

Block chain Technology for Smart City and its Security Threats

M. J. Abinash, V. Vasudevan

Abstract: The current modern year shows quick growth in metropolitanization and population growth of the world that causes various impacts on environmental, social and economic problems. The problems aroused in society influence the livelihood of the people and excellence of existence. "Smart City" passes many opportunities to resolve these urban inconveniences and unsolved issues. The chief fact of a smart city is to create the finest use of resources gathered from the public, make available with reliable services to the citizens with enriched quality and efficiently enhance the day to day life standard of peoples. In the smart city establishment Information and Communication Technology (ICT) shows greater impact. Block chain is a intensifying technology with many excellent aspects likely intelligibility, automation and security. A characteristic of block chain is supportive in improving the standard services and advances the expansion which applies information technology that integrates several areas of interest. Block chain manages the business, physical and social infrastructures to provide effective services to needed users. With the advancement of technologies namely interconnected networks, cloud computing and the Internet of Things (IoT), for smart cities can carry creative as well as novel solutions. Smart cities can offer people with interface and association between the general public as well as the local government. Despite several possible remunerations, digital interruption postures many objections related to privacy and along with information security. Here in this paper, we discussed in detail about blockchain technology and the security framework that assimilates the smart devices and blockchain technology together.

Keywords : Smart City, Block chain, Security, Privacy, Internet of Things, Secure Communication.

I. INTRODUCTION

The populace rate of world in the metropolitan cities are growing much faster and in an unstable manner [1]. Migration of peoples from the countryside to metropolitan areas growing rapidly in recent year. This will result in increased population growth and the statistical report was taken by United Nation. Population growth in the United State will increase by 70% in 2050 in metro cities [2]. Urbanization has drastically improved humans based on living standard in many aspects, namely education, health, working environments, transportation, living and economy [3].

Revised Manuscript Received on July 22, 2019.

* Correspondence Author

Abinash*, Department of Information Technology, Kalasalingam Academy of Research and Education, Srivilliputhur, India.

Vasudevan, Department of Information Technology, Kalasalingam Academy of Research and Education, Srivilliputhur, India.

A metro city people growth shows drastic increase and passes several confronts or struggles. Due to the huge concentration in the count of people's in metros, human's existence excellence has been influenced by several phenomenon's namely limited reserve of ecology, contaminated air, traffic congestion, corrosive gas secretion and discarding devastates [4]. Entire issues, confronts or difficulties aroused in and private body have to expose their concentration in the direction of elegant advancements which make each and every work of the humans to be easier as well as smarter. This makes the upholding progression of metropolis and the improvement of human excellence. To attain this progression of growth in the lifestyle standard, a new scheme is initiated which comes as an explanation of "Smart City" [4, 5, 6, and 7]. The key fact of this invasion is progress the human's eminence of existence by incorporating the circumstance with sophisticated contemporary ICT together.

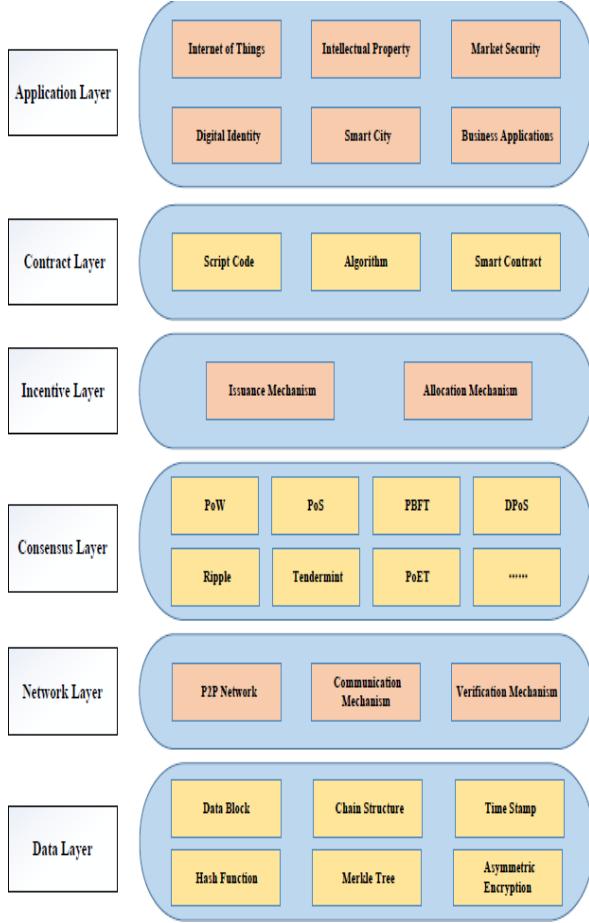
A smart city has numerous high-quality standards and characteristics, such as a contribution of the citizen in every aspect is encouraged, openness has improved in public government activities, finest utilization resource, better environmental protection, improved health, public transport, energy, effective management of traffic, education services, and intelligent device control. ICT plays a major and prominent role in smart cities implementation as well as in utilization [8, 9 and 10]. ICT be evidence for the expansion and endorsement of reliable development. Bit coins and crypto currencies are the foremost reasons for the progression of blockchain and is initiated with Bit coin [11].

The blockchain is mostly an unchangeable, decentralized and unrestricted collective database which is a shared type of data. Entire transmissions in this stored and permitted to admittance of any type of activity to anyone. With the stored information in the any authenticate user can send, receive and verify these transmissions. Blockchain technology is mainly applied to smart cities that can arise several good descriptions. It doesn't need any proprietor to take in charge of the access control and can be man oeuvre easily.

Transparency of the transaction of data to all persons who are all involved in the broadcast of data is enhanced by this technology and assessments are accomplished by whole node in a system to system communication mode. Transportation of information among the nodes makes the nodes as independent. Encroachment made the expertise to make decision, data's can be stored

Block chain Technology for Smart City and its Security Threats

without any human intervention and transaction or business deal execution as well. Blockchain technology is a decentralized system that makes it essential to guarantee constancy as well as reliability by operating effective algorithms in the midst of decentralized nodes. The protection system is associated with confidentiality, uprightness and permission of admittance. Blockchain technology is integrated in smart cities to fill the gap and is



reviewed. Research on implementing this technology shows that improved smartness, performance, security, and efficiency of smart cities is presented.

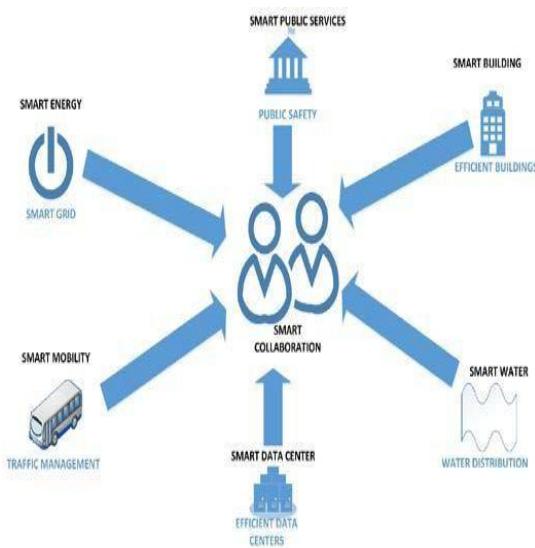


Fig. 1.A spectrum of blockchain architecture [8 & 9]

Fig. 2. In the circumstance of smart city with smart alliance

II. BLOCKCHAIN TECHNOLOGY

It is a decentralized registry and not placed in one location. In Blockchain technology, where the specific informations cannot be altered later whether the duplicate form of performers can hold at the load specific tasks. The enciphered form of information is enrolled in various way and it get computerized by victimization of numerical formulas. Every geometric formula validates and certifies one more geometric formula that incorporate some specific content of an alternative enciphered information successively. This database holds entire information of dealing involves, worth that are enciphered on the emerging blockchain, with the proper agreement and support of their validity at any time.

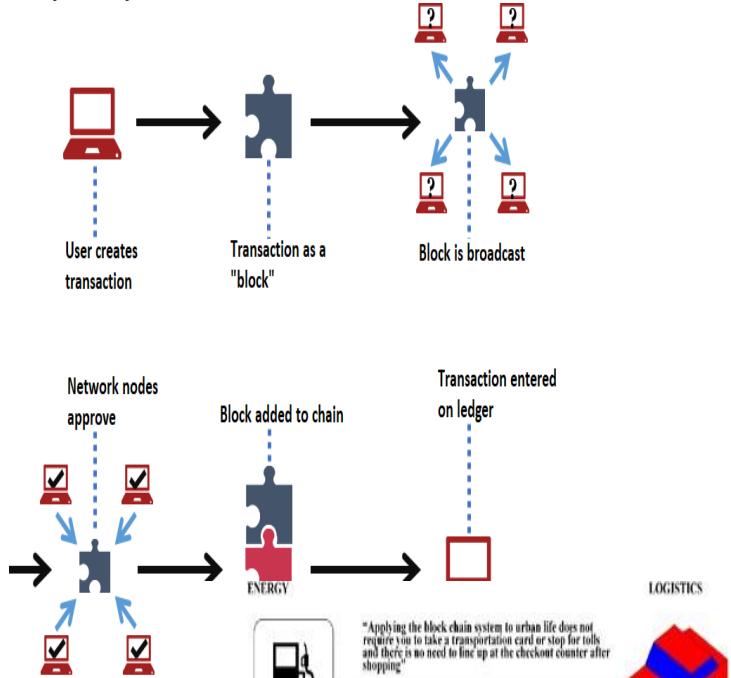
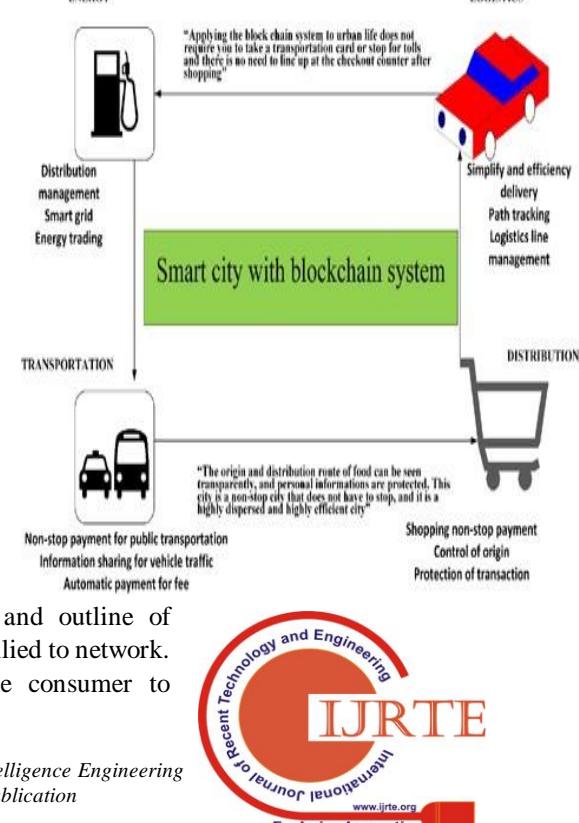


Fig. 3.Blockchain principle

Fig. 4.Blockchain in smart city

Figure.3 and Figure.4 elucidate the standards of blockchain and their exertion nature.

The blockchain is self-possessed and outline of computer that is allied to network. It uses an online consumer to



resolve retransmission tasks and transaction validation. This node obtains a duplicate of the block, which keeps informed repeatedly once logged on. In Bit coin, nodes contend to resolve procedure to form bit coins. It is not anticipated utterly for dealings and crypto currency. It also used to preserve beneficial data, rather in collect taxes, and it gives the unbroken solution for e-voting [12].

Table- I: Name of the Table that justify the values

Block Chain System	Data Structure	Permissioned	Consensus Smart	Contract Language
Bitcoin [11]	Block chain	No	PoW	C++,Golang
Litecoin [18]	Block chain	No	PoW	C++, Golang
ZCash [19]	Block chain	No	PoW	C++
Hyperledger [20]	Block chain	Yes	PBFT	Golang, Java
Sawtooth Lake [21]	Block chain	No	PoET	Python
Ethereum [22 & 23]	Block chain	No	PoW/PoS	Solidity, Serpent, LLL
Quorum [24]	Block chain	Yes	Quorum Chain	Golang
Monax [25]	Block chain	Yes	Tendermint	Solidity
Tezos [26]	Block chain	No	PoS	Michel son
Kadena [28 & 29]	Block chain	Yes	Scalable BFT	Pact
IOTA [30]	DAG	No	PoW	Java
Byteball [31]	DAG	Yes	Main Chain	Node.js

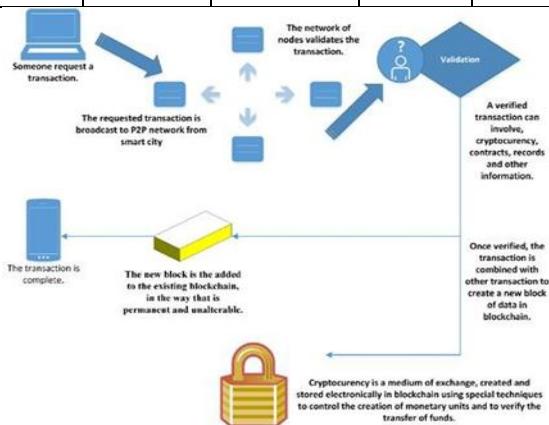


Fig. 5. Link between blockchain, user and smart city [12]

III. SECURITY THREATS

The varied personality of integrated reserve inhibited devices and a smart city is susceptible to several sanctuary hits. Recognizing the significant coercion and their

possible consequences will lead to designing an effectual elucidation. Several kinds of exploration have been performed numerous examination in this domain namely Computer Emergency Response Teams (CERT) which offers the graphical illustration of several possible imposes as well as attacks, Cloud Computer Service Provider (CCSP) needs G-Cloud that deals with the sequence of Open Web Application Security Project (OWASP) procures widespread security offences [13], [14], [15] [16]. Threats are classified and recognized for the smart cities are all explained below:

A threat to accessibility- It is concerned with the (unauthorized or third part) continuation of resources.

Threats on Integrity- It includes illegal alteration of data such as an altered form of information and manipulation.

Threats on Confidentiality- It includes unveil of perceptive information by an illicit entity to other irrelevant persons.

Threats on legitimacy- These are fretful with the acquisition of illicit access, usage to reserve and perceptive information.

Threats on responsibility- It comprises defiance of reception or transmission of a communication by the related person to other.

IV. SECURITY FRAMEWORK

A. Physical Layer

Devices using for smart city are enrooted with smart objects such as actuators, sensors. These objects are responsible for collecting and forwarding the data to the higher layer protocols. Some of the smart object based devices namely thermostat and Fit bit are susceptible to several vulnerabilities and breaches due to lack of admittance mechanisms and many encryption techniques [17]. Further, technology has no available distinct benchmark the data produced for smart devices get scattered and later it incorporated to deal with the cross functional things. Hawker needs to overcome these problems by agreed-upon functioning and data communication standards.

B. Communication Layer

Meanwhile the diverse communication of the smart city uses Wi-Fi, Bluetooth, Ethernet, 6LoWPAN, 3rd Generation, and 4th Generation in this layer to swap info amongst completely on the various schemes. There are certain rituals are required in this layer for supply protection and isolation mechanisms of spreading of information. The dealing of records in the network may be reworked, by using broadcast technology the networks are transmitted in the form of blocks using telehash. Bit Torrent is one form of rituals it can be practiced into peer-to-peer (P2P) communication standards while Ethereum will offer good contract functionalities for the data transmission among the

network. However, amalgamation of available communication protocols is one among the key challenges since the necessities vary from application to application and it depends on the character of the transmission.

A possible resolution found by implementing many block chains by the contribution of access layer have the specific usage in accomplish to the data transmission network.

C. Database Layer

The scattered records of the block chain will be kindly circulated one after another. Every record within the ledger comprises of a novel crypto graphical signature and a time stamp. The history of the record is easily auditable and verified by the authenticated user. There are two differing types of scattered records in habit. They are

- Permission less
- Permission available.

The main advantage of the clearance less record is that clear and censorship-resistant. In spite of, public record needs to manage advanced as well as complex shared records. Public ledger consumes supplementary time to achieve the accord compared to the non-public ledger. Additional, public ledgers may expose to unidentified attacks. Therefore, it is well to utilize non-public ledgers. It ensures improved recital, measurability, and it provide security for applications in real-time like traffic systems.

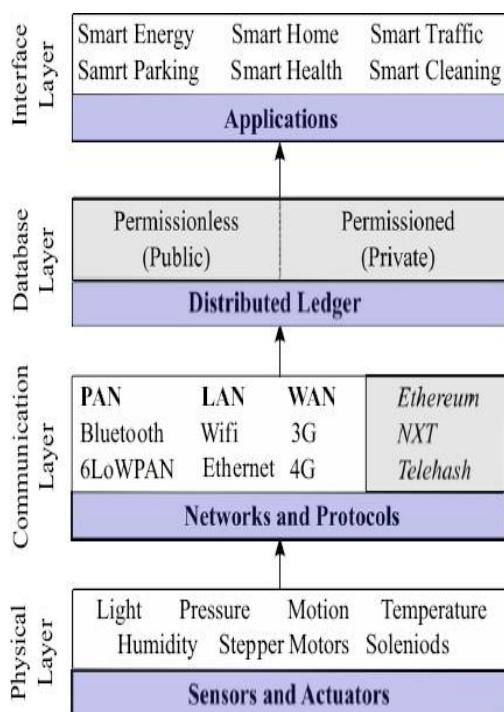


Fig. 6. Outline of security frame

D. Interface Layer

Numerous smart objects, applications, and devices coagulate with each other to forms a device which in turn manipulates effective and timely decisions. The interface layer acts as a medium between the device and the user. Intermediary layer helps to activate or deactivate any smart device in their home connected with the mobile application

can be accomplished in no time. Design consideration has also included the security features to make it safe from the intruder or third- party access.

V. CONCLUSION

This paper discussed a blockchain based security framework to facilitate data communication and transmission of data in a smart city securely. For implementing the block chain in smart cities is the elastic nature is supposing to the major advantage against various threats and privacy issues. Further, it gives numerous unique characteristics such as better improved reliability, scalability, quicker operation, efficient operation, and capability of forbearance to faults. Thus, the incorporation of block chain technology along with smart objects inside smart city will generate a familiar stage where the whole devices will be equal to transmit the data firmly in a distributed environment.

ACKNOWLEDGMENT

The authors would like to thank the management of Kalasalingam Academy of Research and Education, Tamilnadu, India for permitting to use the computational facilities available in the open source research laboratory.

REFERENCES

1. United Nations, "Population Division," Dec. 2017. [Online]. Available: <http://www.un.org/en/development/desa/population/>
2. National Bureau of Statistics of China, "China's population and its composition," Dec. 2017. [Online]. Available: <http://www.stats.gov.cn/english/>
3. K. Davis, "The urbanization of the human population," *The City Reader*, 2011, pp. 2–11.
4. R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in Proc. *IEEE ISC2'17*, Wuxi, China, Sept. 2017, pp. 1–4.
5. T. Nam and T. A. Pardo, "Conceptualizing smart city with dimensions of technology, people, and institutions," in Proc. *ACM dg.o'11*, CollegePark, Maryland, USA, 2011, pp. 282–291.
6. E. Tabane, S. M. Ngwira, and T. Zuva, "Survey of smart city initiatives towards urbanization," in Proc. *IEEE ICACCE'16*, Durban, SouthAfrica, Nov. 2016, pp. 437–440.
7. J. Sun, J. Yan, and K. Z. K. Zhang, "Blockchain- based sharing services: What blockchain technology can contribute to smart cities," *Financial Innovation*, vol. 2, 2016, p. 26.
8. G. Cui, K. Shi, Y. Qin, L. Liu, B. Qi, and B. Li, "Application of blockchain in multi-level demand response reliable mechanism," in Proc. *IEEE ICM'17*, Chengdu, China, April. 2017, pp. 337–341.
9. R. Xu, L. Zhang, H. Zhao, and Y. Peng, "Design of network media's digital rights management scheme based on blockchain technology," in Proc. *IEEE ISADS'17*, Bangkok, Thailand, March. 2017, pp. 128–133.
10. Y. Yuan and F. Y. Wang, "Towards blockchain- based intelligent transportation systems," in Proc. *IEEE ITSC'16*, Rio de Janeiro, Brazil, Nov. 2016, pp. 2663–2668.
11. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: <http://www.ildgroup.si/uploads/product/20/bitcoin.pdf>
12. MihaiRebrisoreanu, CosminRus, Monica Leba and AndreeaIonica "Exploring the Possibilities of Blockchain Use in a Smart City", *International Journal of Systems Applications, Engineering & Development*, vol. 12, 2018.
13. OWASP Foundation, *OWASP Top 10-2013: The the Most Critical Web Application Security Risks*, 2013.
14. W. R. Claycomb and A. Nicoll, Insider Threats to CloudComputing: Directions for New Research Challenges, in 36th Annual *Computer Soft. and Appl. Conf.*, 2012, pp. 387–394.
15. HMGovernment, *Government cloud strategy*, 2011, pp. 1– 24.

16. K. Christidis and M. Devetsikiotis, Blockchains and SmartContracts for the IoTs, *IEEE Access, Special section on theplethora of Research in IoT*, 2016, pp. 2292– 2303.
17. M. Selinger, *Test: Fitness wristbands reveal data, Test AVTESTGmbH*, Klewitzstr, Germany, 2015, pp. 1–7.
18. “*Litecoin: An open source P2P digital currency*,” June. 2018. [Online]. Available: <https://litecoin.org/>
19. E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, “*Zerocash: Decentralized anonymous payments from Bitcoin*,” in Proc. *IEEE SP'14*, San Jose, CA, USA, May. 2014, pp. 459–474.
20. E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Lavington, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, “*Hyperledger Fabric: A distributed operating system for permissioned blockchains*,” in Proc. *ACM EuroSys '18*, Porto, Portugal, 2018, pp. 30:1–30:15.
21. “*Sawtooth Lake*,” June. 2018. [Online]. Available: <https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html>
22. “*Ethereum*,” Dec. 2017. [Online]. Available: <https://www.ethereum.org/>
23. G. Wood, “*Ethereum: A secure decentralised generalised transaction ledger*,” Ethereum Project Yellow Paper, vol. 151, 2014, pp. 1–32.
24. J. Morgan, “*Quorum*,” June. 2018. [Online]. Available: <https://www.jpmorgan.com/global/Quorum>
25. “*Monax*,” June. 2018. [Online]. Available: <https://monax.io/> L. Goodman, “*Tezos: A self-amending crypto-ledger*
26. “*position paper*,” Aug. 2014. [Online]. Available: https://tezos.com/static/papers/position_paper.pdf
27. R. Brown, “*Introducing r3 cordatm: A distributed ledger designed for financial services*,” R3CEV Blog, 2016.
28. “*kadena*,” June. 2018. [Online]. Available: <http://kadena.io/> W. Martino, “*Kadena: The first scalable, high performance private blockchain*,” White Paper, 2016.
29. S. Popov, “*The tangle*,” Oct. 2017. [Online]. Available: <http://iotatoken.com/IOTA Whitepaper.pdf>
30. Churyumov, “*Byteball: A decentralized system for storage and transfer of value*,” 2016. [Online]. Available: <https://byteball.org/Byteball.pdf>

AUTHORS PROFILE



Abinash he is a full-time research scholar in the department of information technology of Kalasalingam Academy of Research and Education Krishnankoil Srivilliputhur India. His areas of interest are big data analytics, bio informatics and block chain technology. He has published 5 papers in international journals and conferences.



Vasudevan he is working as senior professor in the department of information technology of Kalasalingam Academy of Research and Education Krishnankoil Srivilliputhur India for past 27 years and his areas of interest are big data analytics, cloud computing, network security and block chain technology. He has published 170 above papers in international journals and conferences. He has produced twenty above PhD scholars and currently guiding five PhD scholars. He is a life time member in ISTE and IAENG. He received Dr. APJ Abdul Kalam Award for life time contribution in teaching on 2016.