Strategy and Synergy for Security

Enhancing PKI Security in Hyperledger Fabric with an Indigenous Certificate Authority

(Funded by MeitY)

Dr. M. Gayathri Santhosh
Project Associate, SETS

Dr. TR. Reshmi
Principal Investigator, SETS

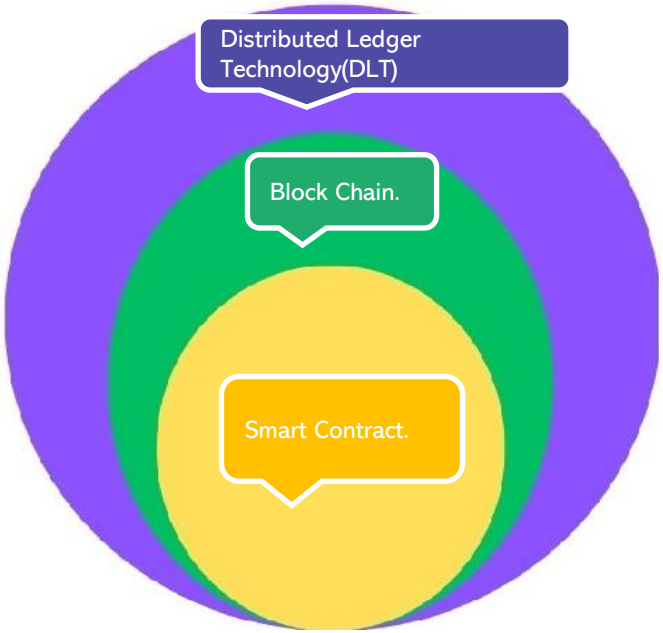
Ms. P. R. Laxmi Eswari
Chief Investigator, CDAC

Society for Electronic Transactions and Security (SETS) Chennai

Strategy and Synergy for Security

What is Block Chain??

- A technology that permits transactions to be gathered into blocks and recorded.
- All the blocks are cryptographically chained in chronological order
- It allows the resulting ledger to be accessed by different servers.
- DLT, Block Chain and Smart contracts are interrelated but have a distinct significant purpose.



"A peer-to-peer distributed ledger forged by consensus and a system for smart contracts and other assistive technologies"

Society for Electronic Transactions and Security (SETS) Chennai

Permissioned vs. Permissionless Blockchain

Strategy and Synergy for Security

PERMISSIONLESS/PUBLIC	PERMISSIONED/PRIVATE
Open network and fully decentralized across unknown parties	Closed network and distributed across known parties
Full transparency of transactions, based on open source protocols	Controlled transparency, based on organizations·
Development via open source and mostly anonymous, with some exceptions	Development via private entities and not anonymous
No central authority and often involves digital asset or token for incentives	A private group authorizes decisions and may or may not involve digital assets or tokens
Highly transparent and is beneficial for speed and reconciliation across unknown parties	Highly customizable to specific use cases through diverse configurations, modular components and hybrid integrations
Less user privacy and information control	Less transparent to outside oversight, since participants are limited and operators determine privacy requirements
Suitable for • Cryptocurrency • Business-to-consumer • Eg. Bitcoin, Ethereum	Suitable for • Government-to-citizens • Governments -to-organizations • E.g. Hyperledger fabric, Sawtooth

Types of Hyperledger Blockchain Framework

Strategy and Synergy for Security

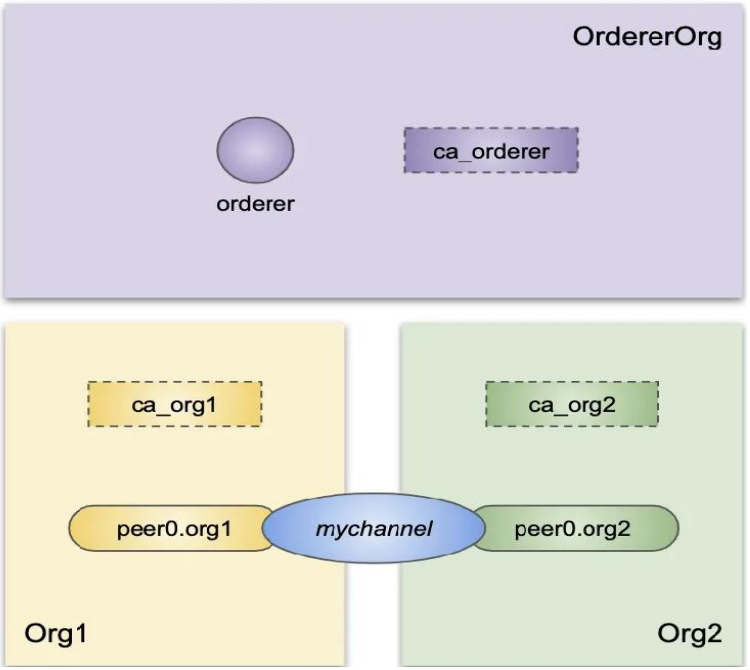
FRAMEWORK	DESCRIPTION
Hyperledger Fabric	Intended as a foundation for developing applications or solutions with a modular architecture, Hyperledger Fabric allows components, such as consensus and membership services, to be plug- and-play.
Hyperledger Iroha	A business blockchain framework designed to be simple and easy to incorporate into infrastructural projects requiring distributed ledger technology.
Hyperledger Sawtooth	A modular platform for building, deploying, and running distributed ledgers. Hyperledger Sawtooth includes a novel consensus algorithm, Proof of Elapsed Time (PoET), which targets large distributed validator populations with minimal resource consumption.
Hyperledger Burrow	A permissionable smart contract machine. The first of its kind when released in December, 2014, Burrow provides a modular blockchain client with a permissioned smart contract interpreter built in part to the specification of the Ethereum Virtual Machine (EVM).
Hyperledger Indy	Tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other silo.

Why PKI in Hyperledger?

Strategy and Synergy for Security

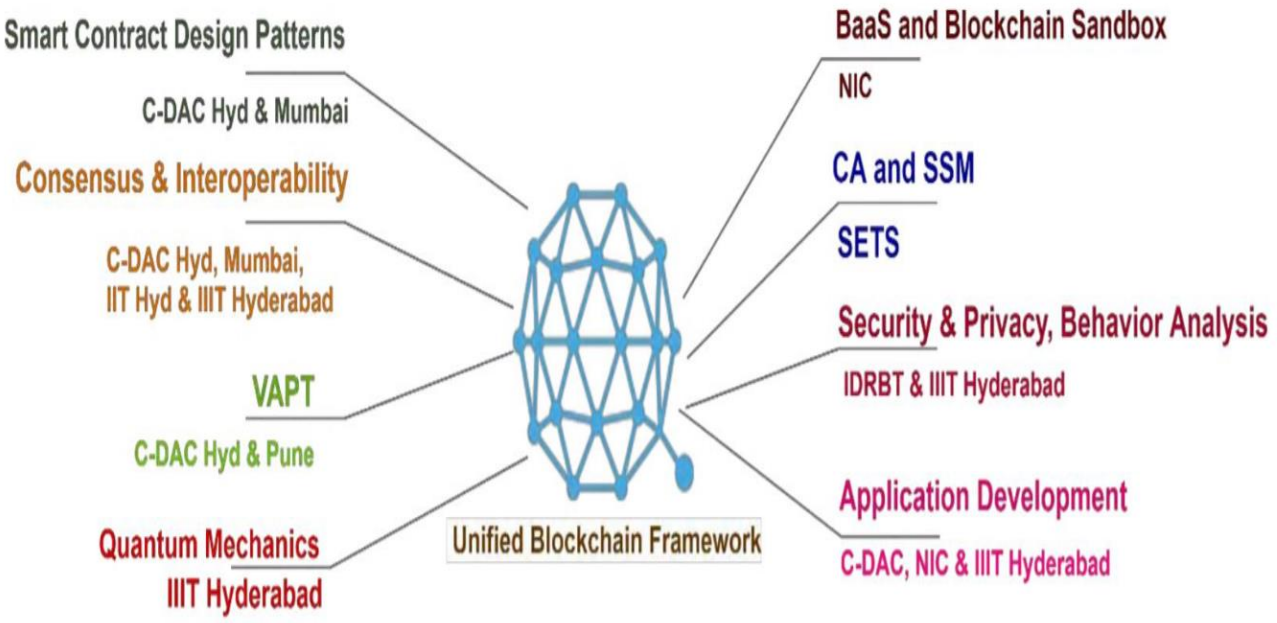
Hyperledger relies on strong security mechanisms to maintain trust and integrity within its blockchain networks.

- **Certificate Issuance**
  - Participants request certificates from the CA.
  - CA validates the identity and issues certificates.
- **Secure Communication**
  - Participants use certificates for secure communication.
- **Transaction Signing**
  - Transactions are signed with the keys.



Test Network Architecture

MeitY Initiative of National Blockchain Framework for National e-Governance Services



Society for Electronic Transactions and Security (SETS) Chennai

SETS-PKI

Hyperledger Fabric needs a membership identity service that helps to manage all the identities in the permissioned block chain network.

- Decentralization
- Scalability
- Customization and Integration with Fabric Components
- CAs Seamless Integration with Fabric Tools and Utilities
- SETS CA is an in-house designed and developed product/software.

Society for Electronic Transactions and Security (SETS) Chennai

Creation of CA for Hyperledger

Strategy and Synergy for Security

- Creation of CA's (organization)
  - TLS-CA
  - Enrolment CA
- Creation of Enrolment Certificate for establishing the identities of the components(peers)
- Registration and Enrollment of the admin, users and peers
- Certificates of all the network components are organized into an MSP directory structure and placed inside the organization folder.
- Local MSP(ca certs, tls certs, key store, sign certs)
- Organisational MSP((ca certs, tls certs, key store, sign certs)

Integration of CA

Strategy and Synergy for Security

- Modify the network.sh file, there is an

  if [“CRYPTO” == CA”];

- Now build the network components using

  $./network.sh up createChannel -ca

- Now SETS CA dockers are build and brings all the containers and creates default channel “mychannel”

```
    fi

  fi

  # Create crypto material using Fabric CA
  if [ "$CRYPTO" == "Certificate Authorities" ]; then

    infoln "Generating certificates using SETS CA"
    sudo cp -r /home/sets/UBF_PKI/organizations/peerOrganizations  /home/sets/UBF_PKI/organizations/ordererOrganizations organizations/
    docker-compose -f /home/sets/UBF_PKI/compose-ca.yml up -d 2>&1
    sleep 30
    infoln "##################"

    #infoln "Generating certificates using Fabric CA"
    #infoln "${CONTAINER_CLI_COMPOSE} -f compose/$COMPOSE_FILE_CA -f compose/$CONTAINER_CLI/${CONTAINER_CLI}-$COMPOSE_FILE_CA up -d 2>&1"

    # ${CONTAINER_CLI_COMPOSE} -f compose/$COMPOSE_FILE_CA -f compose/$CONTAINER_CLI/${CONTAINER_CLI}-$COMPOSE_FILE_CA up -d 2>&1


    # . organizations/fabric-ca/registerEnroll.sh

    # while :
    # do
    #   if [ ! -f "organizations/fabric-ca/org1/tls-cert.pem" ]; then
    #     sleep 1
    #   else
    #     break
    #   fi
    # done

    # infoln "Creating Org1 Identities"

    # createOrg1

    # infoln "Creating Org2 Identities"

    # createOrg2

    # infoln "Creating Orderer Org Identities"

    # createOrderer

  fi

  infoln "Generating CCP files for Org1 and Org2"
  ./organizations/ccp-generate.sh
```

Dynamic User Registration

Strategy and Synergy for Security

- Adding dynamic user via CA of Organisation is done using Rest API
- Get the IP and port of the running CA's.
- It includes two steps:
  - Registration
  - Enrolment
- Http methods

Method	HTTP Header	Body

Structure

Register	Role	mail_id	Org_Name	CA_Name

Attributes for registration(Body)

Enrolment	Role	mail_id	Org_Name	CA_Name	CA_Host	MSP Location

Attributes for enrollment(Body)

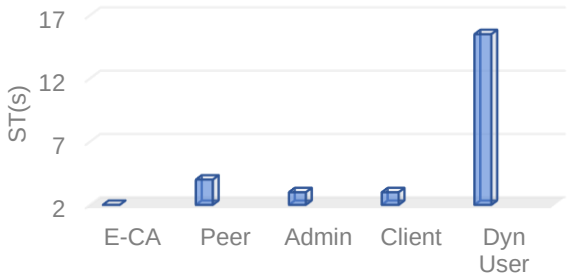
Performance Evaluation

Strategy and Synergy for Security

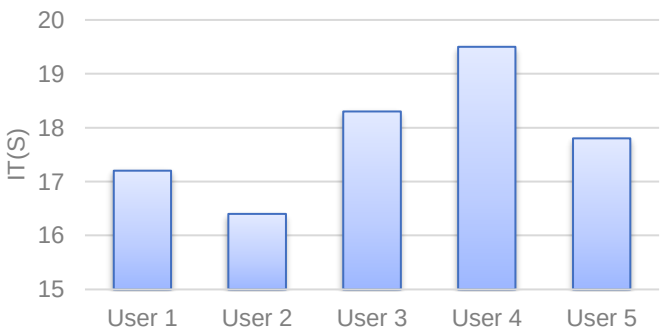
- HLF provides several performance metrics to monitor the performance of the CA
  - Throughput

$$Throughput = \left(\frac{processing \quad power}{SS \cdot TPS} \right)$$

  - sign time



  - Issue Time



Future Directions

Strategy and Synergy for Security

- **Objective Achieved**: We've presented an approach to create an indigenous Certification Authority (CA) integrated into Hyperledger Fabric (HLF) for real-world use.
- **Security Milestones**: Our approach ensures secure peer-to-peer communication at the channel level and provides the capability to validate certificates, enhancing network security and reliability.
- **Identity Management**: Our solution offers a robust identity management framework, a fundamental aspect of any blockchain network.
- **Future Directions**: To further fortify privacy and security:
  - Keys will be transitioned into Software Security Modules (SSM).
  - The shift to SSM not only enhances privacy and security but also guarantees data confidentiality in the digital realm.
- Our proposed solution enhances the network's security and trustworthiness and also provides easy integration with HLF.
- The suggested approach would be helpful for any organization looking to use Hyperledger Fabric networks.