WHITE PAPER

RELEVANCE OF PUBLIC BLOCKCHAIN FOR INDIAN FINANCIAL ECOSYSTEM

Abstract

With the surge in adoption of blockchain technology globally, organizations across geographies have recognized the potential of the technology and have embarked on their blockchain journey in multiple domains. Within Financial Services, over the last decade, the Private & Permissioned blockchains have already demonstrated & proven their effectiveness.

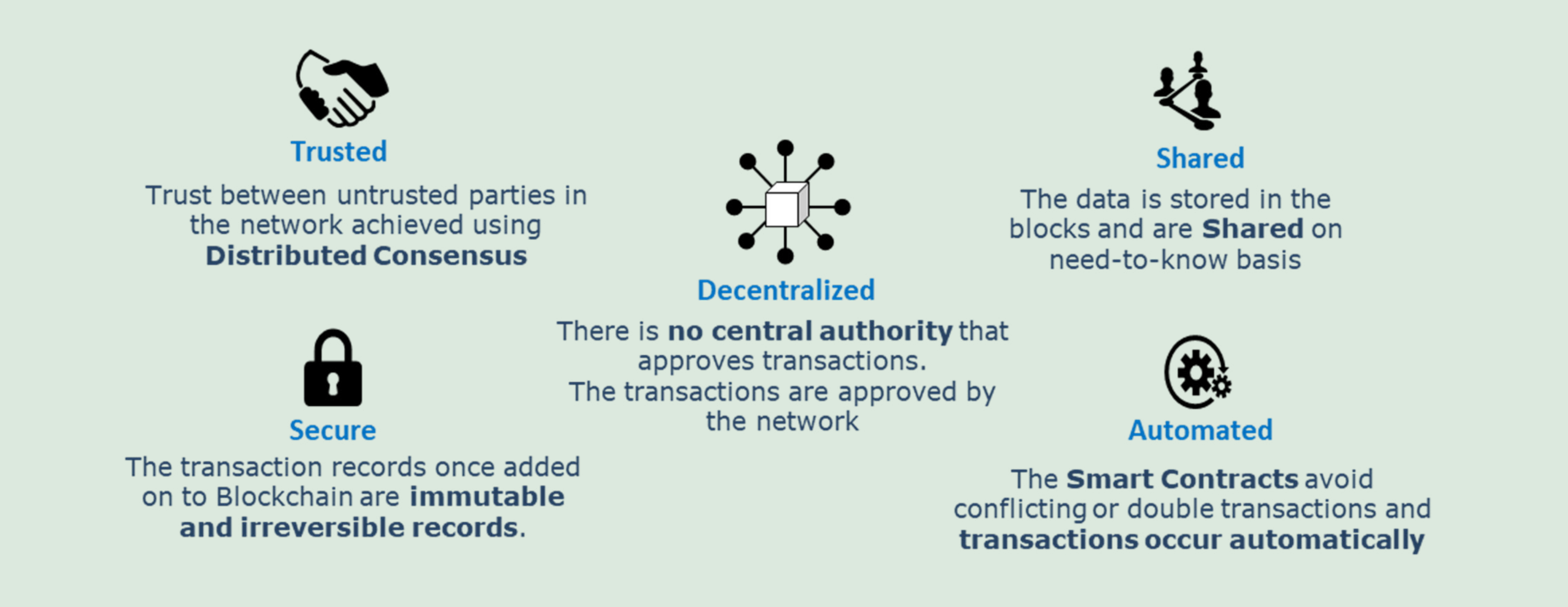
This white paper discusses the various aspects of a Public Blockchain considering the Indian Jurisdiction. It also provides the considerations on the suitability of the technology from the upcoming subtleties of the Indian legal & regulatory framework in the financial sector.

Infosys®
Navigate your next

Table of Contents

Blockchain Technology Overview

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. Any asset, be it tangible or intangible, anything of value, can be issued, tracked & traded on a blockchain network. Blockchain is a promising and revolutionary technology because it helps reduce security risks, stamp out fraud and bring transparency in a scalable way.



Trusted

Trust between untrusted parties in the network achieved using **Distributed Consensus**

Decentralized

There is **no central authority** that approves transactions.
The transactions are approved by the network

Shared

The data is stored in the blocks and are **Shared** on need-to-know basis

Secure

The transaction records once added on to Blockchain are **immutable and irreversible records.**

Automated

The **Smart Contracts** avoid conflicting or double transactions and **transactions occur automatically**

Fig1. Characteristic of Blockchain

As the name implies, the blockchain consists of a chain of blocks that are cryptographically linked and secured. Each block contains user transactions that have been checked for validity. A new block can be added to the blockchain only through a decentralized consensus process that ensures all network participants can independently verify and accept the block. Using cryptography, decentralization, and consensus, blockchain is a highly secure system that is nearly impossible to tamper with.

Private Vs Public Blockchain Network

Public blockchain networks are decentralized, and transparent ledgers which allow anyone to participate in the consensus and record transactions. Interested party can participate in consensus process by staking native crypto currency. Users carry out transactions by paying transaction fees or charges in native crypto currency. All nodes of the network maintain a copy of the ledger ensuring security and transparency. Public blockchain foster trust, as all participants can independently verify the data on the ledger. Usually, public blockchain networks are governed by a non-profit organization or a decentralized autonomous organization.

Private blockchain networks are tailor made networks designed to meet requirements of a specific group of participants seeking to benefit from blockchain technology. These networks leverage blockchain technology to achieve transparency and security with restricted data visibility thereby making it suitable for use cases requiring quick transaction finality, efficiency, and confidentiality. Private blockchain networks implement multiple levels of access control and participants are granted access appropriate to their role. Such networks are governed as per policies agreed with all network participants and often do not require crypto currency for transacting with the network.

While both network types have their own pros and cons, the selection of appropriate framework depends on the requirements of the business use case, Laws of the land, cost, governance model and technical requirements like privacy, scalability, throughput, consensus process, transaction volume, and atomicity. While considering public blockchain, volatility in the prices of cryptocurrencies is yet another aspect for consideration. As we enter the era of network of networks, interoperability becomes an especially important dimension to consider.

Here is a quick comparison of the key factors that may help in decision making when deciding between public and private blockchain:

(Note: this is not a comprehensive list of all the factors)

	Public Blockchain Network	Private Blockchain Network
Consensus Mechanisms	- Energy efficient, secure, and more democratic - High number of nodes participate in consensus	- Energy efficient, secure, and customizable - Small set of consensus nodes with controlled participation
Transaction Finality	- Delayed finality - Some networks like Hedera, provide quick finality	- Quick finality
Transaction Fee	- Per transaction fee, payable in crypto currency - Variable, depends on prevailing price of crypto currency	- No inbuilt transaction fees
Network Governance	- Through a governing body - Governing body may not always work in the best interest of all stakeholders	- Governance model is customized for each implementation - Based on network requirements, business ecosystem, and sponsorship model
Data residency	- Data resides on nodes that can be spread globally	- Private networks can restrict data to specific geographies and jurisdictions
Data Privacy	- Data is visible to all participants	- Offers inbuilt privacy mechanisms
Scalability	- Scale effectively as volume increases - Some networks support off-chain solutions that enhance performance	- Can scale effectively through proper design

Suitability of Public Blockchain for Indian Financials Institutions

Most of the public blockchains need their native tokens to execute transactions that imposes an essential, nuanced examination before their widespread adoption. While public blockchains' scalability, security, and cost-effectiveness hold immense benefits, several considerations must be navigated to ensure a smooth and legally compliant implementation as per the Indian jurisdiction. In Union Budget 2022, the Government of India has introduced taxation on virtual assets and is also working on furnishing the Cryptocurrency Bill which shall be open for consultation in near future. While current Indian laws may not have the crypto or virtual assets' regulations laid out clearly, the role of Financial Institutions becomes more significant to take watchful steps while deciding their future roadmap involving crypto, virtual assets or blockchain as a technology. The aspects of data privacy, operations & governance for blockchain network should be given through consideration.

Data Residency:

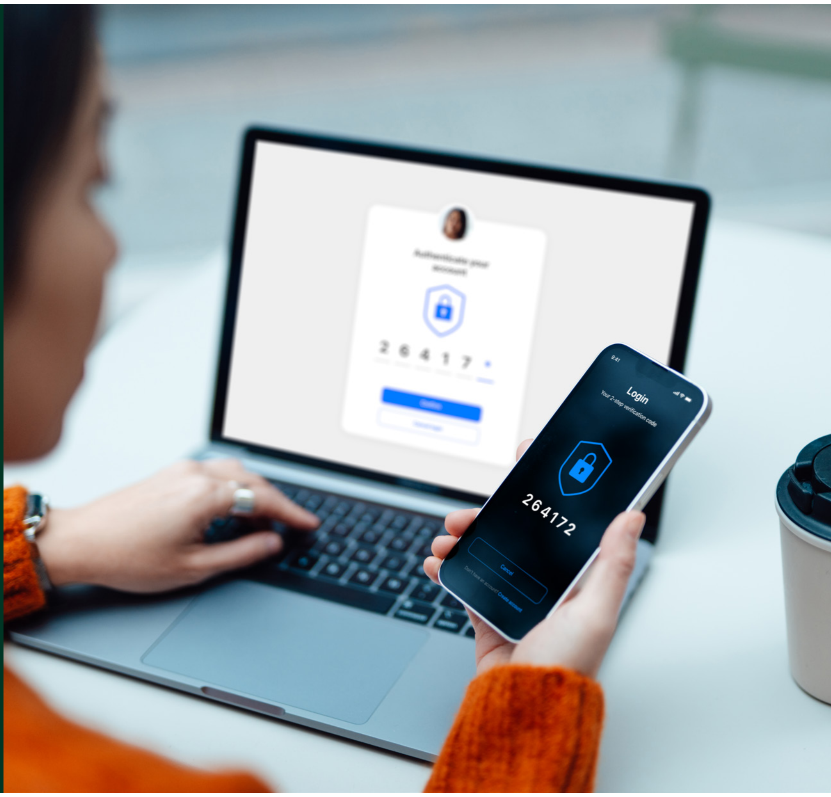
The data in a blockchain network resides on more than one node. In a private network, the nodes are controlled and could be monitored, however this is not the case with public blockchain. The public blockchain can have the copy of data on the network anywhere across the globe. As per the 'National Strategy on Blockchain[1]', "Data localization should be enabled in the framework. This may be achieved by hosting the Blockchain infrastructure, data and smart contracts within the country." So, the Financial Institutions must consider the ways to ensure data does not reside outside the Indian geography. One way could be to store signatures/fingerprints/hash of data instead of the actual data on the blockchain network. However, in future there may be regulations that do not permit storage of signatures/fingerprints/hash outside of Indian jurisdiction. This would need to be taken into consideration appropriately in purview of risk management and needs to be addressed before deployment of any solution on a public blockchain network.

Data Privacy:

The recent Digital Personal Data Protection Act[2], 2023 (DPDP Act), provides the guidelines for data privacy. According to the Act, while developing solutions, processing of digital personal data within India, and outside India if related to goods/services offered in India, entities collecting/processing data are responsible for its protection and respecting individuals' rights.

In public blockchains, the data and transactions are visible to all network participants and validators. This raises a concern on data privacy and confidentiality with the use of public blockchain. Any Personally Identifiable Information (PII) and other sensitive information must be categorized, and the solutions must be designed in such a way that this sensitive information is protected at all instances.

'National Strategy on Blockchain[1]' also emphasizes on the Data Privacy aspect with recommendations like, (a) Security and privacy should be considered as vertical components and it should be addressed across various layers in the Blockchain infrastructure, and (b) Personal data protection, data life cycle management, provisions relating to right to be forgotten/right to erasure.



Operations & Network Governance:

In a blockchain network, 51% of the user base (or nodes to be more precise) in public or private blockchains need to approve a transaction before it is written on the chain. This 51% attack remains a point of concern for public blockchains where sometime the majority of stake of tokens which are required for selecting the validator node (e.g., PoS consensus) are in control of a single authority or the majority of nodes are owned by a group of people or institutions. This may also lead to challenges in the governance of the network and is a possible threat for other participants as the concentration of authority may lead to fraudulent activities.

Another aspect is with respect to the crypto tokens that are required for executing the transactions on the blockchain platform. Crypto prices are highly volatile, resulting in high variation in transaction costs on a yearly, monthly, or even on a daily basis. This variance in transaction costs could lead to high risks in future. Therefore, it is recommended that the price volatility & transaction cost risks should be factored in and tracked actively when an application is planned to be taken live on a public blockchain.

In India, cryptocurrencies are not regulated by any central authority and are not valid as a legal tender. The transaction cost needs to be provided in the form of native blockchain tokens (which is a cryptocurrency) and the risk of it not being regulated or legally permitted remains valid. Using intermediaries to procure tokens or execute transactions via an intermediary based out of India could potentially carry legal & the tax implications or security risks with transaction data being submitted via a third party. Hence, the Financial Institutions must remain cautious while deploying solutions on public blockchain. This is also applicable for other network stakeholders as well that will also need to execute transactions on the network.

Technical Considerations

The adoption of a public blockchain in Indian financial industry requires a comprehensive approach to address range of Operational, Regulatory and Technical considerations. These considerations are crucial to ensure the resilience, security, scalability, interoperability, reliability, and compliance necessary for the financial systems in India.

a. **Resilience** – Fault tolerant architectures are crucial to keep the system functional in adverse conditions. Robust consensus mechanisms ensure network resilience against malicious attacks and failures. Designing decentralized and distributed architectures, combined with redundancy and backup strategies, eliminates single point of failure, and ensures continuous operation and data integrity even in the face of failures.

b. **Quick Finality** – Adopting consensus mechanisms with quick finality and probability of no forks helps in meeting real-time nature of the financial transactions and accelerate settlement times. Solutions should adopt fast and fault tolerant consensus algorithms, for example Pure PoS is fast and helps in achieving transaction finality in near real-time.

c. **Security of Cryptographic Keys** – To keep financial application secure, it is essential to safeguard cryptographic keys from unauthorized access. Secure key management practices include use of HSM and have ability to rotate keys at regular intervals to prevent any dilution due to regular use.

d. **Privacy and Confidentiality of the Data** – Financial data is considered sensitive and private. It must be protected from unauthorized access and tampering. On public blockchain, financial transactions may need to be encrypted by employing various techniques like encryption, zero knowledge proofs. Further, it may be necessary to maintain anonymity of the transaction through use of stealth addresses.

e. **Scalability** – With special focus on digital economy, financial transaction volume in India has seen rapid growth. To support ever growing transaction volumes, the solution must be both vertical and horizontal scalable. Off-chain or layer 2 scaling solutions can alleviate the load of layer 1 blockchain.

f. **Meeting Semantics and Legal Standards** – Adhering to semantic standards, like ISO20022 for messaging, ensures consistency in communication. Compliance with financial regulations, such as AML and KYC, are important from legal perspective. Choosing token standards that align with industry practices and regulatory requirements is vital. Adhering to recognized token standards such as ERC-1404 (Security token) ensures compatibility with existing financial systems. Automation of legal compliance through smart contracts may be necessary for many use cases.

g. **Auditability and Traceability** – Leveraging blockchain immutability and transparency facilitates regulatory audits and forensic analysis. It may help in enhancing accountability, trust, and transparency in financial systems.

h. **Interoperability with Legacy Systems** – Integration, innovation, and intelligent automation (3i framework) with existing systems is a fundamental requirement of the financial industry. Ensuring seamless integration with existing legacy financial systems requires development of standardized APIs and protocols to facilitate gradual transition to blockchain technology without disrupting current operation.

i. **Extensible and Flexible Modular Design** – A flexible modular design allows for easy upgrades, customization, and integration. Microservices architecture helps in achieving extensibility. It enhances flexibility and scalability by breaking down complex systems into independent, manageable components.

By addressing aforesaid technical considerations, financial organizations can embrace the transformative potential of blockchain technology fostering enhanced efficiency, security, scalability, interoperability, and compliance in their systems.

Conclusion

The applicability of public blockchain technology within the Indian legal and regulatory landscape, presents both substantial opportunities and complex challenges regarding data privacy, residency, security, operational & network governance. Practical implementation also necessitates addressing fundamental regulatory and technical challenges by the financial institutions, as well as the Government. Unmitigated, these challenges could impede successful deployment and negate anticipated benefits. Firm commitment to data privacy, residency, and adaptable security practices will unlock the transformative potential of public blockchain.

Any Financial Institution planning for designing solutions on public blockchain should be cautious about the upcoming subtleties of the Indian legal & regulatory framework along with evolving architecture and business model of the public blockchains. The challenges & risks highlighted in this report are advised to be addressed or mitigated in advance prior to initiating any implementation on public blockchain.

References

1. Ministry of Electronics & Information Technology (MeitY) - National Strategy on Blockchain, Dec2021.
2. The Digital Personal Data Protection Act, 2023 - Digital Personal Data Protection Act 2023.
3. Reserve Bank of India, Speeches & Media Interactions - Cryptocurrencies – An assessment.
4. Forbes - All You Need to Know About India's Crypto Bill.

About the Authors

Anubhav Bhatnagar

Principal Consultant, Infosys Blockchain

Anubhav has rich industry experience in consulting, product management, and software development in BFSI. He provides strategic guidance and consulting services on how to apply blockchain for specific business units. His expertise lies in helping clients identify contextualized use cases with their ecosystem partners to derive shared business value. Anubhav also supports his customers in their innovation journey towards blockchain-powered digital transformation.

Vivek Rastogi

Senior Technology Architect, Infosys Blockchain

Vivek has extensive experience and expertise in harnessing state-of-the-art technologies such as cloud, and blockchain to address the specific needs of various industry sectors, particularly with in banking and financial realms. He has worked with prominent clients across multiple geographic regions and played a crucial role in guiding them through their digital transformation journey by creating high-performing innovative solutions to modernize business and deliver value to the customers.

For more information, contact askus@infosys.com

Infosys®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected