top four percent of the real Bitcoin problems own 97 percent. PoP (Proof-of-Probability) is the technique used to fix these issues.

Algorithm 2 Proof-of-Probability PoP
if the transaction occurs **then**
$transmission(hash\ [\,])$

$newhash[\,] = sort(hash\ [\,])$

else
Wait until the transaction created
end if
if $GetHash$**then**

Create transaction block
else
$GetHash$

end if
procedure$SORT(hash\ [\,])$

$sort\ hash\ [\,]$ by independent algorithm

end procedure
procedure$GETHASH$

// Definition of each function
while satisfied with $hash\ [|nz]$**do**

$SHA\ 256(nonce)$

$gethash = nonce$

end while
end procedure

1. Each node *(A, B, C, D)* has its own algorithm for hash sorting.
2. An encrypted hash and a lot of false hash via the blockchain network is sent, when a transaction takes place.
3. Every node gives priority to hashes with its own hash sorting algorithm.
4. The node places the input value in the hash to locate the nonce value that satisfies the calculation. You must have a waiting time in case of false hash to discover the nonce value corresponding to the next hash.
5. The hub that finds the nonce that looks like the real hash that gets the crypto currency remuneration.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

3.1.4 Delegated PoS (DPoS)

DPoS[31] is very different from PoS. Here, token holders don't work on the validity of the blocks by themselves, but they select delegates to do the validation for them. In a DPoS system, there are usually in between 21–100 selected delegates. The chosen delegates are periodically altered and an order for their blocks to be delivered. If you have less number of delegates, it enables them to organize effectively and generate time slots intended to publish blocks. If the representatives regularly miss their blocks or publish invalid transactions, they are voted out by the token holders and replaced by some other chosen delegate. Unlike PoW and PoS, miners can work together to create blocks in DPoS to develop blocks. With a collaborative effort and a partially centralized process, DPo Scan execute magnitude orders that are quicker than any other algorithm of agreement.

Within a DPoS frame work, the stakeholders vote to choose any number of spectators to produce the blocks. Amid every conservation interim, the list of spectators has shambled, as well as each spectator is assumed a swing to deliver a block at the permanent agenda of one block for every n number of seconds (where $n$relies upon the employment). Spectators are paid for each block fashioned; be that as it may, should a spectator neglects to deliver a block subsequent to being chosen, they might be voted out in future elections. Explicit to the EOS blockchain, the blocks are formed at regular intervals by the approved producers and, every 21 blocks in the list of producers has rearranged. On the off chance that a producer has not fashioned any block within the most recent 24 hours, they are expelled from the contemplation until the point when they advise the blockchain of their expectation to begin delivering blocks once more.

3.1.5 Proof of Importance (PoI)

Proof of Importance (PoI) [32] has utilized inside the NEM network, which utilizes hidden crypto currency termed as XEM. Each record inside the NEM network has an XEM equilibrium that is partitioned into two sections: vested and unvested. At whatever point, a record obtains XEM, this new XEM has supplemented to the record's unvested equilibrium. One-tenth of each record's unvested equilibrium has enthused into the vested part at every 1440 blocks. Likewise, when a record directs XEM, which has drawn from both the unbalanced and the unbalanced equilibrium in order to maintain the unbalanced equivalent. For a record to be qualified for a significance calculation it must hold somewhere around 10,000 vested XEM. Given qualification, significance has determined dependent on the measure of vested XEM held, the position of the record within the system (discovered utilizing the NCD aware Rank algorithm), a weighting factor dependent on the topological area of the record (as in, regardless of whether the record is an exception or part of a cluster of hubs), as well as two appropriate constants dictated by the NEM network.

3.1.6 Proof-of-Property (PoP)

The established knowledge of the projected technique is to incorporate a Proof-of-Property [33] (individually the evidence that the information locations of a specific exchange claim enough coins to satisfy the expressed exchange) in every exchange. To be practical in an untrusted domain like blockchain applications, this Pop needs to speak to the express the block chain organize has concurred onto without presenting any potential outcomes of misrepresentation. Other than different changes, the architecture of the Ethereum network varies from the Bitcoin design in the manner in which the worldwide condition of the framework is stowed. As officially expressed, after the Bitcoin design the condition of the system (separately the credit of the diverse locations) is just accessible in a roundabout way through the prepared exchanges. Rather than this, the Ethereum design instructs that the condition of the framework is expressly assumed in each block. To do as such effectively a Merkle Patricia Tree has utilized where unaltered hubs just point to hubs accessible in prior blocks. One favorable position of Patricia trees over basic Merkle trees is that the inclusion request of new hubs does not influence the subsequent structure of the tree, in this manner bringing about a similar root hash. This empowers clients to allude to hubs in a preceding tree rather than expressly including them without influencing the determined root hash esteem. Along these lines, this property of the information structure permits the advancements on which Ethereum depends on and which would not be conceivable with typical Merkle trees.

3.1.7 Proof-of-Exercise (PoX)

Proof-of-eXercise (PoX) [34] is a way to deal with mining in crypto currencies-concentrating on Bitcoin-through settling a genuine Xercise: a logical calculation matrix-based issue. The decision behind matrix-based issues is two-overlay: (1) matrices have fascinating composability possessions that assistance in tuning trouble, communitarian confirmation, as well as pool mining; and (2) matrix-based issues length a wide scope of helpful real-world issues, being a rule reflection for most logical calculation issues, among them: DNA and RNA sequencing and information

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

examination, protein structure investigation, image correlation, object superposition, surface coordinating, cooperative-separating suggestion, information mining, computational geometry, confront recognition, and numerous others. It is a way to deal with supplants the hash-based riddle by resolving matrix-based logical calculation issues. To distinguish the difficulties of PoX and address them, we require the benchmark properties to analyze.

3.1.8 Byzantine Fault Tolerance (BFT)

Byzantine Fault Tolerance (BFT) [35] is a classification of replication algorithms that mean to take care of the issue of achieving the consensus when hubs can produce self-assertive information. As depicted, BFT can ensure the security (the shot that something negative will occur in the framework) besides liveness (the possibility that advancement will be made inside the framework) of a framework given that close to $\left\lfloor \frac{(n-1)}{3} \right\rfloor$imitations are defective over the framework's lifetime, where n is the total number of copies inside a framework. BFT can deal with up to 33% of hubs being defective. Ordinarily, up to $3f + 1$ imitations so as to provide security and liveness in the framework, where f is the total number of flawed reproductions controlled within the said framework; be that as it may, no less than one known BFT employment can lessen this to $2f + 1$ required copies.

3.1.9 Delegated Byzantine Fault Tolerance (DBFT)

As the name infers, Delegated Byzantine Fault Tolerance (DBFT) [36] is a variation of standard BFT. Portrayed in the NEO whitepaper, this fault tolerance algorithm parts customers inside a P2P framework into two separate sorts: accountants and common hubs.

Normal hubs don't partake in deciding consensus at the same time, rather, vote (consequently the "delegated") on which accountant hub wishes to help. The accountant hubs that were effectively chosen are then incorporated in the consensus procedure. In this procedure, an irregular accountant hub has chosen to communicate its exchange information to the whole system. It ought to at least 66% of the alternate accountants concur that the exchange information is legitimate, it is submitted forever to the blockchain then another round of consensus is begun with another arbitrarily chosen accountant.

3.1.10 Ripple Protocol Consensus Algorithm (RPCA)

As the name infers, Ripple Protocol Consensus Algorithm (RPCA) [37] is a consensus algorithm used only by the Ripple crypto currency and explicitly created to tackle inactivity problems within the various algorithms. As characterized in the whitepaper, RPCA works as pursues:

- Each server takes every single substantial exchange it has seen preceding another consensus around and places them into a public rundown named the candidate set.
- Each server joins all hopeful sets found on its "Unique Node List," which is a lot of other Ripple servers that the server reserved the reference to.
- Each server votes on the veracity of every exchange in a progression of one or different rounds.
- All exchanges that meet at least 80% "yes" votes in the last round are kept in touch with people in general record and the record is shut.

3.1.11 Stellar Consensus Protocol (SCP)

Stellar Consensus Protocol (SCP) [38], characterized, as a decentralized consensus protocol wherein hubs inside the system don't have to confide in the total of the system in any case, rather, can pick which hubs they trust. This cluster of hubs which trust each other has alluded to as a "quorum slice," an idea originally presented by this protocol. A "quorum" is a collection of hubs suitable for an interpretation, whereas a quorum slice is a subset of a quorum that persuades one particular hub of the statement.

SCP begins with a "nomination protocol" by suggesting new, competitor esteems for understanding. Every hub which gets these qualities will vote in favor of a solitary incentive among these, which in the end results in single esteem winning the larger part vote. After the assignment protocol has been effectively executed, the "ballot protocol" is deployed. Amid this stage, hubs start voting on regardless of whether to submit or prematurely end the qualities that were chosen amid the past stage. If a lot of hubs can't achieve consensus, the esteem has stimulated to a higher esteemed ballot to be voted on once more.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

IV. Applications of Blockchain Technology

Blockchain-based solicitations are leaping up, wrapping various arenas comprising financial administrations, notoriety framework as well as the Internet of Things (IoT), etc. Since public blockchain remains available to the world, it can draw in numerous users besides the networks are dynamic. Numerous open block chains develop step by step. Concerning the consortium blockchain, it could be connected to numerous business applications. At present, Hyper-ledger is emerging business consortium block chain systems. Ethereum likewise has given instruments to build consortium block chains. Besides, business applications, for example, electric vehicle charging, picture acknowledgment for tags, area-based administration data, in addition to dynamic scene to help vehicle navigation, can be executed on a devoted stage.

It is utilized to encourage machine-to-machine (M2M) communications and inaugurate an M2M power showcase with regards to the synthetic business by including two power makers and one power purchaser exchanging with one another over a block-chain. The potential applications for the block-chain technology are almost without limit. At the moment, several of these applications are banking, manufacturing industry, financial, block-chain could be utilized to encourage M2M ware exchanging.

4.1 Internet of Things (IoT)

In an IoT biological system [40], the greater part of the correspondence is as like Machine-to-Machine (M2M) cooperation. Hence inaugurating trust between the partaking machines is the major challenge that IoT innovation still has not been met widely. Nonetheless, Blockchain may go about as an impetus in such manner by empowering upgraded adaptability, security, reliability, and confidentiality. This can be accomplished by conveying Block chain innovation to follow billions of gadgets associated with the IoT eco-frameworks and used to empower and additionally arrange the exchange processing.

Relating Block chain in the IoT environment [41] will likewise build dependability by cutting out the Single Point of Failure (SPF). The cryptographic calculations utilized for encryption of the block information just as the hashing methods may give better security. In any case, this will request all the more processing force which IoT gadgets presently experience the ill effects of. In this manner, supplementary investigation is obligatory to defeat this contemporary restriction. A portion of the instances of block chain IoT are

- Smart Appliances
- Supply Chain Sensors and so on.

Specifically, the blockchain could be extremely useful in building the security safeguarding IoT. A private-by-structure IoT could be encouraged by the amalgamation of the block chain besides a P2P stowage framework.

4.2 Smart Contracts

Advanced smart contracts [42] with an if-this-then - that (IFTTT) code are installed, which stretches them self-execution. All things considered, a delegate guarantees that all parties follow through on terms.

The block chain defers the requirement for third parties as well as guarantees that all record realizes the agreement subtleties also those legally contractual terms actualize naturally once conditions are met. The smart contracts have utilized for a wide range of circumstances, for example, Including insurance premiums, property law and crowd-financing contracts. Some of the smart contracts of Blockchain are,

a) Blockchain Healthcare

Individual Health records could be encoded and placed with a private key on the blockchain with a private key which would allowance the admittance only to the explicit people [43]. The similar system could be utilized to guarantee that the exploration has been conducted through HIPAA (secure and secret) legislation. Surgery receipts could be kept on a blockchain and sent naturally to protective suppliers as proof of transportation. The ledger, as well, could be utilized for human services, for example, administering drugs, direction consistency, testing results, as well as overseeing the medicinal services supplies.

b) Blockchain Music

Key problems in the music business include ownership rights, distribution of royalties and simplicity. The sophisticated music industry focuses on monetizing productions, while ownership rights are frequently disregarded. Innovation in blockchain and smart contracts can address this problem by creating a comprehensive and precise decentralized music rights database.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

Meanwhile, the ledger offers a simple transfer of craftsmen's sovereignty and steady circulation to all the marks needed. Players would be paid in computerized currency according to the agreement's predetermined reports.

4.3Food Safety

One more captivating usage for blockchain could be in the outlining nourishment from its inception to your plate [44]. Along these lines, the block chain data is changeless; you'd have the ability to pursue the vehicle of wherewithal things from their motivation to the store. In addition, ought to there be a nourishment-borne ailment; block chain would enable the wellspring of the pollutant to be originate significantly snappier than it tends to be now.

4.4 Financial Service

a) Payment Processing and Money Transfers

Apparently the most intelligent use for blockchain is as a way to assist the exchange of assets starting with one party to another [45]. As noted, with banks expelled from the condition, as well as approval of exchanges continuous 24 hours every day, seven days a week, most exchanges handled over a blockchain can be settled inside merely seconds.

b) Asset Management: Trade Processing and Settlement

Customary resource exchange procedures (where parties exchange and supervise assets) can be expensive and harmful, particularly in cross-border transactions. Each party, for instance, representative, caretaker or settlement manager, maintains its own documents that generate enormous wasteful elements and room for error. The record of blockchain reduces error by scrambling the documents. Meanwhile, the record streamlines the procedure while dropping the arbitrator requirement.

c) Insurance: Claims Processing

Claims handling can be a disappointing and unacknowledged practice. Processors of assurances need to swim through false instances, disjointed sources of data, or abandoned user strategies to express a couple – and physically exercise these constructions. There is enormous room for the error. The blockchain provides an optimal structure for risk-free administration and simplicity. Its encryption characteristics allow security network suppliers to arrest the liability to be protected.

d) Payments: Cross-Border Payments

The global payments industry is misleading, costly and open to illegal tax avoidance. Crossing the world requires days if not longer for money. The blockchain now provides agreements with settlement organizations such as Abra, Align Commerce and Bitspark, which give end-to-end blockchain-fueled settlement administrations. Santander finished one of the main banks in 2004 to combine blockchain with installment apps, empowering customers to make universal payments 24 hours a day while clearing the next day.

4.5Weapons tracking

One of the hot-catch themes on any news network right now is firearm control and additionally weapons responsibility [46]. Blockchain could make a straightforward and constant vault network that permits law implementation as well as the central government to follow firearm or weapon proprietorship, just as track weapons sold secretly.

4.6 Enabling and Securing Spectrum Sharing

The block chain confirmation protocol has utilized for empowering and anchoring spectrum partaking in moving cognitive radio (CR) networks [47].

The spectrum-sharing component is utilized as a medium-access protocol for retrieving wireless data transmission among contending CRs. A virtual currency to contact the spectrum, called Specoins. A bartering system dependent on first-come-first-served queue has utilized, with the cost for the spectrum publicized by every essential client in a decentralized manner. The blockchain protocol encourages the exchanges among essential and optional clients and has utilized to approve and spare every client's virtual wallet. Additionally vital for portable systems, the block chain fills in as an appropriated database that is obvious by every single participating party, and any hub can volunteer to refresh the blockchain. The volunteer hubs are entitled *miners*, and they are granted *Specoins*.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

V. Security Issues and Challenges

However, there are several benefits in the blockchain technology; still here are numerous difficulties related to the block chain expertise, for example, scalability plus safety issues and so on, which are waiting to be overcome.

5.1 Security Issues

Since blockchain is one of the fundamental expertise in FinTech (Financial Technology) production, users are exceptionally worried about its refuge [48]. Certain safety susceptibilities as well as assaults have been freshly detailed. Some of the drawbacks related to the security issues are reported here, such as,

- The smart contracts with safety susceptibilities may prompt money related misfortunes.
- Smart contracts may have safety susceptibilities can origin program imperfections, and so on.

The security problems of blockchain concept has been broadly classified into three phases, namely,

1. Technological security issues
2. Organizational security issues
3. Environmental security issues

5.1.1 Technological Security Issues

The technological security issues [49] are categorized into three sub-categories which are explained below.

a) Scalability

As the number of exchanges increases gradually, the block chain turns out to be overwhelming. Bitcoin blockchain has now exceeded 100 GB of storage [50]. To approve the exchange, all transactions must be stored. In addition, due to the original block size containment and the interim time used to create another block, the Bitcoin blockchain can only process about 7 transactions per second, which can't fulfill the need to prepare a big amount of exchanges in a continuous design. Mean while, as the block limit is low, countless tiny exchanges can be delayed as miners are inclined towards those exchanges with a heavy exchange charge. Be that as it may, expansive block size would cause blockchain branches to return from spreading velocity. So the problem of scalability is very intense.

b) Interoperability/Compatibility

Interoperability is the capacity to unreservedly share data crosswise over block chain frameworks [51]. In a completely interoperable condition, if a user from another block chain directs you a bit on your blockchain, you will have the capacity to effortlessly peruse, fathom, and cooperate with or react to it with slight exertion. Tasks that need to execute interoperability in their framework expect to make a platform that will empower different distinctive block chains to discuss effectively with one another, without the requirement for an outside delegate.

c) Reliability/Adaptability

Adaptability and adequacy of the innovation are accomplished through a lowering of the load on the EON stage [52]. The decentralized system accepts the basic capacity associated with security. Right now, the less critical information, for example, symbols and pictures, are deposited with external service providers. This design takes into consideration a wide scope of choices to be actualized, which are exhibited on the "Solutions" page.

5.1.2 Organizational Security Issues

The organizational security issues [53] are categorized into two sub-categories which are explained below.

a) Accessibility

In order for individuals to embrace Blockchain, availability is a must for decentralized apps and game-changers for Blockchain apps[54].As designers, we are committed to ensuring that we do not alienate disabled people, or other adoption rates will not be as common and this absence of integration will face a enormous proportion of the population with legislative and social repercussions

b) Trust

Trust is one of those concepts [55]. As we embed trust into blockchain transactions, new transformative possibilities emerge.

As blockchain increases trust and transparency across value chains, organizations will collaborate and compete in new ways that can't yet be foreseen. As blockchain-supported value chains evolve, many intermediaries will inevitably fall away. The boundaries between industries could blur or fall away completely for new ecosystems evolve.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

5.2 Challenges [56]

As a rising innovation, Blockchain is confronting different difficulties as well as issues. We abridge four typical difficulties:

a) Privacy Leakage

Users trusted that the blockchain gives enhanced privacy when taking care of sensitive information. In blockchain, users could just create the address rather than their identity. The blockchain can't ensure the transnational security. The ongoing investigation demonstrates that Bitcoin transactions are connected together to a record deliver to uncover the personality of the client. The issues were spilled out the user's identity Elliptic Curve Diffie- Hellman- Merkle (ECDHM) can be utilized to defeat this issue. It will manage the public and private key. This will interchange shared secrets between two individuals. It will support to anchored message transaction over the internet. An anchored stage like smart contract and Ethereum is likewise industrialized to keep anchored exchange.

b) MITM Attack

MITM implies Man in The Middle Attack [57] which is recognized as third-party interaction. Here a user came into the middle, which may have a bogus public key. By utilizing this key, he can effortlessly decrypt the delicate information. In blockchain, the general public key is dispersed over the partaking nodes. Each block ought to be associated with a link to the previous as well as the following blocks. Along these lines, the public key is unchanging and it ought not to attack by any bogus keys.

c) DDoS Attack

Distributed Denial of Service (DDoS) is an attack which is the objective to attack one specific framework such as computer, website, server or other network assets. In this way, the approaching messages or association with the objective framework may back off, or even smash or close down. Particularly in blockchain DDoS assault generate some noteworthy business hazard. For all intents and purposes, it is difficult to keep this kind of assault.

b) Selfish Mining

Selfish mining is a type of assault on the veracity of the Bitcoin network. This is the place one miner or mining pool does not distribute and convey a legitimate answer for whatever is left of the system. It is a technique for mining pools towards expanding their profits by without reasonably playing. In spite of the fact that this can be found in some digital currencies where pool shares are not genuinely disseminated which is progressively hard to take away with Bitcoin. The selfish miner [58] then proceeds to mine the following square, etc. keeping up its lead. At the point when whatever remains of the system is about to get closer to the selfish miner, he, or they, at that point discharge the part of explained blocks into the system. The outcome is that their chain and PoW is longer and increasingly troublesome, so whatever remains of the system receives their block solutions and they guarantee the block rewards.

VI. Confinements and Susceptibility

Several Block chain link generally relies upon the measure of dynamic clients within it [59]. So as to work to its maximum capacity, a system must be a vigorous one with a generally conveyed grid of nodes. Besides, there is no Blockchain network in presence that could withstand the indistinguishable measure of exchanges from significant card backers as Visa or MasterCard do. Starting at 2017, Blockchain still has far to go before it will be equipped for supplanting the hulks of the financial world. At last, there is dependably a hypothetical plausibility of a vast-scale capture of any given Blockchain network. In the event that a solitary association will somehow manage to pick up control of most of the system's nodes, it will never again be decentralized in the full sense of the word.

VII. Recent Advances in Tackling the Challenges

The block chain innovations consist of immense influence on numerous businesses [60], and that it won't be restricted to economics. Notwithstanding, it may not occur in the manner in which it is currently envisioned. Both the entrants as well as the incumbents are beholding with enthusiasm at the possessions of Bit coin's block chain in addition to the smart contracts. In any case, as they understand the welfares of dissimilar elements related to the system, it might transpire that while innovative encryption apparatuses as well as the automated execution of transactions have vast and clear advantages, disseminated databases may have a progressively restricted intrigue. A large portion of all, we have to understand that outside of Bitcoin (or different crypto currencies).

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

We have no innovation that provides "less distributed ledgers allowance that cryptographically ensures immutability without the need for trusted third parties." The block chain rebellion may give us different instruments and change the scene of a few enterprises. Be that as it may, meanwhile the advantages of encryption also the smart contracts can be acknowledged without a circulated record, the world after the block chain transformation likely well be a world without the blockchain.

VIII. Conclusion

The blockchain, also called distributed ledger technology, is essentially a digital database managed by a decentralized system, consisting of a number of different computers, in lieu of a single centralized server. These different computers are referred to as nodes and all of them are connected in a randomized way. It is a journal which is practically difficult to produce. It is extremely considered and authorized for its decentralized set-up and peer-to-peer identity. Nevertheless, numerous sorts of research around the blockchain are safeguarded by Bitcoin. In any case, it is critical to reminder that blockchain and Bitcoin isn't a similar object. In this article, we have surveyed the overall concepts of the blockchain technology, which consists of basic definitions, characteristics, key concepts, advantages, limitations, consensus algorithms and along with security challenges and the future work. We intend to take an exhaustive exploration of smart contract in the future which incorporates both the centralized and decentralized models. Like any new innovation, the blockchain is a notion that originally interrupts, and over time it could endorse the improvement of a superior biological community that incorporates both the ancient method as well as the innovative invention.

References

[1] Dwyer, Gerald P. "The economics of Bitcoin and similar private digital currencies." *Journal of Financial Stability*, vol.17, pp.81-91, 2015.

[2] Peters, Gareth W., and EfstathiosPanayi. "Understanding modern banking ledgers through block-chain technologies: Future of transaction processing and smart contracts on the internet of money." *In Banking Beyond Banks and Money*, pp. 239-278. Springer, Cham, 2016.

[3] Becker, Jörg, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer, and Rainer Böhme. "Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency." *In The Economics of Information Security and Privacy*, pp. 135-156. Springer, Berlin, Heidelberg, 2013.

[4] Hawlitschek, Florian, BenediktNotheisen, and TimmTeubner. "The limits of trust-free systems: A literature review on block-chain technology and trust in the sharing economy." *Electronic Commerce Research and Applications*, vol.29, pp.50-63, 2018.

[5] Saberi, Sara, MahtabKouhizadeh, and Joseph Sarkis. "Block-chain technology: A panacea or pariah for resources conservation and recycling?" *Resources, Conservation and Recycling*, vol.130, pp.80-81, 2018.

[6] Shim, Jung P., Merrill Warkentin, James F. Courtney, Daniel J. Power, Ramesh Sharda, and ChristerCarlsson. "Past, present, and future of decision support technology." *Decision support systems*, vol.33, no.2, pp.111-126, 2002.

[7] Kasturiwala, S. B., & ladhake, S. A spatial domain image super resolution approach for soybean leaf diseased image.

[8] Peters, Gareth W., and EfstathiosPanayi. "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money." *In Banking Beyond Banks and Money*, pp. 239-278. Springer, Cham, 2016.

[9] Alvi, Sheeraz A., Bilal Afzal, Ghalib A. Shah, Luigi Atzori, and Waqar Mahmood. "Internet of multimedia things: Vision and challenges." *Ad Hoc Networks*, vol.33, pp.87-111, 2015.

[10] Burchert, Conrad, Christian Decker, and Roger Wattenhofer. "Scalable Funding of Bitcoin Micropayment Channel Networks." *In International Symposium on Stabilization, Safety, and Security of Distributed Systems*, pp. 361-377. Springer, Cham, 2017.

[11] Sompolinsky, Yonatan, and Aviv Zohar. "Secure high-rate transaction processing in bitcoin." *In International Conference on Financial Cryptography and Data Security*, pp. 507-527. Springer, Berlin, Heidelberg, 2015.

[12] Ølnes, Svein, and Arild Jansen. "Block-chain Technology as s Support Infrastructure in e-Government." *In International Conference on Electronic Government*, pp. 215-227. Springer, Cham, 2017.

[13] Peters, Gareth W., and EfstathiosPanayi. "Understanding modern banking ledgers through block-chain technologies: Future of transaction processing and smart contracts on the internet of money." *In Banking Beyond Banks and Money*, pp. 239-278. Springer, Cham, 2016.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

[14] Kumar, S., Srivastava, S., & Kumar, V. Cloud computing with real life case studies and a new approach of solving security issues and putting data in cloud.

[15] Kshetri, Nir. "1 Block-chain's roles in meeting key supply chain management objectives." *International Journal of Information Management*, vol.39, pp.80-89, 2018.

[16] Xu, Quanqing, KhinMiMiAung, Yongqing Zhu, and Khai Leong Yong. "A block-chain-based storage system for data analytics in the internet of things." *In New Advances in the Internet of Things*, pp. 119-138. Springer, Cham, 2018.

[17] Yin, Wei, Qiaoyan Wen, Wenmin Li, Hua Zhang, and ZhengpingJin. "An anti-quantum transaction authentication approach in Blockchain." *IEEE Access* 6 (2018): 5393-5401.

[18] Bartoletti, Massimo, Stefano Lande, LivioPompianu, and Andrea Bracciali. "A general framework for blockchain analytics." *In Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, p. 7. ACM, 2017.

[19] Serguieva, Antoaneta, H. Ishibuchi, Ronald R. Yager, and V. P. Alade. "Guest Editorial Special Issue on Fuzzy Techniques in Financial Modeling and Simulation." *IEEE Transactions on Fuzzy Systems* 25, no. 2 (2017): 245-248.

[20] Lei, Ao, Haitham Cruickshank, Yue Cao, Philip Asuquo, Chibueze P. AnyigorOgah, and Zhili Sun. "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems." *IEEE Internet of Things Journal* 4, no. 6 (2017): 1832-1843.

[21] Azeemi, N. Z. Delivering 4g (lte) to 5g migration with supply chain management.

[22] Scriber, Brian A. "A Framework for Determining Blockchain Applicability." *IEEE Software* 35, no. 4 (2018): 70-77.

[23] Peck, Morgen E., and Samuel K. Moore. "The blossoming of the blockchain." *IEEE Spectrum* 54, no. 10 (2017): 24-25.

[24] Fairley, Peter. "Blockchain world-Feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous." *IEEE Spectrum* 54, no. 10 (2017): 36-59.

[25] Dinh, Tien Tuan Anh, Rui Liu, Meihui Zhang, Gang Chen, Beng Chin Ooi, and Ji Wang. "Untangling blockchain: A data processing view of blockchain systems." *IEEE Transactions on Knowledge and Data Engineering* 30, no. 7 (2018): 1366-1385.

[26] Li, Lun, Jiqiang Liu, Lichen Cheng, ShuoQiu, Wei Wang, Xiangliang Zhang, and Zonghua Zhang. "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles." (2018).

[27] Zheng, Zibin, ShaoanXie, Hongning Dai, Xiangping Chen, and Huaimin Wang. "An overview of blockchain technology: Architecture, consensus, and future trends." I*n 2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557-564. IEEE, 2017.

[28] Gatteschi, Valentina, FabrizioLamberti, Claudio Demartini, Chiara Pranteda, and VíctorSantamaría. "To Blockchain or Not to Blockchain: That Is the Question." *IT Professional* 20, no. 2 (2018): 62-74.

[29] Pîrlea, George, and Ilya Sergey. "Mechanisingblockchain consensus." *In Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs*, pp. 78-90. ACM, 2018.

[30] Turkanović, Muhamed, Marko Hölbl, KristjanKošič, MarjanHeričko, and Aida Kamišalić. "EduCTX: A blockchain-based higher education credit platform." *IEEE Access* 6 (2018): 5112-5127.

[31] Aitzhan, NurzhanZhumabekuly, and DavorSvetinovic. "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams." *IEEE Transactions on Dependable and Secure Computing* 15, no. 5 (2018): 840-852.

[32] Tripathy, A., & Goyal, T. Cloud data security using encrypted digital signature & 3d framework.

[33] Wang, Jingzhong, Mengru Li, Yunhua He, Hong Li, Ke Xiao, and Chao Wang. "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications." *IEEE Access* 6 (2018): 17545-17556.

[34] Kim, Sungmin, and Joongheon Kim. "POSTER: Mining with Proof-of-Probability in Blockchain." *In Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pp. 841-843. ACM, 2018.

[35] He, Yunhua, Hong Li, Xiuzhen Cheng, Yan Liu, Chao Yang, and Limin Sun. "A Blockchain Based Truthful Incentive Mechanism for Distributed P2P Applications." *IEEE Access* 6 (2018): 27324-27335.

[36] Bore, Nelson, Samuel Karumba, Juliet Mutahi, Shelby Solomon Darnell, Charity Wayua, and KomministWeldemariam. "Towards Blockchain-enabled School Information Hub." *In Proceedings of the Ninth International Conference on Information and Communication Technologies and Development*, p. 19. ACM, 2017.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

[37] Ehmke, Christopher, Florian Wessling, and Christoph M. Friedrich. "Proof-of-property: a lightweight and scalable blockchain protocol." *In Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*, pp. 48-51. ACM, 2018.

[38] Shoker, Ali. "Brief Announcement: Sustainable Blockchains through Proof of eXercise." *In Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*, pp. 269-271. ACM, 2018.

[39] Sousa, Joao, AlyssonBessani, and Marko Vukolic. "A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform." *In 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 51-58. IEEE, 2018.

[40] Nguyen, Hoang-Long, Claudia-LaviniaIgnat, and Olivier Perrin. "Trusternity: Auditing Transparent Log Server with Blockchain." *In Companion of the Web Conference 2018 on The Web Conference* 2018, pp. 79-80. International World Wide Web Conferences Steering Committee, 2018.

[41] Mitra, Prasenjit, Jaewoo Kang, Dongwon Lee, and Byung-won On. "Comparative study of name disambiguation problem using a scalable blocking-based framework." *In Digital Libraries, 2005. JCDL'05. Proceedings of the 5th ACM/IEEE-CS Joint Conference on*, pp. 344-353. IEEE, 2005.

[42] Koujalagi, A., patil, S., & akkimaradi, p. The wannacry ransomeware, a mega cyber attack and their consequences on the modern india.

[43] Yuan, Yong, and Fei-Yue Wang. "Blockchain and cryptocurrencies: Model, techniques, and applications." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 48, no. 9 (2018): 1421-1428.

[44] Puthal, Deepak, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Chi Yang. "The blockchain as a decentralized security framework." *IEEE Consum. Electron. Mag.* 7, no. 2 (2018): 18-21.

[45] Li, Zhetao, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, and Yan Zhang. "Consortium blockchain for secure energy trading in industrial internet of things." *IEEE Transactions on Industrial Informatics* 14, no. 8 (2018): 3690-3700.

[46] Liu, Zhe, and HwajeongSeo. "IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms." *IEEE Transactions on Information Forensics and Security* 14, no. 3 (2019): 720-729.

[47] Álvarez-Díaz, Néstor, Jordi Herrera-Joancomartí, and Pino Caballero-Gil. "Smart contracts based on blockchain for logistics management." *In Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, p. 73. ACM, 2017.

[48] Kshetri, Nir, and Jeffrey Voas. "Blockchain in Developing Countries." *IT Professional* 20, no. 2 (2018): 11-14.

[49] Wang, Maoning, MeijiaoDuan, and Jianming Zhu. "Research on the Security Criteria of Hash Functions in the Blockchain." *In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, pp. 47-55. ACM, 2018.

[50] Aste, Tomaso, Paolo Tasca, and Tiziana Di Matteo. "Blockchain technologies: The foreseeable impact on society and industry." *computer* 50, no. 9 (2017): 18-28.

[51] Kshetri, Nir, and Jeffrey Voas. "Blockchain-Enabled E-Voting." *IEEE Software* 35, no. 4 (2018): 95-99.

[52] Kotobi, Khashayar, and Sven G. Bilen. "Secure Blockchains for Dynamic Spectrum Access: A Decentralized Database in Moving Cognitive Radio Networks Enhances Security and User Access." *IEEE Vehicular Technology Magazine* 13, no. 1 (2018): 32-39.

[53] Kang, Jiawen, Rong Yu, Xumin Huang, Sabita Maharjan, Yan Zhang, and Ekram Hossain. "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains." *IEEE Transactions on Industrial Informatics* 13, no. 6 (2017): 3154-3164.

[54] Henry, Ryan, Amir Herzberg, and Aniket Kate. "Blockchain Access Privacy: Challenges and Directions." *IEEE Security & Privacy* 16, no. 4 (2018): 38-45.

[55] Li, Wenting, Alessandro Sforzin, Sergey Fedorov, and Ghassan O. Karame. "Towards scalable and private industrial blockchains." *In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pp. 9-14. ACM, 2017.

[56] Vukolić, Marko. "Rethinking permissioned blockchains." *In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pp. 3-7. ACM, 2017.

[57] Chiang, Chun-Wei, EberBetanzos, and Saiph Savage. "Exploring Blockchain for Trustful Collaborations between Immigrants and Governments." *In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, p. LBW531. ACM, 2018.

[58] Miller, Dennis. "Blockchain and the Internet of Things in the Industrial Sector." *IT Professional* 20, no. 3 (2018): 15-18.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019

[59] Wang, Fei-Yue, Yong Yuan, ChunmingRong, and Jun Jason Zhang. "Parallel Blockchain: An Architecture for CPSS-Based Smart Societies." *IEEE Transactions on Computational Social Systems* 5, no. 2 (2018): 303-310.

[60] Beck, Roman, Jacob StenumCzepluch, NikolajLollike, and Simon Malone. "Blockchain-the Gateway to Trust-Free Cryptographic Transactions." *In ECIS*, p. ResearchPaper153. 2016.

[61] Batubara, F. Rizal, JolienUbacht, and Marijn Janssen. "Challenges of blockchain technology adoption for e-government: a systematic literature review." *In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, p. 76. ACM, 2018.

[62] Zheng, Zibin, ShaoanXie, Hong-Ning Dai, and Huaimin Wang. "Blockchain challenges and opportunities: *A survey."* Work Pap.–2016 (2016).

[63] Orman, Hilarie. "Blockchain: the Emperors New PKI?." *IEEE Internet Computing* 22, no. 2 (2018): 23-28.

[64] Ritzdorf, Hubert, Claudio Soriente, Ghassan O. Karame, SrdjanMarinovic, Damian Gruber, and SrdjanCapkun. "Toward Shared Ownership in the Cloud." *IEEE Transactions on Information Forensics and Security* 13, no. 12 (2018): 3019-3034.

[65] Tapscott, Don, and Alex Tapscott. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. *Penguin*, 2016.

DOI: 10.5373/JARDCS/V11/20192690
ISSN 1943-023X

Received: 24 July 2019/Accepted: 20 August 2019