International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)
ISSN: 2456-236X
Vol. **11** Special Issue **03** | **2026**

Blockchain Technology for Protecting Banking Transaction without Using Tokens

Manjiri Gawas[1], Tejas Gaonkar[2], Yash Kadam[3], Cajetan Gonsalvis[4] Heenali Korgaonkar[5]

[1,2,3]*Student, Electronics and Telecommunication Engineering, Metropolitan Institute of Technology & Management Sindhudurg, Maharashtra, India*
[4,5]*Assistant professor, Electronics and Telecommunication Engineering, Metropolitan Institute of Technology & Management Sindhudurg, Maharashtra, India*

DOI: 10.5281/zenodo.20609659

ABSTRACT

Increasing digital technology has revolutionized the life of people. There are many threats and frauds detected in banking system. A centralized database is used by banking system which makes the attacker easy to get access to data and this makes the system insecure. Image theft and copyright issues have been increasing rapidly with the rise of internet. Therefore, copyright protection of images has become an unavoidable issue. Blockchain is a distributed database that provides a secure, yet transparent way to protect any type of records. Blockchain provides an effective way to prevent copyright violation by providing a proof -of-property solution. This project has proposed a model of image copyright protection using blockchain. There are many methods to protect the images such as disabling right clicks, disabling external linking of websites, digital watermarking and many more. Adding a digital watermark makes it easier to identify that the image is copyrighted. Blockchain stores the images securely and also provides the proof -of-property for the copyright holder. This system also provides a cross -check functionality for commercial users to avoid copyright issue by checking whether the image is copyrighted or not. Blockchain is transforming the banking sector and offering opportunities for significant cost reduction and efficient banking services. However, implementing blockchain is a challenge due to lack of adequate knowledge and skills on how to implement the technology. As a result, there are very few market-ready blockchain banking products and organizations are unable to realize the promised value. This paper presents an overview of the banking sector's blockchain use cases, design and implementation considerations and techniques. The drawback of this centralized system can be reduced by reforming the system by implementing blockchain technology without using tokens. In conclusion, Blockchain uses decentralized architecture for storing and accessing data over the database. This reduces attacks on database hacked. Transactions done through blockchain technology are verified by each block in the chain, which will make the transaction more secure and help banking system work faster. Opportunities for further research are noted in the areas of interoperability, governance, security and privacy.

Keywords: Blockchain Technology; Distributed database; Cryptocurrency; Consensus; Security and Protection.

1. INTRODUCTION

Copyright ownership gives the owner the exclusive right to use the work. When a person creates an original work, fixed in a tangible medium, he or she automatically owns copyright to the work. Copyright protects original works such as literary, dramatic, musical and artistic works. Copyright protection is automatically provided under the Copyright Act 1968 and gives the creator of the work exclusive rights to reproduce it, commercialize it and be recognized as its creator. As with other forms of intellectual property, there is no authenticated method to see whether the material is copyrighted or not. Copyright material is protected from the time it is first written down, painted or drawn, filmed or taped. The storage of the copyrighted material needs to be done in a secure place and with the proof of-property concept hence claiming the ownership of the copyright. The traditional database might not be the solution that can update or delete the data reducing the factor of security for the stored material. Blockchain can be an appropriate solution to securely store copyrighted material. Copyright is one of those thorny issues that are always causing pain to creative types. After all, if you write something, make music, take a photograph, or in some other way create, in theory you should receive full recognition (and payment). In the US this falls under title 17, which deals with "original works of authorship", including literary, dramatic, musical, artistic, architectural, and some other intellectual works. Many websites host their content with the work that is unauthorized. The content creator may suffer loss in case the work is used for revenue purposes. The person that does not hold the copyright for the work gets paid for it. The creators may claim the work when the work is seen on an unauthorized website. But the proof-of-property record is not maintained in the case, so the

creator faces some difficulties in claiming the copyright content. Unfortunately, particularly with the vast free market that is the social media, it's increasingly common for people to feel they should get everything for nothing. The copyright holder is usually not get paid for their content and someone else takes their credit. It is more disappointing when someone earns money through the content created by another person. Copyright data can be stored in various storage systems but blockchain is the ultimate solution to protect the copyright information. Blockchain is similar to a database but only supports create and read operations. Data is stored in form of blocks which are coupled to each other and hence form a long chain. The data in the blocks is in encrypted form that makes it difficult to crack or change. Each block contains the address of its previous block and the follow feature makes the blockchain immutable (i.e.no one can change the block in between of the chain). Blockchain works in distributed environment that makes it immune to failures providing a restore point from other blockchain in the network.

1.1 Survey of similar systems / products in India and abroad

The following paper works helps us to know about similar systems/products in India and abroad.

1. Distributed Ledger Technology (DLT): Blockchain is a type of DLT that enables the creation of a shared, decentralized database where transactions are recorded in a series of blocks. By using consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS), DLT ensures the integrity and immutability of transaction records, reducing the risk of fraud or tampering.
2. Cryptographic Hash Functions: Blockchain networks employ cryptographic hash functions to secure transaction data. These functions generate unique digital signatures for each transaction, making it virtually impossible to alter the data without detection. By verifying the integrity of the transaction data using cryptographic hashes, the authenticity of banking transactions can be protected.
3. Smart Contracts: Smart contracts are self-executing contracts with the terms and conditions of an agreement written into code. They automatically facilitate, verify, and enforce the terms of the contract without the need for intermediaries. Smart contracts can be utilized in banking transactions to ensure secure and transparent execution of agreements, such as loan contracts, trade settlements, or asset transfers.
4. Consensus Mechanisms: Consensus mechanisms are algorithms used in blockchain networks to achieve agreement among participants on the state of the ledger. While tokens are often used in consensus mechanisms, alternative approaches like Proof of Authority (PoA) or Delegated Proof of Stake (DPoS) can be implemented. These mechanisms rely on reputation or stakeholder participation rather than tokens to secure and validate transactions. Private/Permissioned Blockchains: Instead of using public blockchain networks, banks can employ private or permissioned blockchains. Private blockchains restrict access to a select group of participants, such as banking institutions or trusted entities, ensuring a higher degree of control and privacy. Permissioned blockchains allow predefined participants to validate and verify transactions, maintaining security without relying on tokens or open participation.

Blockchain technology has gained significant attention in the financial sector for its potential to secure and streamline banking transactions. While tokens are commonly used in blockchain systems, there are alternatives that can protect banking transactions without relying on tokens.

Blockchain (India): Blockchain is a consortium of Indian banks that aims to explore and implement blockchain technology in the banking sector. It focuses on various use cases, including secure transactions, identity management, and supply chain finance. While Blockchain's specific implementation details are not publicly available, it represents a collaborative effort by Indian banks to leverage blockchain for transaction protect

1.2 Need of Project

Blockchain technology offers several benefits for protecting banking transactions, even without the use of tokens. Here are some reasons why blockchain can be valuable in securing banking transactions:

1. Immutable and Transparent Ledger: Blockchain provides a decentralized and immutable ledger that records all transactions. Each transaction is linked to the previous one, forming a chain of blocks. This transparency and immutability make it difficult for malicious actors to alter or manipulate transaction records without detection.
2. Enhanced Security: Blockchain employs advanced cryptographic techniques to secure transactions. Each transaction is digitally signed and verified by participants, ensuring the integrity and authenticity of the data. This cryptographic security makes it highly resistant to unauthorized tampering or fraud.
3. Distributed Consensus: Blockchain relies on a consensus mechanism where multiple participants validate and agree on the transactions. This distributed consensus ensures that no single entity has control over the transaction verification process. It reduces the risk of fraudulent activities and provides a high level of trust among participants.
4. Data Privacy: While blockchain transactions are transparent, the underlying technology allows for the implementation of privacy features. Encryption techniques can be employed to protect sensitive information, ensuring that only authorized parties can access specific transaction details.

5. Smart Contracts: Blockchain platforms often support smart contracts, which are self-executing agreements with predefined rules and conditions. Smart contracts automate the transaction process and ensure that all parties involved adhere to the agreed-upon terms. By eliminating manual intervention, smart contracts reduce the risk of errors, delays, and disputes.

By leveraging these features, blockchain technology can enhance the security, efficiency, and transparency of banking transactions, thereby reducing risks and building trust among participants. While tokens are commonly associated with blockchain-based systems, they are. not a prerequisite for using blockchain in banking transactions. Blockchain can be implemented to secure and streamline existing banking processes without the need or tokens or cryptocurrencies.

2. BLOCK DIAGRAM

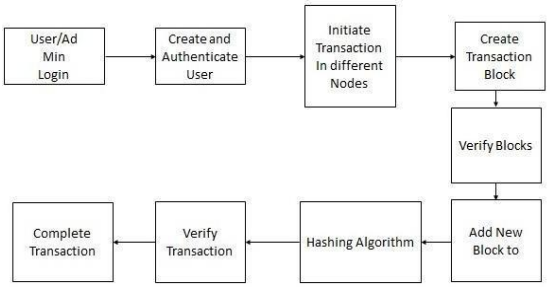


Fig.2.1 System Block Diagram

2.2 Block Diagram Description

In the proposed system, the typical bank design, which comprises on a centralized database, would be eliminated in the suggested system. The data will be dispersed widely over the block chain, making banking institutions decentralized. This will not only make data more secure, but it will also decentralize authority. There are two advantages to the transaction method outlined above. To begin with, it will speed up transactions by eliminating the intermediary procedures that are now used in regular transactions, and it will also make it almost difficult for an individual to hack the system since it will demand a massive amount of computing power that no one possesses. To implement the above-mentioned system, we can have two different types of nodes, verification nodes belonging to the bank and the user node for customers. And there will be multiple user nodes and verification nodes in a distributed system. Verification nodes will be responsible for the authorized tasks such as verifying a customer's account, verifying a transaction and creating a block for a number of transactions for a given timestamp. And after creating the block it has to broadcast it in the network. User node is used by the customers so they can initiate a new transaction, view their account history and so on. Each user node is meant to store the public and private key required for the user's transaction. Also, it will store the most updated blockchain. This will not only make the data ore secure but also will remove the power centralization. The transactions over the block chain will be in form of encrypted tokens which will be verified by each node on the block chain. To make any transaction valid, the nodes of the block chain will have to give the proof of the processing it has done in order to verify the transaction. That proof will be taken in terms of the amount of processing done. The above-mentioned transaction system has two benefits. this system would be able to implement a distributed system as well as the banking nodes could be semi-automatized so as to reduce work.

2.3 Technical details of the project work

To design a blockchain-based system for protecting banking transactions without using tokens, you would typically need to consider the following technical details:

- Data Structure: Define the structure of the blocks in your blockchain. Each block typically contains a header, transaction data, and a reference to the previous block. Determine the specific data fields you need to store in the blocks to represent banking transactions accurately.
- Cryptographic Techniques: Utilize cryptographic algorithms to secure the transactions. This includes digital signatures to verify the authenticity of transactions and cryptographic hashing to ensure data integrity. Public-key cryptography is commonly employed in blockchain systems.
- Smart Contracts: Consider implementing smart contracts, which are self-executing contracts with predefined rules encoded on the blockchain. Smart contracts can automate various banking processes, such as fund transfers, loan agreements, or compliance checks.
- Network Infrastructure: Determine the network architecture and protocols for communication among the blockchain nodes. You may choose between a permissionless (public) or permissioned (private) network based on your requirements. Consider factors such as scalability, privacy, and performance.

- Consensus Governance: Define how the blockchain network will be governed. Decide whether it will be operated by a consortium of banks or managed by a decentralized community. Establish rules for adding new participants, validating transactions, and resolving conflicts.
- Privacy and Confidentiality: Address privacy concerns related to banking transactions. Depending on the regulatory requirements, you may need to implement privacy-enhancing techniques such as zero-knowledge proofs or secure multi-party computation to ensure sensitive information is protected.
- Integration with Existing Systems: Consider how the blockchain solution will integrate with the existing banking infrastructure. Determine the mechanisms for connecting the blockchain network to banking applications, databases, and external systems.
- Security Measures: Implement robust security measures to protect the blockchain network from potential attacks. This includes securing private keys, employing firewalls and intrusion detection systems, and regular security audits. It's important to note that developing a blockchain-based solution requires significant technical expertise and thorough understanding of the banking domain. Additionally, regulatory compliance and legal considerations should be taken into account to ensure the solution aligns with industry standards and legal frameworks.

3. SOFTWARE DESIGN

3.1 Algorithm

PHash: - To find the hash value of an image. Pre: Requires jpg/png/jpeg image
Post: Hash value of given image is obtained as result

1. Reduce the size of the image.
2. Reduce the color of the image (i.e., convert the image to grayscale).
3. Calculate the average pixel colors of the image.
4. Calculate the brightness value of each pixel for every pixel in image.
5. Appending the result of previous step will result in hash value of length that is equal to size of reduced image.

3.2 Flowchart

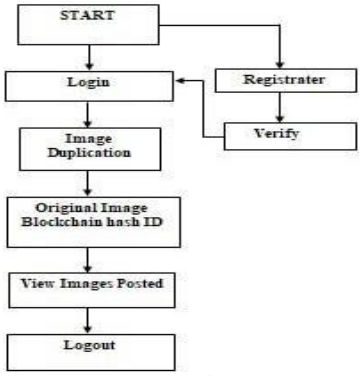


Fig.3.1 Project flow chart

4. TESTING AND TROUBLESHOOTING

Testing of various modules, details of test procedures adopted, tools and instruments used etc.
To test a blockchain technology project aimed at protecting banking transactions without using tokens, you would typically follow a systematic test procedure. While the specific details may vary depending on the project's requirements and implementation, I can provide you with an overview of the general test procedure, tools, and instruments commonly used in blockchain testing.

1. Test Planning:
   - Define the objectives, scope, and success criteria for testing.
   - Identify the different modules/components of the blockchain system.
   - Determine the testing approach and strategies to be used.
2. Unit Testing:
   - Test individual modules or smart contracts in isolation.
   - Verify the correctness of code logic, data structures, and algorithms.
3. Integration Testing:

- Test the interaction between different modules and components.
- Validate the flow of data and transactions across the system.

4. Functional Testing:
- Validate the functionality of the blockchain system as a whole.
- Test various use cases, such as creating accounts, making transactions, etc.

5. Performance Testing:
- Evaluate the system's performance under different loads and scenarios.
- Test transaction processing speed, scalability, and throughput.

6. Security Testing:
- Identify and mitigate potential vulnerabilities and security risks.
- Conduct penetration testing to uncover security weaknesses.

7. Tools and Instruments:
- Truffle: A popular development framework for Ethereum-based projects.
- Postman: A collaboration platform for API testing and documentation. Troubleshooting debugging of modules in project, Methodology employed; remedies found etc.

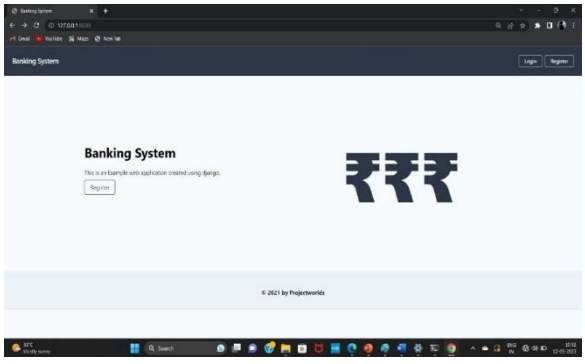
When it comes to troubleshooting and debugging modules in a project, there are several methodologies that can be employed to identify and fix issues.

- Logging: Implementing logging statements in the code can help to identify where the problem is occurring. This involves adding statements to the code that print out relevant information such as variable values, function calls, and errors.
- Debugging tools: There are several debugging tools available for Python such as PyCharm, Visual Studio Code, and pdb. These tools allow developers to step through the code, set breakpoints, and examine variables to identify issues.
- Error messages: Python provides error messages that can help to identify where the problem is occurring. These messages often include a description of the error and the line of code where it occurred.
- Code review: Another effective method of identifying issues is to have another developer review the code. This can help to identify logical errors, syntax errors, and other issues that may not be immediately obvious.

Once the issue has been identified, here are some remedies that can be applied:

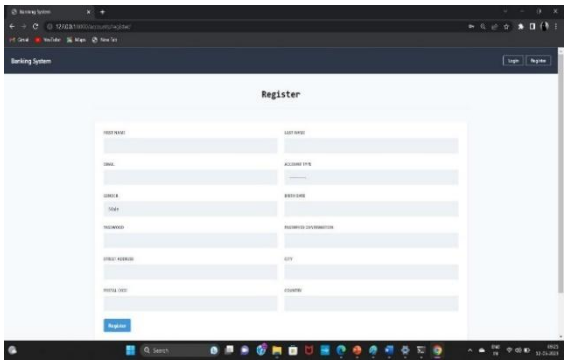
- Fixing the code: Depending on the nature of the issue, the code can be fixed to address the problem. This may involve correcting syntax errors, logical errors, or updating the code to use a different approach.
- Refactoring the code: If the issue is related to the design or architecture of the code, refactoring may be necessary. This involves restructuring the code to make it more maintainable, scalable, and easier to understand.
- Updating dependencies: If the issue is related to a dependency, updating the dependency may resolve the issue.
- Rebuilding the environment: If the issue is related to the environment, rebuilding the environment may resolve the issue. This involves updating or reinstalling software components, libraries, and dependencies.

5. PROCESS, OBSERVATIONS & RESULTS

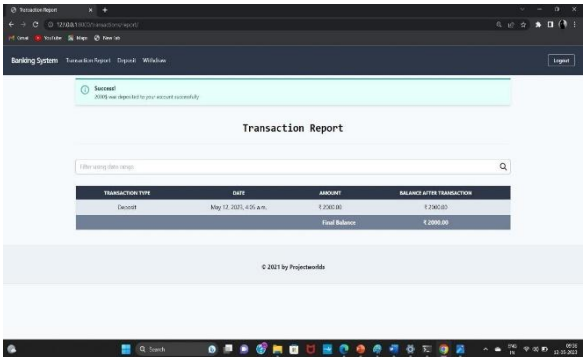


Output:

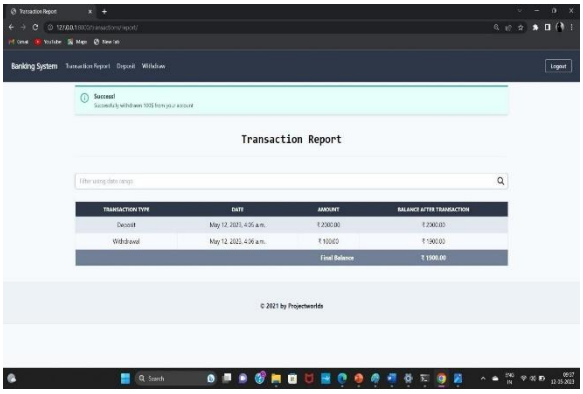
Step 1:



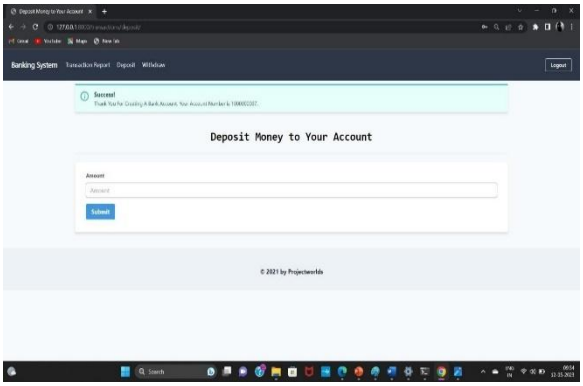
Step 2:



Step 3:



Step 4 :



6. CONCLUSIONS

Blockchain technology offers significant potential for enhancing the security and protection of banking transactions without the need for tokens. By leveraging the decentralized and immutable nature of blockchain, banks can improve the integrity and transparency of their transactional processes.

One of the key advantages of blockchain technology is its ability to create a tamper-proof and transparent transaction ledger. Each transaction recorded on the blockchain is securely linked to previous transactions, forming a chain of blocks. This provides a high level of security and prevents unauthorized modifications to transaction data. As a result, banks can mitigate the risks associated with fraud, hacking, and data tampering.

Furthermore, blockchain technology enables the use of smart contracts, which are self-executing contracts with predefined rules and conditions. By removing manual intervention, smart contracts reduce the potential for errors and improve the efficiency of transaction processing. Another significant benefit of blockchain technology is its potential to eliminate the need for intermediaries in banking transactions. Traditional banking systems often rely on multiple intermediaries, which can introduce complexities, delays, and additional costs. With blockchain, banks can establish direct peer-to-peer connections, stream lining the transaction process and reducing dependence on intermediaries.

Scalability, interoperability, regulatory compliance, and integration with existing systems are some of the challenges that need to be addressed. In conclusion, blockchain technology has the potential to revolutionize banking transactions by enhancing security, transparency, efficiency, and privacy. By leveraging the decentralized and immutable nature of blockchain, banks can create a robust and trusted ecosystem that protects transactions without the need for tokens. While challenges exist, the benefits of blockchain technology make it a promising solution for the future of banking.

7. REFERENCES

[1] Ms Supriya Maglekar, Dr. Dinesha H.A., “Block Chain: An Innovative Research Area” FOURTH International Conference on Computing Communication Control and Automation (ICCUBEA) Year:- 2018

[2] Yaguang Wang, Aina Su, Wenlong Fu, "Research on Image Retrieval Technology Based on Image Fingerprint and Color Features", 978-1-5090-0654-0/16/$31.00 ©2016 IEEE

[3] Jasmine Joeph, Anu Chalil, Gawtham G Dath, "Publicly Verifiable Digital Watermarking

[4] Technique for Copyright Property Protection", Proceedings of the International Conference on Communication and Electronics Systems (ICCES 2018) IEEE Xplore Part Number: CFP18AWOART; ISBN:978-1-5386-4765-3 Year: - 2018

[5] Brian A. Scriber, CableLabs, "A Framework for Determining Blockchain Applicability", Published by the IEEE Computer Society Year:-2018

[6] Arpita Nayak, Kaustubh Dutta, "Blockchain: The Perfect Data Protection Tool", International Conference on intelligent Computing and Control(I2C2) Year:-2017

[7] XUE Feng, SHI Xue-fei, "The Copyright protection about digital images based on web", International Conference on Communication Systems and Network Technologies Year: -2013

[8] Harry Halpin, Marta Piekarska, "Introduction to Security and Privacy on the Blockchain", EuroS&P 2017 - 2nd IEEE European Symposium on Security and Privacy, Workshops, Apr 2017, Paris, France. IEEE, Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on, pp.1-3, 2017, 10.1109/EuroSPW.2017.43. hal-01673293 Year: - 2017

[9] Huaiqing Wang, Kun Chen and Dongming Xu, "A maturity model for blockchain adoption", DOI 10.1186/s40854-016-0031-z Year: - 2016

[10] Chaw-Seng WOO, "Digital Image Watermarking Methods for Copyright Protection and Authentication," PhD thesis, Queensland University of Technology, March 2007

[11] Alexander Savelyev, "Copyright in The Blockchain Era: Promises and Challenges", National Research University Higher School of Economics (HSE), Basic Research Program Working Paper, 2017.