International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor (2018): 7.426

A Survey on Blockchain Based Smart Applications

Saranya A[1], Mythili R[2]

[1, 2]Department of Information Technology, SRM Institute of Science and Technology, India

Abstract*: Most of commercial and industry applications are centralized and time consuming and also need third party to audit the information. Need of middle man in every application are prone to error sometimes. The Blockchain technology merely conquers the issues of centralized –middle party communication. The decentralized computation and information sharing platform that enables multiple authoritative domains, to cooperate, coordinate and collaborate each other with rational decision making process. A Blockchain is an open distributed ledger, which can record transactions between two parties efficiently and in a verifiable and permanent way. A decentralized database with strong consistency support provides to update the local copy of the global information. Every transaction ensures the integrity at the last minute of the Blockchain to make the entire chain to be tamper proof. Here our study gives the overview of blockchain terminologies, consensus algorithms and various fields of applications of Blockchain. In this paper, we discussed smart contract based applications, government information sharing systems, healthcare, b-voting systems. Consensus algorithms will be differed based on the blockchain types. This paper will direct the researchers with correct path towards the blockchain.*

Keywords: Distributed, Decentralized, Blockchain, Consensus algorithms, Applications

1. Introduction

The technology without central authority of management is called Blockchain. In other words there is no intermediate party is required for transferring and storing the assets from one to other using Peer-to-Peer communication [13]. All the participants in the network can view and verify the accessed and transferred information via ledger. Blockchain relies on container data structure.

Blockchain consists of three main parts namely block, chain and network. Block [4] comprises the list of transaction stored over a particular period. The factor which defines the block size, period, and triggering event, that is unique for every block. Block has two components viz. block header and list of transactions. The block header consists of previous block hash, mining statistics used to construct the block and Merkle tree root. Every block inherits from the previous block i.e. previous block hash is used to create the new block hash and make the blockchain tamper proof. The mechanism to [6] generate the hash contains timestamp, nonce and difficulty. The transactions are organised in a Merkle tree structure. It is used to verify the all transaction and construct the block hash. If there is any change in the transaction, all the subsequent block hash will be changed. Blocks are connected using hashing function which is termed as chaining. Hash function is one of the strongest mechanisms it cannot be decrypted at any cost. Blockchain technology uses double (Secure Hash Algorithm) SHA-256 hash algorithm to make the blocks unaltered. Interconnection of node forms network, it consists of all the transactions that have been carried over by the Blockchain. The nodes can be operated by anyone and it is time consuming and expensive process. The system which has high processing power, operates a node is called as Miner. Miner receives the reward in the form of crypto currencies for their service.

Blockchain [5] is one of the massive technologies which take the control of the world's consistency. It gives the transparent and tracking view to the participants who are all involved in the network. Each and every piece of information about the transaction has been recorded in the public ledger, and it is distributed over the network of participants. Public ledger maintains the high degree of consistency so that the recorded fact remains unaltered at any cost. Because, the entire system is made up of tamper proof concept, if anyone attempts to alter the part of information, it requires higher computational resources and power consumption to break the system. Implementation of Blockchain platforms are differed in three [10] ways namely private, permissioned and permission less model. Private networks are works with limited and trusted people and their transactions are not viewable to the public. So obviously it reduces the delay between the parties and improves the storage capacity as well. Private Blockchain are comparatively very fast and it takes low cost to run. It does not always achieve the decentralised network property of immutability and security. Permissioned models are also called as closed network with limited participants of parties but the records are viewable to the public. This network recurrently works very fast with squat latency and high volume of storage than the public network. Permissioned models are very much suitable for organizations and industries perspective.

Permission less-models are defined as open, public environment [15] in which any of the participants can join the network and involve in the block verifying technique and also establish smart contracts between the parties. Main advantages of the blockchain are the identity pertaining to the participant need not be enclosed in the ledger. We can stick to this system until we are willing to be the participant and thereby extending the Blockchain. The best example of permission less model is mining of crypto currencies, in which anyone can involve into the network and start the mining process. It uses the Proof of Work (POW) or Proof of Model (POM) for reaching consensus. Public networks are comparatively slower and more expensive to use and it achieves high security and immutability than other networks.

2. Consensus Mechanism

By default blockchain are decentralised so that consensus protocols required. As Blockchain works on the global scale the proper security need to be ensured and it is achieved through consensus algorithm [14]. As discussed earlier miner will solve the crypto puzzles which are little complex for which the reward will be distributed in the form of crypto currencies. For the smooth functioning of the above process the network must abide to the consensus rules and thereby if the rules are violated by the participant the blocks will be rejected.

Efficiency of the protocols are laid [2] upon three basic features namely, Security (Consistency of the shared state), real time value and fault tolerance (recovery from the failure of node present in consensus). The consensus protocols are differed based upon the Blockchain network. For permission less model three algorithms has been used to achieve the consistency. Initially Proof-of-Work (PoW), secondly Proof-of-Stack (PoS) and Proof-of-Burn (PoB). Proof-of-Work (POW) provides a robust consistency for Blockchain technology. The block will be forwarded to the persons who solve the crypto puzzles. After solving, [11] the solution is distributed to the other competitive miner for verification. Once the block is verified by them it will be recorded in the ledger. Proof of work strictly denies the double spending transaction. If it is attempted then the transaction will be denied. Proof of Stack requires low CPU computations than proof of work. This is also based upon the token system instead of getting reward for new block generation and verification it will select the miner based on the wealth. The miner takes the transactional files for the security. The proof of stack is again derived by the delegated POS. However it does not work for block validation directly but they will be changed periodically then assign the sequence number for declining the block. If the selected delegates keep on miss their block or publish the valid transactions. The particular delegates will be replaced by other selected delegates Proof of Burn.

Proof of Burn is defined as burn some coins to earn life time access to mine the block on a system based on the random selection technique. The chances of mining the more number of blocks is depending upon the number of coins burned. This algorithm is best solution for handling limited computation resources and it is very good alternative algorithm for proof of work. Comparing to these three algorithms Proof of Work is the power hungry and proof of stack, proof of Burn is a power efficient algorithm. Another mechanism is considered for consensus is Proof of Elapsed Time (PoET). It is proposed by Intel Corporation. Each participant in the Blockchain waits a random amount of time for finishing its task. The first participant in the Blockchain waits a random amount of time for finishing its task. The first participant to finish becomes the leader for the new block. The waiting time of all the participants has been verified by special hardware implemented in the mining system.

In permissioned blockchain consistency will be disturbed under these criteria's namely, crash faults, network/ partitioned faults and byzantine faults (malicious behaviour of nodes). Crash and network faults have been handled by RAFT and PAXOS algorithms, failure and malicious behaviours of nodes has been gripped by Byzantine Fault Tolerance (BFT) and Practical Byzantine Fault Tolerance (PBFT). PAXOS is a first Consensus Algorithm proposed by L. Lamport in 1989. The main objective of this algorithm is choosing a single value under crash or network fault. The system process is divided into three phases called making a proposal, accepting a value and handling failures. All nodes have proposes some value called proposal number, the biggest number among the all nodes has been accepted. If anyone node is failed to update the message to all other nodes, the peer nodes takes responsibility to broadcast the message. This algorithm accepts N/2 -1 failures and this is mainly suitable for leader election.

RAFT consensus algorithm works on distributed manner. This algorithm is used for resolving problem of agreeing same value from the multiple points even in the failure state. Single value is replicated over the network through leader node. The leader node is responsible for gathering the client request and replicating it all other nodes. A leader cannot overwrite the entries in the replication log, everything is recorded by the new entries. The leader node periodically sends the heart beat message to other nodes to maintain the authority. The node which has high term and index is considered as a new leader.

In Byzantine Fault Tolerance (BFT), if any inconsistent information about the transaction is transferred, the reliability steps down since Blockchain is decentralised and no third party to correct it. In order to overcome this issue PoW offers BFT by the means of processing power. In PoS the participants vote in order to recognize the true transaction. The best approach is utilizing the version of PoS with BFT to approve transaction. Consensus algorithm namely (Practical Byzantine Fault Tolerance) PBFT and sieve is supported by hyper ledger, which is to handle the non deterministic chain code execution. For byzantine failure, the PBFT is the first profound solution. In PBFT mechanism each node manages the ongoing information status. After receiving the message the node use the message in connection with the peer nodes. The individual node asks about the opinion regarding the message then the node shares its final decision with other nodes. Sieve allows the network to identify and remove the nondeterministic request and attain consensus on the final output.

3. Applications of Blockchain

Blockchain technology is booming the world towards transparency. Every [3] domain is adopted into this technology because of the decentralised control. Some of the pioneering applications are listed below and explained how it is working beyond this technology.

3.1 Supply Chain Management

Blockchain builds a trust layer for supply chain management. The process [7] involved being transparent the point at which order is placed, manufacturer/ producer of the product followed by the transportation and supply to the end user. Challenges in blockchain are record keeping and

tracking of products. Provenance trading are when a large number of goods are handled by the computer it is difficult to keep track of all the records. It results to transparency lack and cost issues. With the use of Blockchain product information are accessed through embedded sensors and tags. So the products from the production stage to end stage can be monitored and used to detect any fraudulent activities.

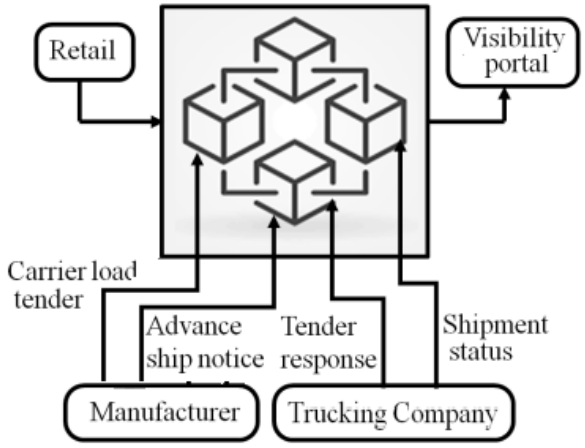

Figure 1: Blockchain based supply chain management system

Blockchain reduces the cost of [9] moving items in supply chain. Elimination of third party middleman and intermediaries in supply chain saves the fraudulent risk and duplicate product. It provides a single view and source of the truth regarding the lifecycle of the purchase order. Payments are done between customer and supplier in the form of crypto currencies. Shadow ledger capturing buyer, seller and carrier data to the blockchain with a web based user interface providing hanced visibility shown in fig1. Risk of misplacement becomes a rare factor. It has the capability of connecting ledger and data points maintaining the data integrity.

3.2 Health care

In order to enhance the quality level of patient health management, the rules and regulations are tedious and procedural lengthy process. So the feasibility is not achieved. The issue encountered is to bridge the gap between service providers and payers. The third party dependency makes the things even worse. For instance, the critical patient information is required urgently the scattered information in various department and systems has to be connected in order to fetch the details immediately. This will not provide us the smooth functioning of the work, handling and exchange of information. It becomes tedious such as missing or misusing of data which is major threat for patient care and health care organization.

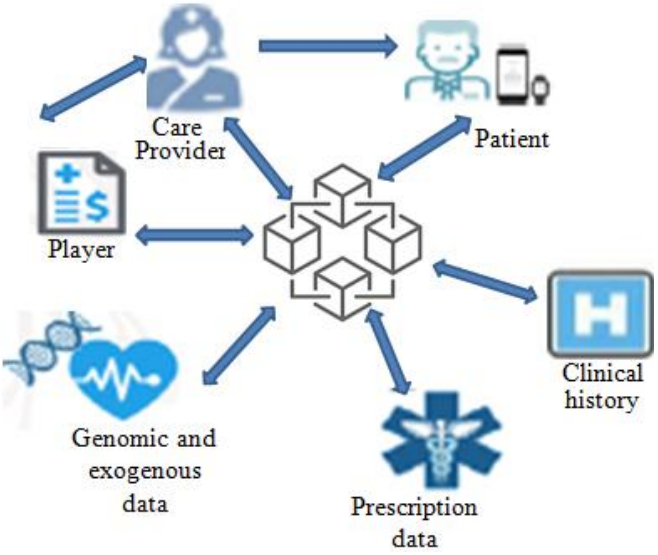

Figure 2: Blockchain based Healthcare management system

Blockchain is one of the leading technologies that influence the world with its high market strategies. Once the information is added to the distributed ledger the alteration cannot be done. The high enhanced security is the strength. If [1] any changes are made the whole subsequent blocks are also to be altered. It provides safe and secure digital relationship. When the blockchain is included in health care the participant will be responsible for their own reports handling and the user have all access rights to control the data. Thereby patient care quality has been improvised by less maintenance cost and multiple level authentications are dropped. Mainly it allows the creation and distribution of single database of health information and easy accessibility to all the entities in the system. Higher security and transparency is allowed and special care and concern is shown to patients by the doctor for their treatment shown in fig2. Permissioned blockchain allows data to be shared among the participants and it is for the use inside the organisation. So that transaction is performed securely. Once transaction is made through consensus it will be the permanent record and it is added to the new block of existing one.

Without Blockchain the information stored is centralized and it is difficult to fetch it. Here patient details are isolated. Once it is decentralised smooth flow of information takes place with the scarce data sets. In the health studies a group of participants enrol themselves and monetize data in form of tokens. With the emerging data sets the implementation of new technologies such as Machine learning and Artificial intelligence would be possible so that discovering the threat and risk factors of health.

With respect to threat if hackers hacks the system the overall data falls into wrong hands. Blockchain can be used to prevent internal infrastructure of an organisation. The different participants have varying levels of access on Blockchain ledger with the encryption embedded in the blocks which prevent the attack from external sources, if it is implemented correctly then issues such as data corruption or hardware failure will be prevented. Payments made through crypto currencies would be tracked and thereby no fraud transaction will be taken place.

3.3 Smart contracts

Smart contracts are a kind of an agreement or contract that implement the self-executing, programmed computer code. It has three core elements [8]: a rate of recurrence to test conditions, a group of conditions and an action that gets activated by those conditions. The smart contracts become immutable, self-executing parts of program meeting on a transparent and auditable public ledger. Once programmed, smart contracts are not taken control of central authority. It helps us to exchange shares, property and money by avoiding a service of third party. By the use of Smart contracts we pay in the form of bit coins into the ledger and the concerned share or property are exchanged. The working of smart contract includes an optional contract between the participants that are written in the form of code into public ledger, which also includes expiry date, strike price etc. Privacy of an individual actor is maintained by regulators and receipt of transaction is held in the form of virtual contract and payment in the form of crypto currencies. Ethereum was designed to support smart contracts.

3.4 B-Voting

In order to minimize the flaws and thereby improving the accuracy of valid votes polled and to check whether the eligible candidates are the voters and thereby permit them to login and vote from any workstation the integration of Blockchain in voting system is introduced. The distributed ledger [12] are used to issue the voting tokens to a poll station which in turn issue token to voters separately and thereby keep a record of voting in side chain at the end the side chain is combined all together to form main voting blockchain and it would be implemented under ethererum and the voting is conducted using smart contracts depicted in fig 3. At the end of voting multi signature is applied by polling station to the recent vote from the voters and smart contracts will be transferred to ballot or candidate. In order to maintain secrecy poll station have capability to keep the votes of the Blockchain and the votes are validated using the smart contract i.e. multi signature element which means both polling station and voter need to sign before the release of Blockchain. By segregating the cryptographic hashes we can build open, verifiable and anonymous voting system.

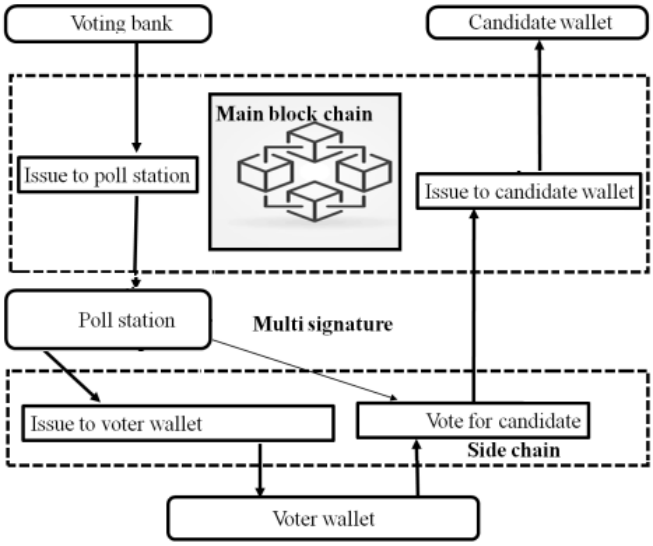

Figure 3: Blockchain based Voting system

3.5 Insurance

By the use of blockchain insurance fraud can be eliminated and efficiencies of claiming can be improved the operation cost insurers who need to minimize fraud. It can be processed using smart contracts. The participants who wish to claim the insurance could be accessed using the distributed ledger in the view to know the policy details. The datasets added to distributed ledger are the proof of insurance, claim form, evidence to support claims. The Blockchain technology can influence the following processes, minimizing paperwork, frameworks should claims can be verified and handled quickly, reducing the frauds, quality of data and efficiency of the insurance value chain. Distributed ledger uses crypto techniques to prevent addition, modification and removal of data.

3.6 Smart Land Registry

The land information is stored on the decentralized public ledger, those records and manages the property rights. It enables the secure and fast instant transfer of land property, when the certain conditions are met from the buyer and sellers perspective. Blockchain based land registries eliminates the registration gap, and automatically update the ledger simultaneously. The user‘s would allow to access and knows the information about the property, it also provides the automatic assurance about the land property ownership.

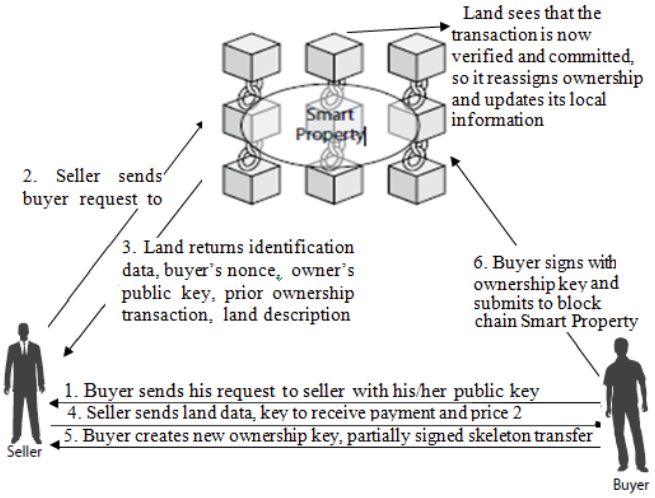

Figure 4: Blockchain based Lang Registry system

Blockchain based land registry reduces the risks involved in frauds, intermediate charges and questionable situations. The framework for smart land registry is explained in below Fig4., initially buyer and seller should register to the permissioned Blockchain network with their identity and it is connected with their mobile for instant updating. The buyer generates a request and forwards it to the seller and asks in return for the details of land. The seller takes the buyer’s request and passes it to the land. Then the land (Blockchain) responds to seller that contains the buyer’s request, the lands public key, other details of land (ownership, area, location etc.,) the current owner’s public key, and the transaction details of the prior ownership transaction. This information is enough for the buyer to know about the land and the seller. Once the buyer is satisfied, transaction will be initialised and ownership

information will be processed and updated to all users.

3.7 B- Music

Major problems in the music industry comprise ownership rights, royal's distribution, and transparency. The digital music industry mainly focuses on ownership rights for currency or asset productions. Blockchain technology creates decentralized database of music rights and the distributed ledger gives transparent communication of artist royalties. Depending upon the specified contract the users paid with digital currency.

Digital copies of artiste's music, they can sell and paid from the customers directly without publishers, it will improve the relationship between musicians and their fans. Artists achieve more independence to market their own music. Blockchain technology provides the complete control and access to their content. For example Ujo music is an ethereum backed music software Services Company or the modern economic landscape of music.

3.8 Digital Identity

People are known by their identities, it drives every business and social interactions. Identity is a collection of attributes like age, name, financial history, address history and social history. Many identity frauds have been happened recent years due to lack of authenticity, authorization and verification. There is no visibility over the identity attributes. Identity data is typically decentralised in passport, driving license, voter card, aadhaar card, banking passbook. Single identity is replicating in multiple purposes. Instead of maintaining multiple copies of single document, place Blockchain technology to decentralise the identities accessed through one password called Single Sign On (SSO).

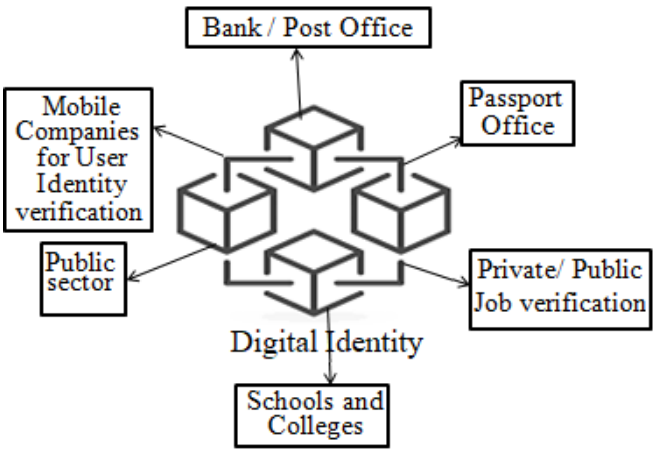

Figure 5: Blockchain based Digital Identity system

Each individual should have full control and ownership of their identity information. Individual can control the usage of their own identity profile for business and social interactions. Fig 5. Ensures the Distributed Trust Model, defines multiple different vendors can access identity profile for different purposes. User can give the two solutions namely consent for identity usage and control identity attributes and identity profile. An automated and real time verification of identity through smart contract can verify identity without revealing the identity data. So no one cab tamper with the identity information of individuals and auditable record of information access.

Hyperledger Indy provides the platform of sharing the user's identity, and working principles are defined with trust anchors, it verifies the Distributed Identifier. Indy calls the pair wise relationship for sharing and verifying the user's identity. Plenum is one of the examples for distributed ledger platform of verifying digital identity.

4. Conclusion and Future Work

Blockchains based application provides decentralized databases, transparent transactions, and distributed public ledger. In this paper some of the potentials applications are discussed with working principle, explicitly B -voting, insurance, supply chain management, B- music copyright, digital identity, smart contract, smart property registration and healthcare. This will be helpful for Blockchain researcher to continue their work towards real time applications and overcome the issues of traditional systems. This paper also discussed consensus mechanisms and their proof for all types of blockchains. Our future work is to build the real time Blockchain for government record keeping and user verification. It will reduce the duplication of records and workload of user and government agencies.

References

[1] Arpita Nayak ; Kaustubh Dutta, Blockchain: The perfect data protection tool, 2017 International Conference on Intelligent Computing and Control (I2C2).
[2] Christopher Ehmke, Florian Wessling, Christoph M. Friedrich, Proof-of-Property - A Lightweight and Scalable Blockchain Protocol, IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 27 August 2018.
[3] https://www.pwc.in/assets/pdfs/publications/2018/blockchain-the-next-innovation-to-make-our-cities-smarter.pdf.
[4] https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-what-is-blockchain-2016.pdf.
[5] http://www.cs.tau.ac.il/~msagiv/courses/blockchain/overview.pdf.
[6] www.blockchain.info.
[7] https://nvlpubs.nist.gov/nistpubs/ir/2018. https://medium.com/swlh/blockchain-benefits-use-cases-d259c823e968.
[8] Imran Bashir, Book: Mastering Blockchain, Distributed ledgers, decentralization and smart contracts explained.
[9] Johannes Hinckeldeyn, Kreutzfeldt Jochen, Developing a Smart Storage Container for a Blockchain-Based Supply Chain Application, 2018 Crypto Valley Conference on Blockchain Technology (CVCBT).
[10] Manav gupta, Blockchain for dummies
[11] Morgen Peck, Book:Understanding Blockchain Technology: Abstracting the Blockchain, ISBN: 978-1-5386-0038-2.
[12] Nir Kshetri, Jeffrey Voas, Blockchain-Enabled E-Voting IEEE Software, Volume: 35, Issue: 4,

July/August 2018.
[13] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org.
[14] Tooba Faisal, Nicolas Courtois, Antoaneta Serguieva, The Evolution of Embedding Metadata in Blockchain Transactions, 2018 International Joint Conference on Neural Networks (IJCNN), arXiv:1806.06738.
[15] Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda, Víctor Santamaría, To Blockchain or Not to Blockchain: That Is the Question, IT Professional Volume: 20, Issue: 2, Mar./Apr. 2018.

Author Profile

A. Saranya received the M.Tech degree in Information Technology from Madras Institute of Technology, Anna University India 2014. She is currently working as Teaching Associate in SRM Institute of Science and Technology, India. Her research is focusing on Blockchain technologies and applications, improving the efficiency of consensus algorithms.

R.Mythili received the M.Tech degree Information Technology from VelTech Dr.RR & Dr.SR Technical University, Chennai- India 2013. She is currently working as Teaching Associate in SRM Institute of Science and Technology, India. Her research is focusing on Blockchain technologies for IoT applications.