भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

VAJRA PLATFORM

A DISTRIBUTED LEDGER SYSTEM

An overview of DLT- a new technology that promises highly secure and tamper-evident transactions.
We welcome your thoughts and suggestions at: innovations@npci.org.in.

Vajra Platform – A Distributed Ledger system for automated payment, clearing & settlement

The team at NPCI researched 'Distributed Ledger Technology' (DLT), a new technology that promises to provide highly secure and tamper-evident transactions stored in a distributed and immutable database which is also versatile enough to be adapted to various cases.

After an initial assessment, DLT based system has been designed for automating payment clearing and settlement processes of NPCI products. The platform is named as ‘Vajra Platform’. A permissioned network will be setup so that only the parties who have been approved by the Network Administrator can be a part of the network. Since Vajra is being developed for a payments processing industry, permission less blockchain systems were not considered.

Node is a fundamental component of a DLT. The clearing house node (NPCI), participant nodes (Bank’s/ASP/PPI/PSP) and UIDAI node (Notary node) will be treated as participants of the DLT platform.

DLT and its Potential Benefits

DLT is a new technology with great potential. It promises to provide highly secure tamper-evident transactions that can be stored in a distributed, immutable database and is versatile enough to be adapted to various cases.

Following are the Key benefits of using DLT in the payment processing industry:

1. Minimal reconciliation of transactions, higher resilience and efficiencies through automation and transparency
2. Near real-time clearing and settlement
3. Minimizing operations and financial risks
4. Economical, immutable, secure and easily accessible
5. Provides a legitimate audit trail

DLT is an incorruptible decentralised ledger that not only provides a transaction medium but also acts as a repository for all transactions in hashed digital packets called blocks. The availability of transaction in distributed ledger will reduce reconciliation steps and also increase transparency among participants.

The Vajra Platform

The Vajra framework aims to derive advantage from the Blockchain framework to achieve the following goals:

ZERO/MINIMAL

Vajra framework will reduce manual processing, FTE for reconciliation

DISPUTE REDUCTION

Vajra framework provides faster resolution of disputes.

INCREASED SECURITY

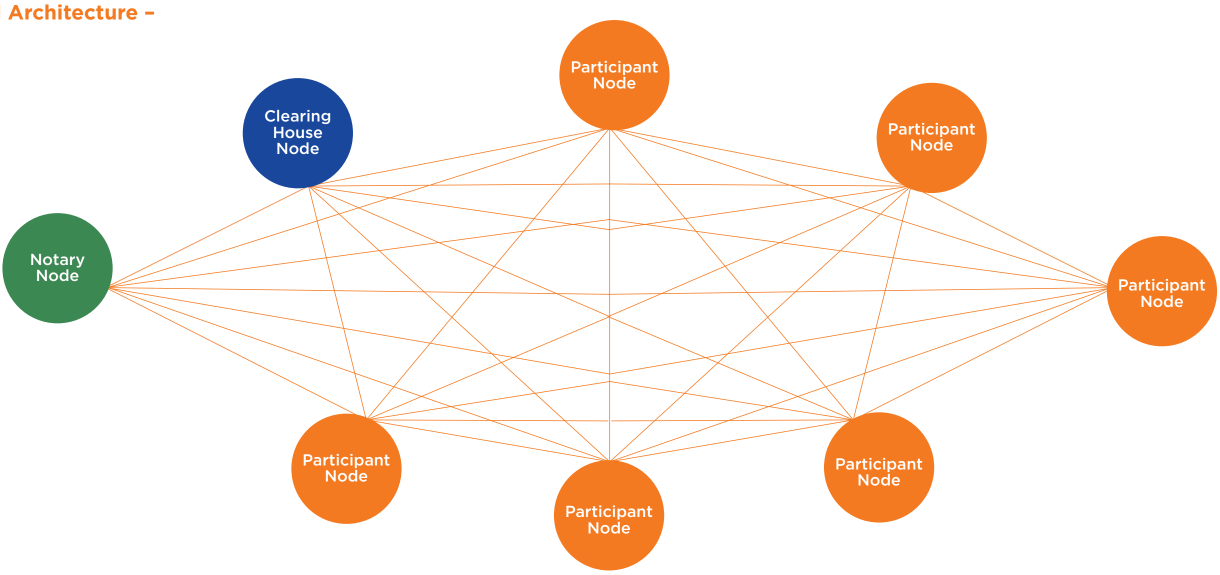
Vajra framework implements cryptography, which will increase the security of payment transactions.

Architecture of Vajra

The Vajra platform will be accessed by multiple payment entities for performing transactions via web interfaces. The bank nodes will receive requests from APIs and will process it on Vajra. The system will have self-executing contracts containing business rules. After successful processing of the requests, the on-chain data (eg. Hashes of the transactions) will be added to the ledger.

Each participant node in the network maintains a ledger of their own. Off Chain database will be used to store information that is not published on the platform (transaction data which doesn't uniquely define the transaction). This data will be accessible only to the node.

High Level Architecture –



There are three types of nodes on the platform:

1. Clearing House node (CHN) for NPCI
2. UIDAI node for Aadhaar authentication
3. Participant node (PN) for all banks/ASP/PPI/PSP

*UIDAI node will only be used in case of biometric authentication.

Node Roles

PARTICIPANT NODE

All banks /ASP/PSP/PPI on the Vajra platform will be the participant nodes. These nodes can post, receive and view transactions on the platform.

For example, for a particular transaction involving 2 banks and 2 PSPs, only the concerned 4 PNs will post and receive transactions. All other banks/ASP on Vajra will be able to only view the header info.

CLEARING HOUSE NODE

The clearing house node will have the Admin rights to this platform and will be maintained by NPCI. It will provide a root-authority-signed TLS certificate from the network's permissioning service to the participant nodes.

NOTARY NODE

The notary node will validate a transaction only if Aadhar biometric is used for authentication. It will receive transactions only from the Clearing House Node.

Node Activities

VALIDATING NODE

- Responsible for validating transactions and adding them to the DLT ledger.
- Ensure performance throughput and security requirements at the platform level.
- Controls access to each external party interacting with Vajra through that participant node.
- Publish keys on the Vajra platform for accessibility and visibility purpose.
- Responsible to whitelist/blacklist merchants and publish account updates to the Vajra platform.

NON - VALIDATING NODE

- Responsible for node management for other participant nodes.
- Controls access rights of other nodes by managing keys.
- Responsible for smart contracts and API management.

Clearing & Settlement on the DLT platform

The current clearing and settlement lifecycle was assessed by NPCI, post which it defined a DLT based processing that focuses on automation of clearing and reconciliation process at NPCI and its partner banks/ASPs.

- When Remitter/Payer/Payee initiates transaction on their App/MicroATM/ Net banking /POS/ E-comm the request for Payment/ Collection/Deposit comes to the server of the Remitter (or Issuing) bank/Payer PSP/Payee PSP

.

- Using DLT APIs or Adapters, the bank/PSP nodes receive the transactions and record the same on the DLT platform.

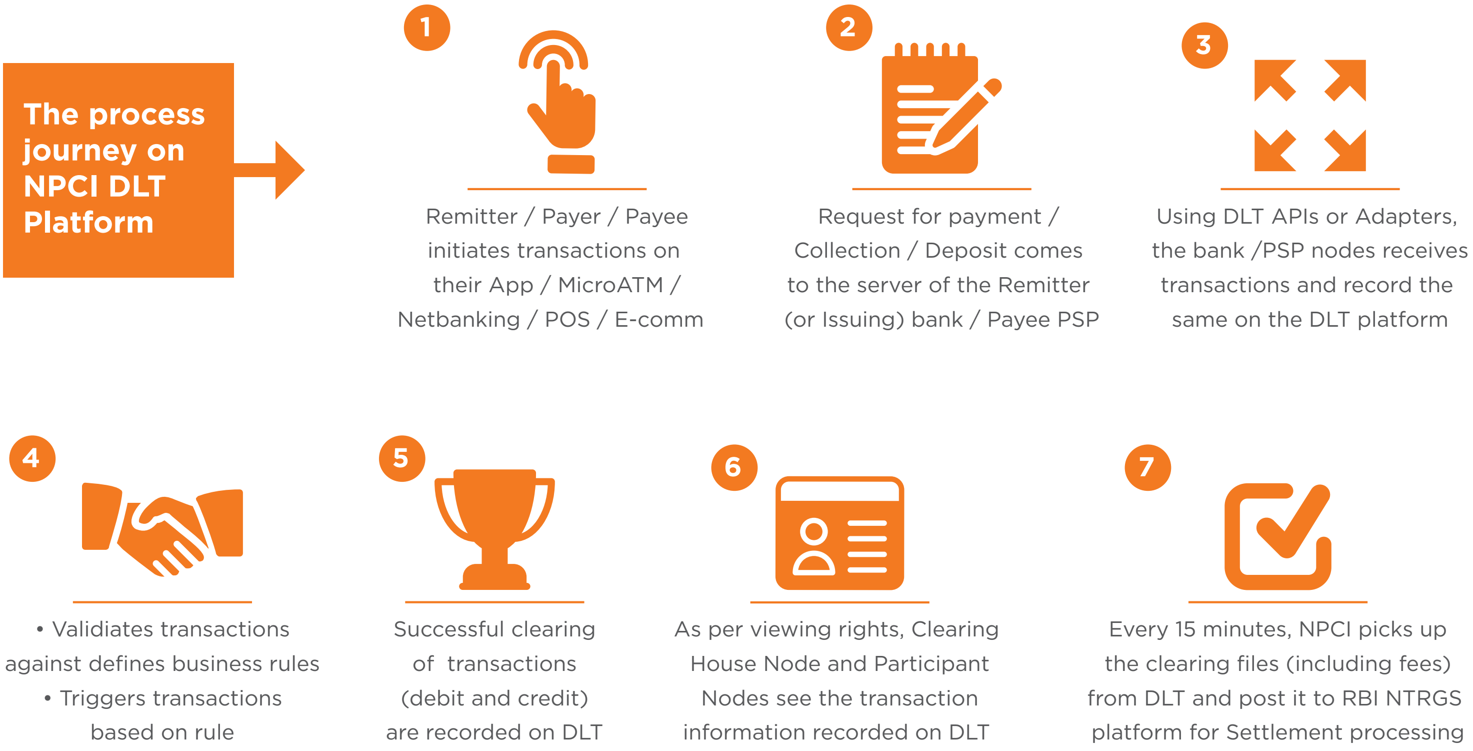
- Smart Contracts running on the DLT platform validates transactions against defined business rules and triggers transaction based on rules.

- On Successful Clearing, transactions (debit and credit) are recorded on DLT. As per viewing rights, Clearing House Node and Participant Nodes see the transaction information recorded on DLT.

- Every 15 minutes, NPCI creates the Clearing files (including fees) from DLT and posts it to RBI NTRGS platform for Settlement processing.

How Clearing & Settlement works on the DLT platform

NPCI assessed the current clearing and settlement lifecycle and defined the Distributed Ledger Technology (DLT) based processing which focuses on automation of clearing and reconciliation process at NPCI and its partner banks/ASPs



The process journey on NPCI DLT Platform

1 Remitter / Payer / Payee initiates transactions on their App / MicroATM / Netbanking / POS / E-comm

2 Request for payment / Collection / Deposit comes to the server of the Remitter (or Issuing) bank / Payee PSP

3 Using DLT APIs or Adapters, the bank /PSP nodes receives transactions and record the same on the DLT platform

4 • Validiates transactions against defines business rules • Triggers transactions based on rule

5 Successful clearing of transactions (debit and credit) are recorded on DLT

6 As per viewing rights, Clearing House Node and Participant Nodes see the transaction information recorded on DLT

7 Every 15 minutes, NPCI picks up the clearing files (including fees) from DLT and post it to RBI NTRGS platform for Settlement processing

Key benefits of Vajra in Payment, Clearing & Settlement

TRANSPARENCY

Real-time visibility into the state of a transaction can help reduce disputes and improve back-end operations at banks and NPCI.

INFORMATION STORAGE

Disparate file systems maintained across banks, NPCI and other participants lead to a lot of reconciliation challenges and disputes. Hence, decentralized and distributed data storage would help reduce the pain of reconciliation across all the participants.

TIME SENSITIVITY

Real time transaction will reduce the clearing and settlement cycle.

MANUAL PROCESSING

Reconciliation and reporting are performed manually which leads to processing error, increased time for settlement and high cost of operation. Now the banks have data setup on node and can do reconciliation as per their convenience.

DATA SECURITY

With highly sensitive customer information being transacted through payment rails, high levels of data security measures are already in place like selective data visibility across nodes (banks/NPCI, etc.)

DISPUTE MANGEMENT

A decentralized and distributed data storage would help reduce the pain of disputes across all the participants.

INTERMEDIARY

Currently Clearing & Settlement process involves multiple unrelated parties transacting with each other. This requires some level of intermediation from a centralized regulator.

Vajra Platform Specific Features

NOTIFICATIONS

DLT Message/Notifications are used for any communication between nodes on the VAJRA platform. Listed below are few categories of Notifications:

- Admin: NDC limits, Network alerts etc.
- Transactions: Debit, Credit, Reversal, Credit adjustment etc.
- Node: Broadcasting keys and node status etc.
- Error notifications: Transaction fail, Node not responding etc.
- Dispute Notifications: Raise dispute, Raise chargeback etc.

COMPLAINTS AND DISPUTES

Vajra network holds the capability of addressing complaints. Due to DLT's transparency, it is very easy to track and address complaints.

It handles the disputes and transfers the queries to the correct entity. This feature covers technical error, technical decline, and business decline for handling proper dispute management.

CONTROLLED ACCESS

Each external party interacting with platform participants are authenticated by the node. The Vajra platform takes care of security in data access / API interaction with key management and defined security procedures

ON BOARD / OFF BOARD PARTICIPANT NODE

Admin Node holds the right to add new nodes onto the platform. The following steps are followed by the CHN to on-board a node onto the Vajra platform.

- Node setup: HA setup, DLT software installation, Convertor application setup.
- Node Identity: Getting node credential from CHN
- Node configuration: Setup access rights, Off-chain db integration, Node certification.

Role of NPCI

ACCESS CONTROL

Vajra platform holds all the access rights of all entities, in order to maintain permissioned network. It provides a root-authority-signed TLS certificate from the network's permissioning service to the participant nodes. Holds the Admin rights to this platform.

HEARTBEAT MANAGEMENT

Vajra network ensures all entities are alive. Nodes – active or down. Monitor the transaction volume node wise and see what nodes are transaction heavy etc. Monitor any anomalies in the NDC/FRM of nodes on the platform.

AI AND ML

Detect frauds using AI and ML as well to connect to external FRM systems. These are external API's which are going to execute against ledger data.

Security and Privacy of Nodes on Vajra

Vajra platform will be a permissioned DLT network where

- The admin node (CHN) holds the right to add new nodes onto the platform
- Validating nodes on the platform are all trusted players
- During Consensus, the trusted validating nodes collect new transactions and exchange the same with intended trusted validating nodes

The Security and Privacy of transactions on Vajra will conform to the Permissioned DLT protocols as listed below:

Security on Vajra platform

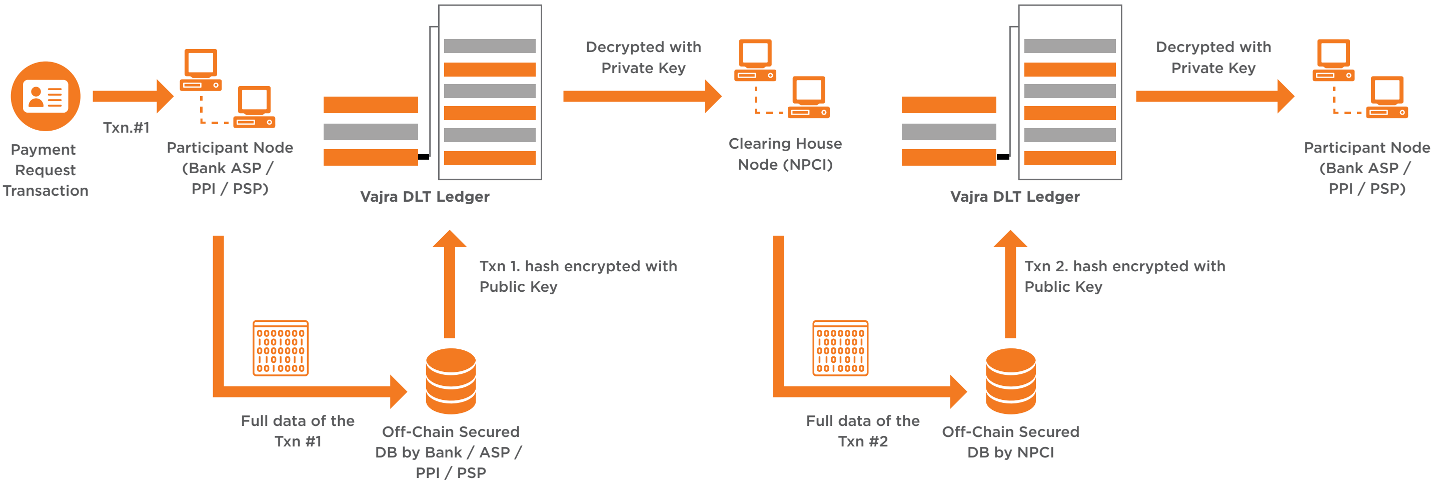
- Permissioned Vajra network will use cryptography security for protection of data.
- Only authorized parties will be allowed to join the Vajra platform.
- Validating nodes will gain access to the Vajra platform only after passing security authentication, for example through the validation of registered digital signature.
- Primary and secondary nodes (meant for DR) on Vajra will ensure no external party can impersonate any of the nodes and thus security of data will be ensured on Vajra.

Privacy on Vajra platform

- Transactions to be encrypted by digital signatures (public and private keys) to prevent unauthorized parties from reading or corrupting transaction data.
- Communication between Vajra and external users to be encrypted to make Vajra data unintelligible to the latter.
- Use of off-chain DB for storing confidential data and storing only the hash pointers to those data on the DLT ledger will ensure data privacy.
- Node identities will be kept confidential to each node except for the public keys.

Data Storage - On-Chain and Off-Chain Mode

On-chain data will contain transaction header with encrypted hashes (visible to all nodes on Vajra).
Off-chain data will contain Transaction data that is not visible (encrypted) to all the nodes on the Vajra platform. Off chain data is compressed periodically using compression algorithms. As and when the data gets older, transaction data is partitioned and compressed in the order of time – yearly/quarterly/monthly/weekly/-daily. By compressing the data, pointers to the data that is stored on the DLT ledger does not change. Whenever the compressed data is to be queried, it will be de-compressed using the compression algorithms.


Payment Request Transaction
Txn.#1
Participant Node (Bank ASP / PPI / PSP)
Vajra DLT Ledger
Decrypted with Private Key
Clearing House Node (NPCI)
Vajra DLT Ledger
Decrypted with Private Key
Participant Node (Bank ASP / PPI / PSP)
Txn 1. hash encrypted with Public Key
Full data of the Txn #1
Off-Chain Secured DB by Bank / ASP / PPI / PSP
Txn 2. hash encrypted with Public Key
Full data of the Txn #2
Off-Chain Secured DB by NPCI

NPCI hopes to achieve higher operational efficiency and zero/minimal efforts by adopting DLT technology (Vajra Platform) for payment, clearing and settlement, thus making transactions a smoother, faster experience for the end user.

Appendix

Disaster Recovery

In Vajra, each participant is provided with two nodes – primary and secondary. Each node will have High Availability and Full Redundancy across primary and secondary. There will be a controller for each participant node to check the availability and load balancing across the primary and secondary.

Only one node per bank will be allowed to initiate a transaction and participate in the consensus. The controller at each participant will redirect the transaction to either the primary or the secondary node depending on availability. Primary and secondary will sync transaction history using external API.

Data archival will not be available on Vajra. Instead, there will be data compression mechanism for external data storage for the participant nodes and clearing house node.

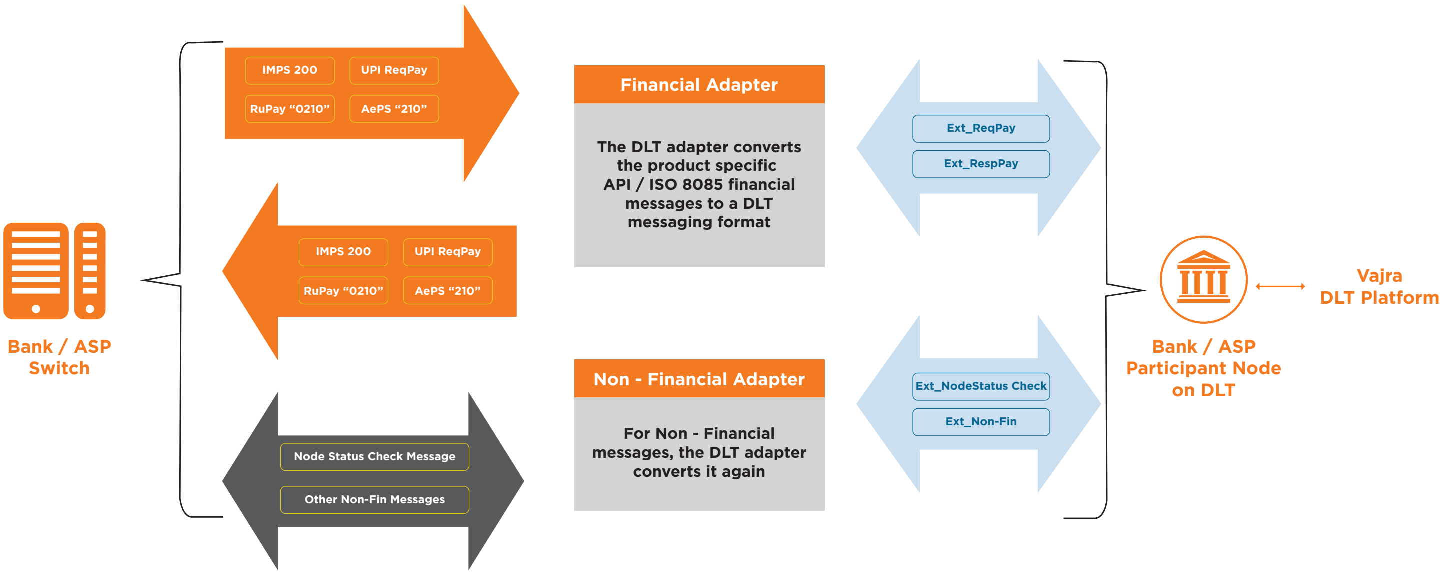
Communication Protocol

The Banks/ASP/PPI/PSP will have 2 options to connect to the Vajra platform.

Using their existing switches

In this case, the banks/ASP/PSP/PPI will get a DLT node and they can connect their existing switches to this node using an adapter provided along with the node set-up. The messages from switches will get converted into a DLT message through the adapter and this will be broadcasted to the intended recipients on the platform. Thus, the node will act like a mirror to the existing switches.

Option 1: How the Adapter works?



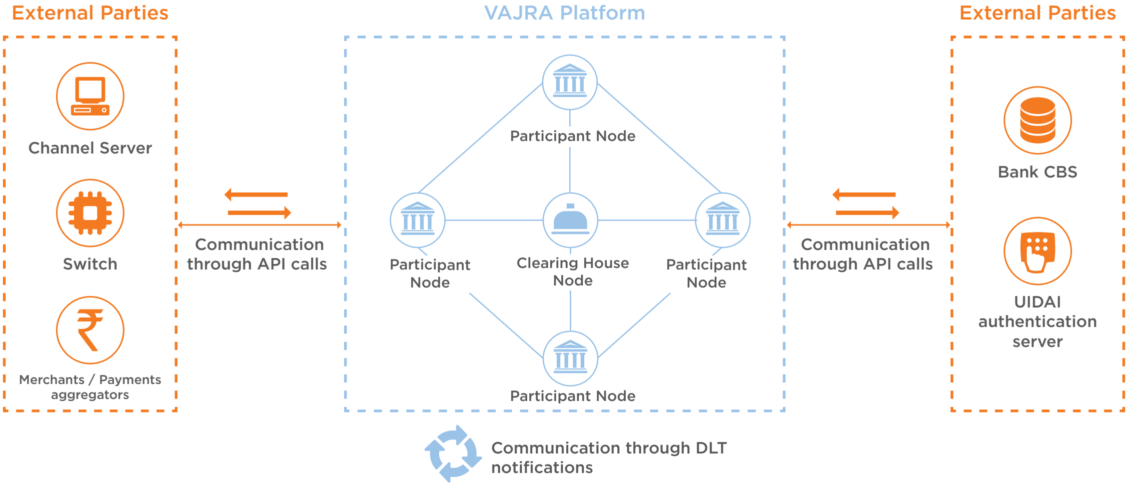
Using a DLT node only (in case the user doesn't have a switch) or replace existing switch with the DLT node

In this case, the banks/ASP/PPI/PSP will have an option to use the DLT node directly to send messages to the DLT platform. The node will essentially incorporate the existing switch and required DLT mapping logic.

Hence, all upstream systems used by the banks/ASP/PSP/PPI like Application/Desktop/ Mobile servers will connect to the participant nodes using DLT APIs provided along with the node set-up.

Communications protocols on VAJRA

There are two types of message formats for communication through VAJRA - APIs and DLT Notifications


External Parties
Channel Server
Switch
Merchants / Payments aggregators
Communication through API calls
VAJRA Platform
Participant Node
Participant Node
Clearing House Node
Participant Node
Participant Node
Communication through API calls
External Parties
Bank CBS
UIDAI authentication server
Communication through DLT notifications

DLT platform parameters:

Network & Hosting Options:
The Vajra platform will be Permissioned, Private and On-Premise. The infrastructure will be maintained by NPCI. Only on-boarded members can have access to Vajra.

API Capability:
The Vajra Platform will develop APIs which can be used by Banks/PSPs to access.

Performance:
High availability, very fast and secured network for enabling payments.

Interoperability:
Ability to interoperate with other platforms if required.

Encryption & Privacy:
High security using public-private key pairs for the Banks/PSPs.

Usability:
Easy to increase number of nodes since banks can be on-boarded on an on-going basis

Components of Smart Contracts:

Contract Terms:
Asset of pre-defined terms and execution conditions agreed by all relevant parties

Event:
One or a series of specific events that can trigger the transaction, which should be carefully defined in the contract.

Execution:
The transfer of value between the contract signing parties when the transaction is triggered.

Data Settlement:
Settlement of both on-chain assets and off-chain assets.

Participant Onboarding Guidelines:

Setting up the Node:
a. Hardware set up with 100% redundancy & HA: Primary and secondary nodes will be provisioned for each participant. Each node will have High Availability and Full Redundancy across primary and secondary. There will be a controller for each participant node to check the availability and load balancing across the primary and secondary.
b. DLT Software set up provided: Deploy the Vajra framework on the nodes and the network.
c. Adapter/API connection: Depending on the bank feasibility will connect bank switch to Vajra using adaptors or DLT APIs directly.

Creating Node Identity:

a. Identity Creation (IP Address): Reserve an IP address for Node in the network.

b. Key Creation (Digital Signature): Create digital certificates, get it signed by the trusted root CA. Store private keys in secure vault.

Node Configuration on VAJRA:

a. Integration with Off-chain DB: Configure off-chain Postgres DB for data analysis.

b. Grant Access as per Node rights: Provide the necessary permissions to the participant nodes to post, receive and view transactions on DLT.

c. Set up UI screens: Create the UI screens for Admin, Participants and the dispute resolution

d. Configure Reports: Develop and maintain Analytics reports.

Operationalizing the Node:

a. Setting up NDC and SGF limits.

b. Publish Node address & identity on the VAJRA platform.

c. Node Heartbeat notifications on the VAJRA platform: Records the status of the primary/secondary nodes every 90 sec and broadcasts to all the nodes on the VAJRA network.

Process level changes in the IMPS flow:

NDC Check

NDC check will happen in an automated way at the Payer PSP/Rem bank PN. NDC check will always happen before the A/C debit request to remitter CBS.

FRM Check

FRM validation will be done by every bank/PSP node using smart contract, which in turn invokes FRM check API to the FRM engine maintained by NPCI.

Credit Request Initiation

Remitter bank node posts debit success message on VAJRA and automated notification goes to Beneficiary bank node to initiate Credit request.

NDC Update & Reset

NDC is maintained at every node on VAJRA and the update is automated through smart contract at the end of each transaction. NDC will be reset after every 15 mins. (New settlement cycle) through Smart Contracts and is updated to all the nodes.

Fee Calculation

Fee calculation is done automatically using Smart Contracts at every 15 mins. (New settlement cycle) at the Clearing House Node level

Payment, Clearing & Settlement

Payment + Clearing + Reconciliation + Fee calculation is automated and Online. Settlement will continue as Offline

DLT Transaction Flow Depiction:

For the 1st payment request, 10 DLT requests (Txn.) will be initiated on the DLT platform, all linked to the first HASH 1. Post reconciliation of clearing information across debit and credit and calculation of fees, the HASH 1 will be completed and added to DLT chain. For the 2nd payment request, a new HASH 2 linked to HASH 1 will get started and will be closed at the end of Txn. #10

At the end of every 15 minutes interval, NPCI operations team pulls out HASH #150 (assuming 150 requests in 15 minutes) which has all the Cleared transactions linked to it and uploads it on the RBI NTRGS system for Settlement. This is Settlement File #1. At the time of creation of Settlement file #1, the NDC limits will be reset. This will happen every time a settlement file is being generated.

Post that when 151st payment request comes to the platform, a new HASH 151 linked to the latest HASH 150 will start and the chain thus continues throughout the life-cycle of the DLT.

DLT HASH creation for UPI 4-party Push scenario:

Let us depict the DLT transaction flow using a real-life scenario:
Remitter with VPA abc@ybl on PhonePe app sends money from his Axis bank A/c
Beneficiary with VPA xyz@oksbi on Tez app receives money into his RBL bank A/c

Step 1: PhonePe Server to make APIs calls to Yes Bank PSP PN for checking the Node Status.

Step 2: Yes Bank PN will send status response to PhonePe server.

Step 3: PhonePe Server requests for Validate Address to Yes PSP PN for VPA resolution of the Payee/Beneficiary.

Step 4: A smart contract for VPA resolution will trigger and will check for the following:
a) If(Bene details contains @oksbi)
b) If(SBI is alive as per latest Heartbeat Notification)
Then post VPA resolution notification on VAJRA for SBI PN with data as xyz@oksbi
Clearing House Node will also be notified for providing consensus.

Step 5: SBI PSP PN validates address and resolves the beneficiary details corresponding to xyz@oksbi from its off-chain DB and posts Beneficiary A/c No., IFSC and MBIN on DLT.

Step 6: On receiving DLT notification, Yes Bank PSP PN sends details to PhonePe App via API and also requests Amount, UPI Pin and Debit Confirmation from user.

Step 7: PhonePe app channel server makes API call to Yes Bank PSP PN with the Beneficiary Address and Amount.

Step 8: On receiving request for payment on any of the PN, it will trigger Smart Contracts to check for NDC limit of Axis & RBL and (FRM check) will fetch the FRM score. The response from both will be captured in a message.

Step 9: If NDC and FRM are successful, Yes PN posts Debit req. notification on the DLT to Axis PN.

Step 10: On receiving Debit request, Axis PN makes Debit API call to Axis CBS for UPI Pin Validation and balance check. If successful, then A/c is debited and the same is posted on VAJRA by AXIS PN as Debit Success message.

Step 11: On being notified about Debit Success, RBL PN makes Credit API call to RBL CBS.
If PN receives successful credit message, then RBL PN posts on DLT the Credit Success message.

Step 12: Yes PSP PN sends success message to Axis Channel Server using API call.

Step 13: A Smart Contract for NDC Limit Update will get triggered in the network after RBL PN receives message then NDC will be updated and broadcasted to all the Participant nodes and CHN.

Step 14: A Smart Contract for Calculation of Fees will get triggered at the end of every 15 mins for all transactions at CHN. It calculate fees and generate a message to the concerned parties involved in transaction.

Challenges and Solutions:

CBS Communications:

In existing system, bank CBS produces and consumes ISO messages only. In order to interact with DLT platform the message format is different. To address this issue an adapter is placed in between bank and Vajra framework. The adapter will be interface between bank and Vajra.

On-boarding banks:

The bank/ASP/PSP/PPI will get a DLT node and they can connect their existing switches to this node using an adapter provided along with the node set-up. The messages from switches will get converted into a DLT message through the adapter and this will get broadcasted to the intended recipients on the platform. Hence, the node will act like a mirror to the existing switches.

The bank/ASP/PPI/PSP will have an option to use the DLT node directly to send messages to the DLT platform. The node will essentially incorporate the existing switch and DLT mapping logic required. Hence, all upstream systems used by the bank/ASP/PSP/PPI like Application/Desktop/Mobile servers will connect to the participant nodes using DLT APIs provided along with the node set-up.

Disaster Management:

As Blockchain doesn't have own disaster recovery mechanism, node architecture redesigned by using node controller and introducing primary and secondary node concept.

Frequently asked questions

What is the difference between public and private block chain?

A Public Blockchain is a permission less blockchain. Anyone can join the blockchain network, meaning that they can read, write, or participate with a public blockchain. Public blockchains are decentralised, no one has control over the network, and they are immutable, as the data cannot be modified once validated and accepted by the network.

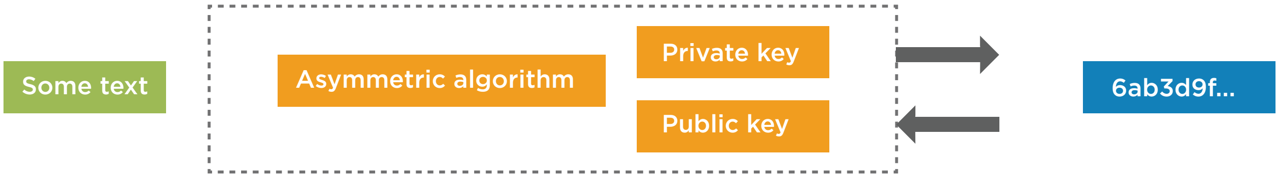
On the other hand, a Private Blockchain is a permissioned blockchain. Permissioned networks place restrictions on who is allowed to participate in the network and the type of transactions.

What Is A Smart Contract?

A Smart Contract is code that is deployed to the blockchain. Each smart contract contains code that can have a predefined set of inputs. Smart contracts can also store data. Following the distributed model of the blockchain, smart contracts run on every node in this technology, and each contract's data is stored in every node. This data can be queried at any time. Smart Contracts can also call other smart contracts, enforce permissions, run workflow logic, perform calculations etc. Smart contract code is executed within a transaction – so the data stored as a result of running the smart contract (i.e. the state) is part of the blockchain's immutable ledger.

What is encryption? What is its role in Blockchain?

Data security always matters. Encryption is basically an approach that helps organizations to keep their data secure.



The encrypted data is encoded or changed up to some extent before it is sent out of a network by the sender and only authorized parties can access that information. In Blockchain, this approach is useful because it simply adds more to the overall security and authenticity of blocks and helps to keep them secure

Blockchain is a distributed database. How does it differ from traditional databases?

Properties	Blockchain	Traditional Database
Operations	Only Insert Operations	Can perform C.R.U.D. operations
Replication	Full Replication of block on every peer	Master Slave Multi-Master
Consensus	Majority of peers agree on the outcome of transactions	Distributed Transactions (2 phase commit)
Invariants	Anybody can validate transactions across the network	Integrity Constraints

What is the advantage of Distributed Ledger Technology?

A distributed ledger gives control of all its information and transactions to the users and promotes transparency. They can minimise transaction time to minutes and are processed 24/7 saving businesses time and cost. The technology also facilitates increased back-office efficiency and automation.

Where does the data of the Blockchain get stored?

Data on blockchain gets stored in a block over the public ledger, which means that every participant has a copy of the entire chain.

What are the changes to be made from the banks for PoC?

No changes are required from the Bank infrastructure. The banks have to whitelist the Vajra adaptor IPs and the ports. Banks have to generate the transaction for the corresponding banks which are the part of POC.

भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA