IJCSN - International Journal of Computer Science and Network, Volume 9, Issue 5, October 2020
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Key Management Scheme for Public Key Cryptography Using Blockchain Network

S. Rajyalaxmi

Assistant Professor, Dept. of IT
Vasavi College of Engineering (Autonomous)
(Affiliated to OU, Hyderabad),
Hyderabad-31.

Abstract- Efficient and secure key management could be a challenge for cryptographic system. Therefore, management of keys is one of the most critical components of the cryptographic system. No infrastructure is secure, without keys to be secure. Public-key cryptography is an important security framework used to provide the authentication and the confidentiality. Authentication and Confidentiality are most critical services in almost all current network applications because of huge amount of data being processed over the networks. These services are currently managed by centralized controller called certificate-authority. Therefore, the services are prone to attacks on the centralized controller. So, we propose key management scheme for public key cryptography using blockchain Network to resolve issues with centralization. This can be possible only due to the presence of the consensus protocol which could be a core a part of Blockchain network. This paper also presents the concept of structure, types and operation of Blockchain.

Keywords*: Block chain, Key Management, Public key cryptography, Consensus Protocol.*

1. Introduction

Blockchain was a technology originally created to support a popular cryptocurrency called Bitcoin. Bitcoin was first proposed in 2008 and launched in 2009 by Nakamoto [1]. In Bitcoin, the normal block creation time is 10 minutes, and the block size is limited to 1 megabyte determining network output [6]. Generally, Bitcoin transaction processing capacity is between 3.3 to 7 transactions per second [7]. However, due to the increasing size of the newly produced blocks, transactions are directly limited to 2-4 per second, which is not the most common. The average size and quantity of blocks and the number of payments in the network can be considered a scalability problem [4]. Scalability is a major problem for blockchain-based platforms [3]. Bitcoin is created, distributed, processed and stored using a separate ledger system known as a blockchain. "Blockchain," a record-keeping technology behind the Bitcoin network. The words "block" and "chain" in this context, referred to as digital information ("block") are stored in the public database ("chain"). It allows both parties to communicate and exchange resources on a peer-to-peer network, where decisions are distributed by the majority rather than by one. As a result, security is a major challenge in current applications.

In Blockchain, data is stored in a multiple node over the network and a copy of each transaction associated with hash of transaction, data is stored in a form of ledger with each member of the network. In blockchain network, for any intruder it is difficult to change the stored data at multiple locations. The decentralized storage provides higher cryptographic security compared to centralized storage. Approval of transactions is given by the bulk of the peer members. So, the blockchain technology completely eliminates the role of central approving authority. Due to decentralization of transaction, hacking is difficult, transactions are automatically approved using consensus protocols and

security costs are also saved. In Block chain, data is quick verifiable; security and privacy are preserved and no alteration is possible without consensus of the majority.

This paper looks at the use of blockchain technology to provide network security services. Rest of the paper is organized as follows: Section 2 introduces blockchain Structure and its variants, Working of block chain network. Section 3 shows the common compatible algorithms used in blockchain, Section 4 introduces key management and its services based on blockchain technology. Section 5 discusses some future indicators and Section 6 concludes the paper.

2. Blockchain Structure

A Blockchain is a chain of blocks that contains information as shown in Fig. 1. The primary block within the chain is termed as **Genesis block**. Each new block in the chain is linked to the previous block. Each Block has

1. Data
2. Hash
3. Hash of the previous block

Hence, all blocks are containing hashes of previous blocks. This is the technique that produces a blockchain so secure. Assume an attacker is ready to alter the data present in the Block 2. Correspondingly, the Hash of the Block also changes. But, Block 3 still contains the old Hash of the Block 2.

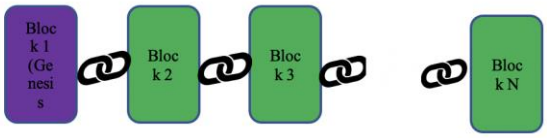

Fig.1: Basic Block chain Structure

This makes Block 3, and all succeeding blocks invalid as they do not have correct hash of the previous block. Therefore, changing a single block can quickly make all following blocks invalid. So, Blockchain is distributed and decentralized network that is cryptographically managed and updated by consensus protocols and agreements among its peers.

2.1. Variants of blockchain networks

The blockchain networks categorized into four types based on the type of access and nodes:

i)Public Block chain: could be a block chain where anyone in the world can become a node in the transaction process. It is a completely open public ledger system. Public blockchains can also be called permission less ledgers. Some popular examples of this type of blockchain are Bitcoin, Ethereum, Litecoin, and so on.

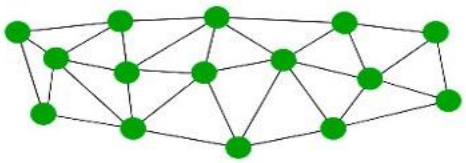

Fig.2: Public Block chain

ii)Semi Private Blockchain: is usually run by a single organization or a group of individuals who grant access to any user, who can either be a direct consumer or for internal organizational purposes.

This type of blockchain has a public part exposed to the general audience, which is open for participation by anyone.

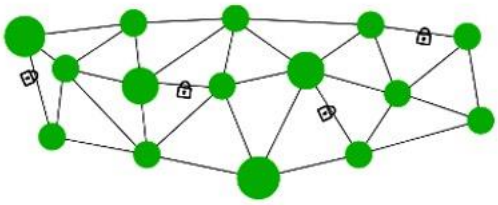

Fig.3: Semi Private Block chain

iii)Private Blockchain: in this one, the write permissions are with one organization or with a certain group of individuals.

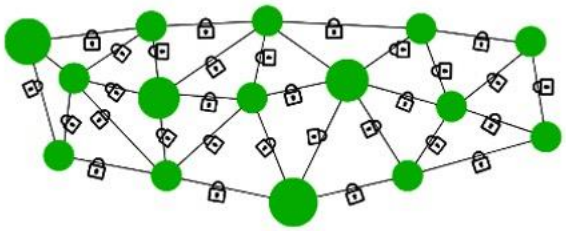

Fig.4: Private Block chain

iv) Consortium Blockchain: In this type of blockchain the consensus power is restricted to a set of people or nodes. It can also be known as a permission private blockchain.

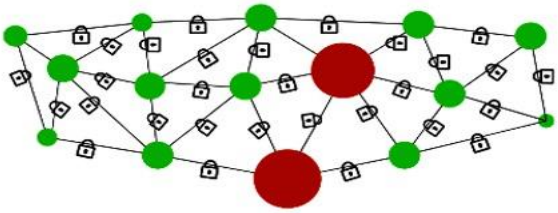

Fig.5: Consortium Block chain

2.2. Working of Blockchain

The main working process of blockchain is as follows:

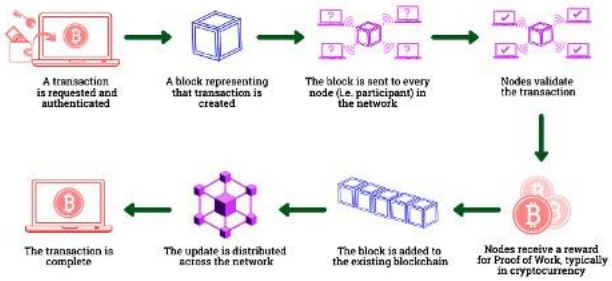

Fig.6: working process of blockchain

Step 1) User requests a transaction and authenticated.
Step 2) A block representing a transaction is created.
Step 3) The block is sent to every node in the network.
Step 4) The network of nodes validates the transaction with the help of known algorithms.
Step 5) All receiving node in the network execute proof- of- work (PoW) algorithm.
Step 6) The block will be added to the existing block chain after executing consensus algorithm.
Step 7) The update is distributed across the network.
Step 8) Then we finish the transaction.

3. Common Compatible Algorithms

Consensus algorithm could be a mechanism that make all blockchain nodes have agreement in same message. Consensus is that the method when all participants of the network agree on the validity of the transactions, ensuring that the ledgers are exact copies of each other. For this process the mechanisms of consensus are used.

The consensus mechanisms of blockchain are:

Proof-of-Work (PoW) : It is the foremost commonly used consensus mechanism.
Proof-of-Stake (PoS): Provides the mining of latest blocks easier for those having the largest amount of cryptocurrency.
Delegated Proof of Stake (DPOS): one small modification it has over PoS is that every node that incorporates a stake can delegate the validation of a transaction to other nodes by means of voting.
Proof of Importance (POI): It is intended to be energy efficient and may also run on relatively less powerful machines. It relies on stake as well as the usage and to determine trust and importance.
Proof of Elapsed Time (PoET): It is designed to have randomness and security within the voting process using a guaranteed wait time.
Proof of burn (PoB): The fundamental concept is that miners should prove that they have burned coins, that is, they need to send them to a verifiable unspendable address.
Proof of activity (PoA): A random peer is chosen during this from the whole network to sign a new block that needs to be tamper-proof.

3.1. Proof of Work (PoW) consensus algorithm

Proof-of-Work (PoW) is that the original consensus algorithm in a blockchain scenario. Proof-of -work may be implemented within a blockchain by the Hash cash proof-of-work system. The Fig. 7 shows the proof of work Consensus algorithm.

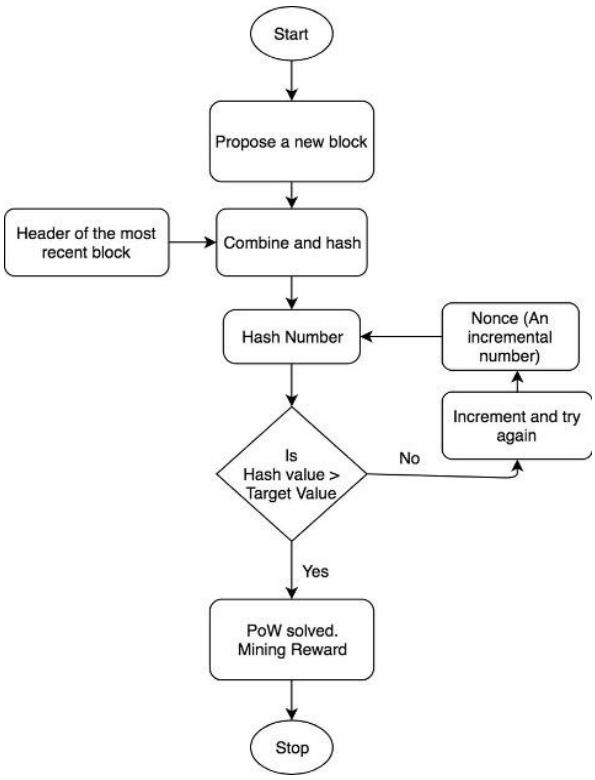

Fig.7: Proof of Work (PoW) consensus algorithm

4. Key Management for Public Key Public Key Cryptography

Public key cryptography (PKC) could be a form of cryptography. In public key cryptography, the key used to encrypt a message is differ from the key to decrypt the received message for secure data communication i.e the public key cryptography, a user has a pair of cryptographic keys-Public Key and Private Key. This pair is that the core component of public key cryptography. The private key is kept secret, while the public key may be widely distributed. These two keys are responsible for carrying out encryption and decryption. Both keys are mathematically related to each other. That means the one private key can only have one public key and vice versa.

This key pair is employed in asymmetric encryption, the encryption system used in SSL/TLS certificates like Bitcoin and other cryptocurrencies.

There are two main branches of public key cryptography such as Public key encryption which provides confidentiality security service where Confidentiality guarantees that data can't be read by unauthorized users and Digital Signature provides security services such as integrity and authentication where the Authentication ensures that the communicating entity is the one who claimed.

Public key encryption: Public key encryption shown in Fig.8 is a technique where a message is encrypted using recipient's public key and the encrypted message could not be decrypted by anyone except the recipient private key.

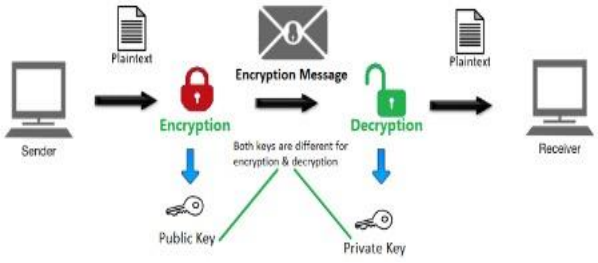

Fig 8: Public key encryption

Digital signature: Digital signature shown in Fig. 9 generally uses two keys one for signing involves the user's private key, and another for verifying signatures which involves the user's public key. The output of signature process is called the "digital signature".

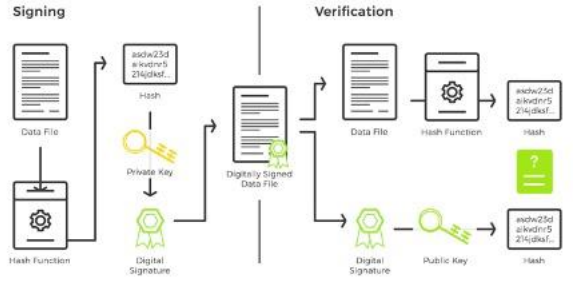

Fig 9: Digital signature

Public Key Cryptography provides secure communication through an insecure channel, which allows a message to be read by the intended recipient only. For instance, userA uses userB's public key to encrypt and send a message to userB, which can be decrypted using userB's private key.

Public Key Cryptography maintains email privacy and ensures communication security while messages are in transit/ stored on mail servers. Public Key Cryptography is also a digital signature standard component used to authenticate a private key verifiable by anyone with authorized public key access, which validates message origin and sender. Thus, Public Key Cryptography facilitates confidentiality, data integrity, authentication.

Public Key Cryptography is bit slow than private key cryptography method, because of high computational requirements. Unlike symmetric cryptography, Public Key Cryptography uses a fixed buffer size, depending on particular and small data amounts, which may only be encrypted and not chained in streams. Although a broad range of possible encryption keys are used, Public Key Cryptography is more robust and less susceptible to third-party security attempts.

4.1. Key Management

The Key management technique is the management of cryptographic keys in a cryptosystem. It deals with whole key lifecycle like generation, exchange, storage, and use of keys.

Why key management is required? With the increase of Cybercrime, companies are investing large amounts in Information Security in order to protect themselves, their employees and partners, but in the end that might not be enough.

Threats:
1.Compromising confidentiality of secret keys
2.Compromising authenticity of private or public keys.
3.Un-authorized use of public or private keys

Key management is an important role in cryptography to deal with security services like confidentiality, entity authentication, data origin authentication, data integrity.

4.2. Public Key Infrastructure (PKI)

The public key infrastructure is method to produce the key management for the public key cryptography. Traditionally, there are two conventional methods to realize public key infrastructure, centralized by a Certificate Authority and decentralized by Web of Trust.

The Certificate Authority - based public key infrastructure is the most typically used method and it has been standardized within the X.509 standard. In this method, the Certificate Authority is a third-party entity that's trusted by all members in the system. The Certificate Authority issues "certificates", which authenticate users and bind each user to a public key.

A signed certificate is binding to a user's public key, and it will authenticate the ownership of that public key to a specific user. The other traditional approach is Web of Trust, which was proposed in 1992 by Phil Zimmerman.

This technique utilizes a decentralized approach during which the keys are generated locally and can be trusted if they are verified by at least one other trusted user in the system.

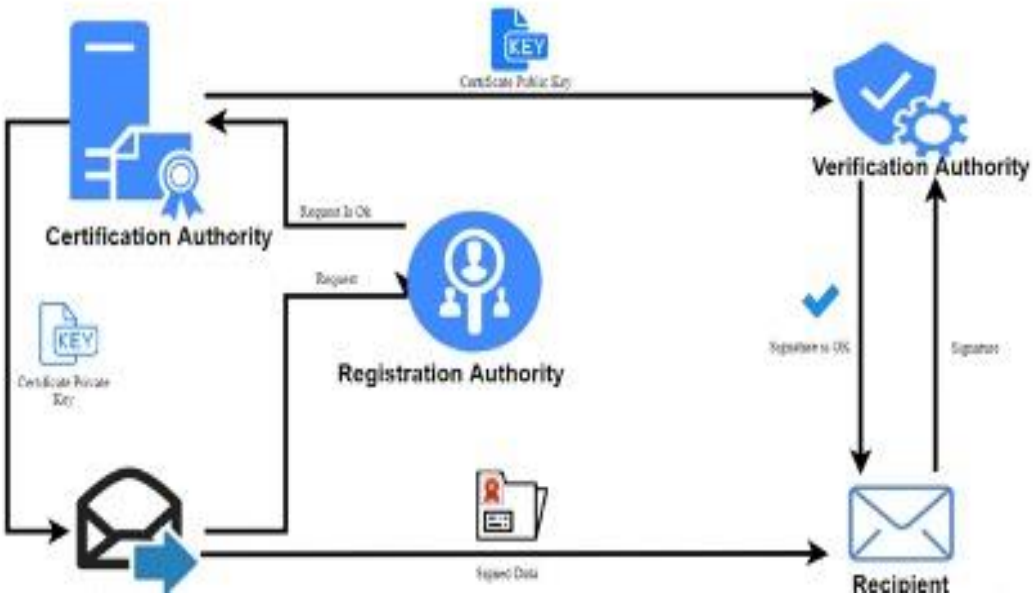

Fig 10: Public Key Infrastructure

i) Problems with the Traditional PKI Systems

The two traditional techniques suffer from several challenges which are discussed here. One is the Certificate Authority-based public key infrastructure comes with three different challenges: a trusted-third-party, a single-point-of-failure, and cost. The users of the systems must trust the Certificate Authority while generating and managing their public keys which insists high-security risks, when the Certificate Authority is compromised. The architecture has a single point of failure as the whole system fails if the Certificate Authority fails. Further, the management of the public keys by a centralized Certificate Authority can be an expensive and in-efficient, especially with the current massively distributed applications where a large number of users are involved.

On the other hand, in the Web of Trust based public key infrastructure, the signers need to build trustworthiness. The users join the network only if they are trusted by another "trusted" member. In other words, new members joining the network need to build prior trust with other members who are already in the system. This may lead to a barrier of new members entering the network.

Moreover, both the Certificate Authority based and the Web of Trust based public key infrastructure are unable to provide identity retention. That is, it is possible for a user to impersonate the identity or the public key of an already registered user. Proposals have been offered to solve this problem, but they are highly complex, especially in the case of the worldwide distribution of the users.

ii) Blockchain-Based PKI Concept

The distributed, the event-recording and non-reproducibility features of the blockchain technology make it a desirable technique for several applications. Particularly, these properties prove the blockchains' suitability for public key infrastructure and domain name services (DNS). Because of the blockchain-based public key infrastructure solutions are distributed; there is no centralized point-of-failure. The trust is built on the majority of the miners; hence, there is no single trusted third party and it does not require prior trust worthiness in the system. More importantly, the blockchain technology has several open-source implementations, which helps build cost-effective and efficient solutions.

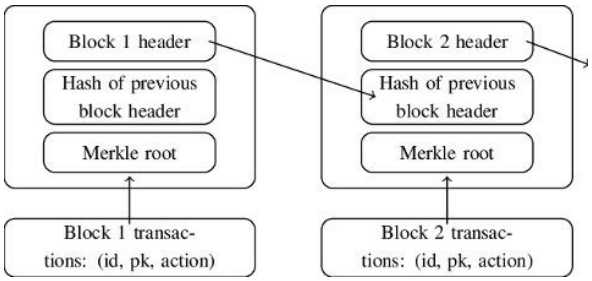

Fig 11: Blockchain-Based PKI

In public key infrastructure a digital certificate or public key certificate is an electronic certificate that

binds with an entity which can be a person or an organization to its public key. The user's public key and its associated certificates are managed by an entity called Certification Authority. As the size of the database is increasing gradually, the management of certificates becomes more difficult. To address this issue an identity-based cryptography is used which is a certificate free paradigm.

4.3. Identity-Based Cryptography (IBC)

The identity-based cryptography has gained interest in the network security community. identity-based cryptography is a public key mechanism that uses the node's ID as the public key rather than generating the traditional public keys. A node's ID may be the node's name or any arbitrary string that can be used as the public key. The encryption approach, as depicted in Fig. 12. consists of four phases: setup phase, extract phase, encrypt phase, and decrypt phase. First the setup phase, a private key generator (PKG) generates a master secret key with system parameters. The private key is kept private while the system parameters are made public. To extract the keys, the generator uses the system parameter in addition to its master secret key and the user's ID. These parameters are used to construct a private key which is sent back to the user. For other nodes to encrypt a message, they use the user ID and the public parameters to generate a ciphertext. The user employs its own private key to decrypt received message. A similar method is used for the signature and the verification, where the signature is generated with the node's secret key while the verification is done with the node's ID and the public system parameters. A generalization of the IBC is to build a Hierarchal IBC where the public key has a hierarchal identity basis that can be represented by a tree.

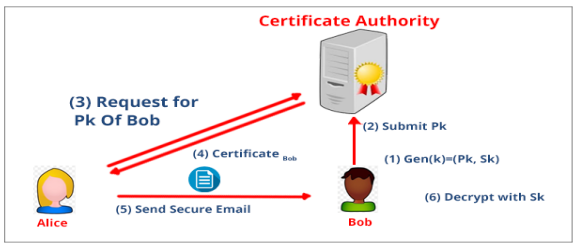

Fig 12: Identity-Based Cryptography (IBC)

i) Problems with the Current IBC Approaches

The problems with identity-based cryptography and the Hierarchical identity-based cryptography approaches are, they require the public-key-generator to generate the private keys. Therefore, the system is centralized which makes it a single point-of-failure and insists a third-party trust requirement. It is centralized as the public-key-generator is the only authority that can generate key pairs. If the public-key-generator is compromised, the whole system is compromised. In other words, the identity-based cryptography and the Hierarchical identity-based cryptography have the same limitation as the Certification Authority -based public key infrastructure of traditional approach. Moreover, the public-key-generator generates the users' private keys; hence, all the users should trust the public-key-generator not to misuse their private keys.

ii) Identity-Based Cryptography (IBC) using Blockchain

Similar to the blockchain-based public key infrastructure methods, the blockchain technology can be used as a distributed database to resolve the issues of the traditional identity-based cryptography methods. Because of the blockchain network support a decentralized database, it resolves the issue of centralization and the single point of failure. The user can generate their own master keys without any third-party trust. However, if user is having a limited resource and not able to generate their own keys. So, it can delegate to any other node which must ensures trust.

The basis of the identity-based cryptography using block chain systems is to let the users generate their own keys. So, because of this, the setup phase and the extract phases are done at the user level and the public parameters are submitted to the blockchain as a transaction. The blockchain nodes check whether these parameters are valid and ensure that they have not been used before. Any user can query the blockchain network later for other users' public parameters which are used to authenticate the user and encrypt the confidential messages.

5. Future Scope of Blockchain Technology

In this section, we have briefly discussed different future scopes for the Blockchain technology. Blockchain technology allows companies to create a digital trail of records of their innovations and can generate a certificate upon registering the new inventions, proof-of-concepts and designs that could prove the integrity, existence, and ownership of any IP asset. With the help of a unique cryptographic layer, all data such as trade secrets or copyright claims could remain private and secured. Another emerging scope of blockchain is smart contract smart contract refers to a digital transaction protocol that executes the rules and policy of a contract. This protocol is a piece of code that is deployed in the blockchain node. The Execution of a smart contract is also initiated by a message which is embedded in the current transaction.

The performance of the smart contract could also become an important research topic.

6. Conclusions

In this paper, we presented a blockchain structure and its working process in providing distributed security services. These services include entity authentication, confidentiality, and integrity assurances. The authentication, the confidentiality and integrity might be achieved by the public key cryptography using encryption method and the digital signature schemes. Thus, we discussed different blockchain-based key management for public key cryptography.

There are still many open issues that need to be further researched and analyzed. Examples of these open issues include privacy, scalability, energy issues, and integration with other systems. The future work is required to address these issues and fill the gaps for more efficient, scalable and secure blockchain applications, testing the different blockchain approaches in large scale and real-time environments.

References

[1] S. Nakamoto et al., Bitcoin: A Peer-to-Peer Electronic Cash System. Citeseer, 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[2] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, ‘‘Blockchain for AI: Review and open research challenges,’’ IEEE Access, vol. 7, pp. 10127–10149, 2019.

[3] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, ‘‘Blockchain challenges and opportunities: A survey,’’ Int. J. Web Grid Services, vol. 14, no. 4, pp. 352–375, 2016.

[4] S. Bano, M. Al-Bassam, and G. Danezis, ‘‘The road to scalable blockchain designs,’’ USENIX, Login, Mag., Dec. 2017, pp. 1–6.

[5] A. Gervais, G. O. Karame, and K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, ‘‘On the security and performance of proof of work blockchains,’’ in Proc. ACM SIGSAC Conf. Comput. Commun. Secure, Oct. 2016, pp. 3–16.

[6] A. Gervais, G.O.Karame,V.Capkun, and S.Capkun, ‘‘Isbitcoina decentralized currency?’’ IEEE Security Privacy, vol. 12, no. 3, pp. 54–60, May/Jun. 2014.

[7] T.Aste,P.Tasca, and T.D.Matteo, ‘‘Blockchain technologies: The foreseeable impact on society and industry,’’ Computer, vol. 50, no. 9, pp. 18–28, Jan. 2017.

[8] M. Kouhizadeh and J. Sarkis, ‘‘Blockchain practices, potentials, and perspectives in greening supply chains,’’ Sustainability, vol. 10, no. 10, p. 3652, Oct. 2018.

[9] F. Casino, T. K. Dasaklis, and C. Patsakis, ‘‘A systematic literature review of blockchain-based applications: Current status, classification and open issues,’’ Telematics Inform., vol. 36, pp. 55–81, Mar. 2019.

[10] M. Alharby and A. van Moorsel, ‘‘Blockchain-based smart contracts: A systematic mapping study,’’ 2017, arXiv:1710.06372. [Online]. Available: https://arxiv.org/abs/1710.06372

[11] R.A.Memon,J.P.Li, and J.Ahmed, ‘‘Simulation model for block chain systems using queuing theory,’’ Electronics, vol. 8, no. 2, p. 234, Feb. 2019.

[12] L. M. Bach, B. Mihaljevic, and M. Zagar, ‘‘Comparative analysis of blockchain consensus algorithms,’’ in Proc. 41st Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO), May 2018, pp. 1545–1550.

[13] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, ‘‘Securing proof-of- stake blockchain protocols,’’ in Data Privacy Management, Cryptocurrencies and Blockchain Technology. Cham, Switzerland: Springer, 2017, pp. 297–315.

[14] S. Matsumoto, R.M. Reischuk, IKP: turning a PKI around with decentralized automated incentives, in: 2017 IEEE Sym- posium on Security and Privacy, SP, San Jose, CA, 2017, pp. 410–426.

[15] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The block chain model of cryptography and privacy-preserving smart contracts,” in 2016 IEEE Symposium on Security and Privacy (SP’16), pp. 839–858, May 2016.

Author: S.Rajyalaxmi received MTech in Computer Science and Engineering from Osmania University, Hyderabad in 2013. Thereafter, she has 15 years of experience from Academia. She is currently an Assistant Professor with the vasavi college of engineering. Her research interests include Computer networks, Cryptography and Network Security and also Blockchain.