BLOCKCHAIN SECURITY IMPLEMENTATION FOR FINANCIAL DOMAINS

Jamuna Prasad Rao[1], Mr.K. Shankara[2]

[1]Reg.no:1116132, MCA VI semester, Department of MCA, Sree Vidyanikethan Institute of Management, S.V.University, Tirupati, Andhra Pradesh.

[2]Assistant Professor, Department of MCA, Sree Vidyanikethan Institute of Management, A.Rangampeta, Tirupati.

Abstract:- *Now a day's security becomes a very major aspect in all online transactions. The online browsing, online transaction needs a security. The security became very questionnaire for the real world. The online transactions need to maintain a strong security towards the finance and other aspects. The SSL security evaluates client information and encrypts the data. The encrypted format of the information will be send to the server. The server decrypt and access the information. This process provides a security for data transmission. The data modification security is required in various domains. The financial domain is one the major required domain to block the modifications. The need for providing the security, for the transactions is fulfilling by Blockchain. The resistance for data modifications is the specialty of Blockchain design required domain to block the modifications. The need for providing the security, for the transactions is fulfilling by Blockchain.*

Keywords: *Chain of transactions, blocking , Non Editable transactions, Byzantine, Decentralized System.*

INTRODUCTION:

Up to 1990 the encrypted based security was implemented on host level. The chain of cryptographic network security was first implemented in the year 1991 [1]. Blockchain is considered as peer-to-peer network collection of protocol for inter-node communication and the new blocks are validated. The distributed computing system was implemented for record transactions [2]. The record transactions are permanent and not editable. The Blockchain contains a strong fault tolerance by the implementation of Byzantine. The complete Blockchain was implemented as a Decentralized system.

LITERATURE REVIEW:

The network chain of security was first proposed by Staurt Haber and W. Scott Stornetta in the year of 1991. They were implemented a system where the document timestamps could not be tampered due to time and person [3]. In the year 1992 Markle trees are designed, to implement several security certificates. In 2008 Hash cash was implemented to add blocks to the chain of networks. In 2014 Blockchain was implemented for providing security to the Bitcoin transactions that supports 50 GB to 100 GB as the file size [4]. In 2016 IBM was Adopted Blockchain technology for their financial transactions and recognized very less frauds.

ARCHITECTURE OF BLOCK CHAIN:

The chain of transactions, in all segments is recorded by the decentralized system and also reflects the distributed system. The block chain is a public digital ledger, majorly implemented to record the transactions with the special property of non editable. The verification of transactions made easy, a user can verify the transaction individually with no cost [5]. The Blockchain supports robust workflow and support a complete secure security. The primary objective of Blockchain is implementing peer network and distributed time stamping. The transaction may take place only once. The transactions are not editable. The Blockchain architecture is shown in figure 1.

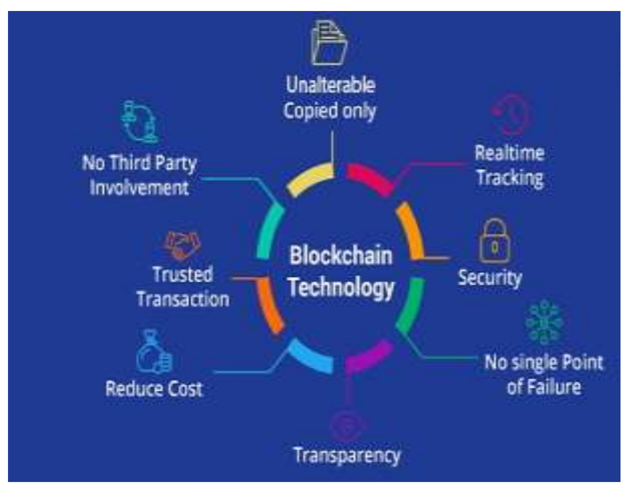

Figure 1. Architecture of Block Chain

IMPLEMENTATION OF BLOCKCHAIN:

Blockchain was completed for Bitcoin Transactions. The users of Bitcoin was increased like a flood of water, so it became essential to implement strong security and the transactions are non editable [6]. Inorder to provide strong security for transactions the Bitcoin organization choose Blockchain. Bitcoin Transactions are implemented with block chain the graph show the Bitcoin transaction within a short spam. The growth of transactions through Blockchain is shown in the figure 2.

Figure2. Graph Representing transactions.

The structure of Blockchain contains various stages:

Blocks formation: the valid transactions are stored in the form of blocks. Each block defines with hashed and encoded format into a tree format. Each block contains a relationship with another block [7]. A separate memory holds address of another block. When the data is storing on different block the link is establish with the next block. The chain of block is formed with linked blocks. The complete block looks like an integrated chain of networks. The Blockchain architecture is shown in the figure3.

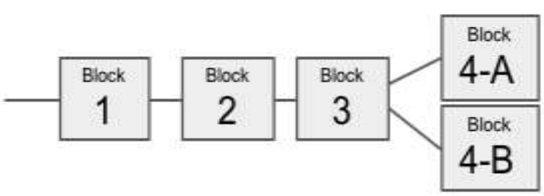

Figure 3: Block Diagram of Block Chain

Block time description:

When the transaction takes place it should be create a block. The average time taken on the network to generate an extra block in the block chain is described as block time. The Blockchain blocks as shown in the figure 4.

Figure 4: Blocks designed by 3D

Hard forks structure:

It describes the change of rule in the block. If any new rule applies for any block, the same rule should be applicable for all blocks. The updating of rules should be unique [8]. The block chain does not allow implementing different rules for the individual blocks. The total set of blocks should be implemented the same rule. The hard forks structure force the users to implement uniform rule for all the blocks.

Decentralization method:

The block chain changes the architecture into decentralized system. Peer-to-Peer is the storage system of data in the network [9]. By the implementation of block chain decentralized system, the user can eliminate most of the risk while storing and providing security. Block chain implements public key and private key cryptography techniques to ensure the security.

ABOUT FINANCIAL DOMAIN:

The financial domain needs a strong security. One of the major problems for financial services is data overriding and modification of data. These problems cost major issues. So it is essential to provide better security for all the transactions. The Blockchain provides non-editable and committed transactions [10]. There is no third party involvement in all the transactions. The block chain transaction security is unalterable and allows only copying of transactions. Depends on the requirement we can verify the transactions. The users are provided complete history verification option with the help of Blockchain. Different types of the financial services for the users through Blockchain as shown in the figure 4.

Figure 5: Areas of Financial Domains

The Block chain provides a strong security for Financial Domains. The security contains digital Rights, Wagers, ESCrow, Equity, Debts, Derivations, crow funding. The Blockchain architecture supports all the above functionalities of Financial Domain. The figure 6 shows the secure transaction of financial transactions in the hands of Blockchain.

Figure 6: Secure Transactions

CONCLUSION:

Providing the security for the online and off line transactions is became a hectic task for the developers and users. The Blockchain gave a sufficient solution for this type of problems. Blockchain with the set of nodes verify the transaction in multiple areas and commit the transaction. The transactions once committed may not be editable. The financial domains need a non editable transactions maintenance system. The purpose of security may be full fill by the Blockchain.

REFERENCES:

1. State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/state-of- blockchain-q1-2016/
2. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
3. G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn.2646618563
4. G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain,"2015.
5. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.
6. B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: https://ssrn.com/abstract=2394738
7. Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.
8. M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.
9. C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning," arXiv preprint arXiv:1601.01405, 2016.
10. I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.
11. A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/ state-of- blockchain-q1-2016/
12. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
13. G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015.

[Online]. Available: http://dx.doi.org/10.2139/ssrn. 2646618563

14. G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain,"2015.
15. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk:The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.
16. B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: https://ssrn.com/abstract=2394738
17. Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.
18. M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.
19. C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning," arXiv preprint arXiv:1601.01405, 2016.
20. I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.
21. A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,
22. C. Decker, R. Wattenhofer, Information propagation in the Bitcoin network. In: Peer-to-Peer Computing (P2P), IEEE Thirteenth International Conference on; p. 1–10, 2013.
23. E. P. Gareth and W. Peters, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," November 2015.
24. A.Dev "Bitcoin mining acceleration and performance quantification". In: Electrical and Computer Engineering (CCECE), IEEE 27th Canadian Conference on; p. 1–6. 2014
25. A. Fernandez, E. Insfran, S. Abraho, Usability evaluation methods for the web: A systematic mapping study. Information and Software Technology.;53(8):789– 817. 2011
26. C. Jentzsch, "Dezentralized autonomous organization to automate governance," 2016.
27. J. Peterson and J. Krug, "Augur: a decentralized, open-source platform for prediction markets," 2015.
28. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
29. M. Swan, "Blockchain: Blueprint for a New Economy", 1st ed. O'Reilly, February 2015.
30. D.Vandervort "Challenges and Opportunities Associated with a Bitcoin-Based Transaction Rating System" vol. 8438. Springer Berlin; Heidelberg; p. 33–42. 2014.
31. A. Beikverdi, J. Song, Trend of centralization in Bitcoin's distributed network. In: Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2015 16th IEEE/ACIS International Conference. p. 1–6. 2015 moto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
32. G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and r State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/ state-of-blockchain-q1- 2016/
33. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
34. G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn. 2646618563
35. G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain,"2015.
36. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.
37. B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: https://ssrn.com/abstract=2394738
38. Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015,pp. 184–191.
39. M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced

Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.
40. C. Noyes, “Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning,” arXiv preprint arXiv:1601.01405, 2016.
41. I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.
42. A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in bitcoin p2p network,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,