BLOCKCHAIN TECHNOLOGY

A mechanism revolutionizing multiple sectors, eliciting accountability and eliminating errors

Edited by
REUBAN K.

Since the blockchain database system provides security, trust, provenance, traceability and availability, the stakeholders of various business systems/ organizations can collaborate with each other. This technology has been initially experimented in the finance sector as in Bitcoin network, insurance payments and cross border payment networks. As a Proof of Concept, Blood Bank Supply Chain Model has been developed and tested on Hyperledger Sawtooth Framework.

B. VINAYA
Dy. Director General
& SIO
vinaya.b@nic.in

T. PECHIMUTHU
Technical Director
tpmuthu@nic.in

A business involves transactions and information exchange among various stakeholders. Since most of the existing systems are centralized, there is greater risk to security, and this necessitates the need for a secure and shareable system to help stakeholders interoperate efficiently. Blockchain is a distributed system where transaction records are bundled in blocks and linked with previous ones. Transaction data within a block is secured because it is encrypted and digitally signed. Bitcoin network is a pear to pear payment network, and it is an application of blockchain technology.

Blockchain Ecosystem

Blockchain is a decentralized distributed database (ledger) of immutable records accessed by various business applications over the network. Client applications of related businesses can read or append transaction records to the blockchain. Transaction records submitted to any node are validated and committed to the ledger database on all the nodes of blockchain network. Committed transactions are immutable because each block is linked with its previous block by means of hash and signature values. Protocols such as Gossip and Consensus ensure that the submitted transactions are transferred to all nodes and committed on all blockchain nodes consistently.

As shown in Figure 1, blockchain ecosystem consists of blockchain client, blockchain node, blockchain network, transaction processor/ smart contract and consensus process.

Blockchain client is an application that creates transaction message in a prescribed format and submits it to blockchain node through web API. It may be any existing application, which posts transaction message to blockchain node. Clients are restricted using Public Key Infrastructure (PKI) technology at blockchain node level.

Blockchain node is a server node that runs blockchain services responsible for receiving the transaction and transmits the transaction to other blockchain nodes. With respect to the design, the node participates in consensus process to commit the block of transaction data to ledger database.

Blockchain network is a network of linked nodes used for read, write transactions into ledger database. The topology (as shown in Figure 2) is based on the nodes participating in consensus process. Traditional systems are centralized where all data and decision-making is concentrated on a single node or cluster of nodes. In decentralized systems, the data and decision-making are spread out among a large number of nodes. These nodes maintain copies of the shared database and decide

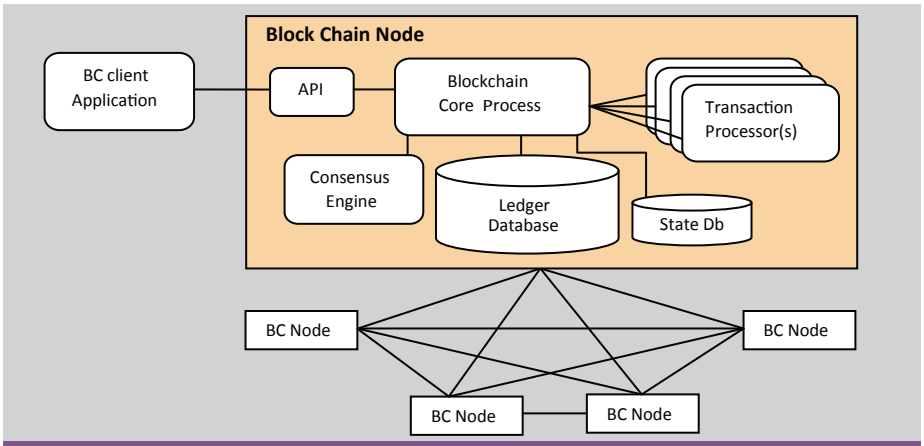

Fig. 1: Blockchain ecosystem

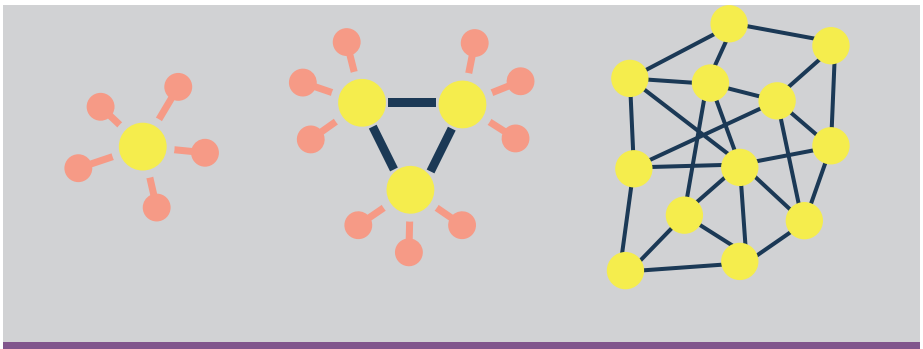

Fig. 2: Blockchain network topology (Centralized, decentralized, distributed)

among themselves which data is to be committed to the database using consensus mechanism. Decentralized networks can be an interconnection of centralized or hub-and-spoke type networks. A distributed network is a special case of decentralized system where every single node in the network maintains the shared database and participates in consensus to determine which data is to be committed to the database.

Blockchain Types

Public, Private and Consortium: In public blockchain, anyone can read and submit transaction, and take part in consensus process. Bitcoin and Ethereum are examples of public blockchain. Private blockchain is controlled by only a single body or an organization that controls who can read and submit transaction, and take part in consensus process. Consortium blockchain operations are controlled by a selected set of participating organizations. Public blockchain is called permission less blockchain. Private and consortium blockchain are called permissioned blockchain.

Transaction Processor/ Chain Code/ Smart Contract is a process that runs at blockchain nodes for processing the transaction data and maintaining the status in ledger database. It is called by blockchain process when the transaction commit is started. During the process, it can call or execute other business process tasks transparently before committing the transaction.

Consensus is a procedure to select a leader node, which decides whether the block of transactions is to be committed or rejected. Earlier versions of blockchain system used Proof of Work (PoW) for consensus process. Every node or participatory node is given a mining task, and a node elected as leader completes the mining task first. Mining task is to find or calculate a certain pattern value of hash value by adding nonce to current hash. Node that participates in mining process requires heavy computing resources. Latest consensus protocol uses PoET, which is called "Proof of Elapsed Time". Every node in the consensus process selects random time and keeps decreasing. The node that reaches zero first is selected as leader.

Transaction is a unit of business data within Hyperledger. **Block** is a set of transactions bundled with signatures and hash value of previous block. Genesis block is the first block of chain created during installation and configuration.

Merkle Tree is a tree data structure (as shown in Figure 3) in which leaf node holds hashes of every transaction and intermediate node holds hash calculated from immediate child nodes. In blockchain, a block consists of one or more transactions and its respective tree of hashes. In a distributed system, this tree is used to maintain data consistency among all participating nodes.

Ledger/Chain Database is a key-value database for a chain of serialized blocks. One block may contain one or more transactions.

State Database is a key-value database for storing transaction state and links of its related transactions.

Hyperledger Sawtooth Framework

Hyperledger Sawtooth is an enterprise blockchain platform for building distributed ledger applications and networks. It is an open source project under Hyperledger developed by Intel. Sawtooth core is a central Sawtooth software, which contains Validator, REST API and Transaction Processors. The Sawtooth Architecture (as shown in Figure 4) separates these core functions from application-specific business logic, which is handled by transaction families.

Validator is responsible for validating batches of transactions, combining them into blocks, maintaining consensus with the

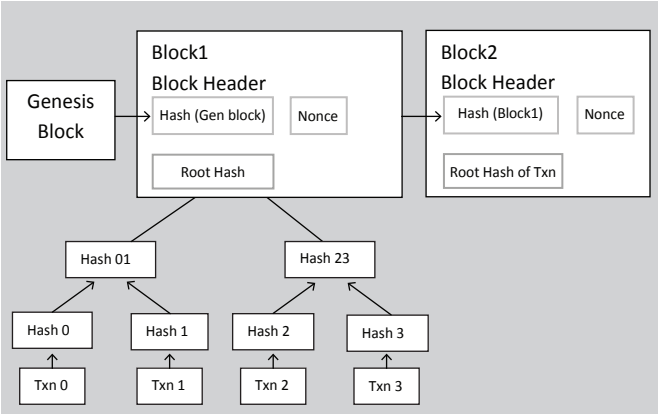

Fig. 3: Blockchain transactions hashed in Merkle Tree

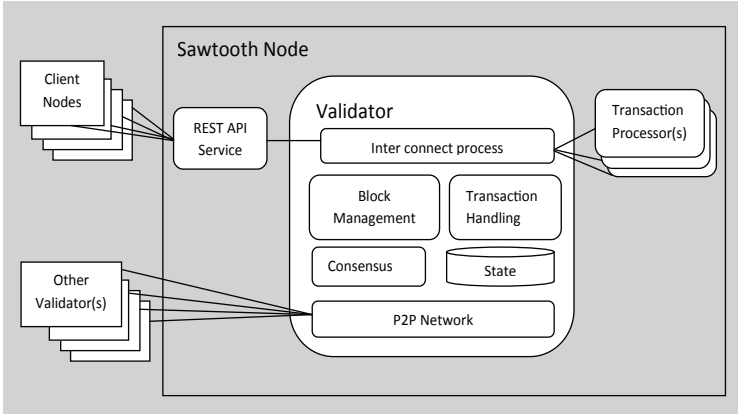

Fig. 4: Sawtooth Node High-level Architecture

Sawtooth network and coordinating communication between clients, transaction processors and other validator nodes.

REST API is a service used by client applications for submitting transactions to blockchain node. It is also used for fetching transactions, blocks and transaction status information from blockchain database ***(https://ipaddress:port/blocks, https://ipaddress:port/transaction/transactionid).***

Transaction Processor validates transactions and updates its state database based on rules defined by the associated transaction family. Sawtooth includes default transaction processors for on-chain permission and configuration settings.

SDK support for application development: Sawtooth provides software development kit for creating and manipulating transactions at client and back end transaction processor level. Sawtooth supports Python, Go, NodeJS, Java and C++.

Consensus protocol supported by Sawtooth: Devmode, PBFT (Practical Byzantine Fault Tolerence), PoET SGX (Software Guarded eXtension), PoET simulator

DevMode is a simplified random ledger algorithm for development and testing.

PBFT is a leader based, non-forking consensus algorithm, and it is ideal for smaller consortium style networks.

PoET SGX: The Proof of Elapsed Time (PoET) Consensus method utilizes a "trusted execution environment" called SGX provided by Intel Processor. It elects individual peers to execute requests at a given target rate.

PoET Simulator: It is same as PoET SGX, but it has simulated SGX environment.

Other blockchain platforms: Ethereum, R3 Corda, Multi Chain and Hyperledger Fabric

Blockchain Technology Use Case: Blood Bank Supply Chain

Blood Bank System

The recording of blood donations is done with paper and pen, and parameters like group, expiry date, and temperature are maintained manually. It could be fatal to patients if anyone receives infected/ contaminated blood. There is no proper way to verify the cleanliness of blood donated without testing it. There is no consolidated repository for the information of blood. Right from donor registration to hospital, multiple actors are involved in the process such as donors, testers, camps, blood bank, doctor and hospital.

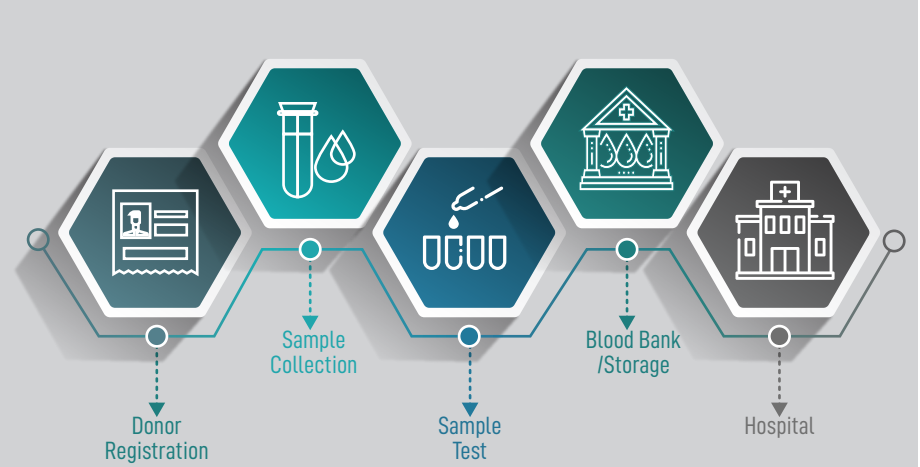

Fig. 5: Blood supply chain workflow

Use case

In the complete supply chain, recording transactions right from donor registration to patient and other important properties of blood such as group, test report, expiry date and temperature are maintained on blockchain.

As a Proof of Concept, the above supply chain workflow has been implemented on Hyperledger Sawtooth Framework with six nodes. In this case, the client application has been implemented in Python and NodesJs. Backend transaction processor is implemented in Python.

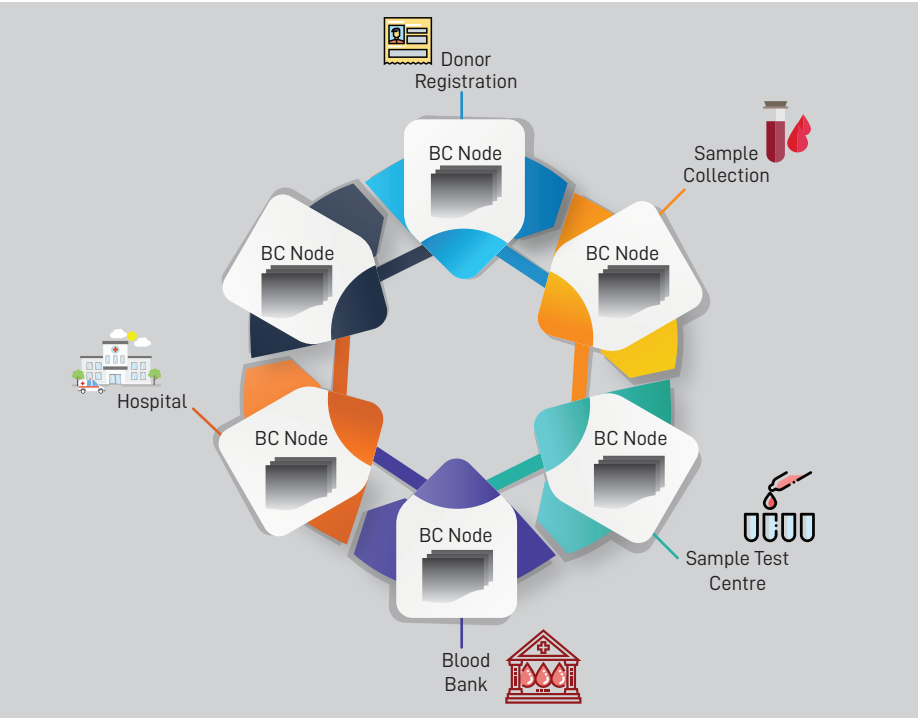

Fig. 6: Blood bank supply chain

Comparison between Blockchain Platforms

	Sawtooth	Fabric	Ethereum	Quorum
Type based on availability to user	Private	Private	Public	Private
Sector focus	Any	Any	Any	Financial
Consensus	Proof of Elapsed Time	Proof of Stake	Proof of Work	Raft
Multi-tenancy	Using family	Using channels	Not supported	Not supported
Language support	Python, GO, Java, NodeJs, C++	Python, GO, Java, NodeJs	Solidity	Solidity
Throughput	~2000tps	~2000tps	~ 500tps	~ 100tps
Security	PKI based, Supports access control policies	PKI based, Supports access control policies and network security	Need to encrypt the data	PKI based
Scalability	Scalable, Performance dependent on consensus algorithm and number of nodes	Scalable, Performance dependent on consensus algorithm and number of nodes	Scalable, Performance dependent on consensus algorithm and block size and compute power	Scalable
Project type and maintainer	Open source and maintained by Intel	Open source and maintained by IBM	Open source	Open source and maintained by JP Morgan
Support and documentation	Extensive documentation for developers and administrators	All support documentation is available as GitHub.	Online documents are available. Not in detail.	Not in detail

Criteria for Adopting Block-chain Technology

Following are some of the questions to assess the need of blockchain technology for existing/ new applications:

Is there a need to remove intermediaries that add complexity?

In order to complete certain main business process, some sort of sub process is required. For example, for loan sanction, the applicants' KYC and income status need to be verified. For recruitment process, employee verification including personal details, qualification details and experience details needs to be done. Nowadays, the above verifications are outsourced to third party agencies, which is time-consuming and costly.

Is non-repudiation i.e., the proof that someone submitted a transaction, needed?

After transporter delivers goods or food grains to retail shop, a transaction about the delivery on blockchain ensures that it has been delivered because it is accessible to supplier. Retailer cannot deny the delivery and delay the payment. At some places, a proof of the financial transaction needs to be provided for getting income tax relief or other benefits.

Is tamper resistance needed?

System that ensures the transaction data can't be tampered. In traditional system, the transaction data can be tampered whereas in the same case in blockchain, it is very difficult because of its immutable property.

Does data need to be shared across multi-ple entities?

In the business process, transaction data requires to be shared among various stakeholders.

Do multiple entities need to modify the data?

Suppose a business needs to be accessed by different entities and modify. A complete trace of what has been modified and by whom is required.

Conclusion

While selecting the sector for adopting blockchain technology, essential care needs to be taken to assess its suitability for the sector. Several blockchain platforms are currently available with different features. Hence, the selection of suitable platform for an application requires detailed survey and testing. Identifying the best platform for different classes of application requires detailed study and evaluation. ■

For further information, please contact:

T. PECHIMUTHU
Technical Director
NIC, 5th Floor, E-Block, Kendriya Sadan,
Koramangala, Bangalore
KARNATAKA – 560034

Email: : tpmuthu@nic.in
Phone: 080-25633608