Journal of Information Technology and Digital World (2019)
Vol.01/ No. 02
Pages: 58- 67
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2019.2.001

EFFICIENT SECURITY AND PRIVACY MECHANISM FOR BLOCK CHAIN APPLICATION

Prof. Dr. Subarna Shakya
Professor, Department of Electronics and Computer Engineering,
Central Campus, Institute of Engineering, Pulchowk,
Tribhuvan University,
Pulchowk, Lalitpur Nepal.
Email: drss@ioe.edu.np

Abstract: The block chain has become one of the predominant term in the applications like financial, automobile, health care, risk management, and internet of things due to its reliability and more beneficial services. It executes every transaction by establishing trust in the open environment. The deployment of the block chain technology in the various applications remains as the recent research topic as the privacy and the security of the bock chain are undecided and unconvinced, so the paper tries to develop an efficient security and privacy mechanism for the block chain applications. The proposed method puts forth the biometric recognition in the block chain technology to improve the security and the privacy mechanism for the block chain application.

Keywords: Block Chain, Challenges, Privacy, Security, cryptographic techniques

1. INTRODUCTION

Recently the block chain technology has been a revolution in securing the events or the transactions associated with the variety of applications excluding the necessity of the central authority in an open network system. In the perspective of data management the block chain is described as the database that is distributed evolving on the transactional records that are arranged in the hierarchically in form of blocks that are chained. The block chain is overlaid on the peer to peer network and the are secured through the intelligent and the decentralized cryptography along with the crowd computing.

The block chain can be expressed as simple secure ledger that layers hierarchically the progressing lists of transactions, as chain of blocks. Every block in the chain is guarded by the cryptography technique that enforces a strong integrity of transaction records; the new blocks are committed into the chain only on the completion of the decentralized consensus procedure. The procedures imposed for decentralized consensus by the network, that regulates the entry of the new blocks, verification of the chain and the consistency of the data content. The figure.1 below provides the regulation provided by the network in creating and adding a new block to the chain.

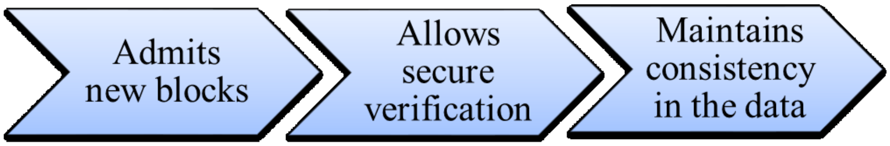
Admits new blocks
Allows secure verification
Maintains consistency in the data

Figure.1 Network Regulation in chaining Blocks

Simultaneously in addition to the transaction records, every block maintains a hash value of its own and the hash value of the predecessor, maintain a cryptographic linkage with the previous block that is in the block chain. The network regulation pictured in the figure.1 ensures the successful creation and the addition of the blocks into the chain respectively. This further retains the integrity of the blocks that the data content in the each block is guaranteed and the blocks once chained are not liable of being altered or damaged. This make the block chain a secured and a decentralized ledger archiving transactions between the two dealers involved in an open network system, persistently in a passible environment with verification. Adding to the above description the definition of the block chain is defined as the “magic computer which can be directed by a program that allows self-executing, where the current and the preceding states of every program are transparent with very strong crypto economically protected with the guarantee that the database in the chain will perform according to the directions specified by the block chain [7].

1.2. POTENTIALS OF THE BLOCK CHAIN

All the above mentioned reasons make the blockchain potentially able and a predominant technique in a wide range of applications that require a secured way of transaction. The block chain being a peer to peer network seated on the top of the internet is termed as the (i) founding technique causing revolution in the government and the business dealings. (ii) Develops new foundation for the economic and the social systems. (iii) Highly secured avoiding loop holes for the tampering or damages and replacing or removal. (iv) Enables transparency among the parties involved. (v) Retains and verifies the digital record of each and every transaction along with the validation and storage. (vi). Ensures communication ease between the organizations, so its key features are listed below in the figure.2

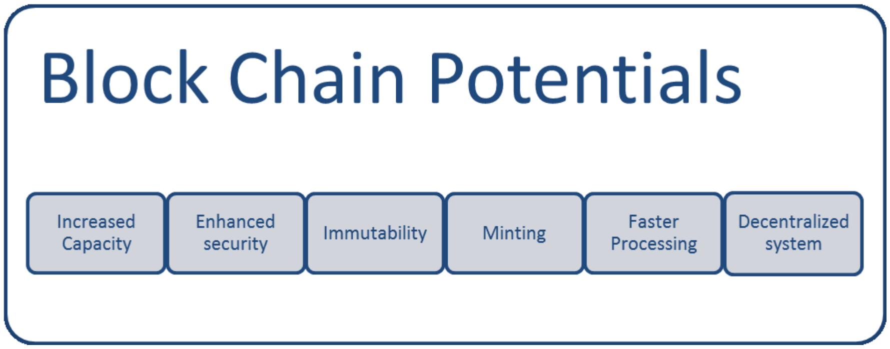

Figure.2 Block Chain Potentials

1.3. SECURITY AND PRIVACY ISSUES IN BLOCK CHAIN

Though the block chain is constructed to handle the inherent security breaches such as the tampering, alterations, inconsistency, distributed denial of service attacks, reduplication , and the attacks related to the double spending, but the block requires more additional attributes for securing the data and maintaining its privacy, when concerned with the distributed storage, data sharing, etc. So the security breaches rise due to the inability in providing the relation between the two entities that are observed from the system that requires confidentiality, the bit coin though ensures the anonymity it does not ensure the inability in describing the relations and this termed as the unlinking-ability, the unlinking-ability makes hard the transactions by creating difficulties in launching the measures against the anonymization attacks, and further causes the anyone to access the files freely , and access any one transaction and relate it with their transaction and making the user to lose his/her privacy on all the transactions. The chain would be open to attacks without the knowledge of the users and her true identity. So it becomes necessary to enhance the security of the block chain using some cryptographic techniques

So the paper concentrates in developing the more reliable block chain network that would enhance the privacy of the block chain addressing the security issues. The remaining paper is organized with the related works detailing the anonymization caused in the network, the benefits of the block chain in wide variety of applications in 2, the proposed efficient security and the privacy for block chain in 3 and the results observed in 4 and the conclusion in 5.

2. RELATED WORKS

The block chain integrates the distributed consensus and the peer to peer networking including the cryptographic algorithms, mathematics and the economic models to handle the synchronization issues existing in the traditional distributed data base. The related works presents the significant particulars of the block chain, and the advantages in it. The author Joshi, Archana et al [1] presents the survey of the blockchain security issues and privacy problems presenting the complete details related to the block chain the concepts driving it, consensus algorithms used etc. and the types of the block chain. The structure of the block chain observed from the paper is presented below in the figure.3

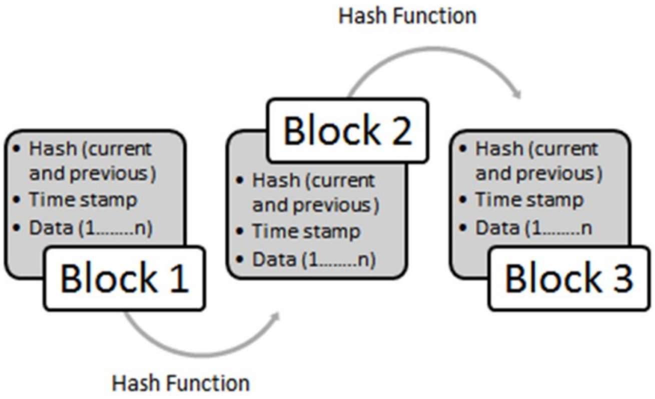

Figure.3 Blockchain Structure

Biswas, et al [2] proposes the involvement of the block chain technology in the securing the smart cities, from the digital disruption and provides a communication platform that is secure for the smart cities. Yli-Huumo, et al [3] presents the systematic review of the current research in block chain. Halpin, Harry et al [4] provides the introduction to the security and the privacy issues in the block chain by "including the peer reviewed papers to gather the unsolved issues that are associated with the security and the privacy of the block chain. The paper even highlights the research challenges in the block chain". Lin, et al [5] highlights the current regulation problems, and the integrated cost problems along with the fork problem faced in the block chain causing the security issues and challenges in it. Suma, et al [6] "Block chain being a foundational technology impacting and attracting a wide range of applications has become predominant in solving the problem of privacy preserving and security in multitude sectors that is under the control of the government and the private. The author proposes the block chain with the RSA digital signature to improve the security in the block chain". Bhalaji, N et al [7] has proposed the block chain to enhance the quality of service and the defense in the wireless networks framed on the fly. Jacob, I. J. et al [8] present the biometric recognition system in securing the information sharing. Sivaganesan, D. et al [9] presents the security of the internet of things manipulated employing the block chain. S. Smys. et al [10] describes and puts forth the "Prevention of inference attacks for private information in social networking sites." Karthiban, K., et al [11] proposes the privacy preserving approaches for the cloud computing. Dinesh Kumar, et al [12] proposes a novel attack detection method for the wireless body network. Though the above methods in the paper highlights the various applications that are afforded to secure the transactions using the block chain, there are still ignorant of the linking-inability problem that causes the security breaches in the block chain and the remedies for them. The proposed method in the paper includes the homomorphic encryption [13] along with the game based smart contracts [14] [15] to secure block chain from the privacy problems caused due to unlinking-ability.

3. PROPOSED EFFICIENT SECURITY ANND PRIVACY FOR BLOCKCHAIN

There are several methods that improve the security and the privacy of the block chain, such as the mixing that includes the mix coin, coin join, etc. taking measures to prevent the user addresses being linked, but they are centralized services that faces the user private information leakage. They next one is the anonymous signatures that hides the identity of the users but requires a trusted third part to manage the deeds happening, /hides the identity of the user even in the time of dispute and few other methods to enhance the security are the secure multi-party computation , non- interactive zero knowledge proof etc. The homomorphic and the smart contract base execution shows effective securing with few short comings that are subsided within the methods. The homomorphic encryption is unlike the other encryption models it is very safe nowadays as it is unbreakable even by the quantum computers. The figure.4 below is the represents the cycle in securing the data in the block chain.

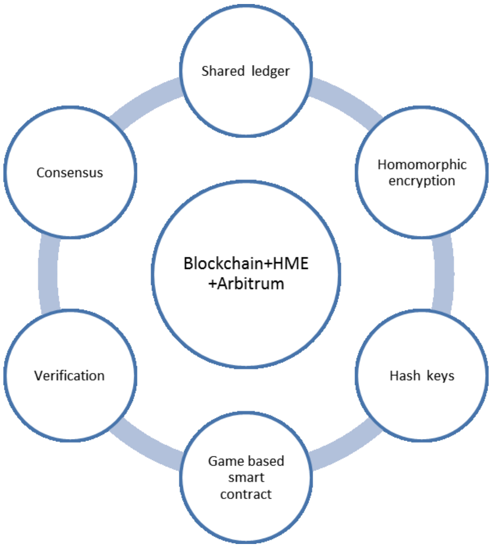

Figure.4 Security Enhanced Block chain

3.1. METHODOLOGY ADOPTED

The proposed methodology clubs the homomorphic encryption and the game based smart contracts to enhance the security and protect the privacy details in the blocks in the block chain.

(a).Homomorphic Encryption (HME): There are three types of homomorphic encryption; they are partial homomorphic, limited homomorphic and full homomorphic encryption performing encryption on the data that are more sensitive by allowing only selected mathematical function, done or performing encryption only for a certain number of times or completely securing keeping the information highly secure and accessible. Similar to other form of encryption the homomorphic also uses the public key for encryption and performs algebraic functions to make the information available only for the appropriate user having the matching private key allowing the data to be completely secure even when used by someone. The proposed method uses the homomorphic based encryption in the blockchain which allows affords to have compactness in the in generation, encrypting, evaluation and decryption. The definitions equation (1) below shows the compactness achieved in the evaluation ($eval_{fhm}$), decryption ($decryp_{fhm}$), encryption ($encryp_{fhm}$) and ($gene_{fhm}$) generation for the full homomorphic.

ISSN: 2582-418X (online)

$$\begin{aligned} gene_{fhm} &= D * Auxillary\ Space \\ encryp_{fhm} &= public\ key\ space * (plain + ciher\ text) \\ decryp_{fhm} &= secret\ key * auxillary\ space \\ eval_{fhm} &= decrypted\ key\ space * information\ space * arbitary\ length \end{aligned} \tag{1}$$

The correct information is decrypted without errors only when the prob $(decryp_{fhm})$ = 1and the prob $(eval_{fhm})$ = 1- $\varepsilon\ (\lambda)$, where the λ is the security parameter. Followed by the application of the HME, the smart game based trust is done.

(b).Game based smart contract: smart game based trust is included to perform smart contract verification; the proposed method employs Arbitrum a scalable, private, game based smart contract to verify whether the computation was performed perfectly, by verifying the HME process and the signatures of the contracts, to identify the dishonest, and assigns penalty to the dishonest parties. The protocol of the Arbitrum has four phases, the first one is the verifier the second is the key and the third is the virtual machine and the fourth is the manager. The figure .5 below provides the phases in the protocol of Arbitrum.

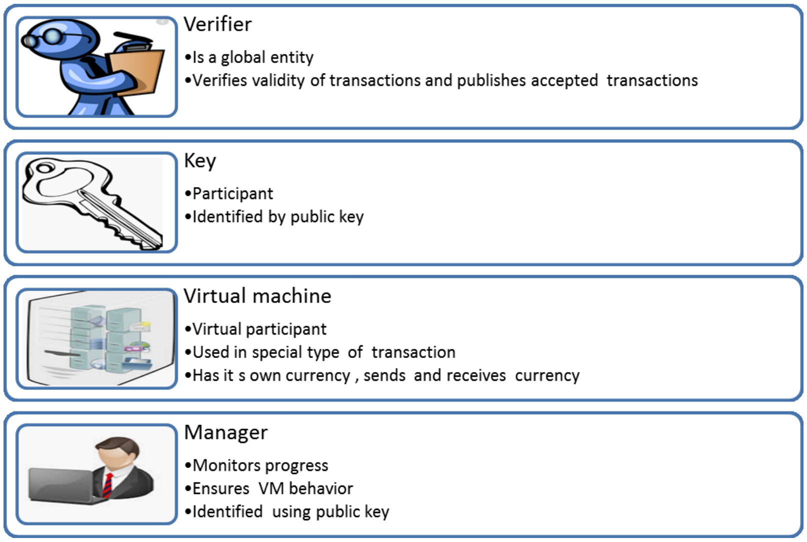
Verifier
•Is a global entity
•Verifies validity of transactions and publishes accepted transactions
Key
•Participant
•Identified by public key
Virtual machine
•Virtual participant
•Used in special type of transaction
•Has it s own currency , sends and receives currency
Manager
•Monitors progress
•Ensures VM behavior
•Identified using public key

Figure.5 Roles involved in Arbitrum

The proposed method clubbing the HME and the Arbitrum can be used in the application like business organization, medical care, banks, smart homes and other areas where block chain is used and a high privacy and security is necessitated.

4. RESULTS

The proposed method shows high scalability, security and privacy, as the lock chain is managed efficiently eluding the security breaches at a very negligible transaction fees and ensures that the disputes are avoided by executing the protocol according to their incentives. The proposed method also offers flexibility; the figure.6 below provides the enhanced security, privacy protection, scalability, flexibility percentage when used along the block chain engaged in the for a health care sector, that holds lots of private and personal information.

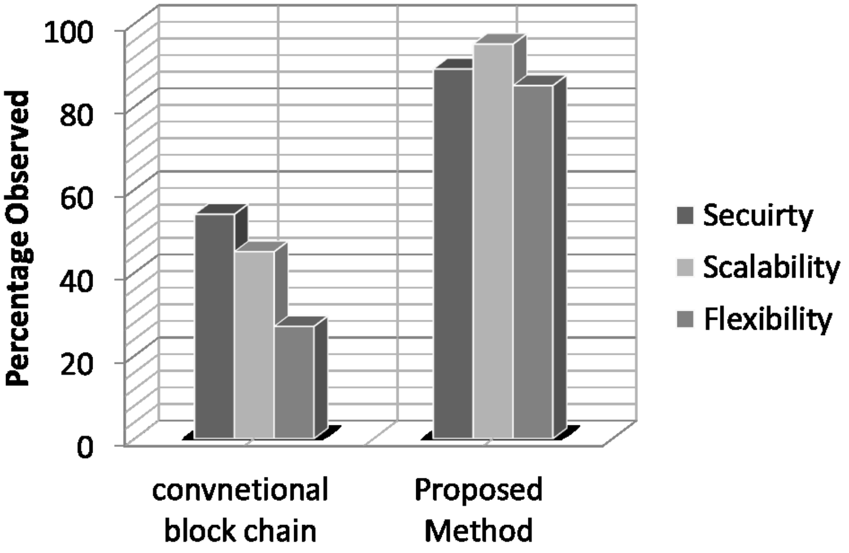

Figure.5 Performance observed

The figure.6 below provides the comparison of the conventional block chain and the block chain enabled with the security enhancements such as the homomorphic encryption and Arbitrum a game based smart contract to further verify the process to identify the fraudulent transactions.

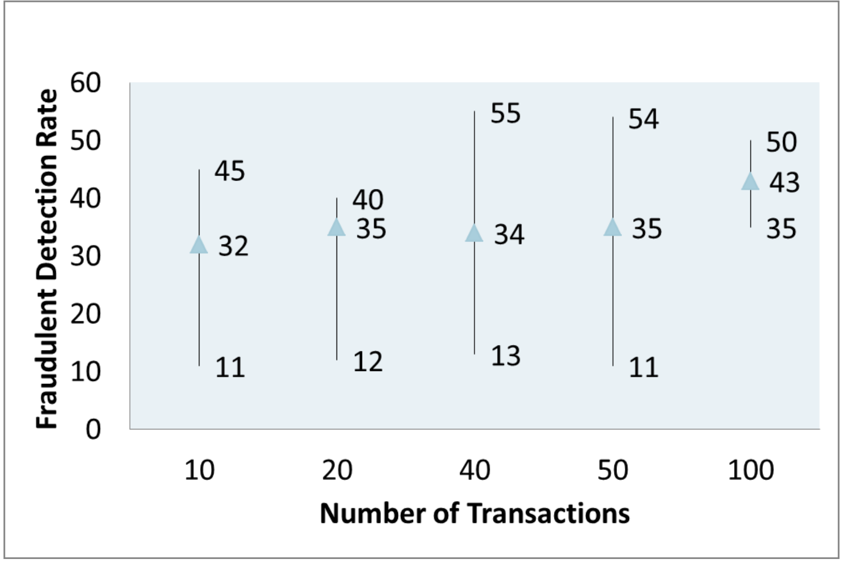

Figure.6 Fraudulent Detection Rate

The figure.7 below provides the level of the deceitful transaction / users detected applying the proposed Blockchain+HME +Arbitrum methods, where the detection rate of the conventional method is below 20% and the detection rate of the proposed method is above 40 percentage, results are observed on applying the proposed method to the healthcare center shows that the Blockchain+HME +Arbitrum methods has a better detection rate than the conventional block chain methods available.

5. CONCLUSION

The paper with the efficient methods to improve the security and the privacy in the block chain utilizes the full homomorphic encryption employing the algebraic calculations over the encrypted cipher, followed by the Arbitrum a game based smart contract to verify the transaction. The proposed method is applied to a hospital environment that holds a huge set of transactions, to observe the scalability, security , and the flexibility offered by the Blockchain+HME +Arbitrum compared to the conventional block chain, the results obtained shows that the proposed method is highly reliable and secure with the enhanced detection rate of the fraudulent users. In future the paper aims to utilize the blockchain as service from cloud for more critical applications with high sensitized data to have a cost effective block chain solution.

References

[1] Joshi, Archana Prashanth, Meng Han, and Yan Wang. "A survey on security and privacy issues of blockchain technology." *Mathematical Foundations of Computing* 1, no. 2 (2018): 121-147.

[2] Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)* (pp. 1392-1393). IEEE.

[3] Yli-Huumo, Jesse, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. "Where is current research on blockchain technology?—a systematic review." *PloS one* 11, no. 10 (2016): e0163477.

[4] Halpin, Harry, and Marta Piekarska. "Introduction to Security and Privacy on the Blockchain." In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 1-3. IEEE, 2017.

[5] Lin, Iuon-Chang, and Tzu-Chun Liao. "A Survey of Blockchain Security Issues and Challenges." *IJ Network Security* 19, no. 5 (2017): 653-659.

[6] Suma, V. "SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 1, no. 01 (2019): 45-54.

[7] Bhalaji, N. (2019). QOS AND DEFENSE ENHANCEMENT USING BLOCK CHAIN FOR FLY WIRELESS NETWORKS. Journal of trends in Computer Science and Smart technology (TCSST), 1(01), 1-13.

[8] Jacob, I. J. (2019). CAPSULE NETWORK BASED BIOMETRIC RECOGNITION SYSTEM. Journal of Artificial Intelligence, 1(02), 83-94.

[9] Sivaganesan, D. (2019). BLOCK CHAIN ENABLED INTERNET OF THINGS. Journal of Information Technology, 1(01), 1-8.

[10] Praveena, A., and S. Smys. "Prevention of inference attacks for private information in social networking sites." In 2017 International Conference on Inventive Systems and Control (ICISC), pp. 1-7. IEEE, 2017.

[11] Karthiban, K., and S. Smys. "Privacy preserving approaches in cloud computing." In 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 462-467. IEEE, 2018.

[12] Anguraj, Dinesh Kumar, and S. Smys. "Trust-based intrusion detection and clustering approach for wireless body area networks." Wireless Personal Communications 104, no. 1 (2019): 1-20.

[13] [n. d.]. Ethereum Project. https://www.ethereum.org. ([n. d.]).

[14] Kalodner, Harry, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten. "Arbitrum: Scalable, private smart contracts." In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 1353-1370. 2018.

[15] Jason Teutsch and Christian Reitwießner. 2017. TrueBit: A scalable verification solution for blockchains. (2017)