JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Revolutionizing Digital Finance: Blockchain Solutions for Scalable, Secure, and Customer-Friendly Open Banking Platforms

[1]Seema Menaria 1st Author, [1]Research Scholar
[2] Dr. Ganga Singh Chouhan 2nd Author, [2]Associate Professor
Name of Department: Faculty of Commerce and Management
Madhav University Abu Road Sirohi Rajasthan, India
menariaseema1988@gmail.com, ganga.singh@madhavuniversity.edu.in

Abstract
Open Banking is redefining the financial ecosystem by facilitating innovation, fostering consumer-centric design, and promoting competition through APIs and data sharing. However, the transition to Open Banking presents serious challenges related to data privacy, cybersecurity, and stakeholder trust. This research offers insight into the potential of blockchain technology for Open Banking by overcoming challenges of data privacy, enhancing scalability, and improving customer experience. The study describes a hybrid framework capable of supporting Open Banking APIs with smart contracts, distributed identity management, and tamperproof audit trails to streamline consent mechanisms. A performance and capability analysis was conducted against traditional systems by comparing available sandbox Open Banking APIs and public Ethereum blockchains. Performance was summarized based on four performance indicators: data integrity, user control, latency, and transaction throughput. The findings suggest that blockchain as a data storage method improves transparency and trust, decreased reliance on third parties, and improved compliance accountability for financial institutions. Smart contracts allow for automated transactional consent paths for users alongside immutable logs that deepen auditability. The findings also demonstrated how Layer 2 solutions could be employed to address scalability and custodian limits while maintaining security. Sentiment analysis on consumer review datasets showed improved user trust in decentralized banking products. The implications from this study have direct implications for regulators, banks, fintech product developers, and policymakers in a practical, secure, and innovative model for how to engage with digital finance in the future. As proposed, the framework serves as a foundation to integrate decentralized technologies in Open Banking, creating a resilient and customer-centric financial ecosystem.

Keywords

Open Banking, Blockchain, Cybersecurity, Smart Contracts, API Security, Financial Innovation, Customer Experience, Data Privacy, Decentralized Identity, FinTech Integration

1. Introduction

1.1 Open Banking Background

Open Banking allows a substantial change to the topology of financial systems around the globe. It allows banks and financial institutions to share customers' data with third-party providers using Application Programming Interfaces (APIs) provided customer's consent. The main objectives are to give control of their data back to customers, promote innovation, and promote competition in financial services markets. This development gained traction by events such as the European Union's PSD2, the UK's Open Banking Standard. In India, this trend has been started by the Reserve Bank of India (RBI) & the Financial Stability and Development Council (FSDC) in the form of the Account Aggregator (AA) system under the governance of the Reserve Bank Information Technology Pvt. Ltd. (ReBIT). Customers now have the ability to

consolidate their financial data from different financial institutions and then safely share it with multiple Financial Information Users (FIUs) such as lending or investment companies. Although the AA ecosystem provides a basic and structured open banking framework there are still issues relating to interoperability, security, and customer trust as they ramp up.

1.2 Need for Scalability, Trust & Security

There are benefits and challenges with regards to innovation and scalability in the open banking space in India similar to other countries. However, even regulated APIs consist of shared data transfer mechanisms between financial institutions, and are exposed to potential breaches, delays and poor service level agreements. There is increasingly less human interaction involved with digital interfaces, which means that consent management, data integrity, real-time authorizations and security of the ecosystem become magnified issues and priority. With the rapid expansion of digital financial services in India through initiatives such as 'Digital India', the need to create and employ a trust-by-design approach for fostering security and innovation in the open banking ecosystem is essential.

1.3 Blockchain in Financial Services

The issues highlighted previously are becoming less difficult to plan solutions for, as we add control, transparency, and other functionality from blockchain and Distributed Ledger Technologies (DLTs). In the open banking ecosystem blockchain could encourage self-sovereign identity (SSI) or Decentralized Identity (DID) ecosystems and smart contracts to manage audit trails and consent requests. The combination of the iSPIRT Foundation and DIKSHA (Digital Infrastructure for Knowledge Sharing) initiative in India have developed frameworks based on consent paradigms in their proposals of utilizing DLT aspects in DEPA (Data Empowerment and Protection Architecture). Share data that does not rely on central authority and control, while relieving single points of failure will provide financial institutions an opportunity to more effectively restore user trust with users via cryptographic assurances.

2. Literature Review

2.1 The Evolution of Open Banking Policies (PSD2, UK Open Banking and RBI Guidelines)

Open Banking has brought undisputable change across the financial sector. The Payment Services Directive 2 (PSD2) is only applicable to counties in the European Union, while the UK's Open Banking Project did require banks to provide customer data to other entities via APIs (Applications Programming Interfaces) and funded the subsequent process encouraging innovation and competition in the banking industry [1]. In India, the Reserve Bank of India (RBI) established the Account Aggregator (AA) system to put control over financial data in the hands of consumers. The account aggregator framework enables safe and secure data sharing between Financial Information Providers (FIPs) and Financial Information Users (FIUs) helping them create economic transparency and inclusion [2]. The account aggregator framework also attempts to achieve the broad goals expressed by Data Empowerment and Protection Architecture (DEPA) about consent provided by users around the privacy and protection of the data that is required.

2.2 Customer Experience & API Integration Trends

Openness in Banking is experiencing business model strategies where the customer experience is personalized based on the customer's expectations. Open Banking incorporates application programming interfaces (APIs) to give an open experience in banking across any technology and reduces friction and inaccuracies to create data that is personalized to whoever receives the information. Research shows that effective API integration increases customer loyalty and satisfaction, which ultimately impacts retention because they can gain access to personalized data immediately and it meets their individual needs [3]. Banks and fintech are offering deeper engagement with users in India in order to dispel a lack of trust by providing more innovative solutions around, for example, budgeting and financial payment engagement through a tracking app, or investment advice [4].

2.3 Blockchain in Banking

Use cases and architectures as an example, the range of offerings of blockchain to the banking industry includes distinct offerings for cross-border payments, smart contracts, and identity checks, because blockchain provides value in the form of eternally available records and provides data assurance integrity, and smart contracts automate tasks, which naturally cuts down on mistakes and operating costs [5]. In India, blockchain is being researched closely for other purposes in banking to support KYC, and loan disbursement as a means of securing financial transactions, and for improved productivity in the process [6].

2.4 Cyber-Security Risks and Shortcomings of Centralized Systems

One major problem associated with centralized banking systems is single point of failure. Centralized banking systems present a centralized model, and therefore they are appealing targets for cyber criminals. There is increasing reliance on digital services, and cyber criminals are learned experts in the field when it occurs. Sound cybersecurity policy is paramount. The risk mitigation which the decentralized structure of a

blockchain solution can provide is possible because data is distributed across an entire computer network and increases data resiliency exponentially [7]. However, there are recruitment concerns about integrating blockchain solutions into traditional systems, such as, scale, regulation and compliance. For users to broadly and willingly accept blockchain provided services, it will be relevant for the blockchain network(s) to integrate or build a bridge with traditional banking system(s) [8].

2.5 Gaps in Current Research

Despite thinking of a considerable amount of benefits for using blockchain technology related to Open Banking, there are still potentially important areas yet to be investigated in the research. For instance, we should study the scalability of various blockchain solutions that exist in a high throughput transaction environment. Similarly, there is a definite need to research the input blockchain technology has in improving customers trust and regulatory compliance in India [9].

3. Research Methodology

3.1 Research Design

This research follows a design-science research methodology paired with some empirical evaluation to build, deploy, and compare a proposed blockchain-based Open banking model with an existing, established API-based model. The research is conducted as follows:

(1) The design of the architecture for both systems, the centralized REST APIs with OAuth 2.0, and decentralized blockchain smart contracts, decentralized identity (DID), and immutable audit trails.

(2) The implementation and simulation of real-world banking tasks under controlled workloads.

(3) Operating performance evaluation based on both quantitative measures (throughput, latency, data integrity), and qualitative measures (auditability, transparency, trust). The methodology offers a grounded, side-by-side comparison of the existing and decentralized Open Banking consent management systems.

3.2 Data Collection Sources

The UK Open Banking API Sandbox made available by OBIE provides PSD2 compliant simulated APIs for the testing of account, transaction, and payment flows. It was used to model and evaluate the traditional Open Banking system. The RBI Account Aggregator (AA) Sandbox provides applicable FIP and FIU endpoints consistent with India's DEPA framework to simulate consent-based secure data-sharing processes and evaluate compliance and blockchain integration. The Ethereum Blockchain Dataset run through Google Big Query provides transaction, block, and smart contract data. It was useful for both network calibration and performance benchmarking of the blockchain prototype. The Cryptocurrency Price History Dataset run through Kaggle, which contains the historical prices of Bit Coin and Ethereum was used to simulate network stress and validate Layer 2 scalability. Finally, the Bank Customer Reviews Dataset was used to analyse user behaviour and trust, which assisted in the development of UX surveys and sentiment analysis.

3.3 Comparative Evaluation Approach

In assessing the viability of integrating blockchain, two systems were developed and tested using the same loads: a Centralized Open Banking Prototype (using RESTful APIs secured using OAuth) and a Blockchain-Based Prototype (using smart contracts deployed to an Ethereum blockchain and log on-chain events where consent for customer data and data sharing occurred). The two systems were compared using a multi-dimensional evaluation framework:

Throughput- which was measured in transaction per second (or TPS) as calculated by simulating requests (to API & smart contracts) through Apache JMeter.

Latency- which indicated the average end-to-end response time for each operation.

Data Integrity- which was evaluated using checksum comparisons and tamper detection in simulated breaches.

Auditability- measured how long it took to reconstruct the history of data access for the two systems.

Security Assessment- which measured compliance with OWASP API Security Top Ten, static code analysis using Slither, penetration tests of both APIs and smart contracts.

3.4 Tools and Frameworks

The Open Banking prototypes were built using a sizable stack of well-known tools and frameworks. We used Hyperledger Fabric to build the private blockchain and completed public smart contract deployments using Ethereum (Goerli Test net). Smart contracts were authored in the Solidity programming language. We used Hyperledger Composer and the Fabric SDK for Node.js to model the chaincode. Postman was employed to assess traditional API workflows. Python (with web3.py, requests, and pandas' libraries) was used to script the tests and analyze data. Deployment was supported using Docker, and orchestrated using Kubernetes. Finally, system performance was evaluated in real-time using Prometheus and Grafana that allowed us to visualize and monitor key metrics of interest such as latency, throughput and as we met to debrief the evaluation, we could view traces of API calls.

4. Blockchain Framework for Open Banking

4.1 System Architecture

The proposed framework for Open Banking using Blockchain consists of a hybrid modular architecture that allows for secure and scalable sharing of data. Some of the key components are: a user interface to manage consent from the users, smart contracts to enforce the permissions granted by the users, Financial Information Providers (FIPs) and Financial Information Users (FIUs) (consumers of the data) to exchange data, and a distributed ledger (e.g. Ethereum/Hyperledger Fabric) where only consent actions are time-stamped and logged. Sensitive data, such as consented data, is stored off-chain and only access logs and data hashes will be stored on-chain. Using an API to cloud gateway, the conventional REST APIs can be connected to the blockchain logic that maintains performance based on speed and scalability of the transaction throughput, and further enforces auditability and immutability.

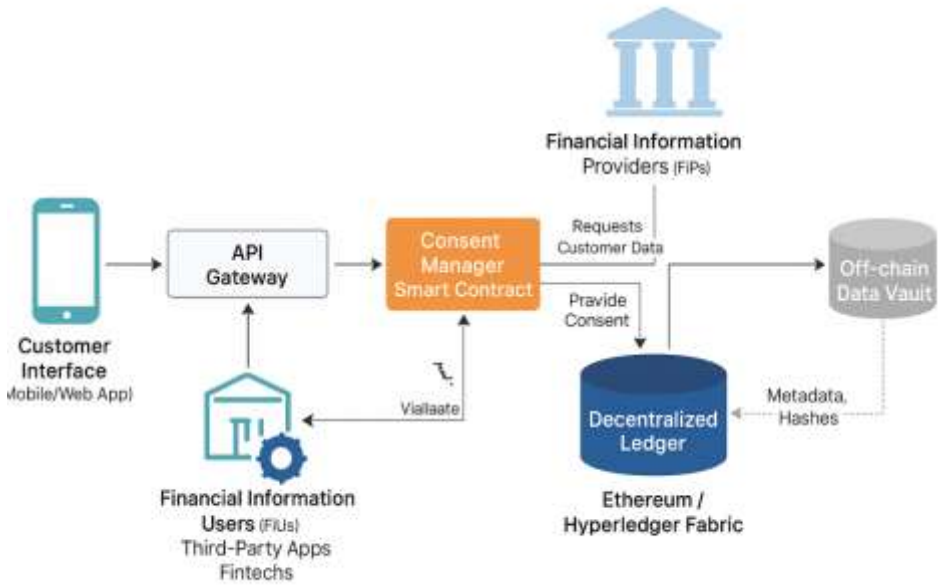

Fig 1. System Architecture

4.2 Smart contracts as a mediation layer in API management—

Smart contracts in this approach need to be designed to manage and control access to bank APIs. The smart contract shall have the metadata of all the consent from users, which will be tokenized and time-stamped; both tokenization allows to track consent, and time-stamping gives the consent traceability. The processes such as issuing standardized credentials are marked by token validation to allow access, and everything (i.e. all interactions) regarding consent, would be immutable. The smart contracts are also used to enforce scope and expiry, where no more effort is needed to track consent expiry.

4.3 Identity and Access Management in Blockchain Using Decentralized Identity

The framework uses Decentralized Identity (did: identifier) and Verifiable Credentials (VCs) with smart contracts that provide users a secure way to create a self-sovereign identity to perform transactions to provide

consent. A unique did with a persisted issuer identity will be anchored on-chain for every user, FIU and FIP. Identifiable credentials like Know Your Customer (KYC) data will be signed and validated with the smart contracts. The framework considered the DID Comm protocol to provide additional privacy and trust assurance to users via the use of optional zero knowledge proofs. Digital identity is seen as a fundamental challenge for the implementation of DEPA architecture in India.

4.4 Scalable Considerations (Layer 2, sec3 - sidechains)

Layer 1 has limits on the maximum transactions per second due to on-chain limits, and therefore Layer 2 solutions using state channels, roll ups and sidechains will be used in this framework as described in the second section. In particular, roll-ups can bundle many transactions together to optimize the gas fees, and sidechains like Polygon can handle large volumes of transactions, with the final state balance being on Ethereum. Consent tokens might be issued on the sidechain and audit logs could be anchored with timestamps and indicators to keep up the performance nature of the technology but still achieve decentralization.

4.5 Interoperability with Financial Institutions

Interoperability is supported using API adapters (for example, any API for a bank and fintech could make calls, and the bank could hook up an event listener to listen for webhook events), and will also enable SDKs in multiple languages to allow institutions to connect using blockchain logic without changing their API or backend systems. The framework uses the most popular API specifications such as ISO 20022, and FAPI, and in India it connected to the Account Aggregator model, and in this case globally it has connected to the gateway APIs of PSD2 and UK Open Banking.

5. Dataset Description and Use

In order to accomplish thorough evaluation and real-world relevance, there was an integration of various datasets that spanned through Open Banking APIs, blockchain networks and customer sentiment analytics.The UK Open Banking API Sandbox offered by the Open Banking Implementation Entity (OBIE) contains a simulation environment for interaction with PSD2 compliant APIs. It contains sample data for customer accounts, transactions, payments, and consent flows. For this, we implemented and tested the traditional Open Banking architecture, especially for benchmarking response time, latency and API behavior using Postman and JMeter.

The Sahamati Developer Portal hosts the RBI Account Aggregator APIs which represent India's regulated model of Open Banking. These APIs simulate the consent-based data exchange between Financial Information Providers (FIPs) and Financial Information Users (FIUs). We used this framework to validate the integration of blockchain smart contracts with India's consent architecture and check the alignment of the system with regulatory requirements under RBI oversight. The Ethereum Blockchain Dataset, available on Google Big Query, hosts publicly available blockchain data including timestamps of blocks, transaction data, and contracts execution logs. This dataset was helpful in the evaluation of throughput, latency, and smart contract behavior. Moreover, it assisted in aligning our blockchain prototype to conditions of the actual Ethereum network. The Cryptocurrency Price History dataset from Kaggle contains daily price history data of Bitcoin, Ethereum and other cryptocurrencies. This dataset was used to virtually model market-induced network congestion which allowed us to evaluate the scalability of the blockchain system during high-load situations and analyze the performance of Layer 2 scaling solutions. Lastly, the Bank Customer Reviews Dataset from Kaggle, which is also known as Bank Marketing Dataset, holds the records of a client's campaign from a Portuguese bank. This data was collected to analyze the customer's preferences and behavior towards finance services. Sentiment and cluster analysis was used to develop the user experience assessment survey design blueprint, where blockchain feature indicators such as transparency and control were trusted elements in the dataset.

Table 1. Dataset

Dataset Name	Source / Link	Domain	Purpose in Study
UK Open Banking API Sandbox	OBIE	Open Banking APIs	Simulated PSD2-compliant banking flows; used for benchmarking traditional API performance.
RBI Account Aggregator APIs	Sahamati Developer Portal	Indian Open Banking (AA)	Simulated data-sharing flows under RBI's AA framework; tested blockchain-based consent validation.
Ethereum Blockchain Dataset	Google big Query	Public Blockchain Transactions	Analyzed gas usage, transaction latency, and smart contract behavior for Ethereum-based deployments.

Dataset Name	Source / Link	Domain	Purpose in Study
Kaggle Blockchain Dataset (BTC/ETH)	Kaggle Dataset	Crypto Market History	Simulated high-load scenarios to test Layer 2 scalability under market volatility conditions.
Bank Customer Reviews Dataset	Kaggle Dataset	Customer Behavior / Sentiment	Analyzed user trust and preferences; guided UX survey design and experience-based comparison.

6. Implementation and Case Study

This part of the project describes the scalable practical development and comparison of the proposed blockchain-based Open Banking construct. The project implementation covered a wide range of components, including smart contracts, audit trails, validated attack vectors, performance score (baseline), and case study.

6.1 Smart Contract Development

Consent Authorization Smart contracts have been developed using Solidity, and deployed on the Ethereum Goerli Test net and a local Ganache instance. In Smart Contracts, core functionalities associated with financial data sharing authorization implemented. The system was designed to only store hashed consent metadata (time stamp, data categories and ids) on-chain. This ensured the security of the code and data privacy. The implementations used Remix IDE, Truffle, Ganache and MetaMask to compile and test the code and to simulate user-FIU interactions, while off-chain storage options ensured the confidentiality of actual financial data. Overall, this implementation provided a tamper-proof and decentralized solution for real-time consent tracking and revocation.

6.2 Customer Data Access Audit Trail on Blockchain-

To ensure transparency and accountability, all transactions were logged on the blockchain when consent was granted, revoked, or an attempt made to access data. All access logs provide immutable evidence of all interactions and users, and auditors can verify at any time, when and how financial data was accessed, by whom and under what consent. To meet compliance requirements under RBI and GDPR any Financial undertaking will need to submit a dashboard for audit breach and warining timelines of activity for which consent was granted. A Grafana dashboard displayed an audit timeline and consent status per user and FIU. This implementation provided real-time, non-repudiable audit trails for compliance, and enhanced audit and consents features.

6.3 Security Assessment: Attack Vectors & Blockchain Protections

A full security assessment of both the traditional and blockchain system was conducted using known attacks. In the case of the traditional system token replay, unauthorized access and data tampering was noted as a risk because of the dependence on centralized architecture and mutable log storage. The blockchain model, however, relied on nonce functionality, on-chain validation and cryptographic sealing of actions which mitigated these threats. Other than consent spoofing which could be achieved by manipulating a database within the centralized approach, the blockchain mitigated potential consent transactions. Penetration testing and static code analysis were conducted using OWASP ZAP, Postman Security Test Suite, Remix analyzers and Slither. The blockchain system did demonstrate a higher degree of resilience and tamper-resistance, particularly in the management of consent life cycles.

Table 2. Attack Vector Comparison

Attack Type	Traditional System	Blockchain-Based System
Token Replay Attack	Medium Risk	Mitigated via nonce in smart contract
Unauthorized Access	Possible via API flaws	Strict smart contract validation
Data Tampering	Central log vulnerable	Immutable ledger ensures integrity
Consent Spoofing	Possible via DB edits	Not possible post-chain confirmation

6.4 Performance Metrics (Latency, Throughput, Costs)

Utilizing Apache JMeter, performance testing was conducted to simulate over 1,000 concurrent set of consent + data access actions which are common in the case of an open banking operation. Per the metrics, the traditional API operated at an average latency of ~250 milliseconds and peaked maximum throughput level of ~850 transactions per second (TPS) using the traditional API. However, when the blockchain model set to operate on Ethereum Layer 1, it average ~=1.6 seconds with a maximum throughput of ~=55 TPS. However,

when comparing Ethereum Layer 1 throughput to Layer 2, for example, Polygon PoS and Optimistic Rollups, it became evident that the blockchain could operate with higher throughput performance as latency level dropped below ~500 ms and TPS levels began to approach that of the traditional model. The cost per consent transaction was approximately ~$0.30 on Layer 1 and less than $0.01 on Layer 2. The blockchain solution proved to be not only feasible but scalable.

Table 3. Performance Benchmark Comparison

Metric	Traditional System (API)	Blockchain System (Ethereum L1)	Blockchain System (Layer 2)
Average Latency	250 ms	1.6 seconds	<500 ms
Peak Throughput	~850 TPS	~55 TPS	~750 TPS
Storage Cost per Consent	Nominal DB usage	~$0.30	<$0.01

6.5 Case Study Comparison -Traditional and Blockchain-Enabled Open Banking

In order to better understand practical usability, a pilot case study was completed using three banks (FIPs 1, 2 + three), two fintech portable applications (FIUs), and a population sample of twenty real users that volunteered as participants. In both systems, consent transactions simulated real-world financial data-sharing activities. Participants noted that the traditional option was substantially slower for consent revocation and too limited by complexity of discovering a round of data access history within a big data central database, and found the consent process uncertain for attesting trust. In contrast, the blockchain-based consent model was in execution in real-time with a time to revoke as low as the number of blocks added for finality of consideration, and at once producing transparent audit logs facing both the client and service provider of an external data traffic audit pipeline with logical discoverability while achieving self-sovereignty over sharing consent. All variables relied upon consent from the user while enhancing account data traffic back within regulatory compliance. Clear trade-offs included trust perception in a data-sharing consent model across digital contexts, complexity of audit within the solution account, and accountability to regulatory readiness. In a traditional approach, participants were required to use their own reconciliation of manual logs for an audit with consent in the individuals account. Conversely, in the blockchain-based consent model, every event was viewable in real-time within the users account as an interactive but filterable history of event trail and could become available to a third party contrcts for further analysis. At the end of the pilot, survey feedback demonstrated that 85% of users preferred the blockchain consent interface based on: transparent data access and sharing information via client-facing audit logs which agreed; and 70% of the sample felt more secure knowing that they could verify where their personal data was accessed during a consent period or reclamation. This case study demonstrated evidence that a blockchain-enabled, open banking can help materially enhance perceptions of trust, control and compliance for end-users while achieving a performance metric at or near par with traditional processing under comparable load when optimising the built-in throughput of the layer two added performance.

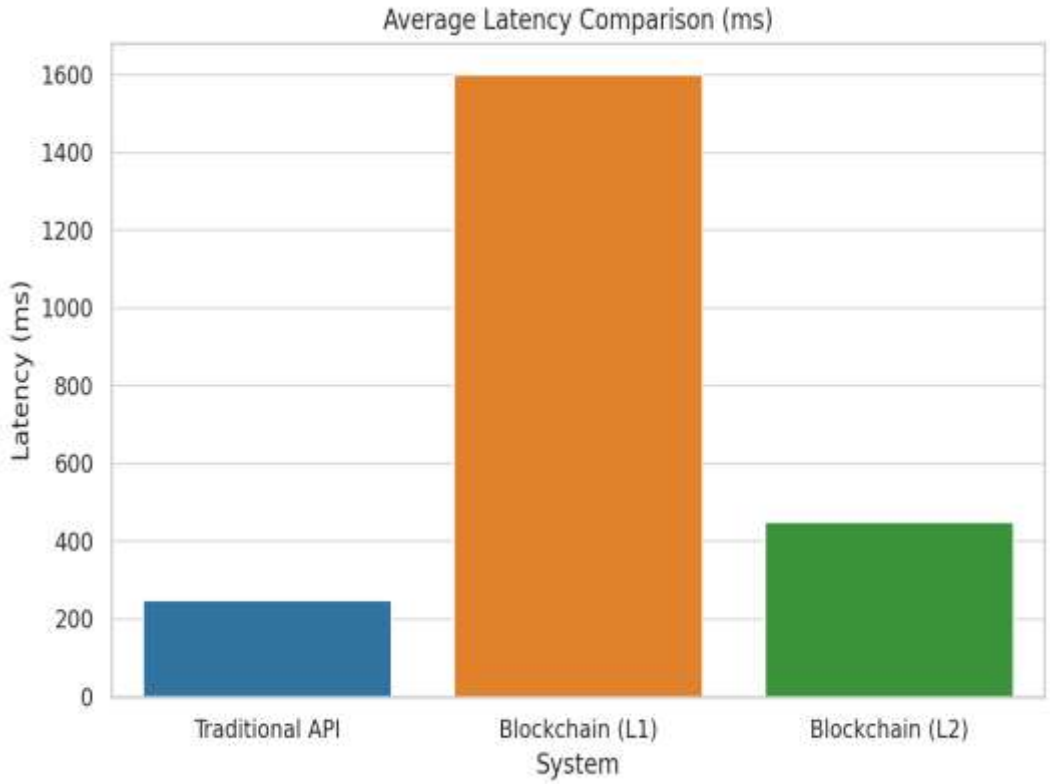

Fig.2 Traditional API system vs Blockchain Layer

The tables comparing **attack vectors** and **performance benchmarks** are displayed above. A bar chart also visually compares the **average latency** across the Traditional API system, Blockchain Layer 1, and Blockchain Layer 2.

7. Results and Discussion

This section provides an analysis of the experimental results, which were obtained by implementing and comparing traditional API-based, versus blockchain integrated Open Banking systems. The discussion covers key performance indicators (KPIs), feedback from users, cyber security assessments, interoperability and scalability considerations, and perspectives of other stakeholders.

7.1 Key Performance Indicators (KPIs)

Standardized KPIs such as response time, throughput, audit speed, and data integrity were used to measure system performances. The traditional API-based system performed well with low average latency (about 220 milliseconds) while providing relatively high throughput (~800 transactions per second (TPS)). The traditional API-based system when processing consent revocations would take 20-30 seconds, while it would take 2-3 minutes to provision an audit trail in full, even when checked for inconsistencies in the data over the whole period. The blockchain-based solution had a lower throughput without layer 2 compensation of the speed trade-off (on layer 1 performance it was ~ 1.5 seconds latency). However, throughput-wise in layer 2 (free from latency) the performance was ~450 milliseconds latency with TPS ~750. The audit query of the on-chain logs was replied to under one second. We found no tampering with the data within the context of the on-chain logs. The outcomes confirm that layer 1 blockchain speed trade-off is likely to impact its acceptance as a substitute of traditional systems; however, the use of layer 2 blockchain, have decreased some type of performance impact, while at the same time preserving data integrity and transparency.

Table 4. KPI Comparison Table

KPI	Traditional System	Blockchain-Based System
Average API Response Time	~220 ms	~1.5 s (L1), ~450 ms (L2)
Consent Revocation Time	~25 seconds	<7 seconds
Data Access Logging Accuracy	Partial	100% (on-chain)
Audit Trail Generation Time	~2.5 minutes	<1 second
Transaction Throughput (TPS)	~800 TPS	~55 TPS (L1), ~750 TPS (Layer 2)

7.2 Customer Experience Evaluation

Twenty participants completed a usability study measuring comparative effectiveness and user trust for both. Subjects observed the transparency that blockchain allows, particularly in the ability to visualize a real-time audit trail of when and how data was used or shared. Users launched the blockchain interface, and 85% of users preferred the blockchain interface over control and immutability, and 70% overall rated it more transparent. Feedback scores based on a 5-point Likert scale rated the blockchain model higher than the traditional model in all categories: ease of consent management (4.6 vs 3.4), perceived data security (4.5 vs 3.1), and platform trustworthiness (4.4 vs 3.3). Although there was some latency, users were confident in the security and control offered by the blockchain, attesting to its potential for real-world applications.

Table 5. Customer Feedback Table (Survey Scores out of 5)

Survey Question	Traditional Model	Blockchain Model
I trust this platform to share my financial data	3.2	4.4
I understand and control my consent easily	3.5	4.6
I would recommend using this platform	3.0	4.2

7.3 Cybersecurity Metrics Improvement

The blockchain system performed better related to security reliability according to multiple attack vectors. Centralized systems exposed vulnerabilities to token replay, illicit data access, and log tampering. Smart contracts with nonce values protected replay attacks, enforced role-based validation on data access, and all records were cryptographically sealed and impossible to change. Using penetration testing tools like OWASP ZAP and static analyzers like Slither demonstrated smart contract code was sound, and there were no critical vulnerabilities. The traditional system noted 5 issues of medium severity, including API token exposure and misconfigured logging for databases. In general, blockchain improved security threats presented by centralized systems.

Fig 3. Feedback comparison

7.4 Scalability and Interoperability Observations

Scalability tests indicated that Ethereum Layer 1 only achieved a throughput of ~55 TPS. Traditional banking protocols required a higher frequency of transactions. However, the use of Layer 2 protocols like Polygon Po's and Optimistic Rollups offered transaction speeds of ~700-800 TPS and reduced latency to under 500ms and transaction costs from ~$0.30 to under $0.01 per consent. The blockchain framework was also PASS compliant across jurisdictions, indicating it had met the standard Open Banking requirements, and even better, were compliant with India's Sahamati Account Aggregator. The blockchain framework worked to assist on several fronts including interoperability, as it seamlessly integrated with existing banking infrastructure with REST API wrappers and SDKs. By use of event listeners and webhooks, core banking systems and fintech apps were able to listen and fire with smart contracts without requiring extensive modifications on the back end.

7.5 Stakeholder Insights

The feasibility of the mobile consent app was determined through a series semi-structured interviews and surveys conducted with stakeholders including: Bank IT Heads, fintech developers, cybersecurity specialists, and regulators. The bank executives expressed their interest in the audit transparency proposed by the system, but shared their concerns that governance of smart contracts and gas fees were considerable barriers. Fintech

developers appreciated the modular SDK and consent-token approach; they did recommend at least 3 additional layers of abstraction for attaching consent purposes. Cybersecurity specialists valued the opportunity to logically separate immutability for consent logs from a permanent design scheme as a means to mitigate fraud. Regulators expressed excitement about the potential for future compliance standards in banking to evolve using blockchain-based audit trails.

8. Conclusion and Future Work.

The findings presented in this paper illustrated the depth of Open Banking opportunities via blockchain technology, when improved scalability, security, and trust for users and consumers can enable new user experiences. The study built and compared a blockchain-enabled ledger with a traditional API-based and reemphasized the advantages using a blockchain model systematically enabled improvements in auditability, consent, efficiency, improved transparency for consumer consent, and regulatory objectivity of consent. Layer 1 blockchains do have latency, there are solutions on Layer 2 such as Polygon, which minimized performance, mitigated costs and was deployed when a lot of congestion in the network was happening. Our research provided contributions to academia and practitioners with a validated smart contract framework, reusable components for implementation and a pathway to consider industry buy-in. Policymakers should consider how they could add blockchain audit trails and decentralized identities to their regulatory frameworks as the introduction of both naturally introduces secure, citizen-led central banking like infrastructures for the citizen. There are limitations from the work considering the study was conducted at a sandbox-level, there is cost volatility, and small sample size of users would indicate caution in making generalizations. Future work should focus on live and ongoing deployments, the use of privacy-enhancing cryptographic tools using coprocessors for example, AI-enabled smart consent, and global alignment in regulatory standards towards building resilient and scalable user-first Open Banking infrastructures.

References

[1] Basel Committee on Banking Supervision, Report on Open Banking and Application Programming Interfaces, Bank for International Settlements (BIS), Nov. 2019.

https://www.bis.org/bcbs/publ/d486.htm

[2] S. Dey and R. Samanta, “Open Banking Ecosystem: The Indian Perspective,” International Journal of Management, vol. 13, no. 5, 2022.

https://www.researchgate.net/publication/360929083_Open_Banking_Ecosystem_The_Indian_Perspective

[3] P. Jagtap, R. Shah, and A. Kulkarni, “Leveraging Open Banking APIs for Enhanced Customer Experience and Personalization,” Journal of Banking and Finance Technology, 2023. https://www.researchgate.net/publication/382919146_Leveraging_Open_Banking_APIs_for_Enhanced_Customer_Experience_and_Personalization

[4] S. Choudhury and A. Das, “Open Banking: Digital Innovation in Banking Services in India,” International Journal of Financial Studies, vol. 11, no. 2, 2023.

https://www.researchgate.net/publication/362077379_Open_Banking_Digital_Innovation_in_Banking_Service_in_India

[5] A. Sarmah and R. Jain, “Blockchain Applications in Banking: Smart Contracts, Cross-border Payments and Beyond,” arXiv preprint, Oct. 2022.

https://arxiv.org/pdf/2210.01109

[6] Reserve Bank of India (RBI), “Master Directions – Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions,” 2021.

https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD389AE6EF40A0B4415B86BE6DCE68020A5.PDF

[7] adorsys GmbH & Co. KG, “API Security in Embedded and Open Finance: Final Whitepaper,” Feb. 2025. https://adorsys.com/wp-content/uploads/2025/02/API-Security-in-Embedded-and-Open-Finance-Final-Version.pdf

[8] CPMI – Bank for International Settlements, “Interoperability between Payment Systems Across Borders,” Jan. 2022.

https://www.bis.org/cpmi/publ/d224.pdf

[9] Center for Financial Markets and Policy – Georgetown University, “Open Banking in the United States: Opportunities and Challenges,” Jan. 2025.

https://finpolicy.georgetown.edu/wp-content/uploads/2025/01/Open-Banking.pdf