reshma kanse anurag group_Report

by RRP_VMR_AMP_HM_RRK_XYZ_PQR_ bharti

Submission date: 09-Jun-2023 03:19AM (UTC-0400)
Submission ID: 2107888318
File name: Implementation-Final-copy-ProfReshmaKanse.pdf (469.7K)
Word count: 2272
Character count: 12872

Trusted Framework for Online Banking Blockchain Framework

Rohit Shendge[1], Indrajit Datar[2], Adwait Shinde[3], Anurag Gulavane[4], Prof. Reshma Kanse[5]
[1,2,3,4] BTech Student and [5]Asst. Prof of Department of Computer Science and Business Systems,
Bharti Vidyapeeth Deemed University, Department of Engineering and Technology
Navi Mumbai

Abstract: Blockchain has established itself as a significant financial software system. They are based on a safe distributed ledger data structure. They are becoming increasingly popular in the world today. People appear to be discovering new ways to use the blockchain's power for intuitive applications that provide solutions to real-world problems. A crucial part of these systems, mining, adds data of prior transactions to the distributed ledger. Every 10 minutes, a block (the structure containing transactions) is mined Miners compete by attempting to use a cryptographic hash technique to solve a challenging mathematical problem. When a block is solved, the transactions contained within it are considered confirmed, and the Bitcoin involved in the transactions is available for spending. Users can reach a strong and secure consensus for every transaction thanks to the Blockchain. Cryptocurrencies are a major application of blockchain. They require robust, secure mining algorithms, and because they are peer-to-peer systems by design, they rely on miners to validate transactions because they lack a central authority to mediate transactions. Companies seeking to save costs and improve efficiency are drawn to the promise of new blockchain and distributed ledger technology (DLT). If completely implemented, it will make it possible for banks to process payments faster and more precisely while simultaneously reducing transaction processing costs and the requirement for exceptions.. Therefore, we find the need to upgrade our banking system to mediate transactions and to this new technology. In this proposed system we design and develop custom blockchain technology with SHA, Mining and Chain Consensus Algorithm for provide security and privacy of secure baking transactions and also addition of designing a secure authentication technique with the help of keylogging secure authentication methodology. Blockchain is a framework which is provide peer-to-peer (P2P) verification and validation protocols and using this protocols provide security and privacy of banking transaction systems.

Keywords: - Blockchain, distributed ledger technology (DLT), mining, transactions, consensus, cryptocurrencies, secure banking transactions, authentication, keylogging etc.

I. IMPLEMENTATION

1. Design and Architecture: The first step in implementing a trusted framework for online banking using blockchain technology is to design and architect the system. This includes identifying the different components of the system, such as the nodes, channels, smart contracts, and consensus mechanism, and defining the rules for how they will interact.

2. Hyperledger Fabric Setup: The Hyperledger Fabric framework is a popular choice for implementing a blockchain-based online banking system due to its unique features such as a permissioned network, confidentiality, flexibility, scalability, and security. The implementation details for setting up a Hyperledger Fabric network can include configuring nodes, channels, smart contracts, and consensus mechanisms.

3. Integration with Existing Banking Systems: Once the blockchain network is set up, it needs to be integrated with existing banking systems toenable seamless transactions between the blockchain network and the traditional banking system. This requires the use of APIs and other integration tools to enable communication between the two systems.

4. Smart Contracts Development: Smart contracts are the backbone of a blockchain-based system, and they need to be developed and deployed on the network to facilitate transactions. Smart contracts can be developed using various programming languages such as Go, Java, and JavaScript, depending on the requirements of the system. 5. User Interface Development: A user interface (UI) is essential to enable users to interact with the system. The UI can be developed using various frontend frameworks such as React, Angular, or Vue.js, and it should be designed to provide a seamless user experience.

6. Testing and Deployment: Once the system is developed, it needs to be thoroughly tested to ensure that it meets the required performance, scalability, and security standards. The system can then be deployed to a production environment for use by customers.

7. Ongoing Maintenance and Support: A blockchain-based online banking system requires ongoing maintenance and support to ensure that it remains up-to-date and secure. This can include regular updates to the system, bug fixes, and security patches.

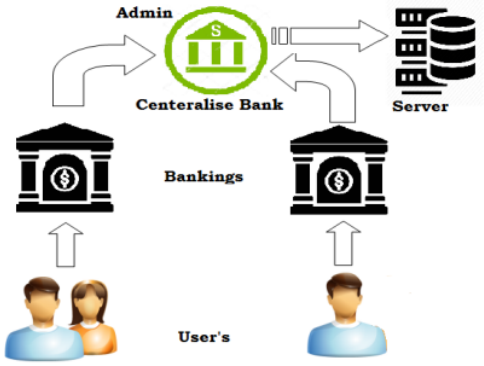
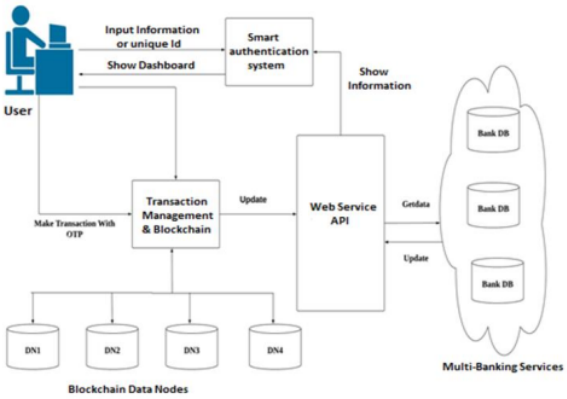


Fig.1: System Overview



Architecture Diagram

II. ALGORITHMS

2.1 Hash Generation Algorithm

Algorithm 1 for Hash Generation

Require: Genesis block, Previous hash, data D

Ensure: Generated hash H according to given data

1: function KeywordSearch(D, Q)

2: Step 1 : Input data as d

3: Step 2 : Apply SHA 256 from SHA family

4: Step 3 : CurrentHash= SHA256(d)

5: Step 4 : Return CurrentHash

A hash algorithm is a function that converts a data string into a numeric string output of fixed length. The output string is generally much smaller than the original data. ... Two of the most common hash algorithms are the MD5 (Message-Digest algorithm 5) and the SHA-1 (Secure Hash Algorithm). 3.3 Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms.

2.2 Protocol for Peer Verification

Algorithm 2 for Protocol Peer Verification

Require: User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchain NodesChain[Nodeid] [chain]

Ensure: Recover if any chain is invalid else execute current query 1: function KeywordSearch(D, Q)

Step 1 : User generate the any transaction DDL, DML or DCL query

Step 2 : Get current server blockchain Cchain Cnode[Chain]

Step 3 : For each NodesChain[NodeId, Chain](GetChain)

End for

Step 4 : Foreach (read I into NodeChain) If (!.equals NodeChain[i] with (Cchain))

Flag 1

Else Continue Commit query

Step 5 : if (Flag == 1)

Count = SimilaryNodesBlockchian()

Step 6 : Cacluate the majority of server Recover invalid blockchain from specific node

Step 7: End if End for

14: End for

All peers on a blockchain network reach a consensus to verify transactions. This consensus is governed by an algorithm fed into the protocol layer of the blockchain. The blockchain gives all peers an identical copy of each transaction which eliminates trust thus making a trustless, distributed network.

3.3 Mining Algorithm for valid hash creation

Algorithm 3 for Mining Algorithm for valid hash creation

Require: Hash Validation Policy P[], Current Hash Values hash Val

Ensure: Valid hash

function ValidHash(D, Q)

Step 1 : System generate the hash Value for ith transaction using Algorithm 1

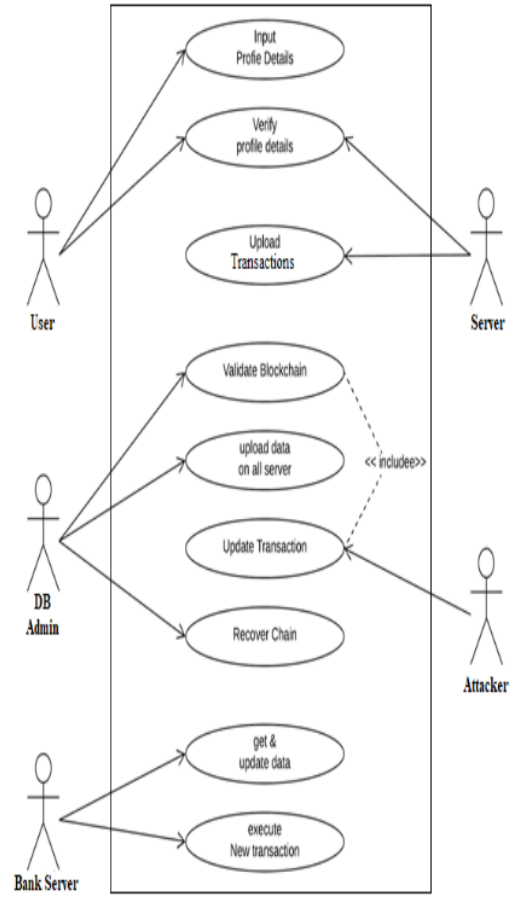
Step 2 : if (hash Val.valid with P[]) Valid hash Flag =1 Else Flag=0

Mine again randomly

Step 3 : Return valid hash when flag=1

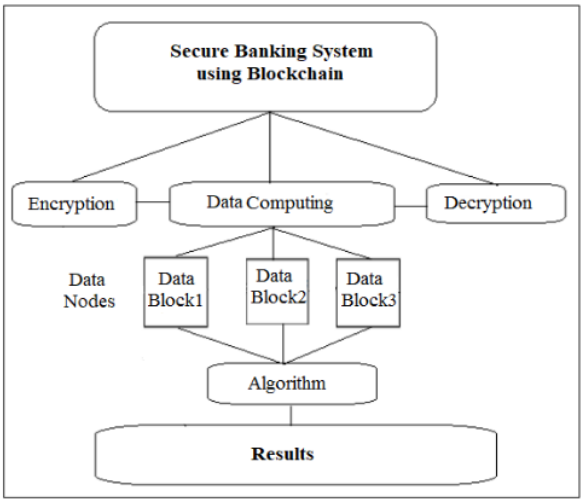
Mining algorithms are the algorithms or functions that make the task of mining crypto-currencies possible. Mining algorithms are the algorithms in charge of making possible the cryptocurrency mining. Normally these algorithms are cryptographic hash functions very complex and they can adjust the mining difficulty. A process that makes it more or less difficult for you to put together the puzzles that must be solved by the miners. This is to get miners to do complex computational work that, once solved, allows them to access a reward for that work.

III. FLOWCHART DIAGRAMS

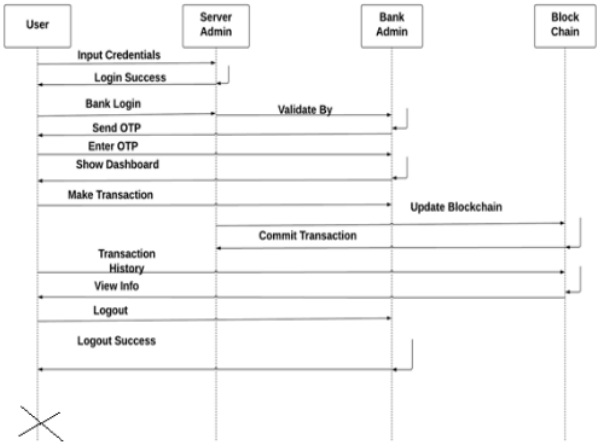


.

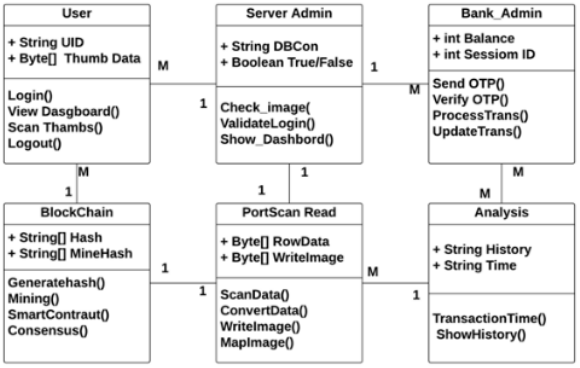
1.Use Case Diagram



2. Activity Diagram

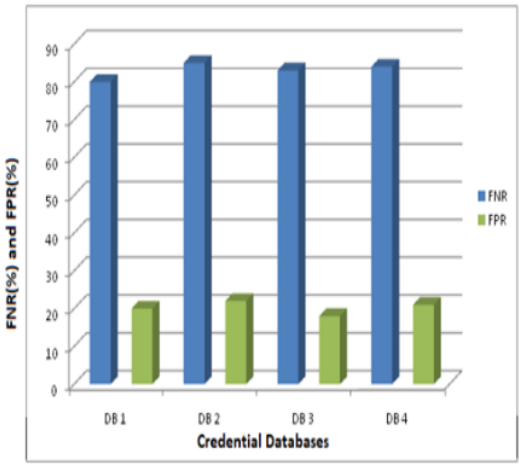


3.Sequence Diagram

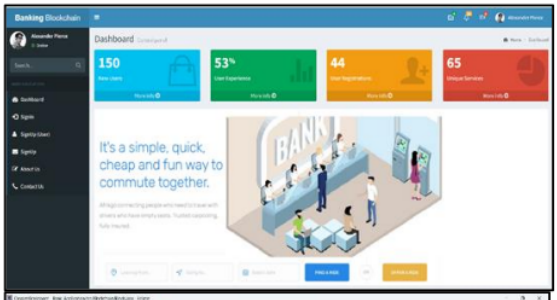


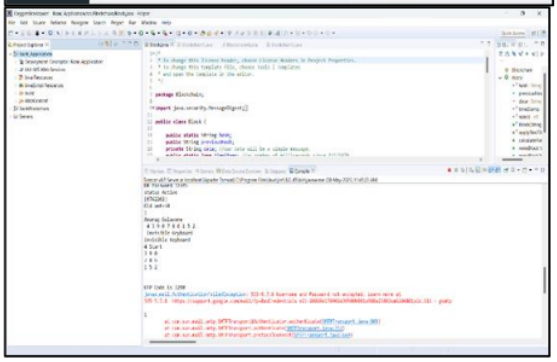
4. Class Diagram

IV. RESULTS



V. Implementation Screenshot





VI. Gap Analysis

Paper Title	Key Points	Gap Analysis
Inter Bank Payment System on Enterprise Blockchain Platform [5]	Introduces an end-to-end inter-bank payment system based on blockchain using Hyperledger Fabric Enterprise blockchain. - Enables gross settlement, reconciliation, and gridlock resolution facility.	it does not address the potential challenges and limitations of implementing such a system on a large scale, such as regulatory barriers, interoperability issues, and the need for consensus among different banks.
Exploration and Practice of Inter-Bank Application Based on Blockchain [6]	Discusses the difference between traditional transaction structure and blockchain transaction structure. - In a blockchain-based system, participants share a common ledger containing all transactions, whereas in a traditional system, transactions are carried out using a central institution.	It does not fully explore the potential impact of blockchain on the banking industry as a whole, including potential changes to business models, customer expectations, and industry dynamics.
Blockchain Enabled Decentralized Time Banking for a New Social Value System [7]	introduces a time banking system based on exchanging the economy not based on money but value of everyone's contribution on a scale, i.e., time expended. - The blockchain network facilitates members to participate in the service exchange process without depending on a centralized third party for maintaining the service time data.	it does not fully address the potential challenges and limitations of implementing such a system, including issues related to scalability, security, and user adoption

VII. Conclusion

In conclusion, a trusted framework for online banking using blockchain technology has the potential to transform the way that online banking services are delivered and consumed. The implementation of a blockchain-based system can enhance security, transparency, and efficiency while reducing the risk of fraud, theft, and cyberattacks. However, the adoption of blockchain technology for online banking also comes with challenges and risks, including regulatory compliance and data privacy concerns. Organizations need to carefully consider these challenges and risks before implementing a blockchain-based system.

VIII. REFERENCES

Sabout Nagaraju and LathaParthiban, "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway," Open Access Journal of Cloud Computing: Advances, Systems and Applications (2015)

1. Dorri, S. S. Kanhere and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions," arXiv: 1608.05187 [cs], 2019.
2. Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." Young Researchers in Electrical and Electronic Engineering (EICon-Rus), 2018 IEEE Conference of Russian IEEE, 2018.
3. Yang, Huihui, and Bian Yang. "A Blockchain-based Approach to the Secure Sharing of Healthcare Data." Proceedings of the Norwegian Information Security Conference. 2020.
4. Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006.
5. Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based crypto-system and blockchain." Journal of medical systems 42.8 (2018): 152.
6. Michalevsky Y, Joye M. "Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy".
7. Wu, Axin, et al. "Hidden policy attribute- based data sharing with direct revocation and keyword search in cloud computing." Sensors 18.7 (2018): 2158.
8. Khan S, Khan R. "Multiple authorities' attribute-based verification mechanism for Blockchain micro-grid transactions". Energies. 2018 May; 11(5):1154.
9. Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems." IEEE Access 776.99 (2018): 1-12.
10. Monika D. Rokade, Dr. Yogesh Kumar Sharma, "Deep and Machine Learning Approach's for Anomaly based Intrusion Detection of Imbalanced Network Traffic." IOSR journal of Engineering (IOSR JEN), _ISSN (e): 2250-3021, ISSN(p): 2278-8719
11. Monika D. Rokade, Dr. Yogesh Kumar Sharma, "MLIDS: A Machine Learning Approach for Intrusion Detection for real time Network Dataset." 2021 International Conference on Engineering Smart Computing and Informatics (ESCI), IEEE.
12. Monika D. Rokade, Dr. Yogesh Kumar Sharma. (2020) "Identification of Malicious Activity for Network Packet using Deep Learning." International Journal of Advance Science and Technology, 29(9s), 2324-2331.
13. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin.org, 2008.
14. D. J. Hwang and K. Lee, "Analysis of security threats and solutions in payment systems," Information Security Journal: A Global Perspective, vol. 25, no. 2, pp. 50–58, 2016.
15. T. Dierks and C. Allen, "The TLS Protocol Version 1.3," Internet Engineering Task Force, 2018.
16. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin.org, 2008.
17. P. Koshy, D. Koshy, and P. McDaniel, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," in Financial Cryptography and Data Security, 2014, pp. 469–485.
18. T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.
19. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.
20. A. Shamir, "How to Share a Secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.
21. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
22. B. A. Forouzan, Cryptography and Network Security: Principles and Practice, McGraw-Hill Education, 2015.
23. B. C. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," IEEE Communications Magazine, vol. 32, no. 9, pp. 33–38, 1994.
24. J. Salowey et al., "The Secure Sockets Layer (SSL) Protocol Version 3.0," Internet Engineering Task Force, 1996.
25. M. C. Rosu, M. Danubianu, and M. V. Rosu, "Blockchain Solutions for the Digital Banking Revolution," Procedia Economics and Finance, vol. 23, pp. 200–204, 2015.
26. P. Koshy, D. Koshy, and P. McDaniel, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," in Financial Cryptography and

Data Security, 2014, pp. 469–485.
27. V. Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum.org, 2014.
28. D. J. Hwang and K. Lee, “Analysis of security threats and solutions in payment systems,” Information Security Journal: A Global Perspective, vol. 25, no. 2, pp. 50–58, 2016.
29. C. N. Chuang, Y. C. Liao, and Y. C. Chen, “A Privacy-Preserving Cloud-Based Electronic Health Record System Based on Blockchain Technology,” Journal of Medical Systems, vol. 42, no. 8, p. 139, 2018.
30. J. Huang et al., “A Trusted e-Contract Signing Framework Based on Blockchain,” IEEE