# A Secure and Flexible Blockchain Based Decentralized Transaction Online Payment Protocol.

Prof.S.B. Nazirkar[1],Aditi Tantak[2] , Komal Halnor[3] , Shraddha Gadekar[4] [1]Asst. Prof. of Department of Computer Engineering, &[2, 3,4] PG Students
Sharadchandra Pawar College of Engineering and Technology, Someshwarnagar, Pune
email address : [1] nazirkar33piyou@gmail.com, [2] adititantak21@gmail.com, [3] komalhalnor9@gmail.com, [4]shraddhagadekar333@gmail.com

**Abstract— This paper proposes a secure and flexible blockchain-based decentralized online payment protocol designed to enable fast, transparent, and low- cost transactions while maintaining user privacy and scalability. The protocol leverages a hybrid blockchain model combining public and private chains to enhance decentralization and transaction speed. It utilizes smart contracts for automated payments, tokenization for multi-currency support, and off-chain payment channels for scalability. Key security features include multi-signature wallets, encryption, and privacy protocols like zero-knowledge proofs. The solution supports seamless integration with existing payment gateways and cross-chain interoperability, offering a scalable, secure, and user- friendly system for decentralized online payments.**

**Keywords— Blockchain, Transaction, Security system, Privacy, Verification system, Banking Security, Online Payments, Bitcoin, Smart contract, Protocol.**

## I. INTRODUCTION

Blockchain is a compelling technology that is getting into every industry from banking, medicine to government sector. Because of security concern banking domain mostly use blockchain technology. The Indian banking system is the most complicated bank payment system in this world. It is based on real time gross settlement system Which follows a central server mechanism where all the personal information of account holders, bank balance, and all necessary information related to bank are stored. All branches of bank are connected to central server from which every branch retrieves personal information, bank balance and history of a customer from the server itself. Failure or modification in the central server causes all banks to fall down which results in great loss and causing large amount of processing time and cost. Considering all the issues of the current centralized banking system, the proposed blockchain based decentralized mechanism will provide a banking system in a cost efficient and secure way. [1].

Payment channels stand as a significant con tributary factor to the development of solutions towards layer-2 blockchain scalability issues. Payment channels would have been more relevant if they did not require to open on-chain settlement transactions (by locking up a chosen amount of cryptocurrency as a security deposit) and were not vulnerable to random failures and targeted attacks channel exhaustion and node isolation attacks. In this paper, we hypothesize that two offline parties, which experience intermittent on-chain connectivity, can engage in blockchain-based transactions without sacrificing security and flexibility: we introduce a

secure and flexible protocol that realizes online payments in blockchain-based solutions.[2].

Blockchain technology helps in the development of a decentralized network where transactions are tracked and managed in the distributed ledger. Such characteristics of blockchain make it possible for various financial applications in terms of security and also reduce paper dependence. Therefore, the main aim of this article is to develop a proto col for financial data processing with secured routing and intelligent learning capabilities. It offers a machine learning- based solution to learn the nodes' information from the neighbors' tables and store the updated information in its memory. Moreover, blockchain technology in the proposed protocol increases the reliability of financial data when it is transmitted on insecure devices. [3].

The demand within societies, for technologies related to the public interest, is increasing. Both government and private-sector concerns put in a critical position technology that can promote social change and bring public benefits. There are even programs and initiatives related to public interest technology inside for-profit corporations. As a part of the function of technology, public interest also shows its value. State governments and citizens' collective actions can shape a social inclination of technological development toward the public interest. Bruce pointed out that society needs a group of scientists with public interest values. Such a group would combine technological expertise with a general interest focus through policy making, executing tech projects for public profit, and a traditional technologist for an organization with a public benefit. [4].

This paper presents a survey of secure and flexible blockchain-based decentralized transaction protocols designed to address the inherent limitations of conventional payment systems. The protocols explored in this survey combine various blockchain innovations, including hybrid architectures, smart contracts, off-chain solutions, and privacy-enhancing techniques like zero- knowledge proofs, to enable fast, secure, and cost- effective online payments. The goal of this survey is to explore how blockchain can redefine the landscape of online payments, offering a more secure, transparent, and accessible framework for both consumers and merchants.

The rapid growth of digital payments has highlighted the inefficiencies, security risks, and high costs associated with traditional centralized payment systems.

## II. SYSTEM ARCHITECTURE

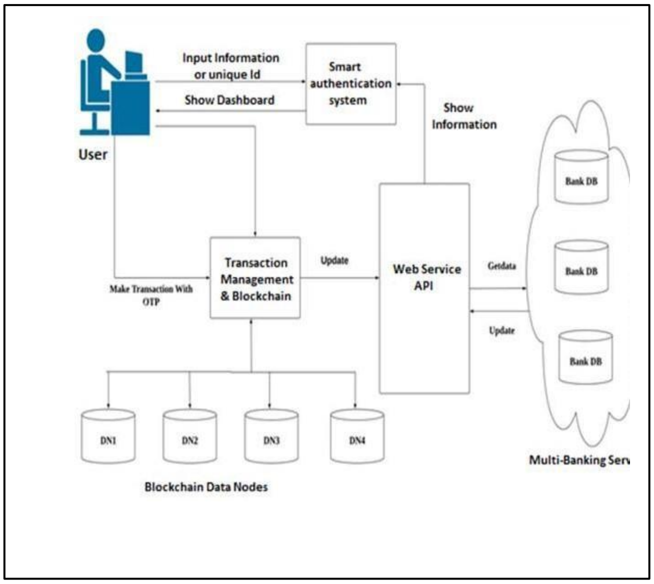

Fig. System Architecture

### A. Blockchain Architecture

The Anatomy of the Blockchain architecture: The blockchain architecture consists of a few fundamental concepts like decentralization, digital signature, mining and data integrity.

• Decentralization: Rather than one central authority overpowering others in the ecosystem, blockchain explicitly distributes control amongst all peers in the transaction chain.

• Digital signature: Blockchain enables an exchange of transactional value using public keys by the mechanism of a unique digital sign i.e. code for decryption known to everyone on the network and private keys known only to the owner to create ownership.

• Mining: In a distributed system every user mines and digs deep into the data which is then evaluated according to the crypto graphic rules and it also acknowledges miners for confirmation and verification of the transactions. • Data integrity: Complex algorithms and agreement among users ensures that transaction data, once agreed upon, cannot be tampered with and thus remains unaffected. Data stored on blockchain acts as a single version of truth for all parties involved hence reducing the risk of fraud.

## III. METHODOLOGY

This paper surveys the design and methodology of a secure and flexible blockchain-based decentralized payment protocol Smart contracts automate transactions, while off-chain solutions like state channels enhance scalability and reduce fees. Privacy is ensured through techniques like zero- knowledge proofs and multi-signature wallets, and cross- chain interoperability allows for multi-currency support. This approach offers a secure, cost-effective, and scalable solution for decentralized online payments.

### A. Flowchart

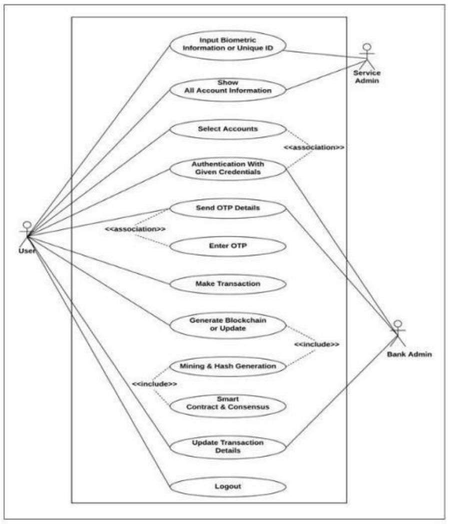
Input Biometric Information or Unique ID
Show All Account Information
Select Accounts
<<association>>
Authentication With Given Credentials
Send OTP Details
<<association>>
Enter OTP
Make Transaction
Generate Blockchain or Update
<<include>>
Mining & Hash Generation
<<include>>
Smart Contract & Consensus
Update Transaction Details
Logout
User
Service Admin
Bank Admin

**Figure 5.4:** Use case diagram

The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted. So in below Diagram, We have represented how User will Intact with the system and which type type of actions he can Do and How System will React as per his action.

## V. ADVANTAGES

• Enhanced **Security**: Blockchain's cryptographic nature ensures secure transactions, reducing fraud and data breaches.

• Decentralization: Removes intermediaries (e.g., banks, payment processors), reducing costs and improving transaction speed.

• Transparency: All transactions are recorded on a public ledger, offering transparency and auditability.

• Improved **Privacy**: Blockchain protocols can maintain user privacy while ensuring secure and verifiable transactions.

• **Reduced Transaction Fees**: Without middlemen, transaction fees are significantly lower compared to traditional payment systems.

• **Global Accessibility**: Blockchain-based payments can be made across borders without relying on currency exchange or national financial systems.

## VI. CONCLUSION

The main goal of this paper was to determine whether two offline parties can proceed with blockchain-based offline payments without sacrificing security and flexibility. Our work shows that there is a definite need for secure and flexible offline payment solutions that improve the user experience and widen the adoption of blockchain technology.[2]. Current banking system is based on the centralized architecture which can't handle the digital revolution happening. The proposed method is designed for implementing a decentralized banking system by adopting blockchain on existing banking infrastructure.[1]. This work proposed a protocol using machine learning techniques and integrating blockchain technology to increase financial security.[3].

## VI. REFERENCES

[1] Sincy Joseph and Smitha Karunan, "A Blockchain Based Decen tralized Transaction Settlement System in Banking Sector," Open Access IEEE Transaction (2021).

[2] Wanqing Jie and Wangjie Qiu, * A Secure and Flexible Blockchain- Based Offline Payment Protocol*, Senior Member, IEEE, and Zhiming Zheng, 2024.

[3] Tanzila Saba, Khalid Haseeb and Gwanggil Jeon " Blockchain- Enabled Intelligent IoT Protocol for High-Performance and Secured Big Financial Data Transaction" , VOL. 11, NO. 2, APRIL 2024.

[4] Chengmeng Zhang,Wenqing Yu, Haoyu Suo, and Gong Chen"Blockchain in the "Time Bank: Toward a Community-Oriented Public Interest Technology" VOL. 2, NO. 2, JUNE 2021

[5] Mohamed Baza, Noureddine Lasla, Mohamed Mahmoud, "B-Ride: Ride Sharing with Privacy-preservation, Trust and Fair Payment atop Public Blockchain," DOI 10.1109/TNSE.2023

[6] M. Xu, C. Liu, Y. Zou, F. Zhao, J. Yu, and X. Cheng, "wChain: A fast fault-tolerant blockchain protocol for multihop wireless networks," IEEE Trans. Wireless Commun., vol. 20, no. 10, pp. 6915–6926, Oct. 2021.

[7] N. Ying and T. W. Wu, "xlumi: Payment channel protocol and off- chain payment in blockchain contract systems," 2021, arXiv:2101.10621.