Blockchain Technology: A Step Towards Sustainable Development

P.Chinnasamy, P.Deepalakshmi, V. Praveena, K.Rajakumari, P.Hamsagayathri

***Abstract**: The goal of this research paper is to summarize the collected works on blockchain concepts, blockchain application area, blockchain problems, and draw appropriate conclusions. Since Blockchain is relatively an innovative technology, a representative sample of research is presented, spanning the last ten years, starting with the early work in this field. Different types of Blockchain use and other digital ledger techniques have been investigated, including their challenges, security and privacy issues. The key motivation of the review study is to detect the most favorable direction for future use of blockchain and research challenges in blockchain.*

*Keywords : **Keywords: Blockchain, Bitcoin, Sustainable Supply chain, Smart Contract, Peer-Peer Networking, Consensus.***

I. INTRODUCTION

Bitcoin is the first blockchain application, it's a kind of digital currency based on blockchain technology that uses money to trade online things [1]. Bitcoin's success can generate a great opportunity to use blockchain technologies in many fields and services such as finance, IOT, sustainable supply chain, voting, cloud storage, and healthcare. The sustainable supply chain is linked to the complicated procedures of products being created and distributed. The supply chain, depending on the item, can include many stages, various geographic places, various accounts and payments, various people, organizations, and mode of transport [2]. Blockchain can improve the supply chain's effectiveness and transparency and impact all logistics procedures favourably, from storage to shipment and payment. Besides enhanced transparency and safety attained through blockchain, the physical flow of products can be accelerated [2].

Blockchain is an all-cryptocurrency transactions digitized, decentralized, and public ledger [1, 3]. These documents are chronologically documented, helping participants to keep track of digital currency transactions without keeping central records. Distributed database is one of blockchains key features. In many copies, this type of database exists across different computer systems forming a peer-to-peer network, denoting that there is no single, centralized database or server. All transactions in blockchain are signed digitally with a public key cryptography.

In this paper, we will have a quick study on blockchain structure, essential blockchain components, consensus algorithms, blockchain types in section 2 section 3 discusses blockchain's security issues, in section 4 describes blockchain's future direction and finally concludes in section 5.

II. BLOCKCHIAN'S CONCEPTS

The blockchain technology is a mixture of Cryptography, Peer-to-Peer networks and Mathematics. It solve the synchronization problem in traditional distributed databases by combining P2P networking and distributed consensus algorithms

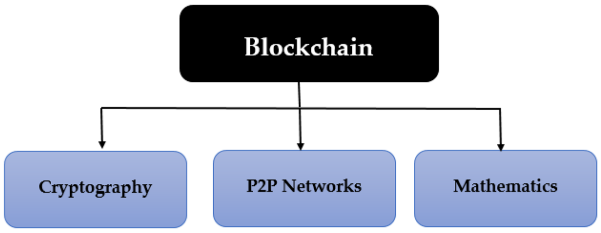

Figure 1. Blockchain Technologies

A. *Components of Blockchain*

The blockchain components are demonstrated in Figure 2 and are explained as follows.

a) **Decentralization:** One of the critical components of blockchain technologies is decentralization. Blockchain system do not rely on centralized third party to keep transactions safe. Due to decentralized nature of blockchain, the data can be record, store and update distributedly.

b) **Consensus Models:** A key aspect of blockchain technology is determining which users publish the next blocks. This is solved by implementing any one of the consensus model [4]. Whenever the consensus algorithms fails, it leads to several issues such as forks problem, dominance issues, and deficient performance of the blockchain network. Based on applicability and efficiency the consensus algorithms has the following properties:

Revised Manuscript Received on December 15, 2019.
* Correspondence Author

P.Chinnasamy*, Department of Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India. Email: chinnasamyponnusamy@gmail.com

P.Deepalakshmi, Computer Science and Engineering, Kalasalingam Academy of Research and Education, Srivilliputtur, India. Email: deepa.kumar@klu.ac.in

V.Praveena, Department of Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India. Email: drvpraveena@gmail.com

K.Rajakumari, Department of CSE, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India. Email: raji1anju@gmail.com

P.Hamsagayathri, Department of ECE, Bannari Amman Institute of Technology, India, Email: palanisamy.hamsagaysthri@gmil.com

I. *Safety:* A consensus protocol have to be safe and consistent, because correct individuals must not delay on incorrect value.

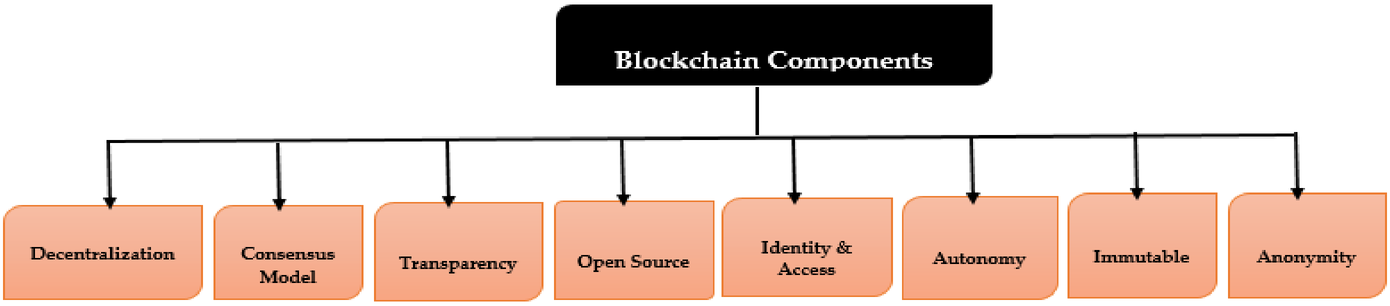

Figure 2. Illustration of Blockchain Components

II. *Liveness:* Every correct value must accepted eventually.

III. *Fault Tolerance:* A consensus protocol offers recovery to some failure node participating in consensus

c) **Transparency:** In blockchain, any one can access and audit the transactions because it is an open file.

d) **Open Source:** Furthermost blockchain system is open to everyone, due to this; anyone can validate and audit the transaction. In addition, people use blockchain technologies to build any applications they really want.

e) **Identity & Access:** The blockchain identity and acessibility are associated to three main principles such as public or permissionless, private or permissioned, and consortium. These principles are discussed in [3]. A public blockchain is designed to cut the intermediary from transactions to maintain the security. Private blockchain restricts the users from having the authority to validate the actual transactions and create the smart contracts. Consortium blockchain is actually partly private and permits some predetermined selective nodes to have full control.

f) **Autonomy:** The main moto of blockchain is to change the trust from one centralized server to the whole system without interfering.

g) **Immutability:** This specific property of blockchain is extremely useful for databases used in financial transactions ever since the records are reserved forever and no one can alter the transaction unless someone will take control more than 51% from the network.

h) **Anonymity:** This property is used to solve the blockchain trust problem between nodes to node. Here, the address of a miner is necessary and no other details is required. There are two different anonymity set is present in a communication system namely sender sets and the recipient sets.

B. *How Block Chain will Works?*

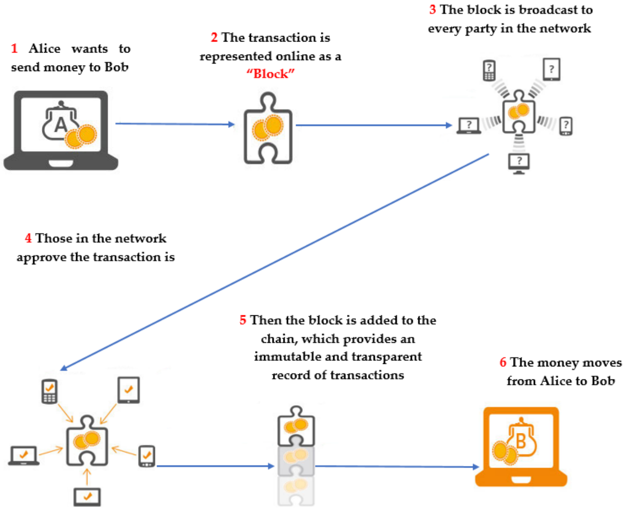
1 Alice wants to send money to Bob
2 The transaction is represented online as a "Block"
3 The block is broadcast to every party in the network
4 Those in the network approve the transaction is
5 Then the block is added to the chain, which provides an immutable and transparent record of transactions
6 The money moves from Alice to Bob
A
B

Figure 3. A Visual representation of blockchain

The Figure 3 shows the working principle of blockchain in a network. It includes

a. Alice is asking for a transaction. Cryptocurrency, agreements, documents or other data could be engaged in the transaction.

b. Using nodes, the desired transaction is transmitted to a P2P network.

c. Using recognized algorithms, the node network validates the transaction and user status.

d. After completing the transaction, the fresh block will be added to the current blockchain.

C. *Structure of Blockchain*

Blockchain owes its name to the way it stores transactions of data in blocks that are linked together to form a chain (see Figure 3). Each block encloses a hash (a digital fingerprint or unique identifier), verified proof of valid transactions with timestamp, and the hash of the previous block. The previous block used to prevent the block from being altered or a block being inserted between two existing blocks. In this way, each subsequent block strengthens the verification of the previous block and hence the entire blockchain.

The method renders the blockchain tamper-evident, lending to the key attribute of immutability [3].

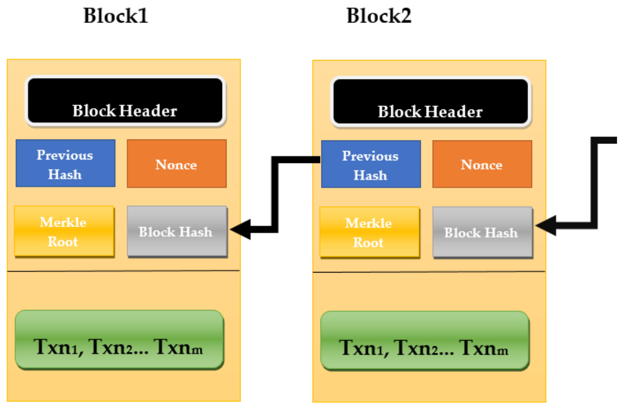

Figure 4. Structure of Block

Each block header should has the following items:

a. **Hash:** A hash function is the one that takes input of any length messages and produce output as distinct fixed length message. If there is any modification in the input, then the output is entirely different. In blockchain technologies the hash functions is utilized in ubiquitously. Each block should containing data is hashed and the modification could be large or tiny. For example, a user named Alice tries to modify the data stored in a block. Once modification can be, done means then the modified block have an entirely different hash value, assuring that every node or miner in the network would have the knowledge of the modification made by updating the ledger copy of the all users. For this reasons, the blockchain is trustworthiness of the data stored.

b. **Merkle Tree:** In a hash tree or Merkle tree every node is represented as a leaf and is labelled with a block. This Merkle tree allows the user to store large data structures in a secure and efficient way.

c. **Timestamp:** With help of this, we can able to track the creation or modification time of a document in a secure way. This item is essential.

d. **Nonce:** A nonce value is basically a 4-byte value staring with 0 and increments each time, whenever hash calculation is performed

D. *Building trust with Blockchain*

Blockchain build's trust through the following five attributes:

- **Distributed:** Every participating party in the blockchain nodes can validate all the transactions. Therefore, there is no need for central server to maintain the data.
- **Secure:** In blockchain all the blocks are immutable hence no can able to alter the transactions.
- **Transparent:** Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data. They themselves can verify the identities without the need for mediators.
- **Consensus-based:** All relevant network participants must agree that a transaction is valid. This can be achieved with consensus algorithms.
- **Flexible:** Smart Contracts that are executed based on certain conditions can be written into the platform. Blockchain Network can evolve in pace with business processes.

E. *Benefits of Blockchain Technology*

- **Time-saving:** No central Authority verification needed for settlements making the process faster and cheaper.
- **Cost-saving:** A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are removed.
- **Tighter security:** No one can temper with blockchain Data as it shared among millions of Participant. The system is safe against cybercrimes and Fraud.

F. *Consensus Algorithm*

A consensus is a procedure to reach a common agreement in a distributed or decentralized multi-agent platform [5]. It is very important for message passing system. Considering a scenario to attack the city by generals who have the certain percentage of Byzantine army circled the city. In this situation, some of the commanding generals favored the option of attacking the city while the other generals are preferred the option of retreating like in Figure 5. Still, the attack would be unsuccessful if only a part of the generals attack the city. This unsuccessful attack leads to a consensus in a disseminated environment. The blockchain also face the same challenge, because blockchain network is distributed with no central server or node.

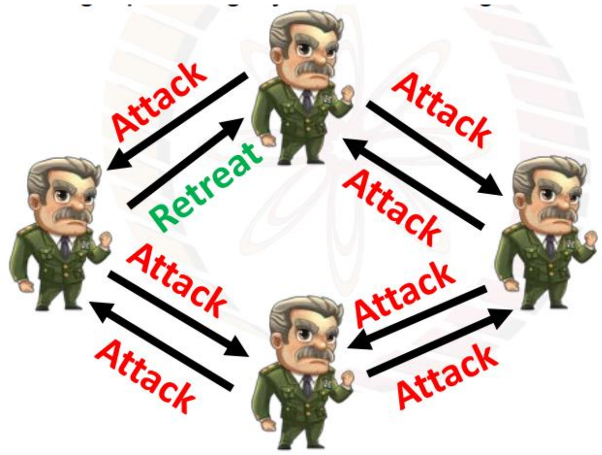

Figure 5. Byzantine General Problem

There are four major consensus algorithm is presented in blockchain and it is shown in the Figure 5. Some blockchain system uses the following consensus mechanisms such as Proof of Bandwidth (PoB), Proof of Elapsed Time (PoET), Proof of Authority (PoA).

1. **Proof of Work (PoW):** In this proof of work, the user publish the new block by being first to solve the computational puzzle. While solving the puzzle many computational operations need to be done to verify the user or node. In PoW, solving the puzzle is difficult however checking that a solution is valid is easy. [1, 3]. After the PoW puzzle is solved the block is broadcast to other nodes as shown in Figure 7. The Bitcoin, Ethereum are examples of PoW.

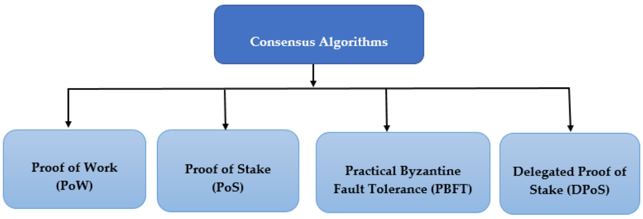
Consensus Algorithms
Proof of Work (PoW)
Proof of Stake (PoS)
Practical Byzantine Fault Tolerance (PBFT)
Delegated Proof of Stake (DPoS)

Figure 6. Consensus Algorithms

2. **Proof of Stake (PoS):** In PoS the integrity of the transaction is proved depending on the amount of cryptocurrency the user holds. The newly created transaction or block can eventually be validated means the amount will be given with bonus otherwise, it will be fined. Compared to PoW mechanisms it requires low computational power [1, 6, 7]. The Ethereum, Casper, Krypton are examples of PoS.

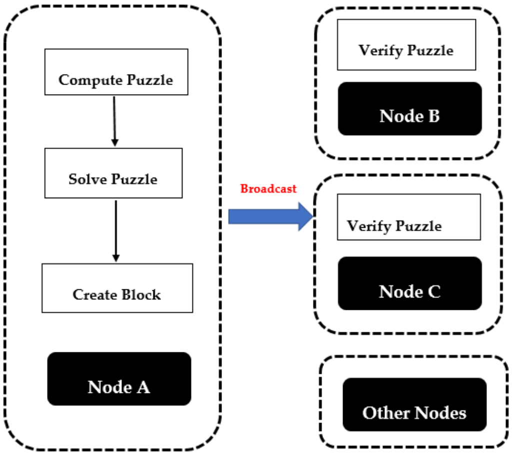

Figure 7. Consensus Mechanism of PoW

3. **Practical Byzantine Fault Tolerance (PBFT):** It is an imitation algorithm created to tolerate byzantine faults [1, 6, 7]. PBFT handles up to 1/3 malicious byzantine replicas. The entire process is divided into three phases namely pre-prepared, prepared and commit. After receiving 2/3 of the votes from all the nodes in the network, then only the node is entered into next phase. Based on three steps, the validation of the transaction is performed. In first step, broadcast a block for prevoting. In second step, precommit a block or transaction. In final step, validates a block or transaction and broadcasts a commit for it.

4. **Delegated Proof of Stake (DPoS):** It is same like PoS protocol and it targets at achieving a distributed consensus in a cryptocurrency system [1, 6, 7]. The Bitshares, Steem, Cardano, and EOS are the best examples of DPoS.

5. **Proof of Authority (PoA):** The publishing new node on blockchain networks, users should prove their identities and validated. This is applicable only to permissioned blockchain with high level of trust [1, 6, 7]. The Ethereum, Kovan testnet, POA Chain are examples for PoA.

6. **Proof of Elapsed Time Consensus (PoET):** The main goal here is to develop a less computational model than PoW with good security guarantees. The publishing new node is depends on random waiting time from a secure hardware [1, 6, 7]. The Hyperledger Sawtooth is example for PoET.

G. *Types of blockchains*

Figure 8 illustrates the three different blockchain types that include blockchain from the public, private, and consortium.

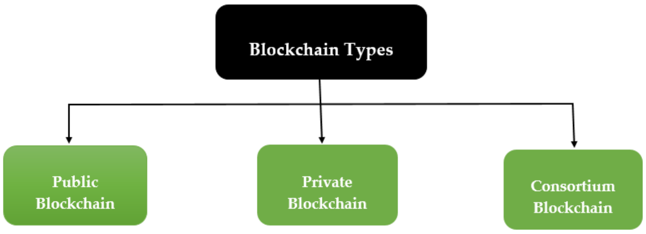

Figure 8. Blockchain Types

1) **Public Blockchain (No Access Restriction):** In this blockchain, every one whose having the internet connection can participate the reading or writing or auditing the transactions [3, 6, 7, 9]. In this type, the decision-making is happened with the help of different decentralized consensus algorithms like PoW and PoS. Examples of public blockchain are the Bitcoin, Ethereum and Litecoin.

2) Private Blockchain (Permissioned): In this type, the participant can join only after getting the invitation from network administrators [3, 6, 7, 9]. Example of private blockchain is Bankchain.

3) Consortium or Federated Blockchain (Semi decentralized): In this type, the selected members of the consortium can run the entire node, make the transaction and review or audit the transaction [3, 6, 7, 9]. Hyperledger and R3CEV are examples of consortium blockchains.

III. Security Issues and Challenges

The table 1 shows the common security issues of blockchain technologies.

Table 1. Security issues of Blockchain

S.No	Security Issues	Reason
1	51% Attacks	Consensus mechanism
2	Private key security	Public key mechanisms for encryption
3	Double spending	Mechanisms for verifying transactions
4	Smart contract vulnerabilities	Flow of program design

a. **The 51% Attacks:** To build mutual trust, the blockchain relies on the distributed consensus mechanism [9, 10]. However, there is a 51 percent vulnerability in the consensus mechanism itself, which attackers can exploit to control the entire blockchain. More specifically, if the hashing power of a single miner accounts for more than 50% of the total hashing power of the entire blockchain in PoW-based blockchains, then the 51% attack can be launched. Thus, the concentration of mining power in a few mining pools can lead to fears of an inadvertent situation, as a single pool controls more than half of all computing power.

b. **Private Key Security:** When using blockchain, the user's private key is considered the identity and security credential that the user creates and maintains instead of third parties. Once the private key of the user is lost, it cannot be recovered [10]. If criminals stolen the private key, the user's blockchain account will face the risk that others will manipulate it. Because the blockchain is not dependent on any centralized trusted third-party institutions, it is difficult to track the behaviors of the criminal and recover the modified blockchain information if the private key of the user is stolen.

c. **Double Spending:** Although blockchain's consensus mechanism can validate transactions, avoiding double spending is still impossible. Double expenditure refers to a consumer using multiple times the same cryptocurrency for transactions. For example, an attacker could use double spending to leverage race attack [9, 10]. The attacker already has the output of the first transaction before the second transaction is mined to be invalid, resulting in double expenditure.

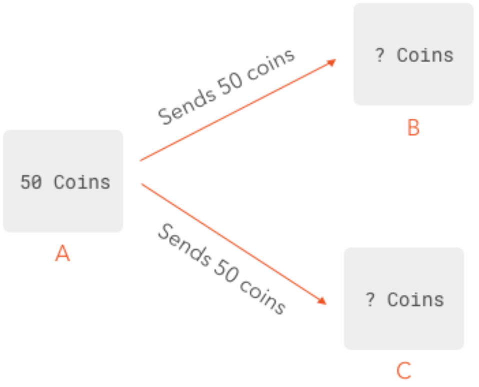

Figure 9. Double spending Problems

d. **Smart Contract Vulnerabilities:** Smart contracts may have security vulnerabilities as programs running in the blockchain due to program failures. Nicola et al.[12] conduct a systematic survey of 12 types of vulnerabilities in smart contracts, including Call to Unknown, Out of Gas Sending, Exception Disorder, Type Cast, Field Disclosure, Immutable Bug and Timestamp Dependency. Loi et al.[11] propose a symbolic execution tool called Oyente to find dependence on transaction ordering, Timestamp dependency, Mishandled exceptions, and vulnerability to re-entry. They find smart contracts vulnerable to 8,833 out of Ethereum's 19,366.

IV. FUTURE OF BLOCKCHAIN

According to Gartner hype circle of emerging technologies 2018, the blockchain could be a game changer for data security leaders as well as it has the potential to improve the reliability, transparency and trust in centralized system [13]. The blockchain experts predict the next big use of blockchain technology as follows;

A. **Digital Identity:** The most gifted application of blockchain technology is digital identity. In past several years, we have seen many issues of privacy and security of digital identity and online social media such as T-Mobile, SingHealth, Facebook, Gmail accounts, Aadhar etc.

The blockchain is the first technology to provide decentralized and self-sovereign digital identities. The term self-sovereign identity describes the ability to deliver blockchain based digital identity system to offer users ownership over the personal data and digital identities. Existing digital identity models have faith in centralized authorities for instance Google and Facebook.

B. **Food and Beverage Supply Chain:** I believe that to ensure quality, security and sustainability, blockchain will be in the manufacture and delivery of food and beverage products. There were a number of high profile blockchain applications in the industry for example IBM Food Trust, which is used in 10 large food companies such as Nestle, Unilever, Walmart.

C. Voting: Voting is the next big room for implementing blockchain technology. It took us weeks to count total voting in Florida for both a governor race and a senate race in the U.S., which is supposed to be the most advanced country in the world. Blockchain has the power to make voting easier, safer, more precise, and more engagement. This could change the course of the United States. I cannot think of a more useful case than that.

D. **Payment Industries:** We believe that in the payments industry is the next big use of blockchain technology. The current system for authorizing and settling credit cards has been designed in the 1970s and has not been updated for the world of today. The technology is very slow and dated, transactions are difficult to track, and fraud is rampant.

E. **Security Tokens:** Security token is blockchain's next important Usecase. In many fields, such as real - estate, intellectual property, fine art, oil stores, it offers tokenization. Every token supports a fraction of an asset. In August 2018, the hotel in St. Regis Aspen was successfully tokenized as an example..

V. CONCLUSION

There is no doubt that in recent years, blockchain has been a hot issue. Due to its decentralized nature and peer-to-peer nature, blockchain technology is highly recognized and valued. These features are capable of supporting a multitude of requirements in various areas and applications. In this article, we propose a comprehensive survey starting with the discussion of blockchain components and their characteristics. Then we try to highlight blockchain technology's security issues. Finally, we provide the Blockchain technology's future direction.

We strongly believe that blockchain will soon become a very common and well-known phenomenon with the speed of its growth and development. Blockchain is compared with various technologies, as the core of blockchain is secure and supportive, as well as the major applications requiring security and non-repudiation are progressively moving on to blockchain. Although, we still have some limitations because it is difficult to implement many innovative applications. Therefore, in the future we plan to undertake a thorough investigation into blockchains

.

REFERENCES

1. D. Yaga, P. Mell, N. Roby and K. Scarfone, “Blockchain Technology Overview”, National Institute of Standards and Technology Internal Report 8202, (2018), 1-66.
2. Edvard Tijan, Saša Aksentijevi, Katarina Ivani and Mladen Jardas, Blockchain Technology Implementation in Logistics, Sustainability *2019*, 11, *1185; doi:10.3390/su11041185*
3. Manav Gupta, “Blockchain for dummies”, John Wiley & Sons, 2018.
4. T. Swanson, Consensus-as-a-Service: A brief report on the emergence of permissioned, distributed ledger system, Report, available online, Apr.
5. V.King and J.Saia, Scalable byzantine computation, ACM SIGACT News, 41, pp. 89-104, 2010.
6. Iuon-Chang Lin and Tzu-Chun Liao, “A Survey of Blockchain Security Issues and Challenges”, International Journal of Network Security, Vol.19, No.5, pp. 653-659, 2017.
7. Archana Prahshanth Joshi, Meng Han, and Yan Wang, “A Survey on Security and privacy issues of Blockchain Technology”, Mathematical Foundations of Computing, Vol.1, No.2,pp-121-147, 2018.
8. “Majority Attack.” *Bitcoin Wiki*, https://en.bitcoin.it/wiki/Majority_attack.
9. Jin Ho Park and Jong Huyk Park, “Blockchain Security in Cloud Computing: Usecases, Challenges and Solutions”, Symmetry, Vol. 9, No. 164, pp. 1-13, 2017.
10. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen*, “A Survey on the Security of Blockchain System”, arXiv.1802.06993v2, 2018.*
11. L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: The ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254-269.
12. N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, 2017, pp. 164-186.
13. https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

AUTHORS PROFILE

Dr.P.Chinnasamy, received his both Bachelor’s in Computer Science and Engineering from Anna University, Chennai and Master’s degree in Computer Science and Engineering from Kalasalingam University. He also received Doctor of Philosophy in cloud security during the year 2019. He was an Assistant Professor of Information Technology at Sri Shakthi Institute of Engineering and Technology. His research interest includes cloud security, Access control, and cryptography. Moreover, he has also published two papers in International Journal and five papers in International Conferences. During 2018. Contact him at chinnasamyponnusamy@gmail.com.

Dr.P.Deepalakshmi is currently working as a Professor in Department of Computer Science and Engineering at Kalasalingam Academy of Research and Education (KARE), Virudhunagar, Tamilnadu, India. She is also serving as Dean, School of Computing. Her research interest includes Optimization Techniques, Network Routing, Distributed Computing, Network Security, Data Analytics, Machine Learning Techniques. She also takes care of KARE ACM student chapter as faculty mentor. Contact her at deepa.kumar@klu.ac.in

Dr.V.Praveena, obtained her both Bachelor’s in Computer Science and Engineering from Bharathiyar University, Coimbatore and Master’s degree in Computer Science and Engineering from Karpagam University, Coimbatore. She also received Doctor of Philosophy in Network Security during the year 2017. She was a dynamic professor of Information Technology at Sri Shakthi Institute of Engineering and Technology. Her talents were soon recognized and propelled her in academic ladder. After 16+ years of experience both in academics and industry. She organized several workshops and seminars for the benefit of both students and professors as well. Her area of specialization includes, IoT Application, Cloud Computing technologies, cyber security and cyber forensics. Moreover, she has also published 16 papers in International and 4 papers in National Conference. During 2018, she had published the book with entitled “Fundamentals of Computer and Computer programming, Web Technology, Operating system”. She is also member of Institute of Electrical and Electronics Engineers (IEEE), Universal Association of Computer and Electronics Engineer (UACEE), International Association of Engineers (IAENG), Indian Society for Technical Education (ISTE).

Dr.K.Rajakumari, obtained her both Bachelor’s and Master’s degree in Information Technology from Anna University of Technology, Chennai. She also received Doctor of Philosophy in Cloud computing during the year 2017. She was a dynamic professor of Information Technology at SNS Institute of Technology. After 12+ years of experience, she moved on to Sri Shakthi Institute of engineering and Technology, Coimbatore to take-up additional professional roles and responsibilities. She organized several workshops and seminars for the benefit of both students and professors as well. Moreover, She hosted both National and International conferences to enhance the knowledge base of the students. She holds rich hands-on experience in C & C++, Java, Python Programming and RDBMS, Software Engineering & Testing. Her area of specialization includes, IoT Application, Cloud Computing technologies, cyber security and cyber forensics. Moreover, she has also published 14 papers in International and 4 papers in National journals. During 2018, she had published the book with entitled “Advanced C Programming”. She is also member of Institute of Electrical and Electronics Engineers (IEEE), Universal Association of Computer and Electronics Engineer (UACEE), International Association of Engineers (IAENG).

Dr.P.Hamsagayathri, received her Bachelor's degree in Electronics and Communication Engineering from Anna University, Chennai during 2006. She had around 8+ years of industry experience where she was involved in working with different technologies like Java, Python, and Web Frameworks. Her thirst in research triggered her to pursue a Master's degree in Communication Systems and Ph.d in Information and Communication Engineering. Much of her research work focuses on designing the cost-effective technical solution for women specific issues to improve their performance standards. Her research interest spans from RF designs for IoT applications, Cloud Computing, Data Analytics and Machine learning. Now, she is serving as Assistant Professor in the Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam. In addition, she has published around 17 papers in peer reviewed International journals and 5 papers in National journals. She also holds the membership of IAENG, IACSIT and Computer and Electronics Engineers.