Digital Transformation for Co-Op Societies

Leveraging Blockchain and AI to decentralise Cooperative society management and operations

Author : Kapil Jain | jain.kapil@outlook.com | https://www.linkedin.com/in/kapil-jain-9829aa4/

Abstract

Cooperative Movement in Bharat has been on-going for more than a century since its formalisation in 1904. Deeply rooted in the principles of cooperation and reflective of the ancient philosophy of 'Vasudhaiva Kutumbakam,', it has undergone a (digital) transformative journey with creation of National Cooperative Database (NCD) as the much needed essential online platform capturing and organizing information on 8.0 lakh+ registered Cooperative Societies having membership of more than 29 Crores people. Needless to say these grass root systems emerge in an organic fashion, sustain and run for the benefits of the participants. Large number of cooperatives (PACS or primary agricultural societies) are the heart and soul of the food production and distribution and so is the milk cooperatives (Amul, Nandani etc.) which still are the household daily need providers of milk.

Even with such widespread usage, there is little work done in terms of digital transformation of these systems. With creation of NCD database, the central registry for all cooperatives is now present, but this ecosystem is missing out on a lot more that can be achieved, specifically with the advancement that have happened in building decentralized p2p systems with Blockchain (DAO) and AI/ML (Automated Agents). Using the DPI philosophy of protocol based network and blockchains, we can democratize and decentralise these systems and put the control of such organizations into the hands of individuals.

Introduction

Cooperatives are true form of P2P network systems which are functional not just in Bharat but across the world. It is but fitting to disrupt cooperative legacy manual systems using digital transformation capabilities provided by blockchain and AI. This will enable the exactly same business and functional structure that currently exists with cooperatives to be implemented digitally enabling decentralisation, privacy and transparency in transactions and contracting.

As a summary, following are the attributes of a cooperative that will be considered unchangable when implementing this system.

1. Voluntary and open membership,
2. Democratic member control (of the organization by members),

3. Member economic participation (in profits generated by the members' activities and losses),
4. Autonomy and independence (from investors control),
5. Education, training, and information (on co-op governance training and co-op-alignment political values),
6. Cooperation among cooperatives, and
7. Concern for the community.

We propose to keep the sprit of cooperative mentioned in above 7 points and implement a P2P/ Decentralised system which enpowers the individuals in same, but efficient manner, while also bringing privacy, security and transparency in formation, administration and managment of cooperatives.

Digital Transformation of Cooperatives using DAO

A DAOs represent a further evolution of the corporate form, fostering the creation of dis-intermediated communities and networks where participants control decision-making and their assets. There is no consistent bright line legal definition for a DAO but, at a rudimentary level, a DAO is a nimble group of people who act together in a joint enterprise for a common purpose. Given the commonalities between DAOs and traditional cooperatives, we will argue that the cooperative is the safest and most ideologically suitable corporate structure for DAOs.

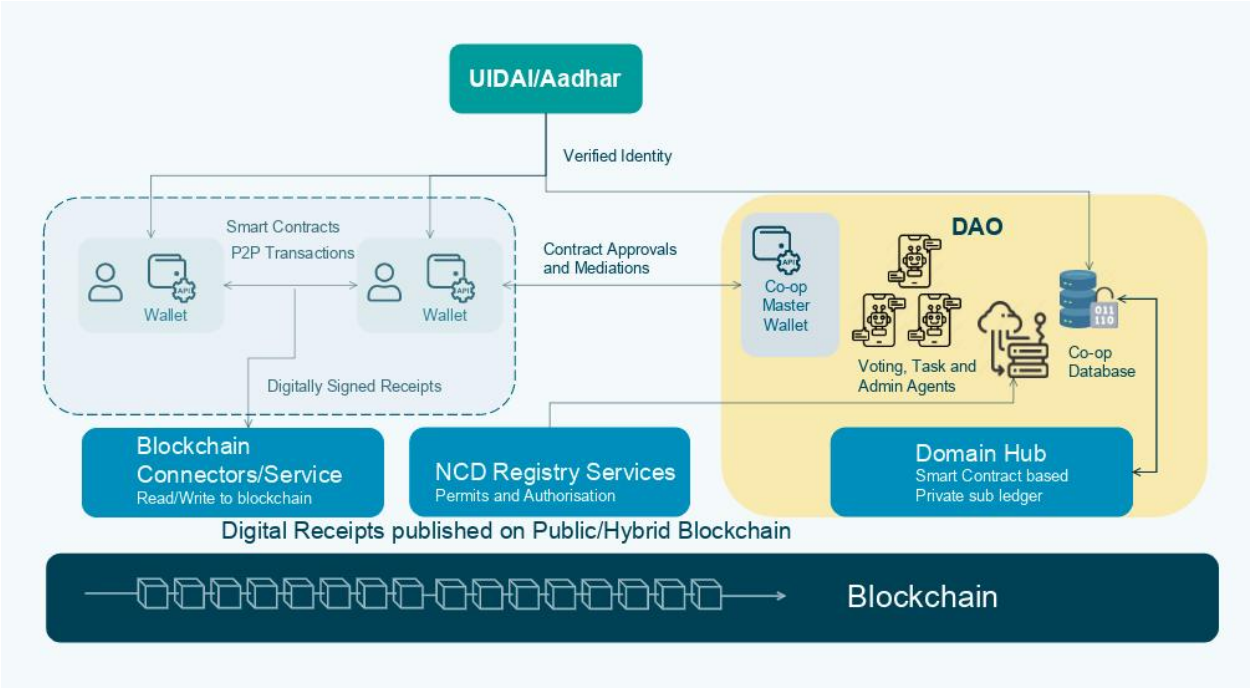
We establish the relationship of a DAO and Cooperative at the formation itself when the DAO issues N tokens to raise money.The tokens represent the company shares. The tokens grant its holder ownership and voting rights. This token will have no relationship with the digital asset in case a public blockchain is used. The Token representing the ownership share will allow the owner participants to vote based on their authority of investment they have put in. Apart from this, there will not be any native currency introduced as part of this system. In case there is a need for creating a virtual token representing the rupee value of the business contracts or transactions, that will be done as a virtual token in the system only for accounting purposes. The actual payment infrastructure used will be the UPI/Banking payment infrastructure, while this (DAO) system will have a entry similar to how an accounting book maintains the entries of transactions done (debit/credit).

We will describe in this paper various steps that this digital transformation would require to be implemented and then capture the benefits for not just cooperative systems but also the participants to expand not just their business but also their outreach and connectivity with fellow cooperatives and their participants (interoperability between cooperatives).

We will assume the availability of following government services which can be leveraged by this system.

1. UADAI – Digital identity provided via Aadhar
2. NCD – Central registration services provided by NCD
3. C-DAC Blockchain/Public Blockchain that is approved to be used for this system.

On a very high level, such a system layers are shown below.



The system will implement the idea of triple entry accounting using a blockchain where the digitally signed receipts of the actual contract will be stored. These receipts will ensure the trust in the system as this receipt will be used to verify and validate the business contract in case there is a dispute between the two transacting entities.

Features Explained

Lets look at various components/features that make up this system.

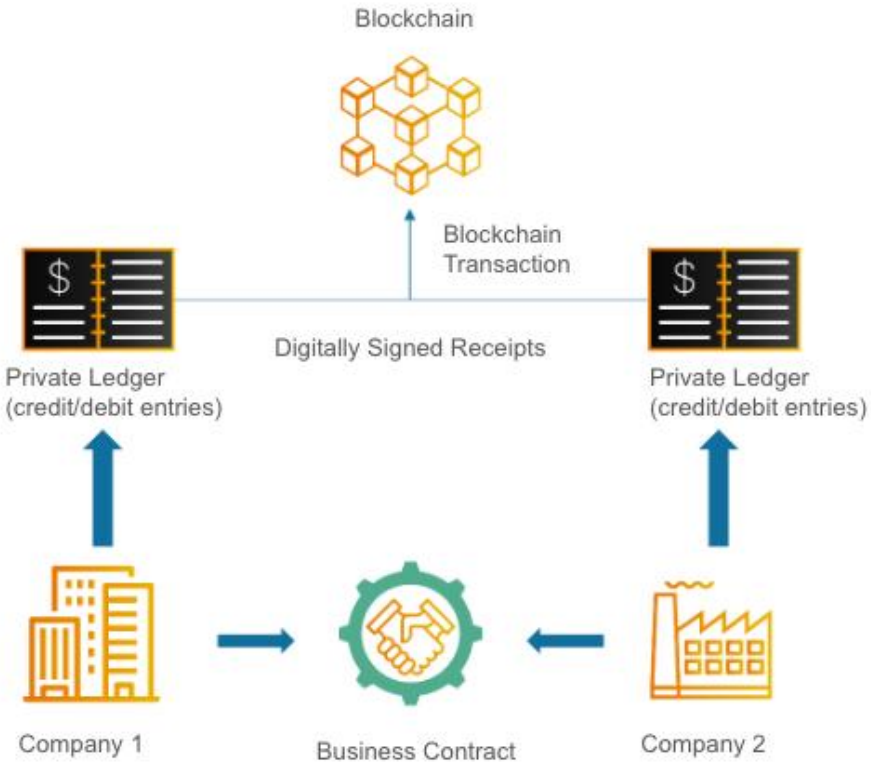
Triple Entry Accounting Ledger

The main idea behind the system is an implementation of a Triple Entry accounting process and that is the main usage of blockchain.

Double-entry accounting is a bookkeeping process where two separate debit and credit entries are made for each recorded transaction, and an external party (an accountant) acts as an auditor.

Double entry was transformational, not only because the system was more trustworthy but also because it helped to create the accounting profession. Accountants act as independently credible third parties outside of a family or business. This degree of separation acts to reinforce the trustworthiness of a ledger. That party has its independent credibility and accountability. However, double-entry accounting is a highly manual and complex process and is therefore prone to errors and sometimes even malfeasance when multiple ledgers are created and maintained by creating and maintaining multiple books.

The main idea behind the creation of a blockchain comes from here; it enables **triple-entry accounting**, which introduces a third entry (time-stamped immutable digitally signed receipt record on the blockchain) in addition to the debit and credit entries. Its purpose is to introduce a degree of automation and transparency into bookkeeping. Once the entry is created, it is public and immutable, making it very difficult to change any records.



The above diagram shows an example of triple entry accounting using a blockchain. When used in this manner, the blockchain becomes a method of storing signed digital receipts of any business contract, providing an evidence log of the contract that happens between two private parties but using this publicly recorded signed receipt which will contain the signature of the actual business contract, either of the participant can prove the existence of the contract providing a legally admissible audit log. This on the face of it looks a simple usage but this is the only new concept that the blockchain technology brings in.

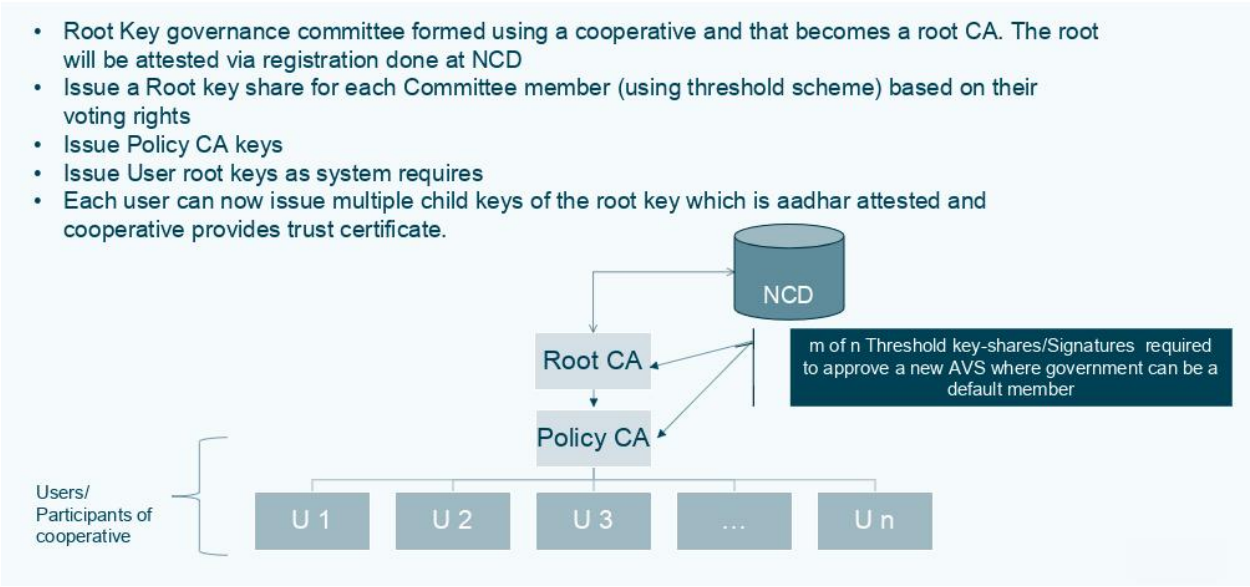
Privacy and Identity

Identities are decoupled from the system by using a Chain of trust implementation of aadhar attested PKI infrastructure. Due to this decoupling, the system can by fully private but still maintaining the legal and compliance requirements based on specific needs as they arise in future.

The Chain of trust system is same as the system used by SSL certificates where the Rook keys are attested by a CA or a trusted entity to identify the engaging party. In addition to that, we will be using standard PKI infrastructure for keys generation and digital signatures. What we propose is use of two set of attesting entities -

1. UADAI attesting identity of individuals via aadhar APIs
2. NCD providing attestation of registration and legal standing of a given cooperative.

The high level structure of these identities are shown below.



Alternative to using threshold signatures, we can also use a multisig setup for simplicity's sake. There is also an aspect of shareholding and voting required which will be address in the section describing autonomous voting agent.

The system is such that a child key of the above described root key is used for any transactions and digital receipt signing on the blockchain enabling a fully private system for everyone except the transacting entities and the auditor.

There will be an on-boarding process, wherein first when the cooperative is established, it will register itself with the NCD and get the registration unique ID associated with itself. Based on that its root key will be generated. Then we will be using HD key generation to derive child keys from the root key. We can have setups where there is a unique root key of cooperative used for attesting every user root key. We have options of using the W3C specification for generating identity/credentials or a custom method of generating digitally signed certificates using x509 specifications (like SSL).

Threshold Signatures

Using cutting edge technology of splitting a private key into n number of shares allows for the unique feature of a private key without existing can be used for signing of transactions. Typically m of n threshold would mean that m number of shares need to be provided so as to sign a transaction which is setup as m of n threshold. These key shares can be done using Shamir's secret sharing scheme. This is one of the advancement that has happened and can be used to setup a root key management system for the cooperative and its policy CA.

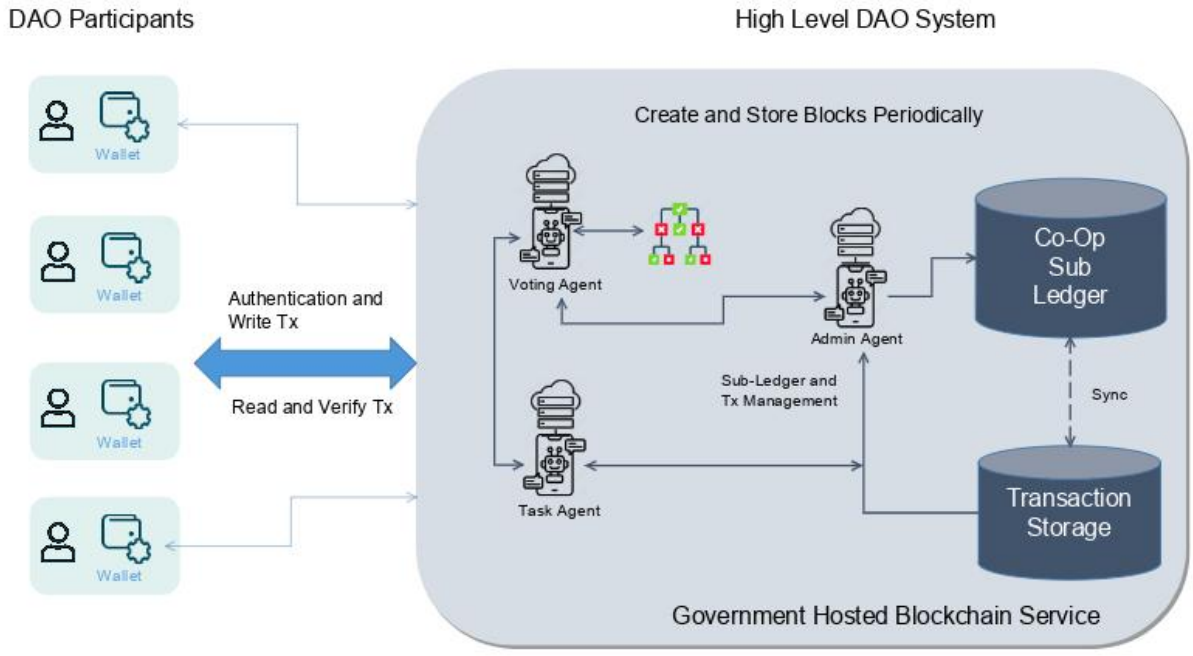
Autonomous Agents

A DAO is decentralised only because it is at the time of setup, set in stone in terms of what rules it will be using to operate on. This is essential for it (DAO) to be resilient in terms of any entities changing the system for their benefit. This also means that it is essential to design and build these automated agent in a transparent and tamper free manner.

We envision three different types of Agents to be used in this system.

1. Administration Agent : Admin agent will be performing basic admin tasks like adding or removing members, managing issuance, transfer and burning of the tokens issued by DAO, Auditing data collection and any other administrative function created based on the policy/rules.
2. Voting Agent : Voting is an essential and critical functionality of this system and ensuing the transparency and integrity of the system is as good as its voting systems's sanctity. Using blockchain transaction as a vote is a unique technology which can provide the features required for building such a voting system. Automating the whole process will define the formation and working of this agent. In future the voting process can add a decision making algorithm or an ML/AI agent for voting on behalf of participant or committee.
3. Task Agent : Depending on the complexity of the system there could be many task agents that can be part of this system. On the initial state, we define the task agent to perform the work needed for establishing and executing smart contracts that are part of this system. This agent will also maintain the sub-ledger for this cooperative which needs to be tied up with any domain/bank level ledger which will depend on how the system is designed.

A high level overview of the system is shown in the diagram below.



The Voting agent will enable end to end voting and result calculation process and with this, it provides a mechanism for the cooperative to seek decision inputs from its participants to sort of

“vote to decide”. This enables democratic decision making in the cooperative. We will have the voting itself private but the digital receipt uploaded to the blockchain to ensure the trust, transparency and tamper resistance in the system functions.

Admin agent will maintain the sub-ledger accounting book for the cooperative. This agent will also interact with the domain hub to retrieve relevant business contract templates which are needed by the participants or the cooperative itself for performing lending, trade and/or exchanges of funds. The sub-ledger can also store the contract original data while the transaction will be only containing hash/signatures as digital receipts to ensure privacy in the system.

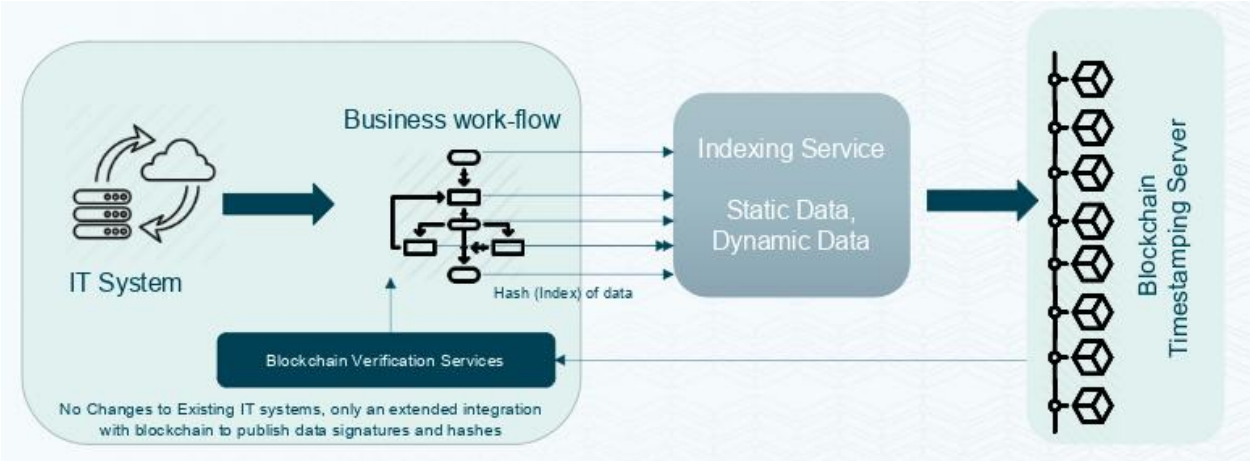
Task Agent as defined here will enable various ad-hoc or planned business logic functions which are specific to the policies that the cooperative has decided for themselves. It could be around the profit distribution as dividends or frequent checkpoints of the system integrity or performing an audit for regulatory and compliance purposes.

Domain Hub and Smart Contracts

Smart contracts are digital contracts that are automatically executed when predetermined terms and conditions are met. They are typically stored on a Public-Blockchain. Smart contracts are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss. They can also automate a work-flow, triggering the next action when predetermined conditions are met.

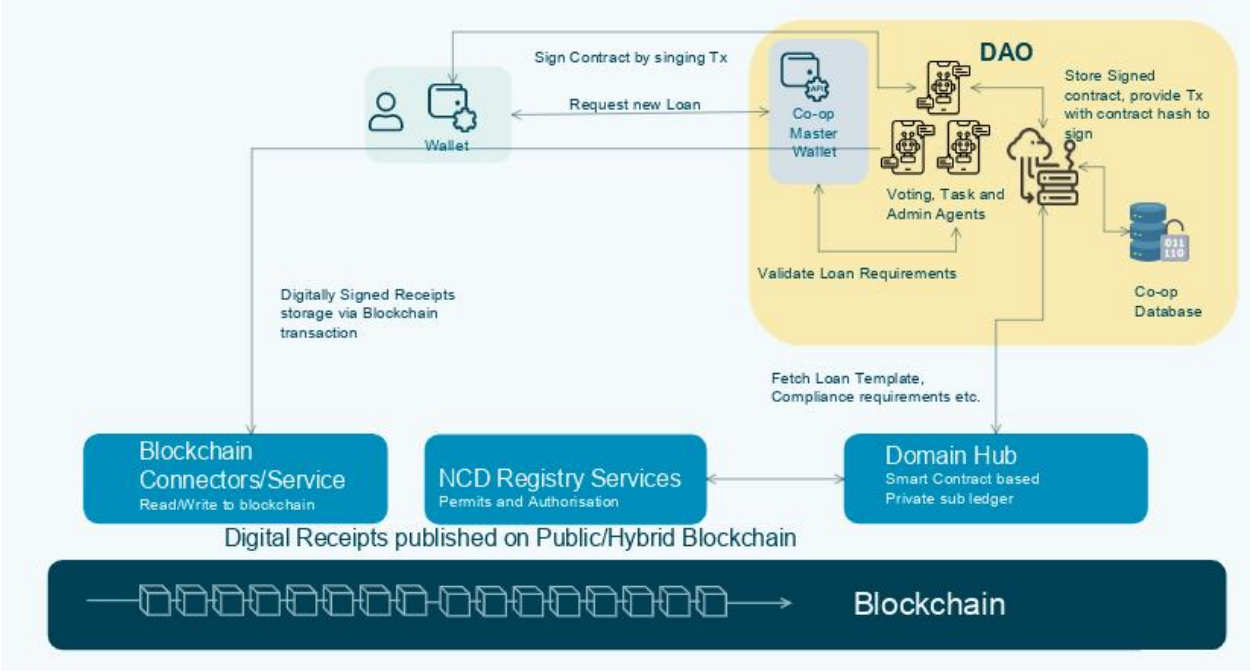
Smart contracts work by following simple “if/when…then…” statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions are met and verified.These actions might include releasing funds to the appropriate parties, registering a vehicle, sending notifications or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.

Since publishing of confidential business contract information on a public blockchain will pose a lot of risks, challenges and private information leakage, we take the approach of storing the actual contract information in a private database but we will generate a signature (called as hash) from the contract data and publish this hash with digital signatures of the participants on the blockchain transaction. This allows us still to have the same results that are achieved using a blockchain stored smart contract but still be able to keep the contractual information private. This process is described as a generic flow below. This is what we will implement.



As shown above, any IT process or business process work-flow will have the data-sets identified which needs protection from data tampering. Then the hash of the data is produced and a blockchain transaction is created which will have a data component which contains this hash value. The signing of this transaction acts as electronic contract singing using digital signatures by the participating entities.

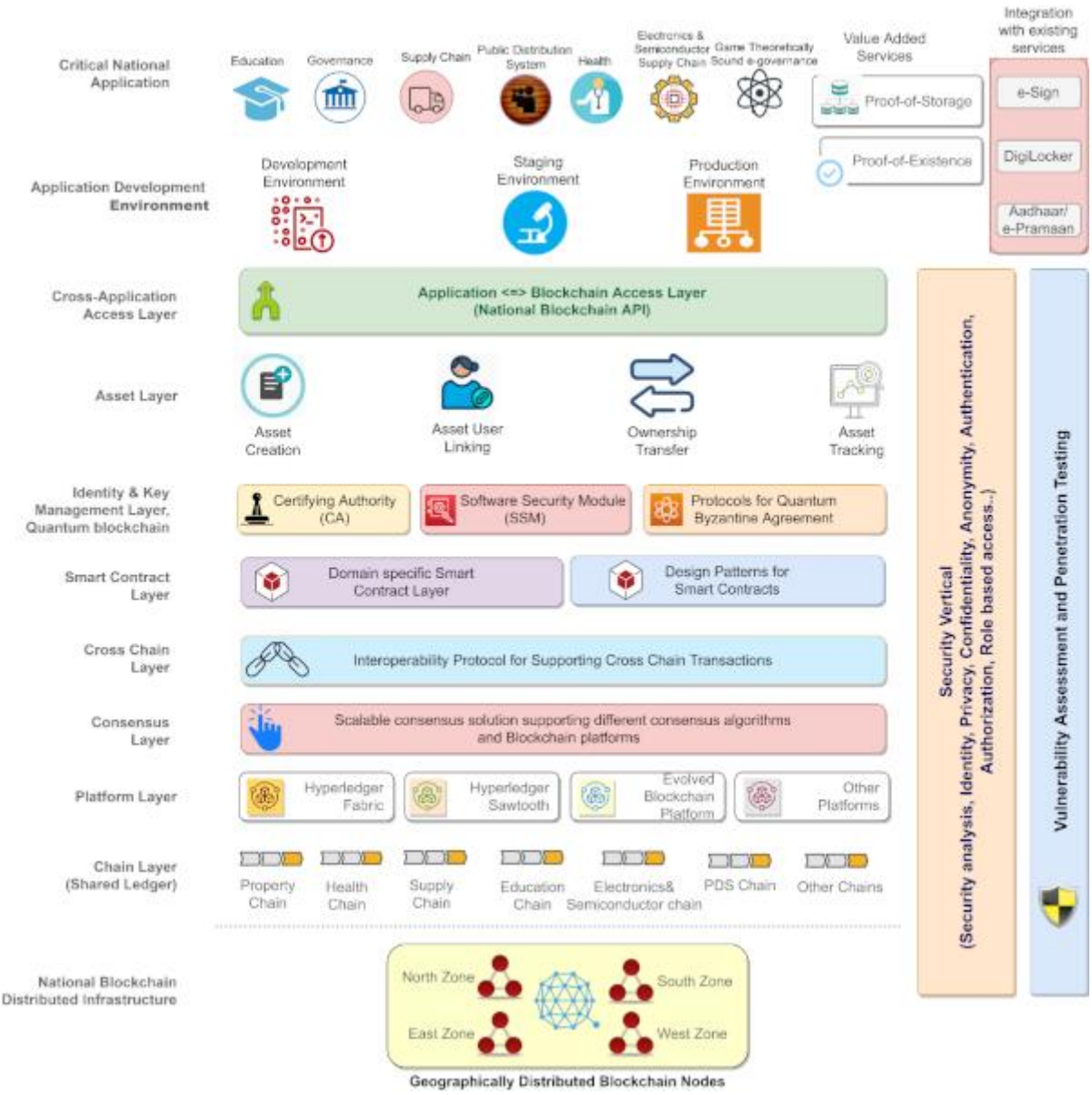
Based on the above described principles, we use domain hubs to publish standardised templates, and when the DAO needs to use one, they fetch the template from the domain hub, create a new instance of it and fill in the PII (personally identifiable information) and store them in the local database. Then a signed transaction with the hash of the contract data stored is provided to the contract co-participants to sign, and this tx is then pushed to a blockchain. This process is described in the diagram below.



Such a cooperative system itself or in collaboration with NCD host a smart contract hub which will define and store standardised business/electronic contract templates that are valid for any cooperative to use. This will ensure the critical aspect of enabling interoperability between any two cooperative and align this system design with the core philosophy of DPI, a protocol based network.

Blockchain Integration

This system does not assume any specific blockchain to be tied up with, but it assumes certain capabilities of the blockchain that it will leverage. These capabilities are described in the below diagram which is published by c-DAC/National blockchain strategy using hyperledger custom implementation to achieve the creation and publication of a national blockchain.

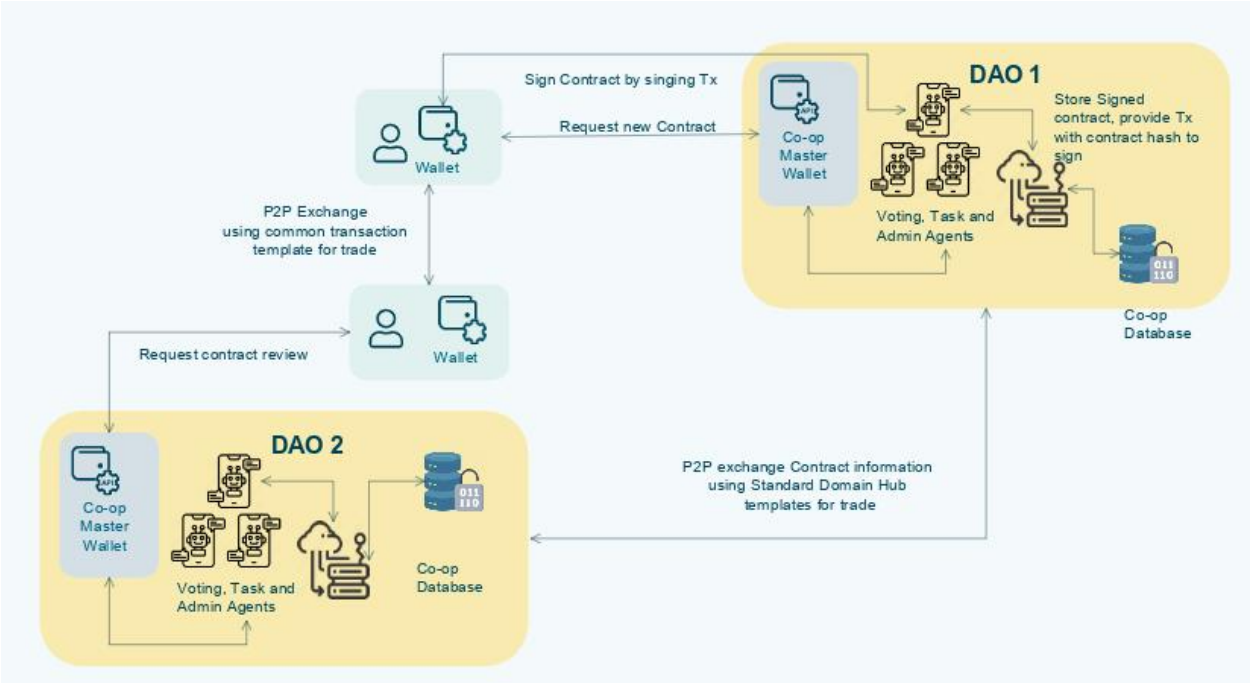


Mapping the system components with the functions mentioned above -

Capability	Component in DAO system
Asset layer	DAO system
Identity & Key management layer	Chain of trust PKI and Identity implementation in a P2P manner
Smart contract layer	Co-Op Ledger
Cross Chain Layer/Chain Layer (shared ledger)	Domain Hub

P2P Accounting

There will be two different types of Peers in this system. The Cooperative hubs will form one type of peers which can interact with other cooperatives using standard domain hub's contract templates and interoperable Identity solution. The other kind of peers will be individuals who are part of a cooperative and can transact with each other within the same cooperative or even with individuals from other cooperatives. However this interoperability requires both the cooperatives to be on-boarded and using the same protocol/design described in this paper.



The diagram shows two individuals, belonging to different cooperatives transacting for a trade with each other. In doing so they will also have their respective DAOs validate and verify their information, contract information and eventually execute the trade. Let us have a detailed steps walk-through for this example.

Lets assume two individuals (Amar and Bikram) belonging to two different cooperatives are engaged in a trade for their business. A is selling B and both want to enter into a contract which would require Bikram to fund the invoice produced by A so as he can use the fund to produce the large order by A. A in turn wants to take a loan from his own cooperative for the manufacturing unit he is running which will produce the raw material to be provided to B. While B will consume the produce in his business and will manufacture the final product based on delivery by A to sell in commodity market. Both enter into following 3 contracts.

1. B enters into a contract of loan from his cooperative to fund the produce so as he can fund the payment he has to make to A. He will return the money once he sells the final product back to his cooperative.
2. A needs funding to produce the raw material that he needs to deliver to B. He also enters into a loan contract with his cooperative. He will return the money once he receives the payment for his invoice from B.
3. Both A and B enter into a business contract which details out their agreement of sale, time-lines and other contingency measures that are needed for addressing various risks.

Based on this, we will now mention the steps these three contracts will use this system. Just to note here, that both A and B will first establish their wallet and keys by first enrolling into their respective DAO's system and getting their identity attested via Aadhar.

Steps :

1. A and B communicate and decide to enter into a contract and agree on contract definition.
2. A requests a contract template from its DAO. DAO(A) fetches the contract from the domain hub.
3. DAO(A) responds with a contract template to A. Signs for attestation as well.

4. A shares the partially constructed transaction with its own signature on the contract with B. The Tx will contain the hash of original filled in contract (without signatures at this point). The contract is also hosted now by the DAO(A) sub-ledger, for authorized entities to access.
5. B receives the transaction, extracts the contract hash using which he will access DAO(A)'s API endpoint to access the contract data. He will then review the contract details to agree or disagree.
6. If B agrees, he will sign the Tx with his aadhar attested key's child key. The now constructed transaction will be returned to A for uploading it to the blockchain.
7. B will submit the contract to its own DAO(B)
8. A will review and publish the transaction to the blockchain. A will also submit back this transaction to its own DAO(A)
9. DAO(A) will store the Tx for future audit purposes. We call this contract C(A,B) from here on.
10. A now applies for a loan based on C(A,B) to DAO(A)'s bank. Bank verifies and validates existence of C(A,B) with DAO(A) and assess the eligibility of A to receive the loan. If met, they disburse the loan amount. DAO(A) updates the loan information.
11. B also applies for a loan based on C(A,B) to its DAO(B) so that he can make the payment for the invoice provided by A in time.
12. DAO(B) will make an assessment of the eligibility of B to receive the required loan amount, and provide the recommendation to its Bank for fulfilling the loan request from B.
13. DAO(B)'s bank will furnish the loan to B. B will make the payment to A using the loan amount once A has delivered the goods.
14. Both B and A will close the contract by updating the final state of contract in DAO(A)'s system. DAO(A)'s system will create an updated Tx with the newly updated contract hash. DAO(A) will pass on the Tx to A who will sign this Tx to provide his approval of closure of contract.
15. A will then pass on the Tx to B. B will validate the closure document by accessing the contract data published by DAO(A) using the new Hash value in the Tx
16. Once satisfied, B will sign the Tx indicating that he has agreed to close the contract. He will then commit the Tx to the blockchain.
17. Both DAO(A) and DAO(B) update the contract status and the new Tx details for audit purposes.
18. A will now will settle in his loan with DAO(A)'s Bank by making the payment from funds he has received from B. DAO(A) and its bank will then close the loan contract.
19. B will sell the produce to open market and receive the funds. He will then repay the loan it has taken from DAO(B)'s bank and close that contract.

Please note that the steps are just mentioned as a proposed work-flow of creating and managing these contracts but actual work-flow can have some changes based on the final business requirements.

Assumptions/Dependencies

- We assume that there will be many contract templates which might be more complex in terms of their execution and enforcement, which will be handled as per the regulatory requirements in the solution.

- There is a number of assumptions made in terms of the usage of blockchain. Firstly we expect that the blockchain supports the UTXO methodology. This is needed as some of the solutions would require UTXO approach of transaction building and spending of tokens. Other assumtions are availability of blockchain integration APIs, and shared ledger programming capabilities.
- We also assume that the cooperative banks and cooperative have a relationship and also these banks can provide the needed payment infrastructure. We also assume a technology support for this new system from the existing IT systems of bank, cooperatives.

POC Requirements

Building a POC for such a system would require building each of the described components but for a limited/single happy path use case. We expect the timeframe to build a POC will be about 6 months -

Business analysis and requirement gathering, documentation : 2 months

Software Development : 6 months

Testing : 6 months

Implementation : 1 month

Project management and buffer : 6+ months

All of the above mentioned streams will be run parallel and will first have to be desined in form of either user stories or delivery block as suitable. There will also be a need of customer engagement (i.e. the pilot customer) during the testing and business analysis phase.

The rough order of magnitude (ROM) estimates for each of the component is mentioned below.

Component	Description	ROM estimate in man days
User wallet	Light weight client of DAO, Identity management and P2P transactions	300
DAO for cooperative with Automated agents	Cooperative will run the DAO software, enabling smart contract functionality, blockchain connects, shared ledger (domain hub) connections	500
Domain Hub/Shared Ledger	Contract templates, common and public data store	300
Connecters with NCD, Aadhar and Blockchain	Various middle-ware	300
Project management		250
Buffer		250
Total Man Days		1900 Man days.

Other POC details :

Appendix I

Multi-State Co-Operative Societies (Amendment) Bill, 2022

The Multi-State Co-operative Societies (Amendment) Bill, 2022, **aims to enhance transparency, accountability, and ease of business in the cooperative sector**. Some key provisions of the bill include:

1. **Election of Board Members**: The bill establishes the Co-operative Election Authority to conduct and supervise elections to the boards of multi-state co-operative societies. The Authority will consist of a chairperson, vice-chairperson, and up to three members appointed by the central government.
2. **Amalgamation of Co-operative Societies**: The bill allows state co-operative societies to merge into an existing multi-state co-operative society, subject to the respective state laws with at least two-thirds of the members' consent.
3. **Fund for Sick Co-operative Societies**: The bill establishes the Co-operative Rehabilitation, Reconstruction and Development Fund for revival of sick multi-state co-operative societies. Multi-state cooperative societies that are in profit for the preceding three financial years shall finance the Fund.
4. Restriction on Redemption of Government Shareholding: The bill amends to provide that any shares held by the central and state governments cannot be redeemed without their prior approval.
5. **Redressal of Complaints**: The central government will appoint one or more Cooperative Ombudsmen with territorial jurisdiction to inquire into complaints made by members of multi-state co-operative societies regarding their deposits, equitable benefits of the society's functioning, or issues affecting the individual rights of the members.

The bill was introduced in the Lok Sabha on December 7, 2022, and passed by the Lok Sabha on July 25, 2023. It seeks to amend the Multi-State Co-operative Societies Act, 2002, in light of the 97th Constitutional Amendment Act of 2011, which inserted Part IXB in the Constitution of India. The amendment aims to make the governance of multi-state cooperative societies more democratic, transparent, and accountable.