Whitepaper

Blockchain Technical Implementation Guideline

Author: Ravindra Ved
Contents

1. Overview ................................................................. 3
2. Blockchain Design Considerations ............................. 3
3. Implementation Approach ......................................... 6
4. Reference Architecture ............................................. 8
5. Appendix ......................................................... 12
Overview

As enterprises across verticals explore the opportunities for innovation and process optimization using blockchain technologies, they are looking for in technical aspects of deploying and integrating blockchain technology, with their existing IT systems.

Based on operating models and blockchain platforms, there are variations in deployment and operations aspects, along with factors like integration & information security. This document provides approach and factors to consider during selection and implementation of blockchain technologies.

Blockchain Design Considerations

There exists a plethora of blockchain platforms, and selecting one over another, is a matter of understanding the business needs and matching them to the features provided by a specific platform. It is advisable to experiment with prototypes before settling on a specific platform. The appendix lists a few popular platforms.

**Suggestion:** Assess if the use-case really demands the use of cryptocurrency and expensive consensus mechanism. There are many variations of platforms around cryptocurrency, but most of the enterprise use-case do not need cryptocurrency. Hence, understanding of the use-case is paramount in the selection of right platform. Enterprise use-cases mostly need an immutable distributed ledger with strong provenance, resource effective consensus mechanism and cryptographically provable audit trails of transactions and events backed by smart contracts, to enforce business rules and compliance needs.

As the technology is evolving, most of the platforms are undergoing a rapid change in the architecture as new features are been added.

There is an effort to build frameworks and abstraction layers to isolate the blockchain development team from these rapid changes, and let them focus on core business use cases. One such framework is Microsoft’s APP Builder. It provides sets of enterprise design patterns and reference implementations, along with abstraction layers for interacting with blockchains. Theoretically, the underlying blockchains are now swappable, like Ethereum with Hyperledger Fabric.

**Type of Blockchains**

*Broadly, blockchains are classified as :*

- Public Blockchains (e.g. Bitcoin, Ethereum)
- Federated Blockchains (e.g. Corda)
- Private Blockchains (e.g. Ethereum & Hyperledger)

The Public vs Private/Federated classifications are also referred to as Permissionless vs Permissioned, respectively. The way participants interact and consensus is arrived at, varies based on the type of blockchain being deployed.

The focus in this paper is on deployment of private (permissioned) blockchains.
Private Blockchains
While there are many industry and vertical-specific blockchain platforms; two widely accepted platforms are Ethereum and Hyperledger Fabric, backed by support services from Microsoft and IBM, respectively.

Blockchain Technical Components
Blockchain deployment comprises of multiple coordinating components and artefacts, which need to communicate for executing smart contracts, arriving at consensus & synchronizing data. Understanding of these components is essential in identifying compute, storage and network requirements during the implementation phase.

In the implementation approach section, we will look into two different skill/roles required to deploy and operationalize these technical components.

- **Peers Nodes**
  - They are networked services that maintain ledger state and run smart contracts
- **Mining / Ordering nodes**
  - The Ordering Service agrees on transaction sequence and distributes blocks to peers.
  - While this is a separate component on Fabric, in Ethereum it is an integral function of a peer/node.

**Artefacts**
- **Channels**
  - Provide mechanism to maintain confidentiality of transactions between two parties
- **Digital certificates (issued by CA) & KeyStore**
  - The Certificate Authorities provide the identity services to participate on the network
  - The certificates are stored on each node’s KeyStore for endorsing and verifying the transactions
  - KeyStore is vital part of blockchain infrastructure, it maintains multiple keys and integrate with client applications to facilitate smooth transactions.
  - In every blockchain transaction, the identity, authenticity and ownership of asset is established using the Keys. KeyStore provides a secure way to backup private Keys.
- **Smart contracts / Chaincode**
  - Constitute the transaction logic whose output is agreed by the peer network.
- **Transactions**
  - The sender of the transaction digitally signs it, and provides the address of the recipient. It then submits it to peer node via RPC or REST API.
  - The transaction is then broadcasted over the network, where they are mined/validated.
- Once the consensus about the transactions is achieved between the participating nodes, the transactions are ordered and grouped into a block to become the next chain in the blockchain.

- The message is broadcasted back to the sender and recipient confirming the addition of transaction as a part of valid block on blockchain.

**Algorithms**

- Consensus

  - Consensus is the process by which agreement is obtained on the peer network.

  - The selection of this algorithm has implication on a network setup and the amount of processing power and network bandwidth consumed by each participating node.

**Platform Differences and Selection criteria**

The following differences between Ethereum and Hyperledger platforms are the key drivers in selecting one over the other.

**Consensus Algorithms**

- **Ethereum Platform**
  - The consensus algorithm used by Ethereum is based on “Proof of Work” and they have plans to move towards “Proof of Stake”.

  - The consensus algorithm approach provides safeguards against “Rogue” nodes on the network.

- **Hyperledger platform**
  - IT uses “Proof of Authority” which consumes less power, but does not provide safeguards against “Rogue” nodes.

**Transaction Throughput**

- **Ethereum**
  - Average block time of 17 seconds
  - 25 TPS on average.

- **Hyperledger**
  - Dependent on network configuration.

  - 700-1200 TPS with correctly optimized configuration.

  - Transaction throughput will decrease for large and growing network.

**Channels**

- While Ethereum can be deployed as permissioned network, it does not support private channels i.e. separate ledger between sub-group of participants.

- Ethereum broadcasts the transactions to every participant on the network.
Blockchain essentially is a state machine recording the state of Assets, as they move from one stage to another, and from one participant to another in a workflow. The implementation comprises of three tracks listed below.

**Implementation Approach**

**Workflow Detailing & Adaptation Track**

The identification of assets to be tracked and their transition within a workflow, is the starting point. This can be recorded as activity diagram, a business process diagram, or on an Excel sheet. Every node in the workflow is detailed by identifying the integration points and detailing user interactions as use-case or user stories in the context of user personas and roles.

“Process SME/Business Analyst” is a role performing these functions.

**Infrastructure Setup & Operations Track**

In this phase, based on blockchain platform, the computational and networking infrastructure is setup and configured. This involves setting up peer nodes, acquiring certificates from certification authorities, configuring digital certificates.

The deployment and configuration vary, based on technical infrastructure, whether on-premise or cloud. Most cloud services provide ready templates to begin with, however they need to be configured and customized.

“Network Admin/IT Operations” is the role performing these functions.

**Business Services Development & Enhancements Track**

Developing blockchain application comprises of developing, deploying and testing multiple modules and their interoperations viz:

- Ethereum
  - LevelDB — For storing and maintaining blockchain

- Hyperledger
  - LevelDB (default), CouchDB (optional)
  - CouchDB adds complex & rich read-only queries

- Official Support
  - Microsoft on Azure Cloud
  - IBM (on-premise and IBM Bluemix cloud)
  - Microsoft to provide on Azure platform
Software Developers perform these functions.

- **Application module**
  - Implementing web application and presentation logic
  - Invoking blockchain transactions

- **Integration module**
  - Developing APIs for integrating with internal and external systems
  - Implementing batch process requirements

- **Blockchain module**
  - Coding the digital assets
  - Implementing smart contracts
Reference Architecture

Consortium & Communities

The arrangements between participating entities in forming a consortium/communicates and selection of consensus protocol, have bearing on a network topology during deployment. This enables transaction propagation and consensus formation between the participating nodes.

We recommend analyzing the tasks on the following six dimensions:

**Consortium-based Network**
- Founders are equal among other participants, may include a joint legal entity among the founders (e.g. – JV).

**Founder-directed Network**
- Individual founder in a position to provide strong direction.

**Community-based Network**
- Driven by industry standards bodies or existing non-blockchain network owners.
Conceptual View

Each Node in an organization participates as Member or a Founder node.

Diagram below depicts the set of services and components that needs to interact within each such node.

Components Overview

- **IDM**
  - LDAP and Access manager component that stored user credentials and provide API for authentication, authorization and perform SSO functions.

- **Internal Systems**
  - The system of records and transactions processing systems are backbone of any enterprise.
  - Transactions origination and their lifecycle are tracked in Internal core ERP or Core Banking systems.

- **Integration Module**
  - Most enterprise have ESB or integration gateway that provides or exposes Internal systems as API services.

- **Blockchain Module**
  - This comprises of blockchain platform and several technical components listed in section above (Blockchain Technical Components).

- **Blockchain Peer Nodes**
  - These are participating nodes on the network, which are hosted on the peer nodes/organizations.

- **External Service Providers**
  - These are specific service providers, which provide feeds or updates on transactions in the given business workflows, have been locked onto the blockchain.
Deployment View

Every participating node may choose to deploy the set of services based on their IT policies and roadmap.

There is a trend towards Blockchain service components being deployed on cloud infrastructures having strong integration, with on-premise core systems (e.g. ERP, Identity Servers).

The diagram below provides reference architecture of Ethereum-based blockchain deployment.
Integration Considerations

Most blockchain projects are integration-oriented, having touchpoints with internal systems and third-party API providers. As an example, for any supply chain project implementation, the transaction flows through core ERP, external suppliers, quality controls agencies, shipping and transporting companies, government agencies like customs, banking and insurance companies, etc. Each of these participants will have different message formats and integration needs.

Every implementation must check for enterprise-wide integration infrastructure, however they may be limited in terms of onboarding all the required parties and their specific APIs.

Special care should be taken in identifying what needs to be recorded on Blockchain and not using it as a shared database for all the data exchanges between participants. Only the relevant and auditable data should be put on the blockchain. Off-chain data should be exchanged using proven integration patterns.
## List of Prominent blockchain platforms

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Blockchain Platform</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="https://www.ethereum.org/">https://www.ethereum.org/</a></td>
<td>A decentralized platform that runs smart contracts on a custom built blockchain. Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference</td>
</tr>
<tr>
<td>2</td>
<td>Hyperledger and its implementations like • Fabric • Indy • Sawtooth • roha • Burrow <a href="https://www.hyperledger.org/">https://www.hyperledger.org/</a></td>
<td>A modular platform with multiple implementations. Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, IoT, supply chain, manufacturing and technology</td>
</tr>
<tr>
<td>4</td>
<td><a href="https://chain.com/technology/">https://chain.com/technology/</a></td>
<td>Chain Core is a blockchain platform for issuing and transferring financial assets on a permissioned blockchain infrastructure. Chain Core runs on the open-source Chain Protocol.</td>
</tr>
<tr>
<td>5</td>
<td><a href="https://www.corda.net/">https://www.corda.net/</a></td>
<td>Corda is an open-source distributed ledger platform with pluggable consensus—“it supports multiple consensus providers employing different algorithms on the same network”.</td>
</tr>
</tbody>
</table>
LTI (NSE: LTI, BSE: 540005) is a global technology consulting and digital solutions Company helping more than 250 clients succeed in a converging world. With operations in 27 countries, we go the extra mile for our clients and accelerate their digital transformation with LTI’s Mosaic platform enabling their mobile, social, analytics, IoT and cloud journeys. Founded 20 years ago as a subsidiary of Larsen & Toubro Limited, our unique heritage gives us unrivaled real-world expertise to solve the most complex challenges of enterprises across all industries. Each day, our team of more than 20,000 LTItes enable our clients to improve the effectiveness of their business and technology operations, and deliver value to their customers, employees and shareholders. Find more at www.Lntinfotech.com or follow us at @LTI_Global

About the Author

Ravindra Ved
Lead Technical Architect with Digital Practice at LTI

He has 19+ years’ of IT experience with proficiency in defining solution and building large scale distributed systems that ties platforms, products, tools and frameworks in a manner that is oriented towards achieving project goals. As a software practitioner, he is experienced on Opensource stack (Java/Linux) and developing cloud native applications. Currently, he is leading Blockchain implementations at LTI. He is an Integrated Architecture Framework (IAF) certified professional, which is a basis for the content framework of TOGAF.

He is a key member of architecture team for flagship programs for the Government of India currently been implemented by LTI. He has been in similar roles during his assignments with General Motors, Walt Disney, Sony Pictures, Mobixell & Citi Bank.