



LINUX
FOUNDATION
DECENTRALIZED TRUST

THE BIG PICTURE OF DECENTRALIZED
TRUST

*Open - source
foundations powering
trust in the digital age*





EDITORIAL NOTE

“Trust is no longer assumed — it is verified.”

Why Decentralized Trust Matters Today

In today’s hyper-connected digital world, trust has become the cornerstone of every interaction — whether it involves financial systems, digital identities, data exchange, or governance frameworks. Traditional centralized models of trust are increasingly challenged by issues of transparency, security, scalability, and control.

LF Decentralized Trust (LFDT), an initiative under the Linux Foundation, addresses these challenges by enabling open, decentralized, and verifiable trust infrastructure. Instead of a single authority, LFDT promotes collaboration, cryptographic verification, and shared governance through open-source technologies.

As digital ecosystems continue to expand across borders and industries, decentralized trust is no longer optional — it is essential. LFDT represents a global effort to build systems where trust is embedded by design, empowering institutions, enterprises, and individuals alike.

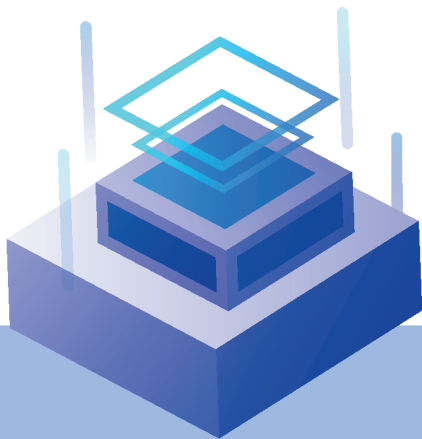
LF DECENTRALIZED TRUST

An overview

LF Decentralized Trust is a Linux Foundation initiative focused on building open-source technologies that enable trusted digital interactions. It represents the evolution of earlier blockchain efforts under Hyperledger, expanding beyond distributed ledgers to address broader trust challenges across industries.

Vision

To be a premier Computer Engineering Department by achieving excellence in Academics and Research for creating globally competent and ethical professionals



Scope of LFDT includes

- Distributed ledger technologies
- Digital identity and verifiable credentials
- Privacy-preserving and confidential computing solutions
- Interoperability across platforms and networks
- Governance frameworks for decentralized systems

Governance Model

LFDT operates under an open governance structure, encouraging collaboration among enterprises, startups, developers, academia, and public institutions worldwide.



Global LFDT ECOSYSTEM

LF Decentralized Trust brings together a diverse global ecosystem committed to building trusted digital systems.

- ▶ Central Banks & Governments: Exploring digital currencies, public infrastructure, and verifiable governance systems.
- ▶ Startups & Innovators: Creating decentralized applications and next-generation trust solutions.
- ▶ Enterprises: Developing secure platforms for finance, supply chains, healthcare, and data sharing.
- ▶ Global Deployments: LFDT technologies are actively used across multiple sectors worldwide.

From Blockchain to Trust Infrastructure

While blockchain remains a foundational technology, LFDT has expanded its vision to create a complete trust infrastructure layer.

Key features include :

- Digital Identity: Self-sovereign identity and verifiable credentials
- Privacy: Confidential computing and privacy-preserving protocols
- Interoperability: Seamless communication between diverse systems
- Governance: Transparent and auditable decision-making mechanisms

Together, these elements position LFDT as a critical enabler of secure, scalable, and inclusive digital ecosystems.

INDIA AND DIGITAL PUBLIC INFRASTRUCTURE

India's leadership in decentralized trust: Innovation, collaboration, and impact. Discover how India's thriving Web3 ecosystem, pioneering enterprises, and strategic collaborations within LF Decentralized Trust are driving global advancements in decentralized technologies

Real world Innovation in action

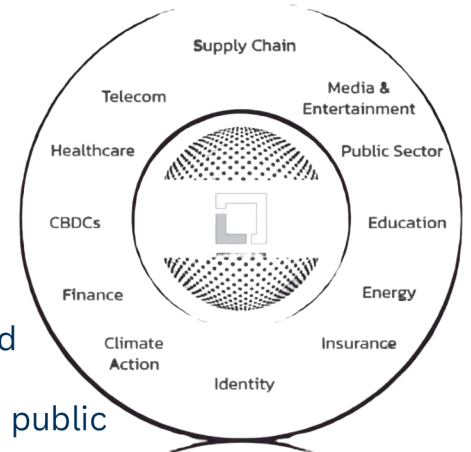
Transforming finance, public services, and digital identity with open collaboration. From powering the Reserve Bank of India's Digital Rupee pilot with Hyperledger Fabric to shaping the National Blockchain Framework and revolutionizing air travel with Digi Yatra, India's LF Decentralized Trust community is leading the way in decentralized innovation. Explore how India's top enterprises and developers are driving blockchain adoption, shaping critical infrastructure, and creating solutions with global impact.

Why Trust Is Challenging at Scale

Any trust system in India must effectively handle:

- Billions of identities, requiring secure, privacy-preserving verification.
- High availability, with uninterrupted services across regions and demographics.
- Regulatory oversight, ensuring compliance, accountability, and public interest.

These conditions push conventional centralized models to their limits.



India as a Natural Testbed for Decentralized Trust

India's Digital Public Infrastructure (DPI) provides real-world validation for decentralized trust systems:

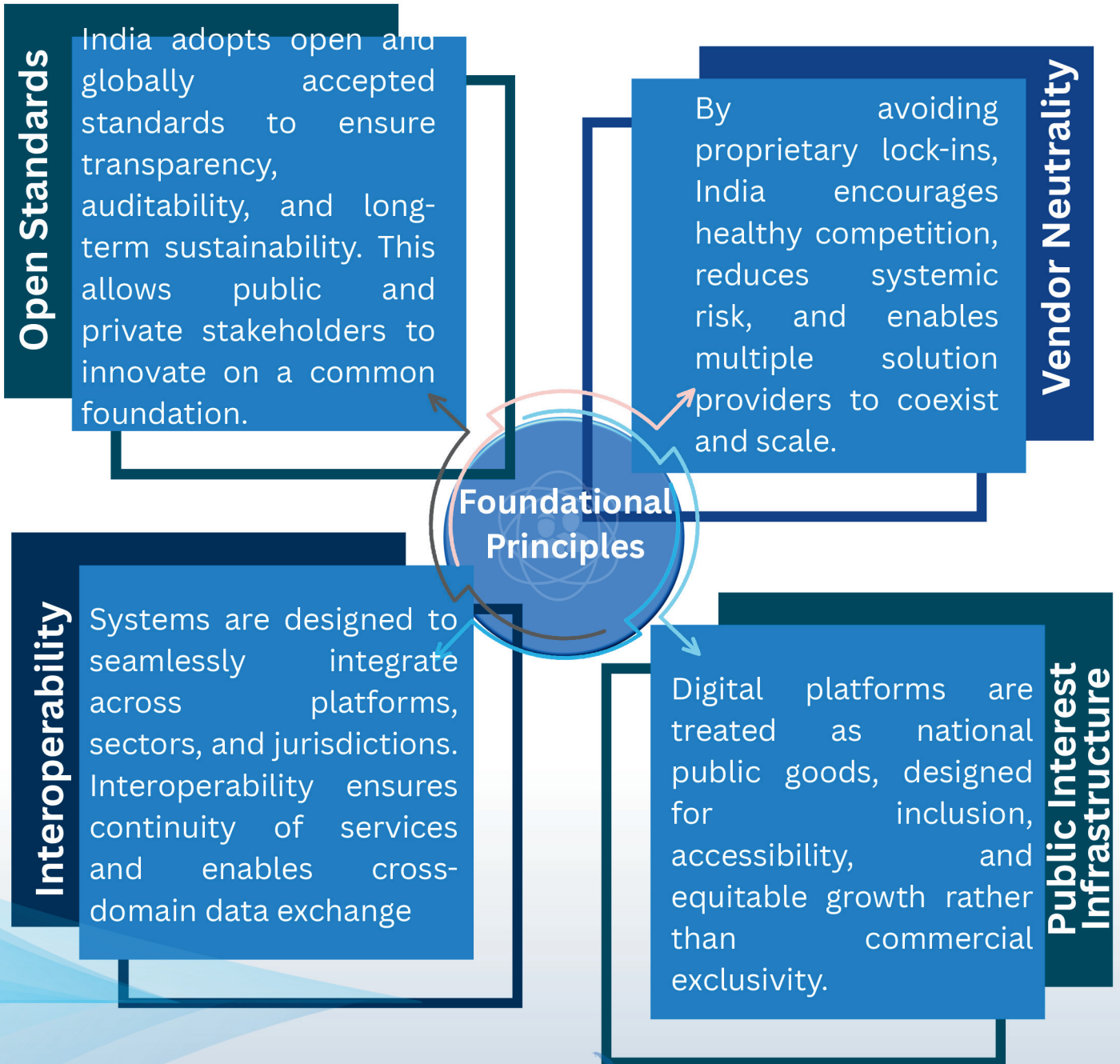
- 34 crore+ documents verified through national blockchain frameworks
- RBI Digital Rupee pilots using enterprise-grade DLT infrastructure
- Digi Yatra, enabling decentralized digital identity for air travel

Such deployments demonstrate how decentralized architectures can operate reliably at national scale.

INDIA'S ALIGNMENT WITH LFDT



India's digital public infrastructure is guided by principles that strongly align with the LF Decentralized Trust (LFDT) governance philosophy. This shared foundation enables scalable, secure, and future-ready trust systems.



Alignment with LFDT Governance

LFDT operates as a neutral, open-governance ecosystem, supporting:

- Blockchain and distributed ledger technologies
- Digital identity and privacy frameworks
- Interoperability and cryptographic assurance

This governance model closely mirrors India's approach to building Digital Public Infrastructure.

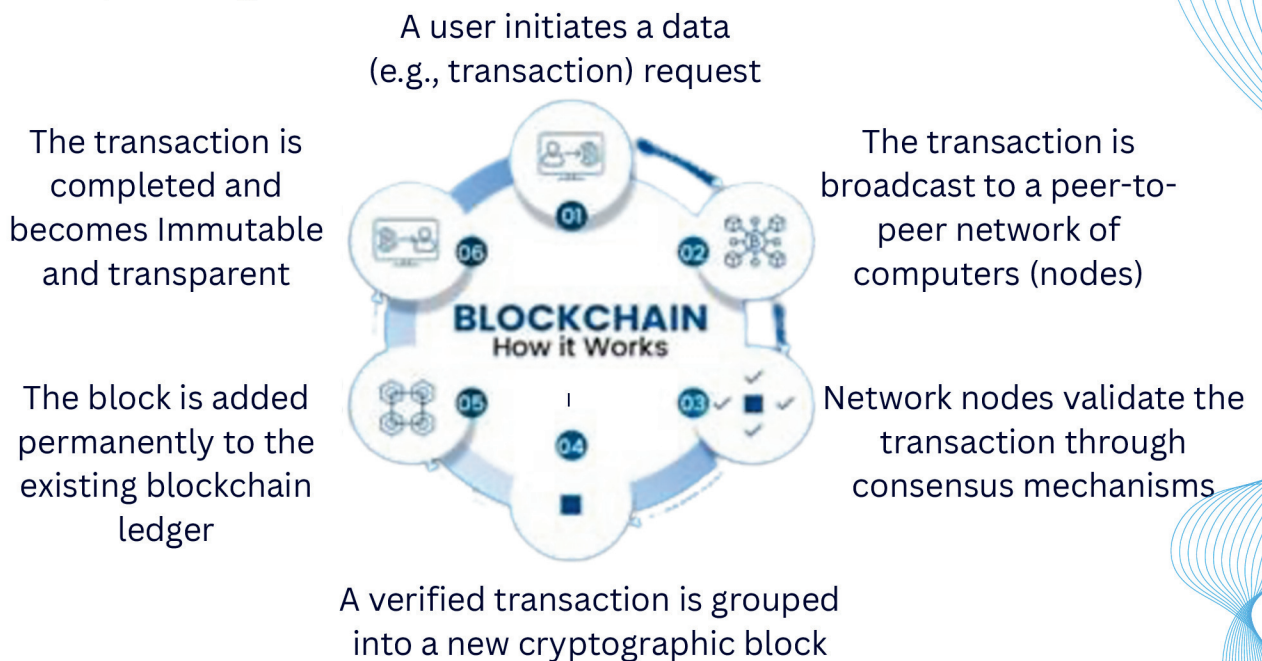
Strategic Benefits for India

- Faster adoption of global decentralized trust standards
- Stronger collaboration with international regulators and institutions
- Scalable deployment with built-in compliance and oversight



NATIONAL BLOCKCHAIN FRAMEWORK (NBF)

As blockchain adoption expanded across government departments and states, India identified a critical risk fragmented and siloed implementations. To address this, the Ministry of Electronics and Information Technology (MeitY) established the National Blockchain Framework (NBF) as a unified, standards-driven approach to blockchain adoption in governance.



Why the NBF Was Created

The National Blockchain Framework was designed to:

- Prevent fragmented blockchain adoption
- Without a common framework, isolated blockchain systems could emerge across ministries and states, limiting scale and reuse.
- NBF allows multiple blockchain networks to securely exchange data while maintaining autonomy.
- Standardize governance and architecture
- It defines common principles for security, compliance, lifecycle management, and system governance.
- Support population-scale deployments

Technology Backbone: Vishvasya Blockchain Stack

At the core of NBF lies the Vishvasya Blockchain Stack, deployed across NIC data centres in Bhubaneswar, Pune, and Hyderabad, ensuring resilience and availability.

Key features include:

- Blockchain-as-a-Service (BaaS) for rapid government adoption
- Open APIs for integration with e-Governance systems Proven at National Scale

As of October 2025:

- 34+ crore documents verified on blockchain platforms
- Active deployments across certificates, land records, logistics, judiciary, and justice systems

NBF ARCHITECTURE

The National Blockchain Framework (NBF) is designed as core digital infrastructure, not a pilot or experimental technology. Its architecture reflects the requirements of governance at national scale—security, accountability, and interoperability.

- **Permissioned Networks**

NBF prioritizes permissioned blockchain networks where participants are verified and authorized. This model supports regulatory compliance, controlled access, and reliable governance—essential for public sector use cases.

- **Identity-Linked Participation**

Every participating node and application is tied to a verifiable digital identity. This ensures traceability, accountability, and trust while enabling role-based access and responsibility across institutions.

Architectural Principles

- **Governance by Design**

Governance is embedded directly into the architecture. Rules for participation, validation, auditability, and lifecycle management are defined upfront, reducing ambiguity and operational risk.

- **Integration with Existing Digital Systems**

NBF is designed to integrate seamlessly with existing e-Governance platforms, databases, and digital public infrastructure through open APIs and standard interfaces.

Blockchain as Infrastructure

Unlike experimental deployments, NBF treats blockchain as foundational infrastructure:

- Built for long-term operation and scalability
- Designed to support multiple sectors and jurisdictions
- Capable of evolving without disrupting existing systems

Operational Impact

This architecture enables:

- High availability and fault tolerance
- Secure data sharing across agencies
- Interoperable blockchain deployments at national scale

RBI DIGITAL RUPEE

Money is at the core of trust in any economy. As payment systems evolve, policymakers face a fundamental trade-off. Cash is anonymous and sovereign, but operationally inefficient. Digital payments are fast and convenient, yet often rely on centralized intermediaries. Central Bank Digital Currencies (CBDCs) aim to bridge this divide.

WHY CBDCs EMERGED

Cash is anonymous but inefficient, while digital payments are efficient but centralized. CBDCs attempt to balance sovereign control, auditability, and user trust.

KEY INSIGHT

CBDCs are not about replacing cash, but about rethinking trust in digital money. They extend the idea of sovereign currency into the digital age while preserving the role of central banks as trusted issuers of value.

INDIA'S APPROACH: THE DIGITAL RUPEE (e₹)

The Reserve Bank of India's Digital Rupee explores how sovereign digital money can operate reliably at a national scale while preserving trust, security, and regulatory oversight. Through phased retail and wholesale pilots, the e₹ examines real-world use cases, interoperability with existing payment systems, and models for controlled privacy that align with regulatory requirements.

WHY IT'S IMPORTANT

The Digital Rupee represents more than a new payment mechanism. It is a practical experiment in designing digital public infrastructure that supports transparency, resilience, and financial stability. As India continues its digital transformation, the e₹ offers insights into how trust in money can be sustained in a digital-first economy.

DESIGN GOALS

A Digital Currency for India's Future

The Digital Rupee (e₹) is a central pillar of India's evolving digital financial architecture. As outlined in publications by the Reserve Bank of India (RBI), the e₹ is designed not merely as a technological upgrade, but as a strategic instrument to strengthen trust, efficiency, and inclusivity in the monetary system

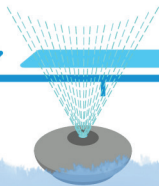
MONETARY SOVEREIGNTY

The e₹ ensures that the control of India's currency remains firmly with the RBI, even as digital payments grow. Unlike decentralized cryptocurrencies, it is fully backed by the central bank, maintaining trust, stability, and confidence in the national financial system.



PAYMENT EFFICIENCY

Designed for speed and reliability, the e₹ allows instant, low-cost transactions across multiple channels. Whether sending money digitally in cities or villages, it reduces delays, minimizes transaction costs, and improves overall efficiency of the payment ecosystem.



FINANCIAL INCLUSION

One of the core goals of the e₹ is to bring unbanked and underbanked populations into the formal economy. With simplified access and minimal technical requirements, it empowers individuals and small businesses to participate in the digital economy, bridging the financial gap in rural and semi-urban areas.



REGULATORY COMPLIANCE

The e₹ is built with compliance by design, ensuring alignment with legal and regulatory frameworks. This allows effective monitoring, fraud prevention, and data security, while maintaining user privacy and systemic stability.

COMPLEMENTING PRIVATE INNOVATION

The e₹ is not meant to stifle private fintech solutions. Instead, it provides a stable digital infrastructure upon which banks, startups, and payment providers can innovate responsibly. This combination of public trust and private creativity fosters a balanced and resilient digital economy.

DIGI YATRA

Digi Yatra represents a real-world deployment of decentralized identity at national scale. Designed for high-traffic airports, it demonstrates how digital trust systems can improve efficiency while protecting individual privacy. Instead of relying on centralized identity databases, Digi Yatra redefines how identity verification works in public infrastructure.

THE IDENTITY PROBLEM AT AIRPORTS

Airports have traditionally depended on physical documents, centralized databases, and manual identity checks to verify passengers. Every checkpoint requires repeated validation of personal information, increasing delays and operational complexity. More importantly, this model exposes sensitive identity data to unnecessary access, creating privacy risks and single points of failure. As passenger volumes grow, these systems struggle to scale securely and efficiently.

A Blueprint for Digital Identity

The Digi Yatra architecture extends far beyond airport travel. The same decentralized identity framework can be applied to education for academic credentials, healthcare for patient records, and government services for citizen authentication. By operating successfully at population scale, Digi Yatra proves that decentralized identity is not experimental—it is deployable, scalable, and effective in real-world systems.

Verifiable Credentials in Action

Digi Yatra replaces document-based verification with verifiable credentials that remain under the user's control. Passenger identity is stored on personal devices rather than in a central database. At each checkpoint, cryptographic proof confirms identity without revealing excess personal data. Only what is required is shared, and nothing is retained after verification. In this model, credentials are verified—not stored—ensuring privacy by design.

Key Characteristics

- User-controlled digital identity
- Selective disclosure of information
- No centralized identity repository

INDIA'S LFDT STACK

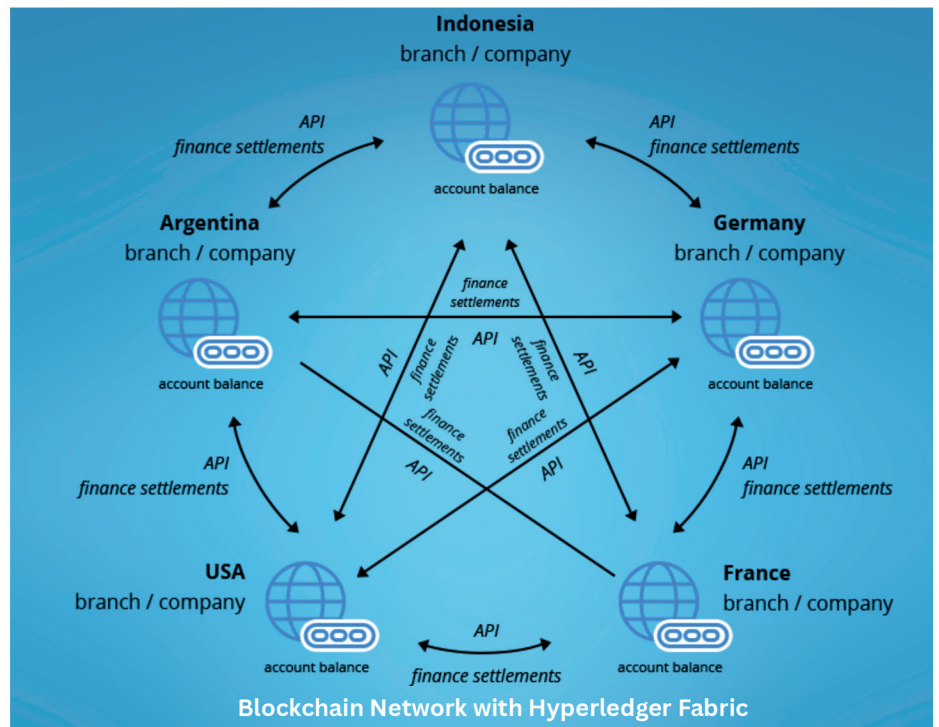


India's decentralized trust infrastructure is built on a modular stack of LF Decentralized Trust (LFDT) projects, each chosen to address a specific infrastructural requirement. Rather than relying on a single technology, the approach combines multiple open-source components that work together to support scale, governance, and interoperability.

Hyperledger Indy supports decentralized identity by providing the underlying ledger and tools for issuing and verifying verifiable credentials in privacy-preserving ways.

Hyperledger FireFly acts as the orchestration layer, simplifying integration, coordination, and scaling across multiple blockchain networks and applications.

Hyperledger Fabric forms the foundation for permissioned blockchain networks used in government and enterprise systems, where controlled participation and high throughput are essential



Hyperledger Besu enables Ethereum compatibility, allowing India's platforms to interact with both public and private blockchain ecosystems while maintaining regulatory oversight.

Hyperledger Iroha is used for lightweight governance use cases, offering simplicity and efficiency for systems that require fast, rule-based transaction processing.

PERMISSIONED VS PUBLIC BLOCKCHAIN

Public blockchains are open, permissionless networks where anyone can join without approval.

-Core Characteristics

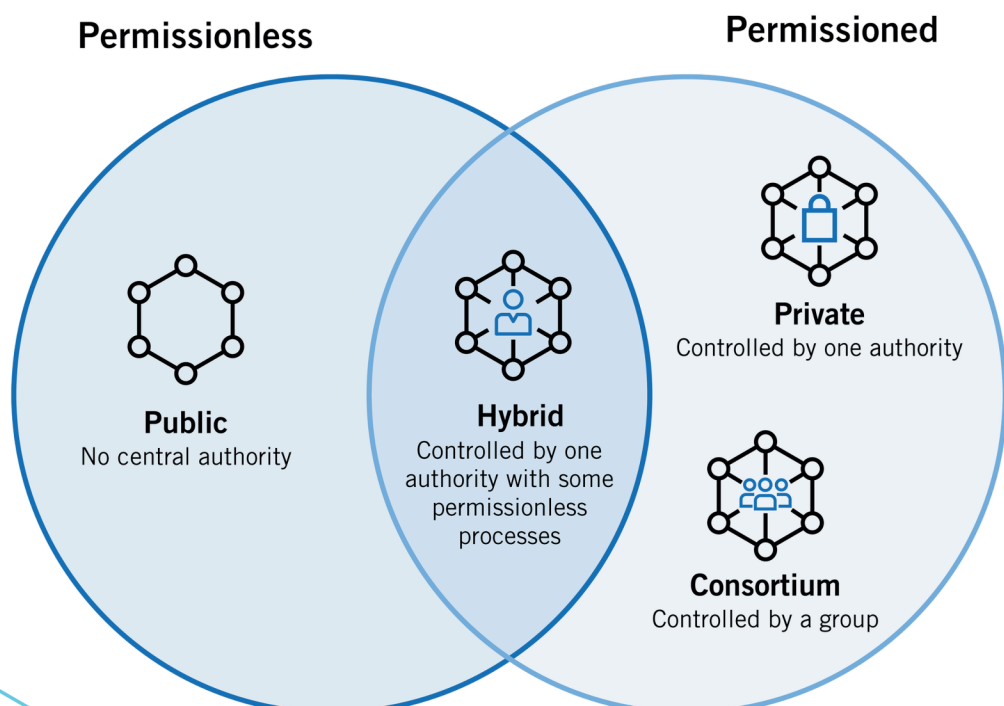
- Open participation: Anyone can run a node, submit transactions, or validate blocks.
- Decentralized governance: No single organization controls the network.
- Trust through consensus: Security is achieved using cryptographic consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS).

Pros

- Trustless & censorship-resistant
- High transparency

Cons

- Slower transactions
- High energy & gas costs



PERMISSIONED VS PUBLIC BLOCKCHAIN

Permissioned Blockchains

Permissioned blockchains restrict participation to approved, known entities.

-Core Characteristics

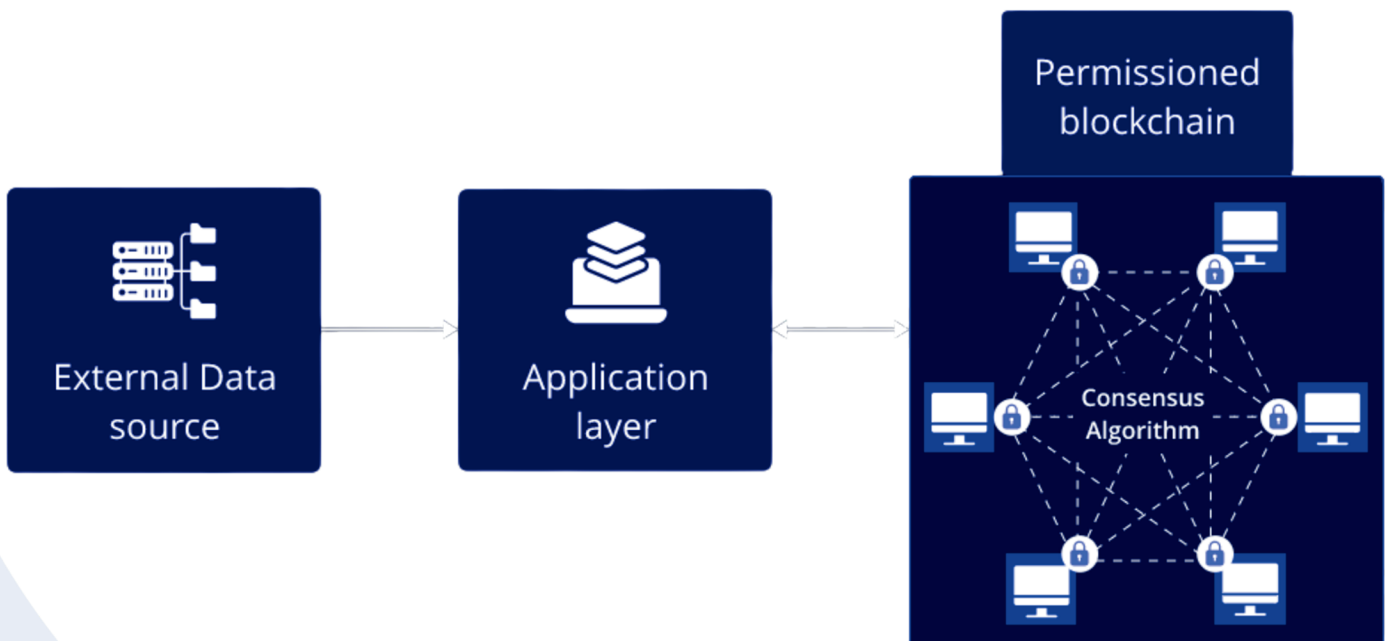
- Controlled access: Only authorized participants can read, write, or validate data.
- Known identities: Participants are verified organizations or individuals.
- Efficient consensus: Uses algorithms like PBFT, Raft, or IBFT.
- Governance structure: Rules are enforced by consortiums or institutions.

Pros

- High performance
- Better privacy & control

Cons

- Less decentralized
- Requires trust in governing entities



DECENTRALIZED IDENTITY (DID & VERIFIABLE CREDENTIALS)

Decentralized Identity (DID)

- A self-sovereign identity controlled by the user, not governments or companies.
- Stored on blockchain or decentralized networks.
- Eliminates centralized identity providers (Google, Facebook, Aadhaar).

Key Idea:

You own your identity, not platforms.

Verifiable Credentials (VC)

- Digitally signed credentials (degree, ID, license).
- Issued by trusted issuers and verified cryptographically.
- No need to reveal full identity (privacy-preserving).

Example

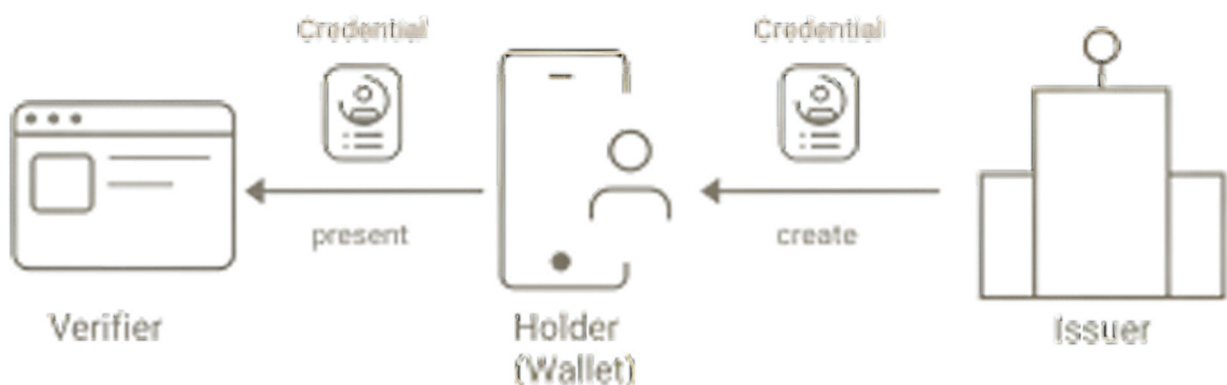
- Instead of sharing your full Aadhaar → you prove “I am above 18”.

DID + VC Flow

1. User creates a DID
2. Issuer provides VC
3. User stores VC securely
4. Verifier checks authenticity

Benefits

- Privacy-preserving
- User-controlled
- Reduces identity fraud



PROGRAMMABLE PRIVACY & SECURITY

Programmable Privacy & Security

Traditional systems rely on policies and trust in administrators.

Blockchain introduces privacy and security enforced by code.

Programmable Privacy

Programmable privacy allows systems to:

- Validate conditions
- Without accessing raw data

Key Technologies

Zero-Knowledge Proofs (ZKP)

- Prove a statement is true
- Without revealing underlying information

Examples:

- Prove income eligibility without revealing salary
- Prove membership without revealing identity

Encryption + Access Control

- Data remains encrypted
- Only authorized smart contracts or users can decrypt

Programmable Security

Security rules are embedded into smart contracts.

What This Enables

- Automated enforcement
- No human override
- No silent rule changes

Common Security Logic

- Multi-signature approvals
- Time-locked actions
- Role-based permissions
- Conditional execution

Why It's Powerful

- Eliminates insider abuse
- Reduces human error
- Ensures deterministic outcomes

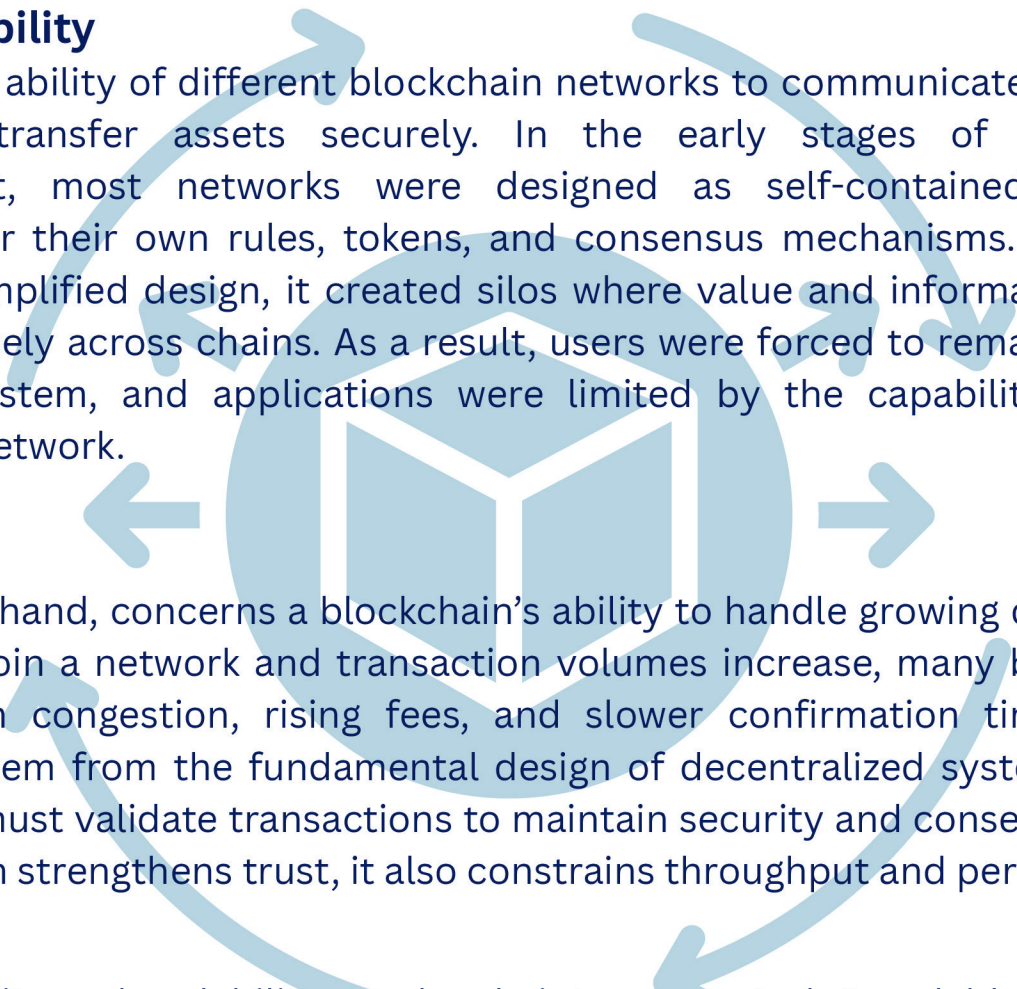
INTEROPERABILITY & SCALABILITY



As blockchain ecosystems expand, two structural challenges become increasingly visible: fragmentation and performance. Interoperability addresses the first problem, while scalability tackles the second. Together, they determine whether blockchains can evolve from isolated experiments into a cohesive global infrastructure.

Interoperability

refers to the ability of different blockchain networks to communicate, exchange data, and transfer assets securely. In the early stages of blockchain development, most networks were designed as self-contained systems, optimized for their own rules, tokens, and consensus mechanisms. While this approach simplified design, it created silos where value and information could not move freely across chains. As a result, users were forced to remain within a single ecosystem, and applications were limited by the capabilities of the underlying network.



Scalability

on the other hand, concerns a blockchain's ability to handle growing demand. As more users join a network and transaction volumes increase, many blockchains struggle with congestion, rising fees, and slower confirmation times. These limitations stem from the fundamental design of decentralized systems, where every node must validate transactions to maintain security and consensus. While this approach strengthens trust, it also constrains throughput and performance.

Interoperability and scalability are deeply interconnected. A scalable blockchain that cannot interact with others remains isolated, while an interoperable network that cannot handle high demand risks becoming unusable. The challenge lies in balancing these goals without undermining security or decentralization. This balance is often described through the blockchain trilemma, which highlights the difficulty of optimizing performance, security, and decentralization simultaneously.

GLOBAL LFDT ECOSYSTEM & IMPACT

Real-World Applications of Decentralized Trust

LFDT technologies are used globally to support secure, transparent, and scalable digital systems. These deployments show how decentralized trust is becoming a backbone for governments, enterprises, and financial networks.

Adoption Areas

LFDT technologies are used in multiple large-scale environments, including:

- Central bank pilots
- National identity systems
- Enterprise supply chains
- Regulated financial infrastructure

Production Deployments

LFDT runs quietly inside real institutional systems:

- Operational in banking environments
- Used within government registries
- Integrated into enterprise digital systems

Ecosystem Players

A diverse global community contributes to the LFDT ecosystem, such as:

- Governments
- Banks
- Startups
- Researchers
- System integrators

Scale Principles

LFDT defines scale through more than performance:

- Fault tolerance
- Long-term maintainability
- Regulatory adaptability

INDIA AT SCALE METRICS



India operates digital systems built to support billions of identities, maintaining high availability and functioning under strict regulatory oversight .

Its national digital infrastructure is rooted in open standards, interoperability, vendor neutrality, and public interest architecture .

National Blockchain Framework (NBF)

India's NBF prevents fragmented blockchain adoption and ensures interoperability across states and sectors. It emphasizes permissioned networks, identity-linked participation, and governance-driven architecture for nationwide consistency .

Digital Rupee (e₹)

The e₹ is designed for monetary sovereignty, payment efficiency, financial inclusion, and regulatory compliance, enhancing India's digital economy at population scale .

Digi Yatra Identity Layer

Digi Yatra showcases user-controlled identity, selective disclosure, and no central storage of personal data, enabling secure, high-volume verification in real environments like airports and future public services .

India's LFDT Technology Stack

India combines Fabric, Besu, Indy, Iroha, and FireFly to build trust systems that are scalable, interoperable, and governance ready, supporting real public-sector and enterprise deployments at national scale .

STARTUPS & INSTITUTIONS IN THE LFDT INDIA ECOSYSTEM



India's LFDT ecosystem combines the strengths of government bodies, enterprises, system integrators, and innovators to build trustworthy digital systems at national scale. Public-sector initiatives create the foundational architecture, while industry partners and startups enhance identity, privacy, and interoperability layers to support India's growing digital trust landscape.

National Frameworks & Enterprise Adoption

Programs like the National Blockchain Framework, the Digital Rupee, and Digi Yatra define unified models for governance, identity, and interoperability across sectors. Banks, registries, and major institutions deploy LFDT technologies in real production environments, focusing on stability, compliance, and long-term maintainability to ensure trusted digital services.

Integrators, Startups & Research Contributors

Key system integrators—such as TCS, AYANWORKS, IDS, KBA, and BBN—translate LFDT frameworks into working networks through configuration, governance alignment, and large-scale implementation. Alongside them, startups and research groups advance identity, privacy technologies, and interoperability tools, keeping India's trust architecture future-ready.

AI WITHOUT TRUST FAILS

The Poisoned Well: Why Data Integrity is AI's Achilles Heel

We treat AI as an oracle, but it is merely a probabilistic engine. It predicts the next likely word based on its training. This creates a critical vulnerability: if the input is compromised, the output is confidently

The Threat of Data Poisoning "Garbage In, Garbage Out" has evolved into a cybersecurity weapon. Attackers don't need to hack the code; they just need to pollute the data



VISUAL HACKS

Researchers proved that placing a simple yellow sticky note on a stop sign in a training image can trick an autonomous vehicle into misidentifying it as a speed limit sign, causing it to accelerate.



"CONFUSEDPILOT"

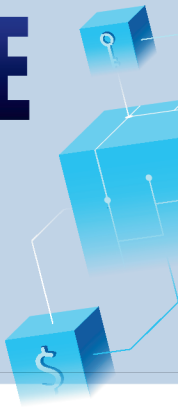
In 2024, attacks on RAG (Retrieval-Augmented Generation) systems showed that injecting malicious text into enterprise documents can manipulate AI assistants into betraying their users.

The Accountability Vacuum AI decisions often happen in a "black box." Without verifiable data, there is no accountability. As we move toward "Agentic AI" that acts on our behalf, the lack of an audit trail becomes a liability.

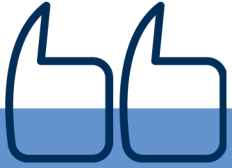
"AI systems are only as reliable as their data. Without verifiable data, AI decisions are unaccountable."

BLOCKCHAIN AS AI GOVERNANCE

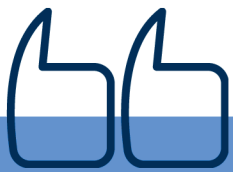
THE ANCHOR OF TRUTH: ENGINEERING INTEGRITY INTO INTELLIGENCE



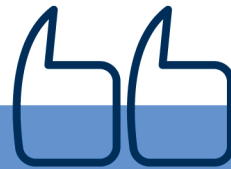
If AI provides the intelligence, blockchain provides the integrity. We use decentralized ledgers to govern the data that feeds the machine.



1. The Flight Recorder (Audit Trails) To trust AI in high-stakes industries, we need a "Proof of History." Hiero (the codebase for Hedera) is used to create Consensus Services that act as a digital flight recorder. They timestamp and hash every AI decision, creating an immutable log for post-incident auditing.



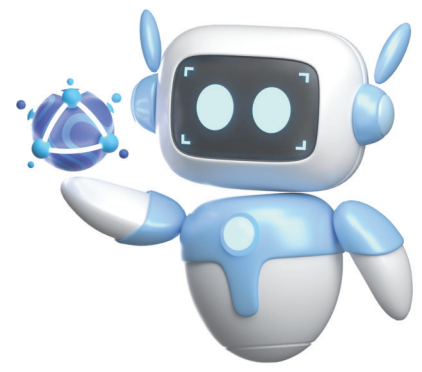
3. Distinguishing Reality (C2PA & CAWG) To fight deepfakes, the Creator Assertions Working Group (CAWG) is implementing C2PA standards. This technology allows creators to cryptographically sign their content, adding a tamper-proof seal that distinguishes human reality from AI generation.



2. Supply Chain for Data (Provenance) Hyperledger Fabric is deployed to create "data provenance" chains. These systems cryptographically verify the origin of a dataset, ensuring the model was trained on ethical, unadulterated data rather than poisoned sources.



POST-QUANTUM CONCERNS



THE CRYPTOGRAPHIC CLIFF: PREPARING FOR THE "Y2Q" EVENT

While we fix AI trust, quantum computing threatens to break the encryption (like RSA) that secures the internet.

The "Harvest Now, Decrypt Later" (HNDL) Threat The danger is immediate. Through HNDL attacks, adversaries are stealing encrypted data today and storing it until a quantum computer can unlock it. Any long-term secrets (health records, government intel) stored on standard blockchains are already at risk.

LFDT's Defense: NightStream & NIST
The Linux Foundation Decentralized Trust is hardening the ecosystem:

- **Standards:** Projects are integrating NIST FIPS 203 and 204 standards for post-quantum cryptography.
- **NightStream:** This cutting-edge LFDT Lab is developing post-quantum Zero-Knowledge Proofs (ZKPs). This ensures privacy tools remain secure against quantum decryption in the long term.

"Quantum computing threatens existing cryptography. LFDT acknowledges this risk and tracks standards-based responses."

LFDT ROADMAP: 2025 AND BEYOND

1. Interoperability: Connecting the Silos Hyperledger Cacti and the Smoot project are building bridges that allow different blockchains to talk to each other. This enables AI agents to securely access data across diverse private and public ledgers without compromising security.



2. Privacy: Programmable & Institutional Paladin offers "programmable privacy" for EVM blockchains. Currently being piloted by the Bank of Korea, it allows institutions to execute compliant, private transactions (like tokenized deposits) without revealing sensitive data to the public network.



3. Governance: The Human Layer The Trust Over IP (ToIP) Foundation has launched specific working groups for AI and Human Trust. They are defining the governance frameworks that ensure autonomous AI agents operate within legal boundaries.

Meet Our Team



Niraj M. Patil
President



Rutuja Jagtap
Secretary



Rupal Patil
Vice-President



Kunal Biradar
Treasurer



**Prithviraj
Sherikar**
Technical lead



**Rohit
Sonawane**
Management lead



**Samruddhi
Sutar**
Design lead



Aditi Kale
Marketing lead



Dishant Gotis
Technical Team



**Mayuresh
Mandalik**
Technical Team



**Mahesh
Avhad**
Technical Team



Mayur Kharat
Technical Team

Meet Our Co-ordinators



Dr. Sonali Patil

**Faculty Co-ordinator,
LFDT PCCOE**



Dr. Meghana Lokhande

**Faculty Co-ordinator,
LFDT PCCOE**



Mr. Vikram Sharma

**Co-Chair, LFDT
India**



Mrs. Ankita Ptidar

**Co-Chair, LFDT
India**



Mr. Kamlesh Nagware

**Co-Chair, LFDT
India**



Dr. Anasuya Therese
Innocent

Lead, LFDT India



Ms. Garima Singh

**Government
Alliance Lead**



Mr. Kartikey Kashyap

**Developer Advocate
LFDT India**



Ms. Ritu Jain

**Lead Event &
Engagements**