A Survey on Role of Block Chain in Smart Cities

Chokkanathan K[1] , Shanmugaraja P[2], Siva Shankar Ramasamy[3], Rujira Ouncharoen[4], Nopasit Chakpitak[5]

[1] Madanapalle Institute of Technology and Science, India, [2] Sona College of Technology, India,
[3,4,5] International College of Digital Innovation, Chiang Mai University, Thailand

Summary

An amazing growth in the field of Internet of Things (IoT) and Blockchain based smart cities from both industry and academia has been witnessed in the recent years. There are many smart applications such as intelligent transportation, smart banking, improving the life style of citizen, energy consumption and managing the waste in the city, handling home needs are supporting the Smart city concept. These applications are profoundly supported by the advanced technologies like Blockchain as well as IoT in the recent past. Smart cities can be supported by the Blockchain core concepts such as secure, transparent, decentralized and immutable nature. Still, Blockchain and IoT technologies implementation in smart cities are in their early stages and significant research efforts are desirable to integrate them. This review article explores the roles and responsibilities of Blockchain and IoT in building smart cities.

Key words:

Block Chain, Smart City, IoT, Artificial Intelligence

1. Introduction

In the last few decades' people are moving towards urban cities and urbanization is growing explosively. The constant growth of the Internet of Things and Blockchain applications are providing the path to construct efficient smart cities. [1, 2]. Smart cities are offering efficient transport, healthcare, banking, waste management and smart home applications where they need high level of security for handling the confidential data of citizens' life. Blockchain and IoT are enabling the smart cities to provide enhanced security and privacy. Particularly Blockchain concepts such as distributed, perceptible, transparent and immutable ledger are more effective and supportive in smart cities construction [3, 4]. Blockchain technology was introduced for the purpose of bitcoin transaction and has obtained substantial accomplishment with a market capitalization of more than US $230 billion after 2017 [5]. Other than the financial industry, Blockchain applications and their potential growth influencing the other domains like IoT, e-Commerce, audit, e-Voting, accounting, supply chain management, taxation, telecommunication [6], healthcare, and government public services etc[7,8].

Smart city idea is influencing the implementation of information and communication technologies in many domains like public welfare, economy, public services, environment, supply chain management, and urban planning etc. [9]. Smart city perception can develop every feature of city life with the help of developing digital technology [10]. The main objective smart city is to afford the restructured services like housing, healthcare, energy, water, waste management, surveillance, education, transportation [11] and law enforcement. Smart cities can integrate the communal, commercial and infrastructure aspects of the city and can manage the difficulties of population growth and efficient suburbanization [12]. Smart cities are supported, protected and instrumented by the latest technologies such as blockchain, IoT, Artificial Intelligence, Big Data and Machine Learning. Moreover, huge volume of data traffic is generated by the information system over network communication [13]. Blockchain technology could be the solution for the key challenges like security, integrity, identity and transparency [14]. Vast amount of transactions can be recorded using blockchain technology and smart contracts provide a great self-sufficiency for accomplishing smart business communications during the smart city functional activities. Blockchain based smart city enables hybrid network architecture to resolve the network and communication issues like latency, scalability, bandwidth, security and privacy etc. [15].

2. Employing Block Chain in Smart City

In this section we present the prominent features of Blockchain technology such as Digital signature, Cryptographic hashing, Merkle tree, Proof of Work (PoW), Peer-to-peer network, Proof of Stake (PoS), Ethereum, Smart contracts, Hyperledger, Decentralization and Consensus algorithm. Figure-1, shows the different functional layers of the blockchain technology and its features.

2.1. Digital signature in Smart cities

A mathematical structure used to validate the reliability and trustworthiness of digital data is known as

Manuscript received July 5, 2021
Manuscript revised July 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.7.1

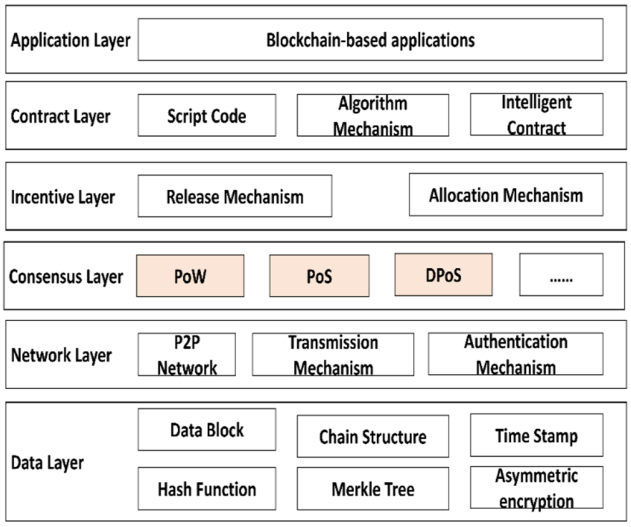

Fig. 1. Functional Layers of Block Chain Technology

Digital signature. It ensures that the receiver is getting the original data without any alteration or fabrication from the sender. Hell-man and Diffie introduced [30] the concept of digital signature in the year of 1976. In general, symmetric cryptography can use single secret key for both encryption and decryption purpose between sender and receiver. Whereas Hellman posses a revolutionary step by presenting Two Key cryptography. This Two Key Cryptography is applied in Blockchain technology with a pair of public and private keys will be distributed to each member in the Blockchain network. Digital signature consists of two steps such as sign and verification. Private Key is utilized for signing process and public key applied for verifying the network nodes in the transaction. So, each and every transaction is having valid digital signature of the originator of the operation. Crypto currency Bitcoin is using elliptic curve digital signature algorithm (ECDSA) [31] for executing digital transaction over the network.

People are focusing more on smart cities and at the time same many Asian countries have attained success with smart city concept. As we know that the smart cities are functioning based on digital transformation, security and privacy. In smart cities, there is no space for paper and physical documents. When they rely more on the digital transformation, digital signature plays a vital role to provide better and safe platform for digital transactions. In a smart city, each and every transaction will be operated electronically. Signing rental agreements, consent forms, employment letter, taxes and consent forms everything will be secured with the support of digital signatures. Moreover, when the document is signed digitally and underlying technology is blockchain technology, we can ensure that the document is tamper proof and the malfunctions can be eliminated from the digital documents.

2.2 Cryptographic hashing

A function that can convert arbitrary size of data into fixed size values is known as hash function. The obtained fixed size value is termed as hash value, hashes, digests or hash codes of the input sequence. This one-way hash function was introduced by Hellman and Diffie in the year 1976 for the purpose of safe digital transaction [30]. A trap door function was introduced by Hellman which will compute values in the forward direction but it is difficult to revert back and highly impossible to get the original content. In 1979, Merkle redefined this one way has function in detail. It provides an ideal hash function which is proficient, non-invertible, effective, deterministic and collision free [32, 33]. Blockchain uses cryptographic hash function for maintaining Tamper-proof storage and block investigation in digital transactions.

Usage of new technologies increases the security vulnerabilities in confidential data and sensitive transactions. But, the blockchain technology provides an alternate solution for the security breaches in many application environments. The important features like distributed structure and cryptographic hash functions of blockchain technology provide more security for the online transactions. Smart city applications like Smart Home, Smart City, and Smart Agriculture are created with end to end encryption [34] using cryptography algorithms.

2.3 Merkle tree

Merkle tree (MT) is a data structure which can be used in many computer science applications to store the data in a protected and proficient manner [35]. Moreover, it provides encoding technique which can protect the data in a tamper-proof manner. Huge volume of data can be verified securely with the help of MT, which is a binary tree where each leaf node consists of the hash value of one data block. Each non-leaf node is named by combining its two children nodes' hash values. The root node of the MT is named as Merkle Root (MR) which is created in the above mentioned procedure. Any change in the leaf node or data block will be reflected in MR. MT is a hash-based cryptography which supports blockchain technology based online transactions. There is special provision in blockchain technology, which can verify partial nodes without downloading the entire block. This provision is named as Simplified Payment Verification (SPV), which employs based on MT's manipulation of hierarchical nature. A simple Merkle tree and hierarchy structure is represented in the figure. 2.

When public key cryptography is used for protecting the data and transaction, there is a possibility of quantum computer attack. Merkle tree is the alternate

solution with low cost for securing the mesh network, where huge number of clients is involved in a network. Comparatively lightweight merkle tree can be generated quickly and also provide better protection for data than the public key cryptography. Particularly Merkle tree is the best solution for the quantum computer attack [36].

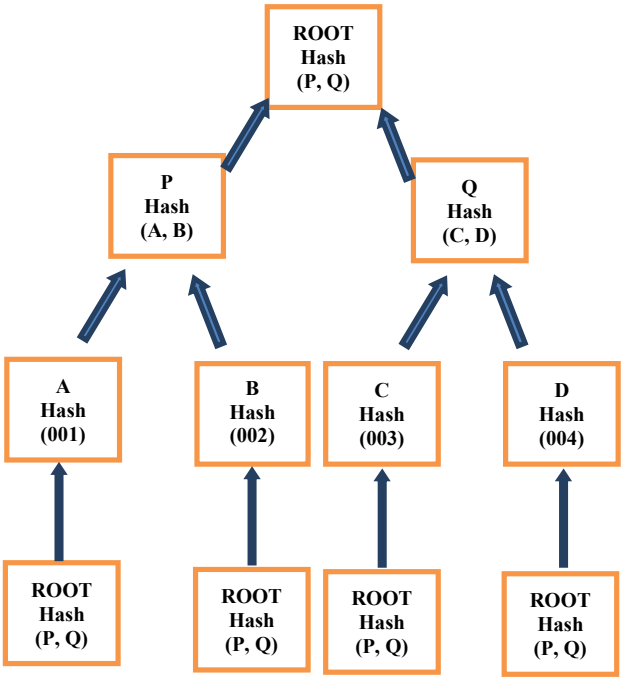

Fig. 2. Merkley Tree

2.4 Proof of Work

Proof of Work (PoW) was introduced by Cynthia Dworkand Moni Naor in the year of 1993 [37]. The main objective of this PoW is to ensure that the resources are utilized by the authenticated persons, to avoid the strangers and protecting the data from Denial of Service (DoS) attack. Also, the computational technique can be used to avoid junk messages. The person involving in PoW has to calculate certain computation within a specific period of time. The verifier will verify this computed result relatively in a simple manner. It is used by the miners to mine the blocks and to get their reward coings. The PoW contains the hash value of the block and the miners have to change nonce of the block header to reveal the original hash value. Once the hash value found the miner has to submit that to other verifier in the blockchain network for further verification and validation of the transactions in the block which is created recently. The important drawback of PoW is the need of more exclusive equipments with high computation power and requires extraordinary electricity power consumption [38]. In general, for a bigger blockchain network, we need more complex PoW to reduce the attack and as well to increase the performance [39].

PoW can be used for evaluating the quality and quantity of web services and web contents. The real and authenticated user can be distinguished from the intruder by applying PoW verification technique. Furthermore, to evaluate the quantity of the information provides by the web pages can be verified using the spatial information theory based metrics. PoW provides the solutions like QoS assurance, observing of user activity, balancing of Web services etc. [40]

2.5 Peer-to-Peer network

Nowadays many organizations extremely prefer Peer-to-peer network for implementing their blockchain network transaction. P2P network supports an effective networking system where the organizations can execute better communication processes, cybersecurity and overall efficiency. It is a distributed and decentralized network infrastructure. Here the workload is shared among the decentralized nodes exist in the network. On top of the physical network the P2P network will be laid virtually and the peers will be connected through logical links. Each node or peer will act as both server and client by invoking special kind of software programs. Also each node has equal status and responsibilities in the network. Initially P2P was introduced in the year of 1999 for the purpose of sharing the files among nodes [41]. In a blockchain network, each full node can store complete distributed ledger and can act as an entry point for multiple user. Each and every peer has the capability of validating the transactions and getting potential incentives. After the validation peer can broadcast the verified blocks to other nodes exist in the blockchain network [42]. Each and every node has equal rights to execute the consensus algorithm which can provide the fault tolerant capacity to the network [43]. Heterogeneous nature the P2P network is the significant constraint of the blockchain size.

P2P technology is playing an essential role in constructing the smart cities by providing good scalability and very low processing cost in content delivery as well as in distributed network environment. It supports acceleration and effective implementation of smart cities. Privacy and security issues are addressed by the P2P network in emerging smart cities. The P2P network also supports wireless healthcare system, effective trust model, location privacy and user authentication in smart cities [44].

2.6 Proof of Stake

The focus of the Ethereum 2.0 engineering is the Proof of Stake (PoS) contract system, which will replace the current Proof of Work (PoW) consensus mechanism. This cryptocurrency based algorithm is used in blockchain network. PoS include number of features like energy efficiency, low constraints, more incentives in crypto economics, generating more revenue for large number of users. Using pseudo random selection process PoS will select a node which will act as a validator for the next block in the blockchain network. Bitcoin is the first online crypto transaction to make use of this PoS consensus algorithm [25]. Minting is the process of generating new blocks and gratifying transaction fees to the miners. All the tokens or coins used for PoS evaluation process will be represented in the genesis block of the blockchain network.

The main objectives of PoS consensus mechanism are to diminish the computational necessities of PoW. In general, the contestants with more volume of coins have greater probabilities to be selected as an evaluator. Moreover, the nodes no need to bather about the complex PoW puzzle. In PoS network the block leaders are designated based on the stakes they hold not on the basis of computational power. Only one block is created in each round of PoS mechanism. So, the block generation and confirmation of a transaction is much faster which makes PoS mechanism to become more popular in recent days [45].

2.7 Ethereum & Smart Contracts

Ethereum is an open source platform [46] which can be utilized to implement decentralized computing environment by executing smart contract. It is used to execute the public blockchain mode of facilities to capture the Business-to-Consumer (B2C) marketplace. Decentralized Applications (DApps) can be enabled with the help of Ethereum. DApps are the applications employed on P2P network and there is no concept of single authority control. Turing complete Ethereum Virtual Machine (EVM) permits the implementation of scripts on Ethereum network. EVM can be used to create blockchain applications having high scalability and interoperability. Ethereum transactions are accomplished based on state transition mechanism [47]. The native cryptocurrency of Ethereum is named as Ether is used for executing the operations on the Ethereum network. An internal pricing currency called Gas is used to allocate the resources for the transaction processes in the Ethereum network. Before initiating and executing the transaction the units in Gas will be measured in the network [48]. EThash is used for mining the participants and their transactions in Ethereum network through PoW algorithm. Still, the cryptographic hashing algorithm employed in Ethereum is Keccak-256, which is a modified version of standardized SHA3 [49].
Smart contract runs on blockchain network which contains set of rules and regulations to impose digital contract system or self-executing electronic transactions. When two predefined parties are accepting the rules and agreed disparately to execute the transaction by triggering some events. The smart contract can be implemented in a decentralized and distributed environment between two parties and there is no need of third party intervention [50]. The transactions and agreements generated in this way are transparent, consistent, unalterable and traceable. No one can alter the transaction committed through the smart contract system. One of the important limitations is mapping the existing immutable codes with real world prescribed objects. If there is a dispute after generating the contract, nothing can be done with smart contracts. However, with the rise of Ethereum network and solidity language, smart contracts reached the heights to code the contracts since 2015 [41].

Smart contracts are tools which can execute transactions automatically without any intermediary entity or organization. Frequently they are associated with Ethereum and blockchain network to succeed the transaction without any issue. Smart contracts are regulating the information or data exchanged between two parties without needing a centralized entity. Smart contracts are involved in multiple tasks such as managing the network, framing the rules and protecting the transaction from violations. These core concepts are supporting the smart cities while designing Smart Banking, Smart Healthcare etc.

2.8 Hyperledger

Hyperledger concept was introduced in the year 2015. An open source community utilized for the purpose of developing a stable framework, tools and libraries for enterprise blockchain implementation. Hosted by Linux foundation and deployed in various sectors like finance, banking internet, supply chain, manufacturing, IoT etc [59][60]. Hyperledger is working based on modular approach which can provide essential support for the business blockchain networks. It helps to achieve the industry goals through smart contracts and decentralized distributed ledgers. Industries which are more interested in blockchain technology realized the fact that they can succeed more by working together with the support of Hyperledger. Main objective is to create repository of resources and to develop a network using blockchain technology to share the resources in an efficient manner. Hyperledger concept makes the blockchain as more popular and industry standard technology. It proves that the cross industry standards and blockchain technology

can improve the worldwide business and related transactions.

2.9 Decentralization

A digital decentralized democratic organization called Decentralized Autonomous Organization (DAO) is administered by the rules and regulations written in a smart contract and activated by distributed network without any central authority [51]. The main objective of the DAO is to attain the goals of the global business by incorporating the predefined business logic. Immutable blockchain ensures the self-governance by incorporating management and decision-making power of the DAO.

Decentralization concept allows the city administration to be distributed among all parties involved in the blockchain network. It is the key factor resolving many sociodemographic related issues. Since the people are relocating to the cities and concentrating more on global economy which can be achieved by decentralized and distributed computing environment. Decentralization is an expected and most preferable concept which will provide solution in various domains like, healthcare, infrastructures, education, safety, etc. Blockchain is a layer that can wrap all these several domains together.

2.10 Consensus Algorithm

In a blockchain network, consensus algorithm plays a vital role in attaining scalability, performance and throughput. It's a procedure of reaching an agreement. Before committing a transaction, parties should understand and accept the agreement [52]. In a centralized organization a leader will make decisions. Whereas in blockchain network, decision is dynamic and the network is decentralized. We can find many consensus algorithms in a blockchain ecosystem like PoW, PoS, Delegated PoS etc. It can be used to bring the entire network to work under single source of certainty. This can be achieved by the decentralized and distributed network environment of blockchain. The originator and monitor of the transaction will be selected based on the wealth of the node. This arbitrary randomized selection evades the centralization of the network to the wealthiest node. One of the consensus algorithms, DPoS leads to the energy consumption, cost reduction and damage avoidance. Many organizations have reasons and plans to move from PoW to PoS [53].

Consensus algorithm works based on the identities and trust on the validators. Here the block validators are recognized with their own reputation instead of staking coins' capability. Each and every block and transactions inside the block are validated by the authorized nodes. Consensus algorithms are suitable for both public and private networks where trust is distributed. These algorithms are having high risk tolerance as well high transaction rate[57][58]. Consensus algorithms have more sustainability than the Proof of Work which require high computational power. Smart cities can be supported in variety of circumstances and best option for logistical applications such as supply chains. Smart cities can maintain their privacy and security using this consensus algorithm through blockchain technology.

3. Conclusion

Blockchain technology employs on decentralized and distributed network. Predominant features of blockchain technology are transparency, reliability, trustworthy, security and immutability. These driving forces make blockchain technology to be integrated with IoT and supports smart cities. Most of the issues confronted by the IoT are eliminated by the decentralization nature of blockchain technology. Main objective of IoT in smart cities is to eradicate the general urbanization issues like environmental pollution, insufficient healthcare amenities, traffic congestion etc. So, the combination of blockchain technology and IoT benefits to leverage the advantages of smart cities in energy, tourism, waste management, education, healthcare, finance, and transportation. In this review paper we discussed the governing features of blockchain technology in various domains of smart cities. This will support and encourage the researchers to explore more on the impact of blockchain technology and IoT in constructing the smart cities.

References

[1] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, C. S. Hong, Edge-computing-enabled smart cities: A comprehensive survey, IEEE Internet of Things Journal 7 (10) (2020) 10200–10232.

[2] L. U. Khan, I. Yaqoob, M. Imran, Z. Han, C. S. Hong, 6G wireless systems: A vision, architectural elements, and future directions, IEEE Access 8 (2020) 147029–147044.

[3] K. Biswas, V. Muthukkumarasamy, Securing smart cities using blockchain technology, in: IEEE 18th International Conference on High Performance Computing and Communications, Syd- ney, Australia, 2016, pp. 1392–1393.

[4] Q. Feng, D. He, S. Zeadally, M. K. Khan, N. Kumar, A survey on privacy protection in blockchain system, Journal of Network and Computer Applications 126 (2019) 45 – 58.

[5]Bitcoin Market Capitalization, (accessed on 20 March 2020). URL https://coinmarketcap.com/currencies/bitcoin/

[6] D. C. Nguyen, P. N. Pathirana, M. Ding, A. Seneviratne, Blockchain for 5G and beyond networks: A state of the art

survey, Journal of Network and Computer Applications 166 (2020) 102693.

[7] T. McGhin, K.-K. R. Choo, C. Z. Liu, D. He, Blockchain in healthcare applications: Research challenges and opportunities, Journal of Network and Computer Applications 135 (2019) 62 – 75.

[8] I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, Blockchain for healthcare data management: Opportunities, challenges, and future recommendations, Neural Computing and Applications (2021) 1–16.

[9] M. Razaghi, M. Finger, Smart governance for smart cities, Proceedings of the IEEE 106 (4) (2018) 680–689.

[10] Umer Majeed, Latif U. Khan, Ibrar Yaqoob, S. M. Ahsan Kazmi, Khaled Salah, Choong Seon Hong, Blockchain for IoT-based Smart Cities: Recent Advances, Requirements, and Future Challenges, Journal of Network and Computer Applications · February 2021,1-33.

[11] J. Yang, Y. Han, Y. Wang, B. Jiang, Z. Lv, H. Song, Optimization of real-time traffic network assignment based on IoT data using DBN and clustering model in smart city, Future Generation Computer Systems 108 (2020) 976 – 986.

[12] S. Musa, Smart cities-a road map for development, IEEE Po- tentials 37 (2) (2018) 19–23.

[13] E. Al Nuaimi, H. Al Neyadi, N. Mohamed, J. Al-Jaroodi, Ap- plications of big data to smart cities, Journal of Internet Ser- vices and Applications 6 (1) (2015) 25.

[14] Y. Yu, Y. Li, J. Tian, J. Liu, Blockchain-based solutions to security and privacy issues in the internet of things, IEEE Wire- less Communications 25 (6) (2018) 12–18.

[15] P. K. Sharma, J. H. Park, Blockchain based hybrid network architecture for the smart city, Future Generation Computer Systems 86 (2018) 650 – 655.

[16] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, C. Rong, A Com- prehensive Survey of Blockchain: From Theory to IoT Appli- cations and Beyond, IEEE Internet of Things Journal 6 (5) (2019) 8114–8154.

[17] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems 107 (2020) 841 – 853.

[18] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F. Wang, Blockchain-enabled smart contracts: Architecture, applications, and future trends, IEEE Transactions on Systems, Man, and Cybernetics: Systems 49 (11) (2019) 2266–2277.

[19] Z. Wang, H. Jin, W. Dai, K.-K. R. Choo, D. Zou, Ethereum smart contract security research: survey and future research opportunities, Frontiers of Computer Science 15 (2).

[20] M. Sookhak, H. Tang, Y. He, F. R. Yu, Security and privacy of smart cities: A survey, research issues and challenges, IEEE Communications Surveys Tutorials 21 (2) (2019) 1718–1743.

[21] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, Khalil, M. Guizani, A. Al-Fuqaha, Smart cities: A survey on data management, security, and enabling technologies, IEEE Communications Surveys and Tutorials 19 (4) (2017) 2456– 2501.

[22] L. Cui, G. Xie, Y. Qu, L. Gao, Y. Yang, Security and Privacy in Smart Cities: Challenges and Opportunities, IEEE Access 6 (2018) 46134–46145.

[23] M. A. Khan, K. Salah, Iot security: Review, blockchain solu- tions, and open challenges, Future Generation Computer Sys- tems 82 (2018) 395 – 411.

[24] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Future Generation Computer Systems 88 (2018) 173 – 190.

[25] T. M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.

[26] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: Research issues and challenges, IEEE Internet of Things Journal 6 (2) (2019) 2188–2204.

[27] T. Alladi, V. Chamola, R. M. Parizi, K. R. Choo, Blockchain applications for industry 4.0 and industrial iot: A re- view, IEEE Access 7 (2019) 176935–176951. doi:10.1109/ ACCESS.2019.2956748.

[28] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, Y. Liu, A survey of blockchain technology applied to smart cities: Re- search issues and challenges, IEEE Communications Surveys Tutorials 21 (3) (2019) 2794–2830.

[29] Sai Sravani E., Sreehitha A.V., Konda Babu A., Nandan D. (2020) Evaluation and Study of IoT Entrances. In: Sharma D., Balas V., Son L., Sharma R., Cengiz K. (eds) Micro-Electronics and Telecommunication Engineering. Lecture Notes in Networks and Systems, vol 106. Springer, Singapore. https://doi.org/10.1007/978-981-15-2329-8_44

[30]. W. Diffie, M. Hellman, New directions in cryptography, IEEE transactions on Information Theory 22 (6) (1976) 644–654.

[31]. M. Conti, E. Sandeep Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Communications Surveys Tutorials 20 (4) (2018) 3416–3452.

[32]. G. Bansod, N. Raval, N. Pisharoty, Implementation of a new lightweight encryption design for embedded security, IEEE Transactions on information forensics and security 10 (1) (2015) 142–151.

[33]. P. Xu, Q. Wu, W. Wang, W. Susilo, J. Domingo-Ferrer, H. Jin, Generating searchable public-key cipher texts with hidden structures for fast keyword search, arXiv preprint arXiv:1512.06581.

[34]. Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed p2p applications", IEEE Access, vol. 6, pp. 27 324–27 335, 2018.

[35]. R. C. Merkle, Protocols for public key cryptosystems, in: 1980 IEEE Symposium on Security and Privacy, Oakland, Califor- nia, USA, 1980, pp. 122–122.

[36] Wikipedia, http://en.wikipedia.org/wiki/Merkle_tree

[37] C. Dwork, M. Naor, Pricing via processing or combatting junk mail, in: Proceedings of the 12th Annual International Cryp- tology Conference on Advances in Cryptology, Springer, Santa Barbara, California, 1992, pp. 139–147.

[38] K. J. O'Dwyer, D. Malone, Bitcoin mining and its energy foot- print, in: 25th IET Irish Signals Systems Conference (ISSC) and China-Ireland International Conference on Information and Communications Technologies (CIICT), Limerick, Ireland, 2014, pp. 280–285.

[39] F. Lin, M. Qiang, The Challenges of Existence, Status and Value for Improving Blockchain, IEEE Access 7 (2019) 7747– 7758.

[40] Alexey Noskov, Smart city webgis applications: proof of work concept for high- level quality-of-service assurance, September 2018, pp 99-106.

[41] Y. Shu, L. Zhang, W. Zhao, H. Chen, J. Luo, P2p-based data system for the east experiment, IEEE transactions on nuclear science 53 (3) (2006) 694–699.

[42] K. Christidis, M. Devetsikiotis, Blockchains and smart con- for the internet of things, IEEE Access 4 (2016) 2292– 2303.

[43] H. Tang, Y. Jiao, B. Huang, C. Lin, S. Goyal, B. Wang, Learn- ing to Classify Blockchain Peers According to Their Behavior Sequences, IEEE Access 6 (2018) 71208–71215.

[44] Li, H., Zhu, H. & Choi, B.J.(. Guest editorial: Security and privacy of P2P networks in emerging smart city. Peer-to-Peer Netw. Appl. 8, 1023–1024 (2015). https://doi.org/10.1007/s12083-015-0393-4

[45] Nguyen, Cong & Dinh Thai, Hoang & Nguyen, Diep & Niyato, Dusit & Nguyen, Huynh & Dutkiewicz, Eryk. (2019). Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. IEEE Access. PP. 1-1.

[46] V. Buterin, et al., A next-generation smart contract and decen- tralized application platform, Ethereum White paper (2014). URL https://github.com/ethereum/wiki/wiki/White-Paper

[47] G. Wood, Ethereum: A secure decentralised generalised trans- action ledger, Ethereum project yellow paper 151 (2014) 1–32.

[48] H. R. Hasan, K. Salah, Blockchain-based proof of delivery of physical assets with single and multiple transporters, IEEE Access 6 (2018) 46781–46793.

[49] D. Guth, B. Moore, D. Park, Y. Zhang, A. Stefanescu, et al., Kevm: A complete formal semantics of the ethereum virtual machine, in: IEEE 31st Computer Security Foundations Sym- posium (CSF), Oxford, United Kingdom, 2018, pp. 204–217.

[50] D. Magazzeni, P. McBurney, W. Nash, Validation and verifica- tion of smart contracts: A research agenda, Computer 50 (9) (2017) 50–57.

[51] V. Buterin, DAOs, DACs, DAS and more: An incomplete terminology guide, Ethereum Blog (2014).

[52] Saqib Hakak, Wazir Zada Khan, Gulshan Amin Gilkar, Muhammad Imran, and Nadra Guizani : Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges, January/February 2020, pp 8-14.

[53] V. Buterin, V. Griffith, Casper the friendly finality gadget, arXiv preprint arXiv:1710.09437.

[54] Eunil Park, Angel P. del Pobil and Sang Jib Kwon 4, The Role of Internet of Things (IoT) in Smart Cities: Technology Roadmap-oriented Approaches, May 2018.

[55]. Sterbenz, J.P. Smart city and IoT resilience, survivability, and disruption tolerance: Challenges, modelling, and a survey of research opportunities. In Proceedings of the 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM), Alghero, Italy, 4 September 2017; pp. 1–6.

[56] Eman Shaikh, NazeeruddinMohammad, Applications of Blockchain Technology for Smart Cities, Aug2020, pp-186-191.

[57] Inbarani H.H., Azar A.T., Jothi G. Supervised hybrid feature selection based on PSO and rough sets for medical diagnosis, Computer Methods and Programs in Biomedicine,Vol.113.

[58] Jothi G, Inbarani H. H, Hybrid Tolerance Rough Set–Firefly based supervised feature selection for MRI brain tumor image classification, Applied Soft Computing,Volume 46, , Pages 639-651.

[59] Shanmugaraja, P & Chandrasekar, S, Accessible Methods to Mitigate Security Attacks on IPv4 to IPv6 Transitions', European Journal of Scientific Research, vol. 77, no. 2 , pp. 165-173, ISSN : 0975-4024 ,2012.

[60]. P. Shanmugaraja, K. Chokkanathan, J. Anitha, A. Parveen Begam, N.Naveenkumar, "Dynamic Packet Scheduler for Queuing Real Time and Non Real Time Internet Traffic", International Journal of Recent Technology and Engineering (IJRTE), Volume-8 Issue-3, September 2019, ISSN: 2277-3878