cwrisec / **LFS171x-An-Introduction-to-Hyperledger-Blockchain-Technologies**

0 stars 0 forks

Star Unwatch

Code Issues Pull requests Actions Projects Wiki Security

master ··· Gitpod

 cwrisec 7777777 ... 4 minutes ago 13

View code

README.md

https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2020/course/

Chapter 1. See written notes in sub-folder.

Chapter 2. See written notes in sub-folder.

Benefits of blockchain

Blockchains are a new infrastructure for securely validating and automating transactions across complex networks, with the potential to dramatically reduce the backend costs of modern financial systems and expedite the delivery of e-government services.

Blockchain / DLT have four IT main benefits:

- **Automation**: Blockchain-based smart contracts automate business logic across multiple parties, reducing settlement time and costs.
- **Security**: Blockchains use advanced cryptography to guarantee tamper-proof data coordination and storage across large networks of counterparties.
- **Reliability**: A blockchain's decentralized architecture prevents single points of failure and ensures the network is highly available.
- **Transparency**: A blockchain's digital, immutable ledger provides auditability and accountability around business transactions and the origin of data.

Advantages of adopting DLT / Blockchain for business:

- Improved business efficiencies
- Product/service differentiation
- Increased profitability
- Cost reductions
- New business insights from incremental data, etc.

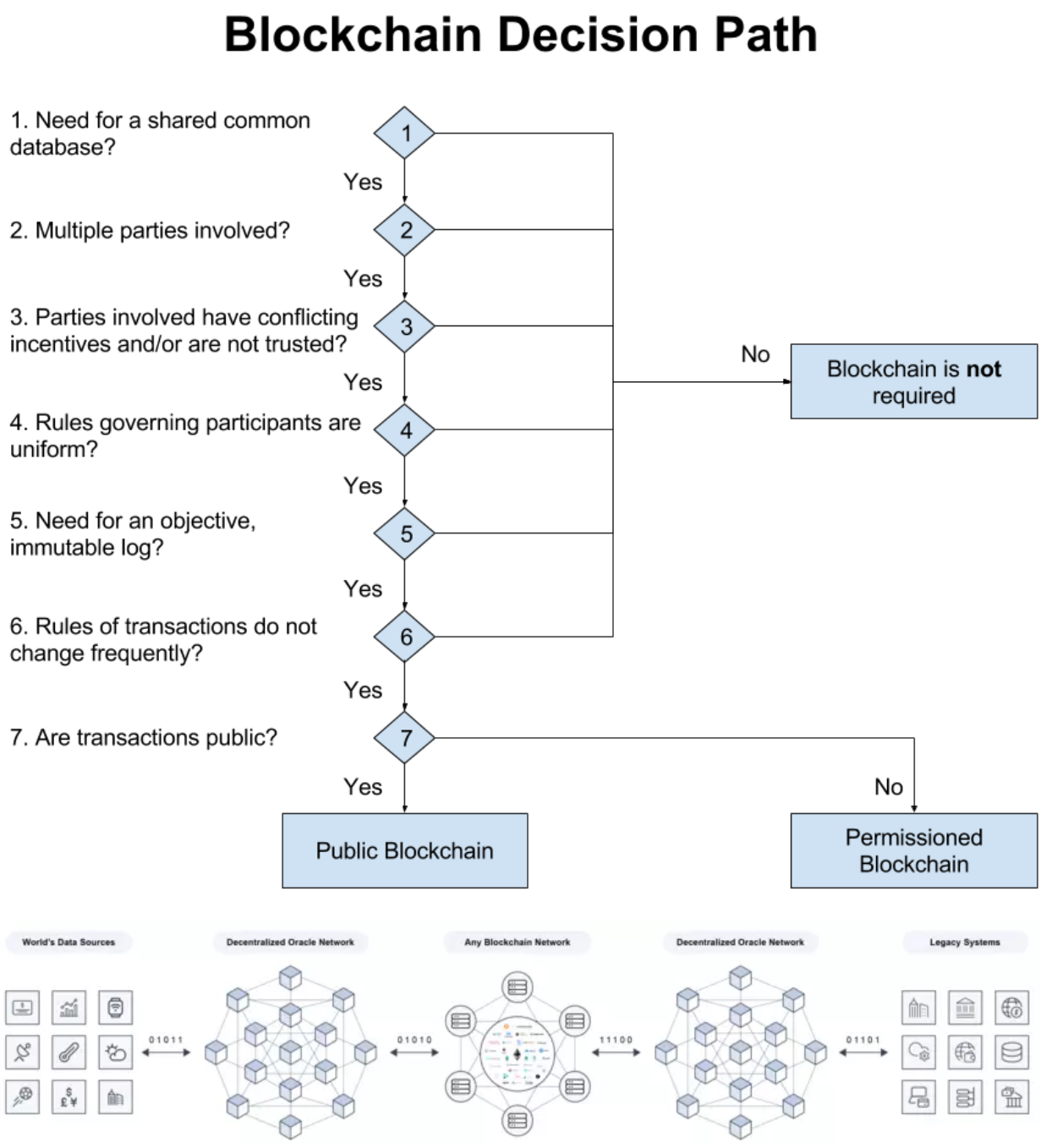
Conditions to have for great blockchain

- There is a need for a shared common database
- The parties involved with the process have conflicting incentives, or do not have trust among participants
- There are multiple parties involved or writers to a database
- There are currently trusted third parties involved in the process that facilitate interactions between multiple parties who must trust the third party. This could include escrow services, data feed providers, licensing authorities, or a notary public
- Cryptography is currently being used or should be used. Cryptography facilitates data confidentiality, data integrity, authentication, and non-repudiation
- Data for a business process is being entered into many different databases along the lifecycle of the process. It is important that this data is consistent across all entities, and/or digitization of such a process is desired
- There are uniform rules governing participants in the system
- Decision making of the parties is transparent, rather than confidential
- There is a need for an objective, immutable history or log of facts for parties' reference

- Transaction frequency does not exceed 10,000 transactions per second.

COnditions for NO GO for blockchain projects

- The process involves confidential data
- The process stores a lot of static data, or the data is quite large
- Rules of transactions change frequently (Blockchain is deterministic)
- The use of external services to gather/store data.



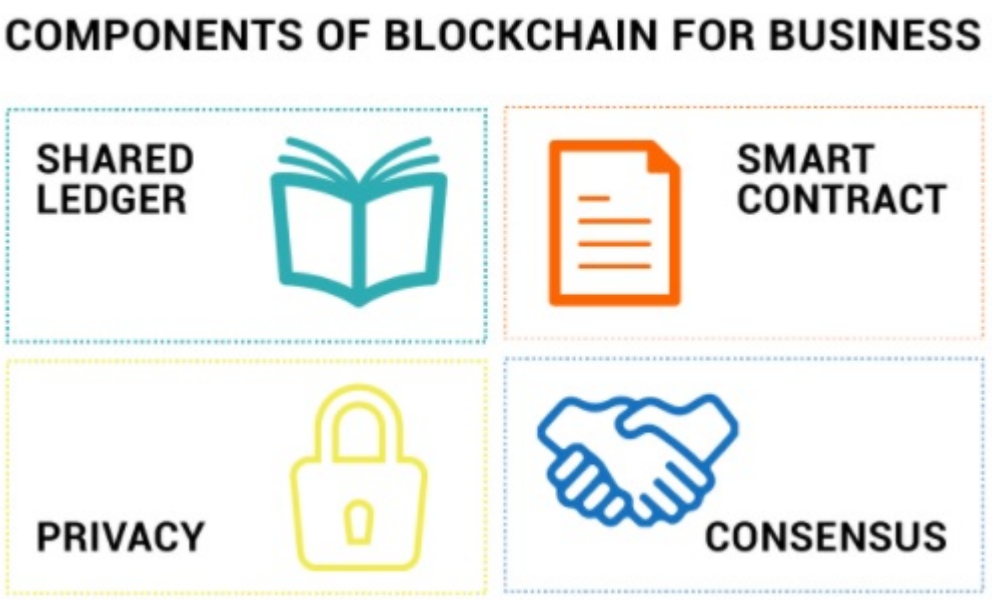
(WEF, Sergey Nazarov - 2020 - https://www.weforum.org/agenda/2020/12/the-missing-link-between-blockchain-and-existing-systems/)

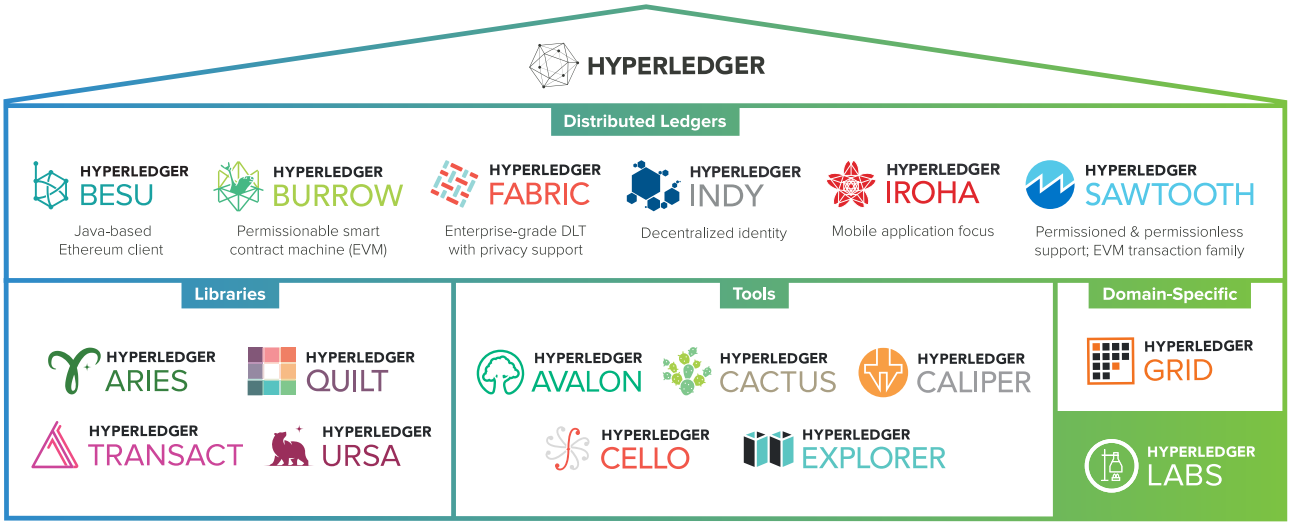
(77 DLT Uses cases - Chainlink - 2020 - https://blog.chain.link/44-ways-to-enhance-your-smart-contract-with-chainlink/)

Chapter 3. Hyperledger: Distributed Ledger Frameworks and Domain Specific Blockchains

3.1 - Components of Hyperledger frameworks

- Append only distributed ledger
- Consensus algorithms for changes in the ledger
- Privacy of the transactions through permissioned access
- Smartcontracts to process transactions process





3.2 - Hyperledger BESU

What:

- Open source **ETH client**, Apache 2.0 License, written in Java.
- Can run on ETH Networks OR on private permissionned network
- Sponsor & main maintainer: PegaSys

Consensus:

- **PoW** : through Ethash
  - Hash function that belons to the Keccak family, it's the same family as SHA-3
  - Ethash is Asic resistant
  - Use 1gb dataset known as DAG (Directed acylic graph) and 16mb for light clients, regenerated every 30.000 blocks known as epoch.
- **PoA** (with Clique (testnets) and IBFT 2.0)

Usage:

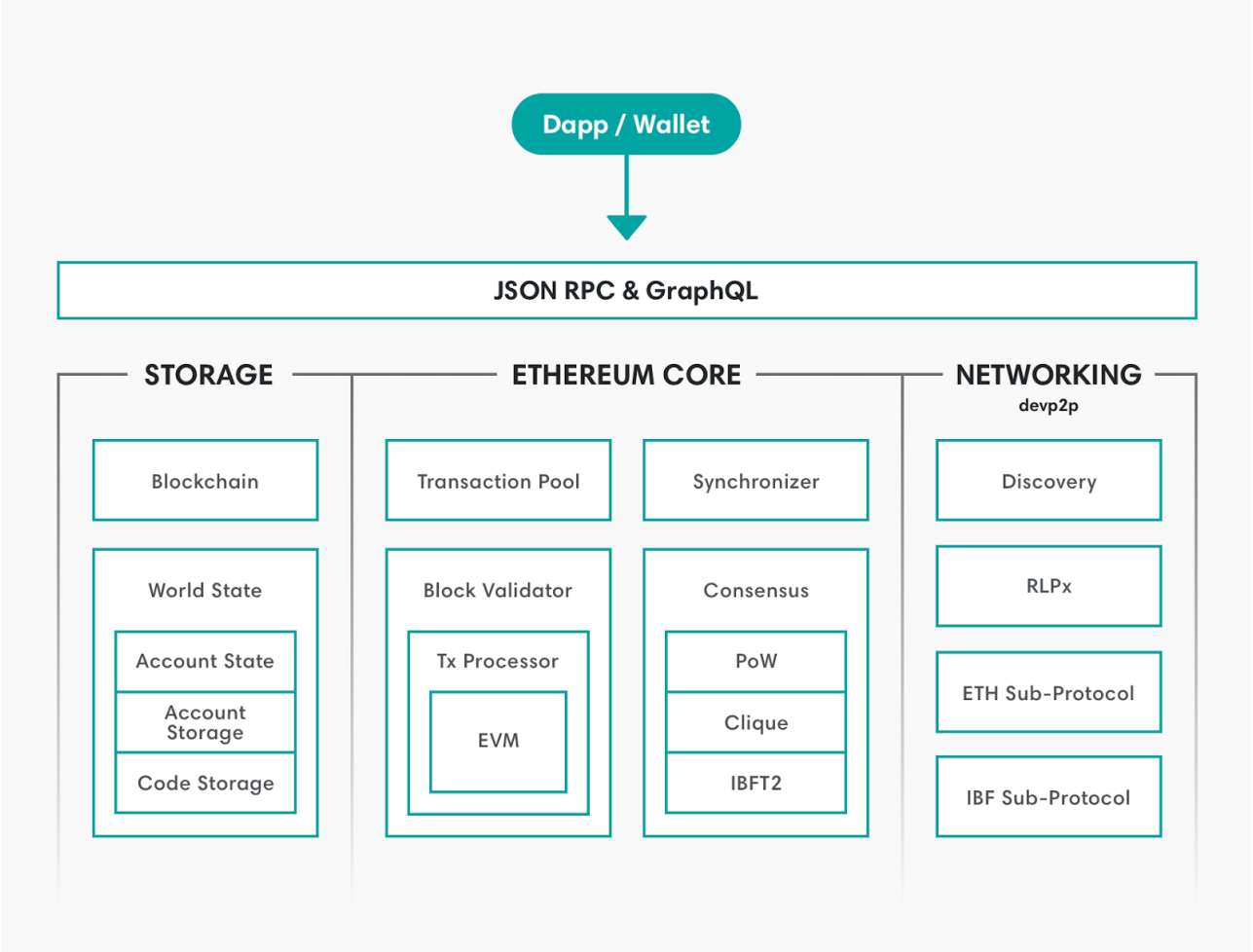
- Consortium environment due to comprehensive permissioning schemes

Features:

- Implements EEA Specs
- EVM Machine, allows deployment and execution of smart contracts via transactions with ETH blockchain Uses a RocksDB key-value database (high performance db) to persist chain data locally
- P2P network

- Provides user-facing APIs
- Allows you to monitor node and networks performance
- Ability to keep transactions private between involved parties
- Allow permissionning

Appendix :



3.3 - Hyperledger Burrow

What:

- Modular blockchain framework, Apache 2.0 License
- Permissionned Solidity smart contract interpreter
- Permissionned EVM
- Follow partly EVM specifications
- Complete single-binary blockchain distribution focussed on simplicity, speed, and developer ergonomics.

- Supports both EVM and WASM based smart contracts
- 2012
- Sponsor & main maintainer: Intel

Consensus:

- BFT consensus via the Tendermint algorithm (a blockchain consensus engine (Tendermint) and a Application BlockChain Interface (ABCI) which enables the transactions to be processed in any programming language

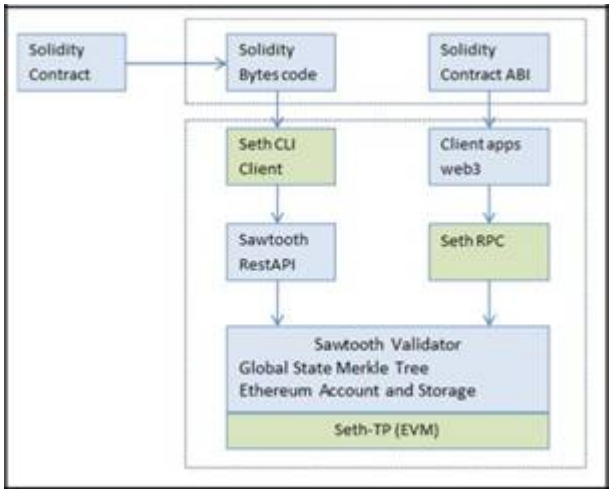
Usage:

- Optmized for sharing processes accross organizations
- We can use Solidity contracts within Hyperledger through the Burrow Framwork

Features:

- API Gateway for systems integration and user interfaces
- Smart Contract Application engine facilitates integration of complex business logic (maintaining the networking stack between the nodes and ordering transactions)
- Permissioned Ethereum Virtual Machine
- Application Binary Interface (ABI) encoding of SC, - transactions must be formulated in a binary format, which is processed by the blockchain node.
- ABCI for consensus engine

Appendix:



3.4 - Hyperledger Fabric

What:

- Enterprisegrade, permissioned, open source, vendor neutral, modular, plug-and-play
- Allow confidential transations through differents channels running within the network and division of labor that characterize the diffferents nodes within the network.
- High-performance, secure, permissioned blockchain network
- Features powerful container technology to host any mainstream language for smart contracts development
- Code written in Go, chaincode written in Go, Javascript, or Java, SDKs written in Node.js, Java, Go, REST and Python.
- Sponsor & main maintainers: IBM, Digital Assets Holdings, Blockstream's libconsensus
- 2017

Consensus:

- Plug and play : Consensus
- Plug and play : Memberships

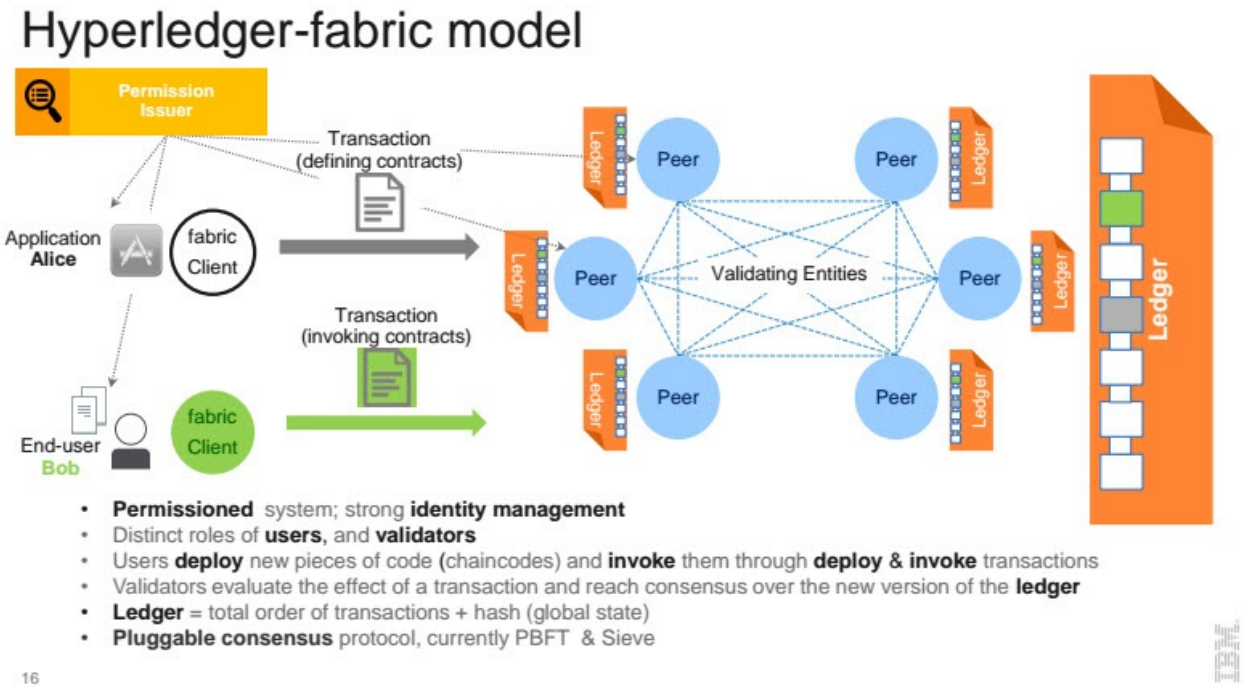
Usage:

- Modularity and versatility for a broad set of industry use cases.
- Fabric offers a modular, scalable and secure platform that supports private transactions and confidential contracts.
- Fabric helps members manage confidential obligations to each other without first passing it through a central authority.
- Solutions developed with Fabric to be adapted for any industry.

Features:

- Plug-and-play components, such as consensus, privacy, and membership services.
- Enable Networks of Networks

Model:



3.5 - Hyperledger Indy

What:

- Distributed ID - Trust & Privacy (user validate)
- **Business blockchain framework for supporting independent identity on distributed ledgers**
- Solution for Digital Crendtials
- It allows to have a route of trust to manage the keys schemas, proofs, and other information
- **Distributed ledger that provides tools, libraries,and reusable components for creating and using independent decentralized identities**.
- Represents the idea of Self-sovereign identity (multiple logins, passwords)
- **DID interoperates accross domains, applications, organizational silos.**
- User control the ID not companies
- Provides strong privacy guarantees, because not stored but exchanged over P2P encrypted connections through Unique ID (masked) for each relationships avoiding leaks.
- Make sure parties knows with who they are doing business.
- Initiatied by Sovrin Foundation 2017

Consensus:

- RFBT
- Cryptography : ZKP

Usage:

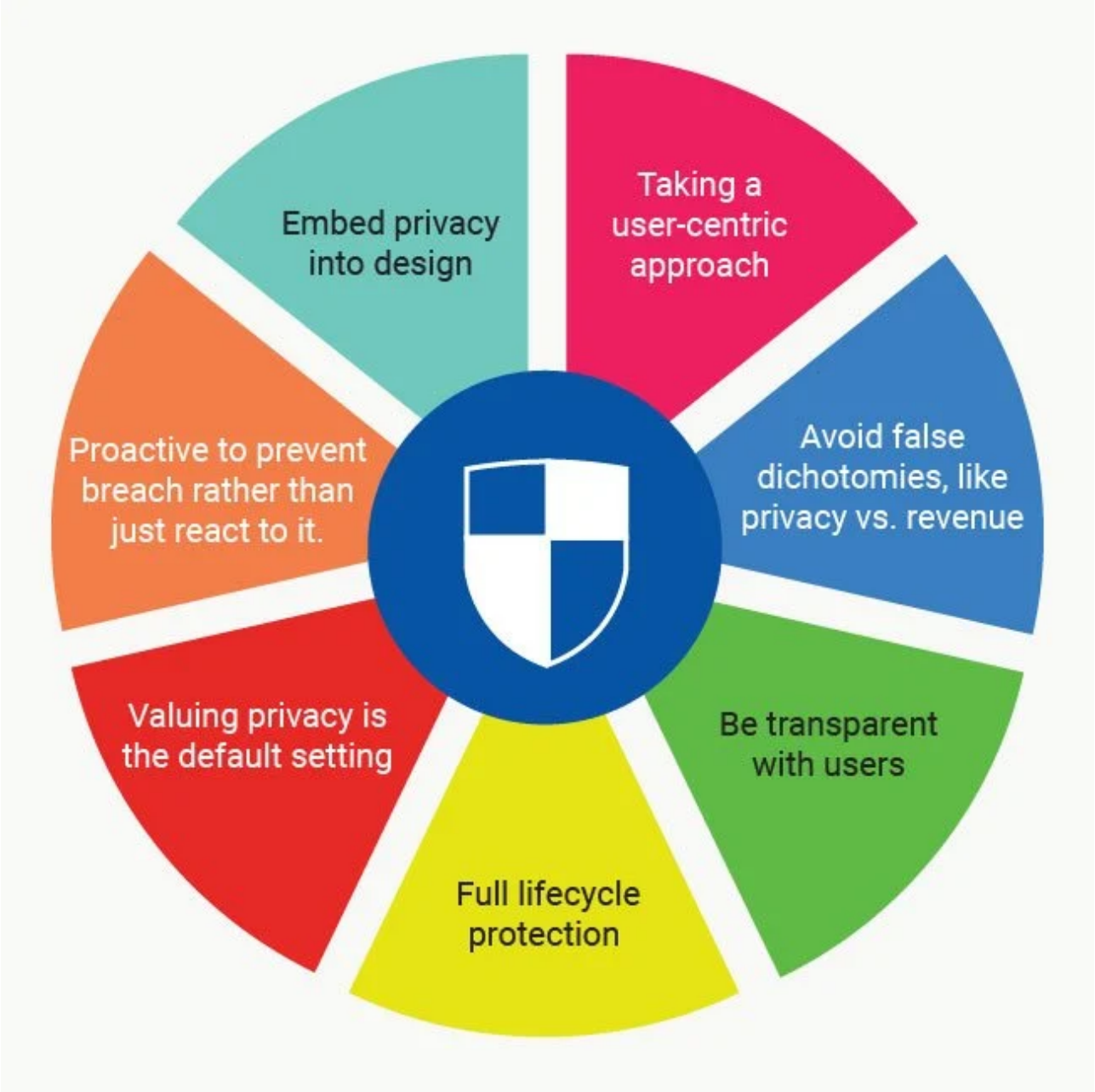
- It allows individuals to manage and control their digital identities. Rather than having businesses store huge amounts of personal data of individuals, Hyperledger Indy allows businesses to store pointers to identity. Once the company verifies the other party's identity, it throws it away.
- Identity is a toxic asset that could present a liability to organizations
- Public Utility solution for Id related, let users authenticate based on the attributes that they're willing to store and share themselves,
- reducing the amount of liability contained within a business
- GDPR Compliant

Features:

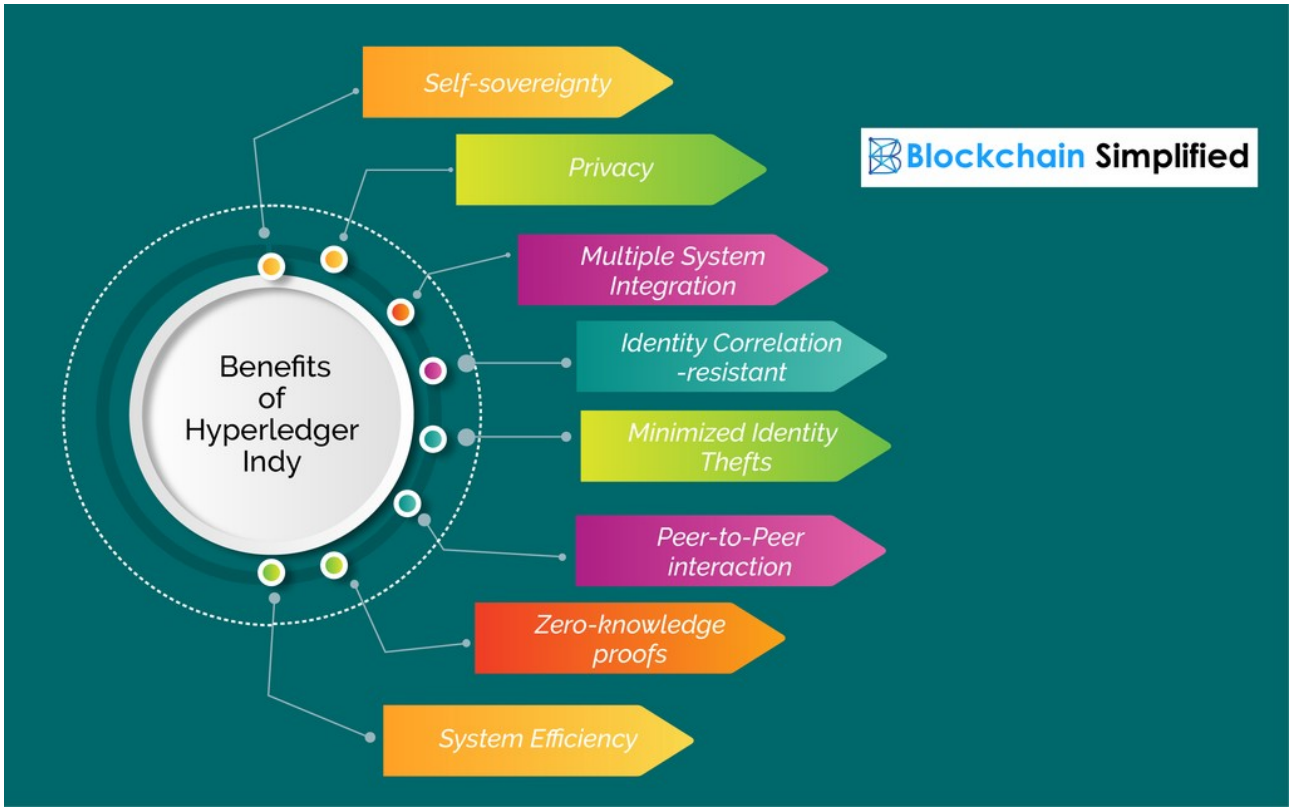
- Provides tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other silo.

Breach Level Index :

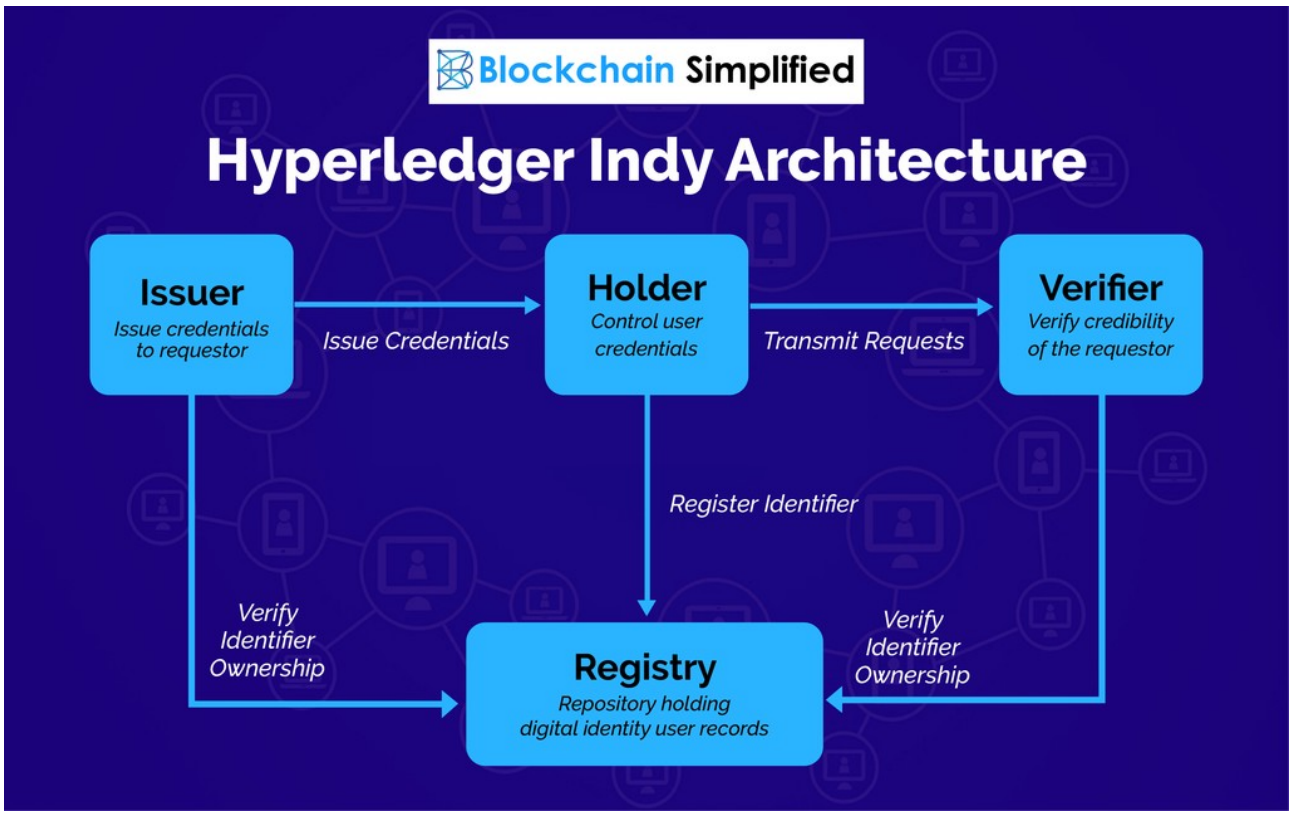
Privacy By Design :


Embed privacy into design
Taking a user-centric approach
Avoid false dichotomies, like privacy vs. revenue
Be transparent with users
Full lifecycle protection
Valuing privacy is the default setting
Proactive to prevent breach rather than just react to it.

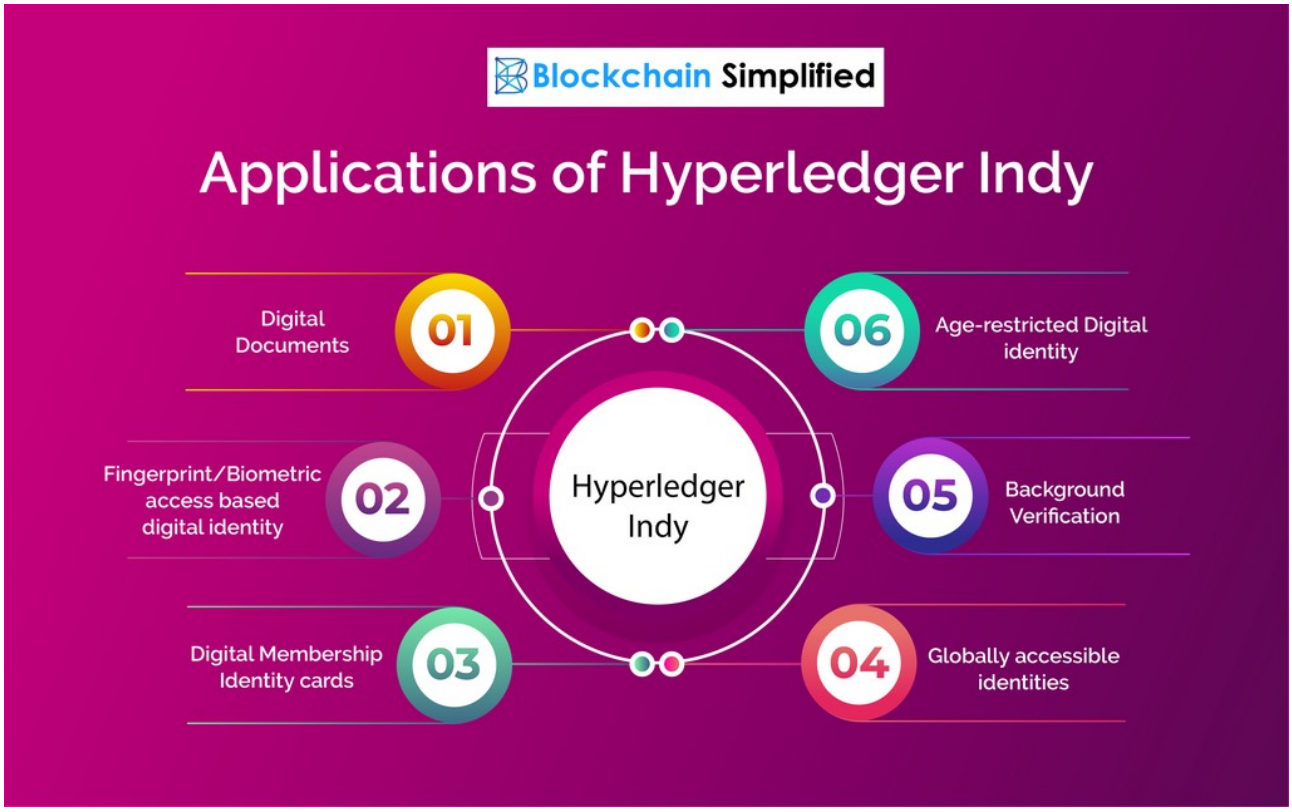
Benefits :



Architecture:



Uses cases:



3.6 - Hyperledger Iroha

What:

- Permissionned
- **Mobile Application focus with client libraries for Android and iOS**, making it distinct from other Hyperledger frameworks.
- Easy integration, same xp as on the web
- 2016 contributed by : Soramitsu, Hitachi, NTT Data, and Colu

Consensus:

- FBFT with no mining, ideal for businesses that require verifiable data consistency at low cost with YAC

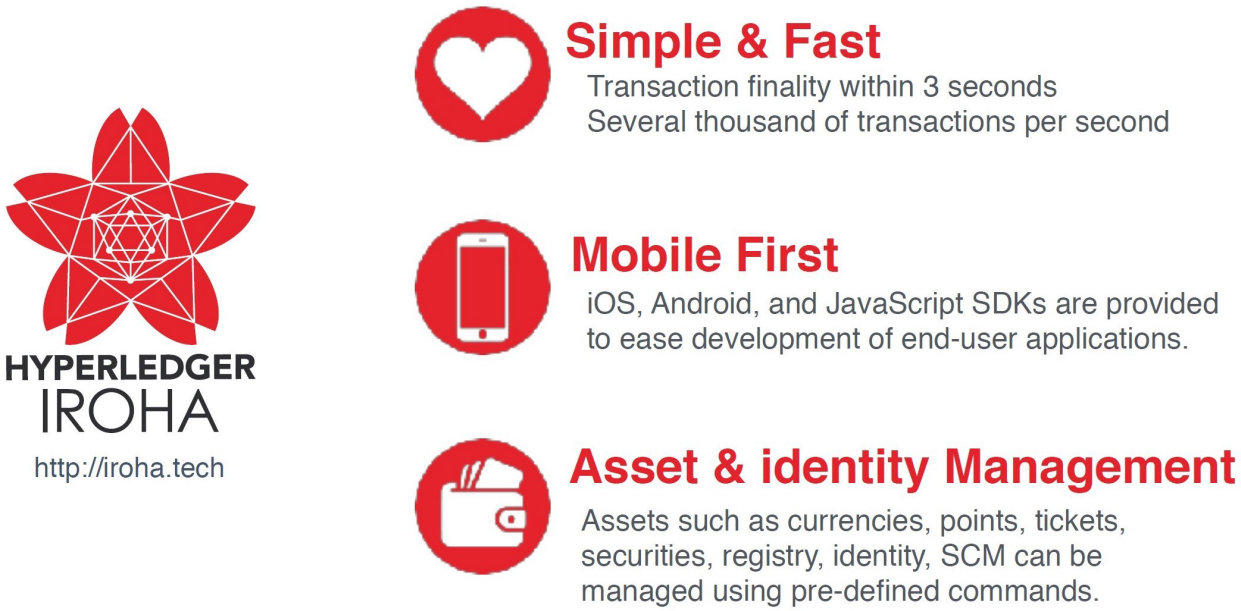
Usage:

- simple and easy management of digital assets.
- it can be used to manage digital assets, identity and serialized data, and can be useful for applications such as interbank settlement, central bank digital currencies, payment systems, national IDs, and logistics, among others.

Features:

- Iroha's **built-in smart contracts, called commands, allow developers to incorporate blockchain into their business processes.**
- Simple deployment and maintenance
- Variety of libraries for developers
- Role-based access control
- Modular design, driven by command-query separation principle
- Ready-to-use set of commands and queries
- Multi-signature transactions
- Uses a high-performance Byzantine fault-tolerant consensus algorithm called YAC.

Model:



3.7 - Hyperledger SawTooth

What:

- Focus on IoT implementations.
- Permissionned and permissionless support
- EVM transaction family (seth)
- Uses single node type -> Simple deployment.
    - **On chain governance** (**CAO** != DAO)

    - Participants can easely add policies and agree on configuration changes using Sawtooth TX,
    - also **change consensus type on the fly** (kind of a DAO)
- Development kits covers lot of != languages
- We can deploy : Java, Solidity, Webassembly contracts
- **Can integrate with existing Database**, and keep value/pairs sync with the network.
- Initial contributor : Intel, 2016
- Clearly separate the core system from the application domain
- Designed for **versatility**

Consensus:

- On demand (start with Raft, then harden with PBFT, or PoEt)
- Can utilize various consensus algorithms based on the size of the network (PoET SGX, Raft, etc.

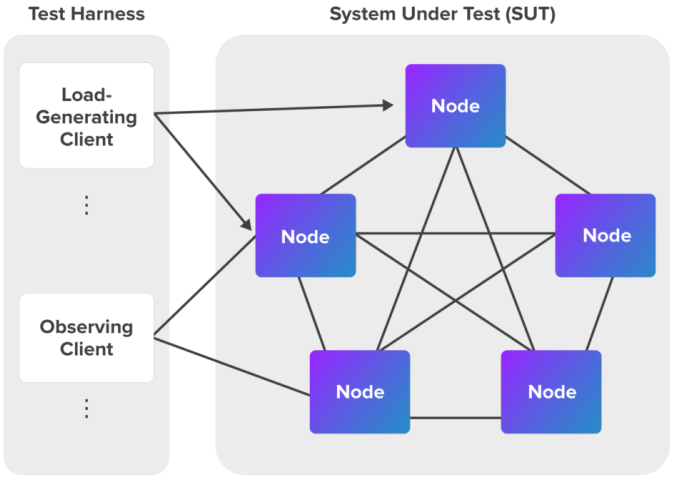
Usage:

- Healthcare
- Finances
- Supplychain

Features:

- Uses pluggable consensus algorithms, which allows consensus to be changed by transaction on the fly
- Smart contracts can be written in almost any language
- Parallel transaction execution for added throughput, while at the same time preventing double spending
- Ethereum contract support via Hyperledger Burrow integration
- No central authority or implementation. This increases security as there is no centralized service that could leak transaction patterns or any other confidential information
- Supports creating and broadcasting events.

Topology:



3.8 - Domain Specific - Hyperledger Grid

What:

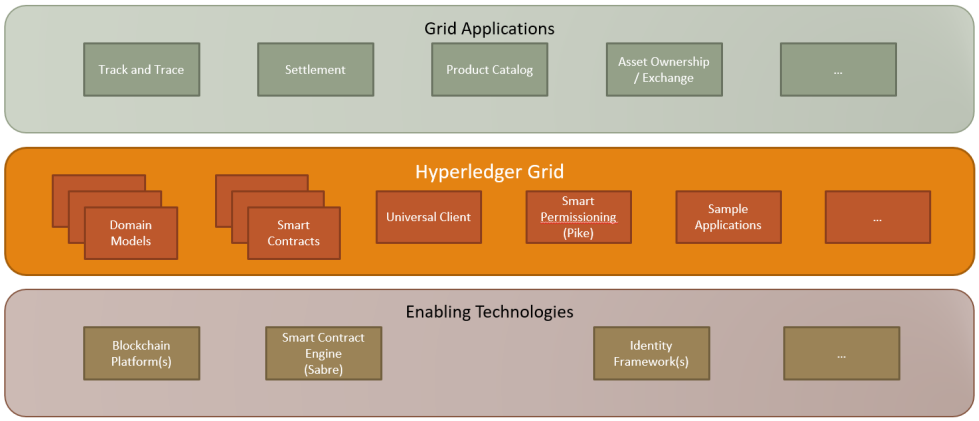
- Domain-specific business blockchain technology Stack including component, ecosystem of technologies, frameworks, and libraries that work together
- Intends to provide
  - Reference implementations of supply chain-centric data types, data models, and smart contract based business logic – all anchored on existing, open standards and industry best practices.
  - Provide authentic, practical ways to combine components from the Hyperledger Stack into a single, effective business solution.
- Initiators : Cargill, Intel, Bitwise, License Apache 2.0

Integrated standards for supplychain:

- **GS1Standards** : (structure around static and dynamic data and increase visibility, standardization, consistency, credibility, neutrality and interoperability)
  - **Global Trade Item Number (GTIN)** - it's a UID composed of Company ID + Product Id - Key for implementation
  - **Global Location Numbers (GLN)** - UID of organisations id and location in the supply chain.
  - **GS1 barcodes** - Provide product specific info, and allow real time view of where products have been and where they are heading to.
  - **Electronic Product Code Information Services (EPCIS)** - similar than a API.

Appendix:

The Stack



Chapter 4. Hyperledger: Tools

We will look at the Hyperledger tools, which are auxiliary softwares used for things like deploying and maintaining blockchains, examining the data on the ledgers, as well as tools to design, prototype, and extend blockchain networks.

4.1 Hyperledger Avalon

What:

- Implementation of the Offchain Trusted Compute Specification pushed by EEA
- Enable the secure movement of blockchain processing off the main chain to dedicated computing resources.
- Link with : SGX, Trustet enclaves encryption
- 2019 Sponsors: Intel, iExec Blockchain Tech, Alibaba Cloud, Baidu, BGI, Chainlink, Consensys, EEA, Espeo, IBM, Kaleido, Microsoft, Banco Santander, Wipro, Oracle, and Monax

Allow :

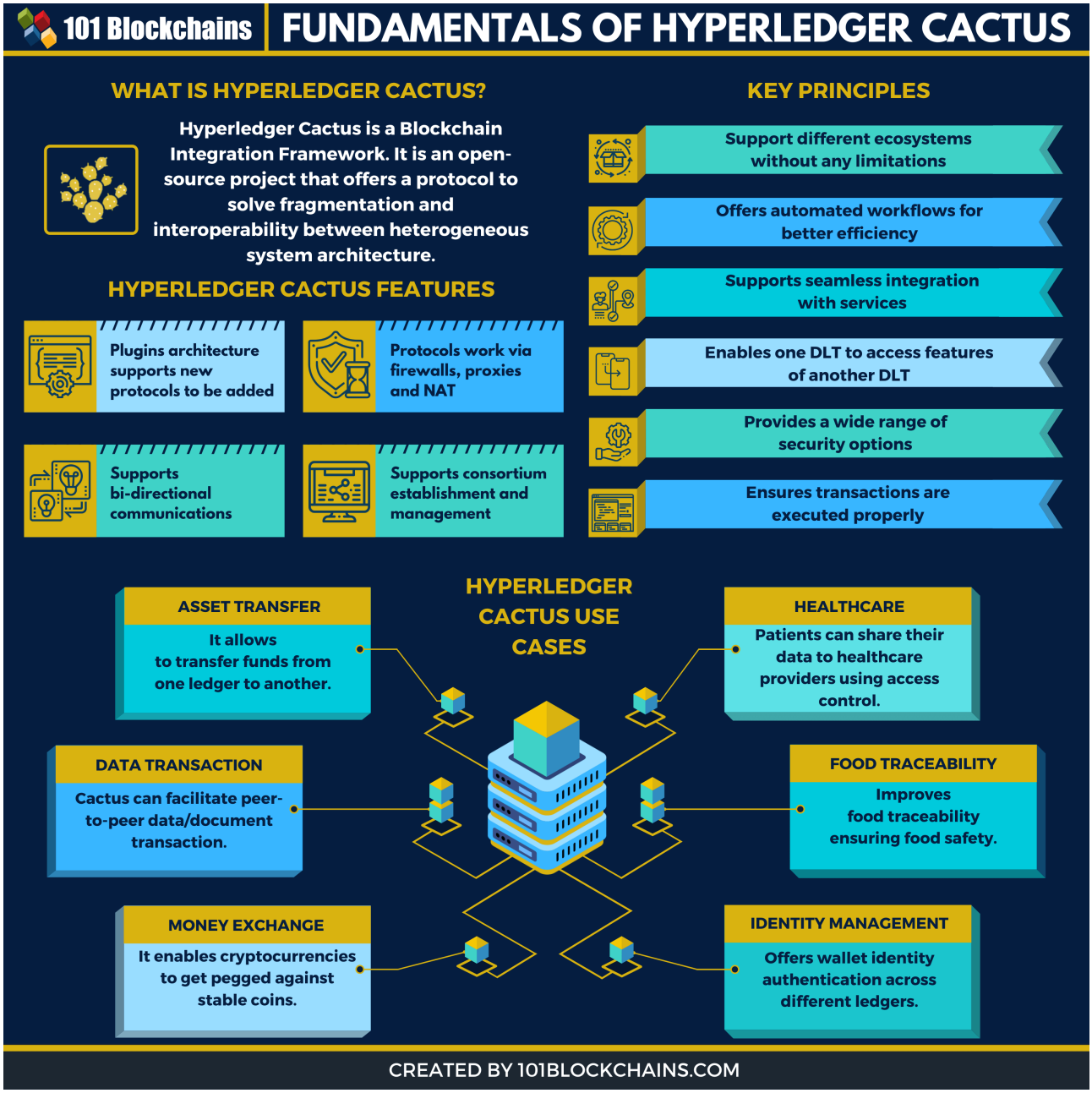
- Enables developers to accelerate throughput and improve data privacy
- The initial implementation of Hyperledger Avalon uses Intel Software Guard Extensions (SGX)

- Uses the Off-Chain Trusted Compute Specification as a starting point to apply a consistent and compatible approach to all supported blockchains.

4.2 Hyperledger Cactus

- Blockchain Integration Framework
- Aims to provide decentralized, secure and adaptable integration between blockchain networks
- 2020 Sponsors: Fujitsu, Accenture
- Plug-in based collaborative development
-

Summary:



4.3 Hyperledger Caliper

What?

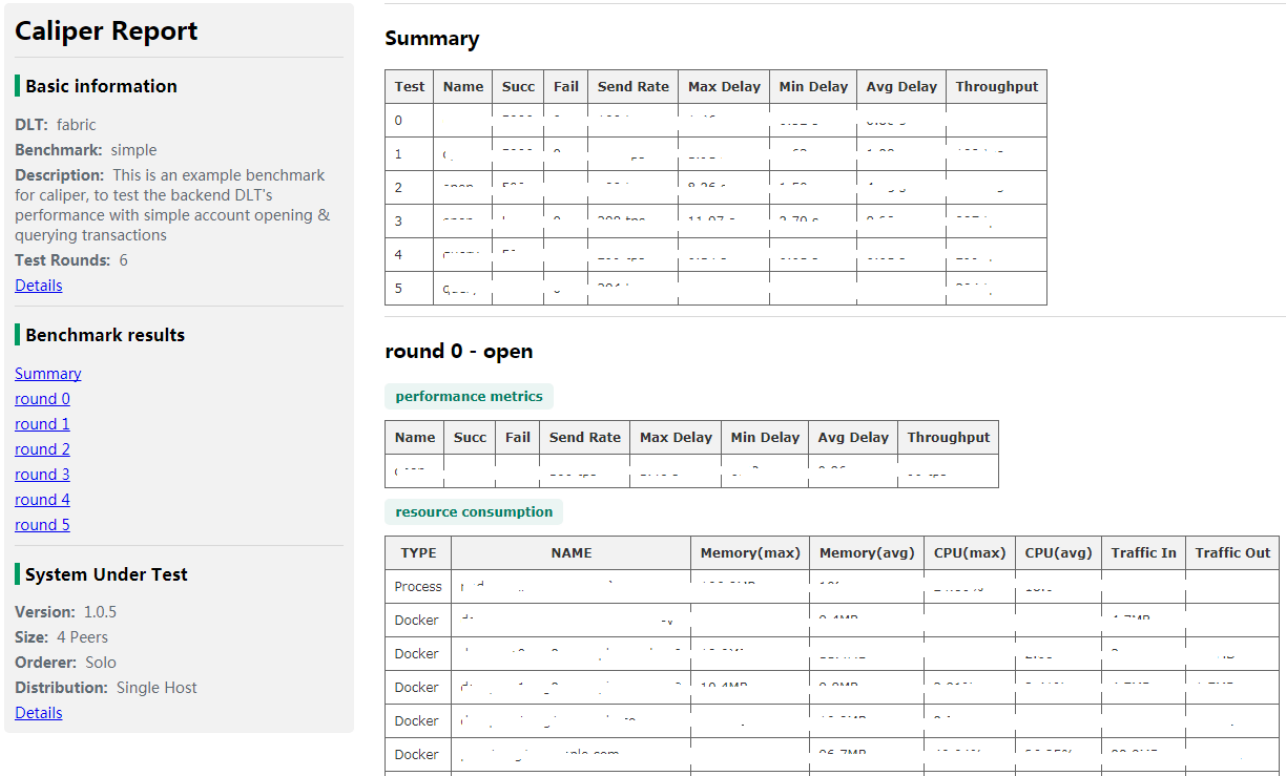
- **Benchmark tool** that measures the performance of various blockchain systems by using a set of predefined cases.
- Normalized rules
- Reporting (ressources utilization, tx, latency, TPS)
- Sponsor : 2018 Huawei, Hyperchain, Oracle, Bitwise, Soramitsu, IBM and the Budapest University of Technology and Economics

Characteristics

- Unified blockchain benchmark framework
- Commonly accepted definition of performance indicators
- Commonly accepted benchmark cases.

Supports

- Hyperledger Besu, Hyperledger Burrow, Ethereum, Hyperledger Fabric, FISCO BCOS, Hyperledger Iroha and Hyperledger Sawtooth.



Caliper Report

Basic information

DLT: fabric
Benchmark: simple
Description: This is an example benchmark for caliper, to test the backend DLT's performance with simple account opening & querying transactions
Test Rounds: 6
Details

Benchmark results

Summary
round 0
round 1
round 2
round 3
round 4
round 5

System Under Test

Version: 1.0.5
Size: 4 Peers
Orderer: Solo
Distribution: Single Host
Details

Summary

Test	Name	Succ	Fail	Send Rate	Max Delay	Min Delay	Avg Delay	Throughput
0								
1								
2								
3								
4								
5								

round 0 - open

performance metrics

Name	Succ	Fail	Send Rate	Max Delay	Min Delay	Avg Delay	Throughput

resource consumption

TYPE	NAME	Memory(max)	Memory(avg)	CPU(max)	CPU(avg)	Traffic In	Traffic Out
Process							
Docker							
Docker							
Docker							
Docker							
Docker							

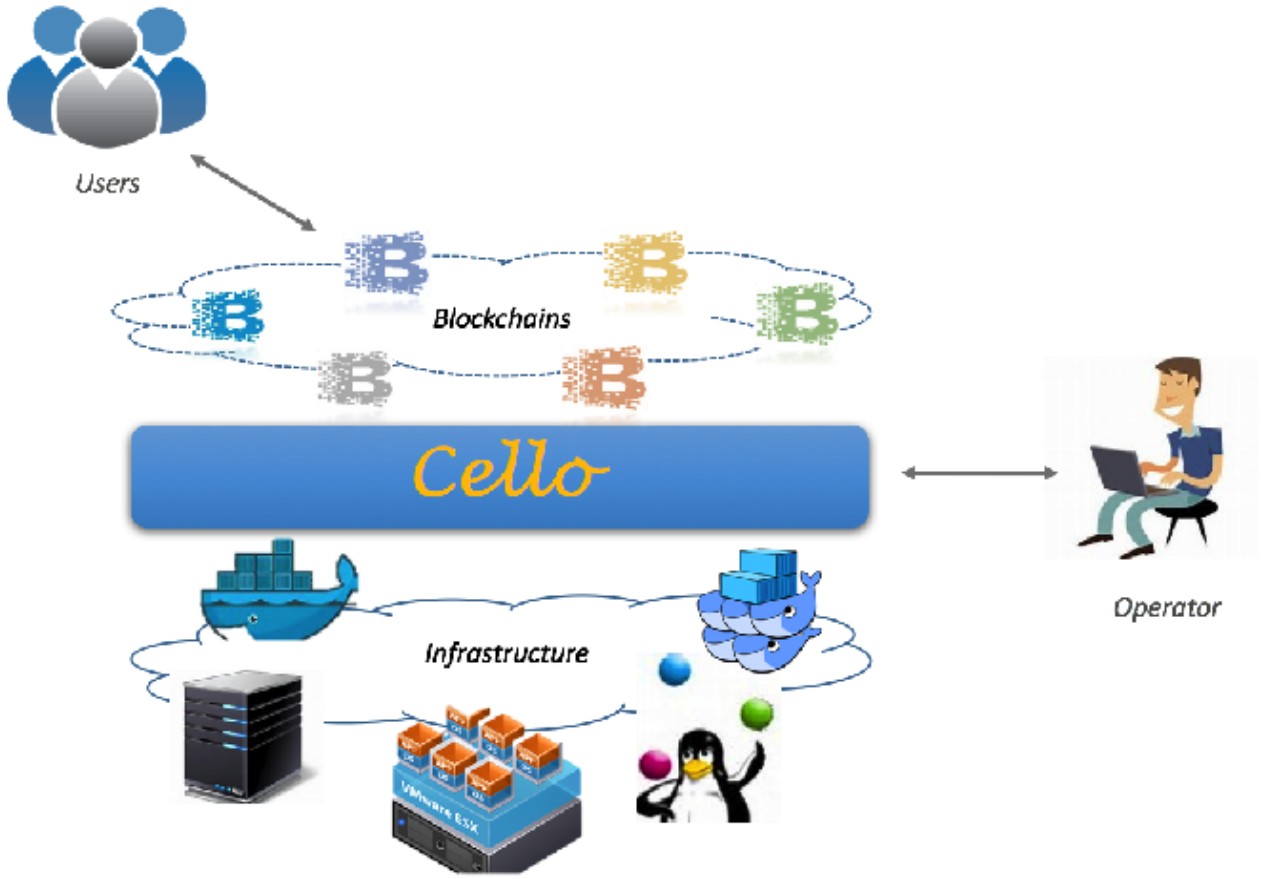
4.4 Hyperledger Cello

What?

- Cello aims to bring the on-demand 'as-a-service' deployment model to the blockchain ecosystem
- Blockchain orchestrator : K8S, Docker....
- Operators can create and manage such blockchains through a dashboard
- Sponsors: IBM, with sponsors from Soramitsu, Huawei, and Intel

Features:

- **Deploy, manage and operate blockchains efficiently and automatically**
- Support customized blockchain requests (support for Hyperledger Fabric)
- Support various infrastructures (baremetal, VM platforms, container cloud)
- Support advanced operational analytics for system status and ledger behavior



4.5 Hyperledger Explorer

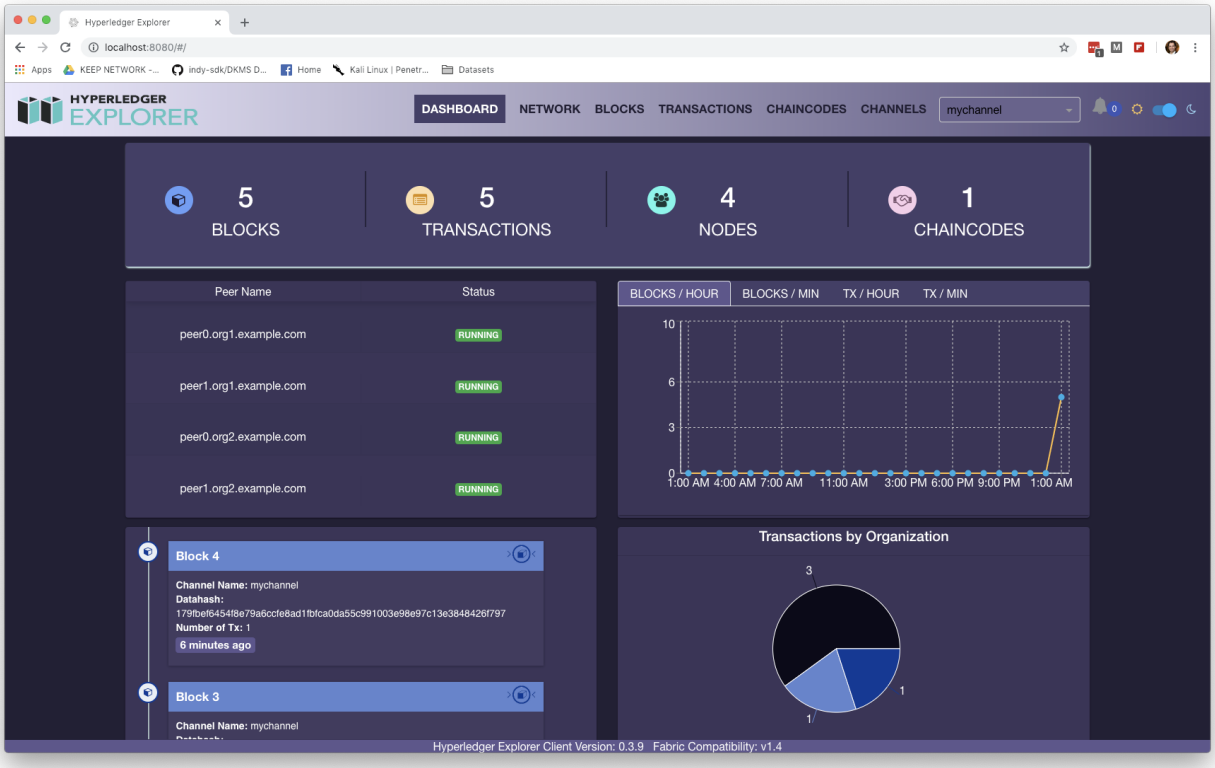
What?

- Open source tool for **visualizing blockchain operations**
- Sponsors : DTCC, Intel, and IBM in 2016.
- Hyperledger Explorer supports Hyperledger Fabric and Hyperledger Iroha.

Features:

- Blocks
- Transactions and associated data
- Network information (name, status, list of nodes)
- Smart contracts (chain codes and transaction families)

- Other relevant information stored in the ledge



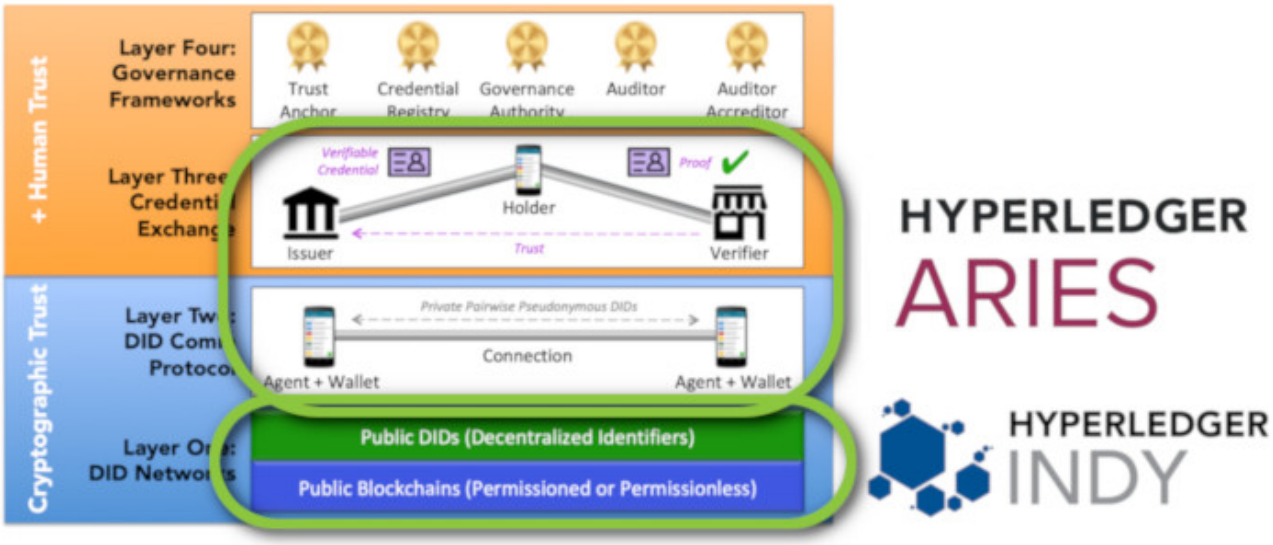
Chapter 5. Hyperledger: Libraries

In this chapter we will take a look at the Hyperledger libraries for **enterprise-grade blockchain deployments.**

5.1 Hyperledger Aries

What:

- provides a **shared**, **reusable**, and **interoperable tool kit** designed for initiatives and **solutions focused on creating, transmitting and storing verifiable digital credentials**
- Aims to change the client layed in HL Indy to be interoperable with others ID projects
- Link with the DLT Framework : Hypeledger Indy
- Link with library : HL Ursa (for cryptography)
- Initiators (2019) : Sovrin Foundation, the Government of British Columbia, and other Indy community developers
- Privacy containers for personnals folders files



5.2 Hyperledger Quilt

What:

- Provide **Interoperability** between ledgers - **Inter Ledger Protocol (ILP)**
- **Java implementation of the Interledger protocol (ILP) which is a payement protocol**
- Provide libraries and reference implementations of the core interledger components.
- With ILP, money can be packetized, routed, and delivered over communication networks with automatic routing and a series of secure, multi-hop payments.
- **connecting bank accounts to digital wallets and everything in between**
- 2017 Initiated by NTT Data and Ripple

Goals of Quilt

Long term, Quilt can become a ledger interoperability solution that enables more than just payment transactions, but a means to exchange any sort of asset across the many different blockchain networks that will exist.

Features

- Provides a set of rules for enabling ledger **interoperability with basic escrow semantics**
- Furnishes a standard for ledger-independent address and data packet formats that enable connectors to route payments
- Supplies a framework for designing higher-level use case specific protocols.

5.3 Hyperledger Transact

What

- Transaction execution platforfm component / library
- Initiators: Bitwise, Cargill, Intel, IBM and Hacera in 2019

Features:

- Serial and parallel transaction scheduling
- Pluggable state backend
- Transaction receipts
- Events that can be generated by smart contracts
- Support for Sabre and Seth, etc.

5.4 Hyperledger Ursa

What:

- Shared cryptographic library
- Initators : Fujitsu, The Linux Foundation, Sovrin Foundation, Intel, DFINITY, State Street, IBM, Sai Infratel, and Bitwise (2019)

Chapter 6. : The Promise of Business Blockchain Technologies

Finance's usage of DLT

- **transferring assets and recording trade agreements** (stock sales, bonds, options, and cash transactions)

Blockchain technologies are very good at **recording state transitions**

Legal industry's usage of DLT

- record property rights and the transfer of those rights

Insurance industry's usage of DLT

- pooling funds from unaffiliated individuals

Health industry's usage of DLT

- record and share data, such as patient health records, or pharmacy information.

Material and product supplychain's usage of DLT

- improved resource, sourcing, and allocation.

6.1 DLT Advantages for businesses

- **Smart contracts eliminate the middleman and add accountability** (used in various industry sectors, such as real estate, healthcare, government, music, etc.)
- **Internet of Things (IoT)-based blockchain applications**:
  - add a higher level of security
  - add transparency (in industries like supply chain, healthcare, banking and financial services, automotive, cybersecurity, etc.). Hyperledger Fabric is at the forefront of this revolution.
- **Identity security is a key area where enterprise blockchain technologies can make a difference**, bringing, for example
  - a much-needed reduction in identity fraud and theft claims
  - cutting the red tape of government and local administration bureaucracy
  - and more.

  Hyperledger Indy, Hyperledger Fabric, etc. are just a couple of technology examples successfully used in production in this area.
- **Blockchain adds data transparency and automation**
  - supply management and logistics
  - by building trust and enabling leaner, more cost-effective processes.

6.2 Production usescases

- **Supply Chain** - IBM Food Trust, powered by Hyperledger Fabric,
- **Airline Industry** - NIIT Technologies developed a new blockchain application, Chain-m, using Hyperledger Fabric.
- **Enterprise Operations Management** - JD.com, the largest retailer in China, has developed its own enterprise blockchain platform aimed at streamlining numerous operational procedures, such as tracking and tracing the movement of goods, charity donations, authenticity certification, property assessment, transaction settlements, digital copyrights, etc.Hyperledger Fabric.
- **Insurance Compliance Data** - The American Association of Insurance Services has developed openIDL (open Insurance Data Link), a system built on IBM Blockchain, thus powered by Hyperledger Fabric, which is designed to automate insurance regulatory reporting.
- **Decentralized Identities and Trusted Credentials** - In an attempt to streamline their business-oriented services, the government of British Columbia started working on a project based on Hyperledger Indy. OrgBook BC is an online directory that can be used to quickly verify if an organization is legally registered to do business in British Columbia as a corporation. This is just the first step of a larger blockchain-based initiative aimed at streamlining government services.

6.3 Supplychain Management

Defintion The oversight of funds, raw materials, components, and finished products, as they move from suppliers, to manufacturers, to wholesalers, to retailers, to consumers, within one or several companies

- Important part of enterprise resource planning (ERP)
- Supplychain + Trade Finance

Why is blockchain useful in supplychain ?

- Blockchain data improves insight into products, as they move through their lifecycle
- Audit trail
- Eliminate the need for a trusted third party to certify raw materials, components, or finished products, as they travel through a supply chain
- Improves resource allocation.
- Although a record of the transaction is public and tied to the movement of physical items across the network, specifics such as the quantity of goods, or the identity of the parties transacting, can be done pseudo-anonymously in a blockchain. Such a granular view of movement through supply chains improves resource allocation.

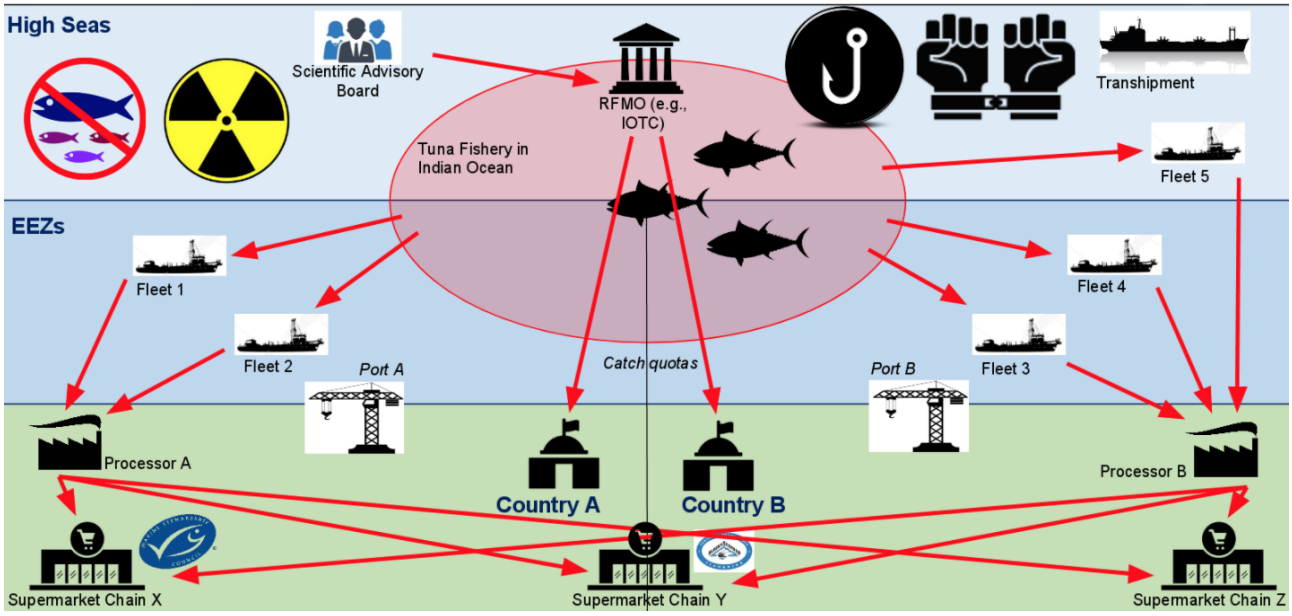
Challenges :

- Stocking the right amount of inventory over time is also known as **supply demand synchronization**
- DLT can provide for **just-in-time lean manufacturing** and distribution
- Overstocking inventory is costly
- Inter companies settlements is difficult because no integration with the differents ERP systems -
- Data doesn't flow well through the handshakes or interface points between systems.
- Transfert of ownership & Changes of status of products through their synchronization between parties
- **Visibility is limited at the hand-off points of funds, raw materials, components, or finished products and it's intented**

Idea developped : Integrate trade finance

- WTO : "up to 80 percent of global trade is supported by some sort of financing or credit insurance" (2016)
- The trade finance industry can also leverage information visible in a supply chain blockchain. trade finance manages capital required for international trade.
- An exporter needs to mitigate the risk of non-payment, while an importer wants to mitigate the supply risk. The function of trade finance is to act as a third party to remove the payment risk and the supply risk, whilst providing the exporter with accelerated receivables, and the importer with extended credit. Institutions that provide capital during these trades can leverage the information visible in a supply chain blockchain to better evaluate companies for lending.

Supply Chain of Tuna



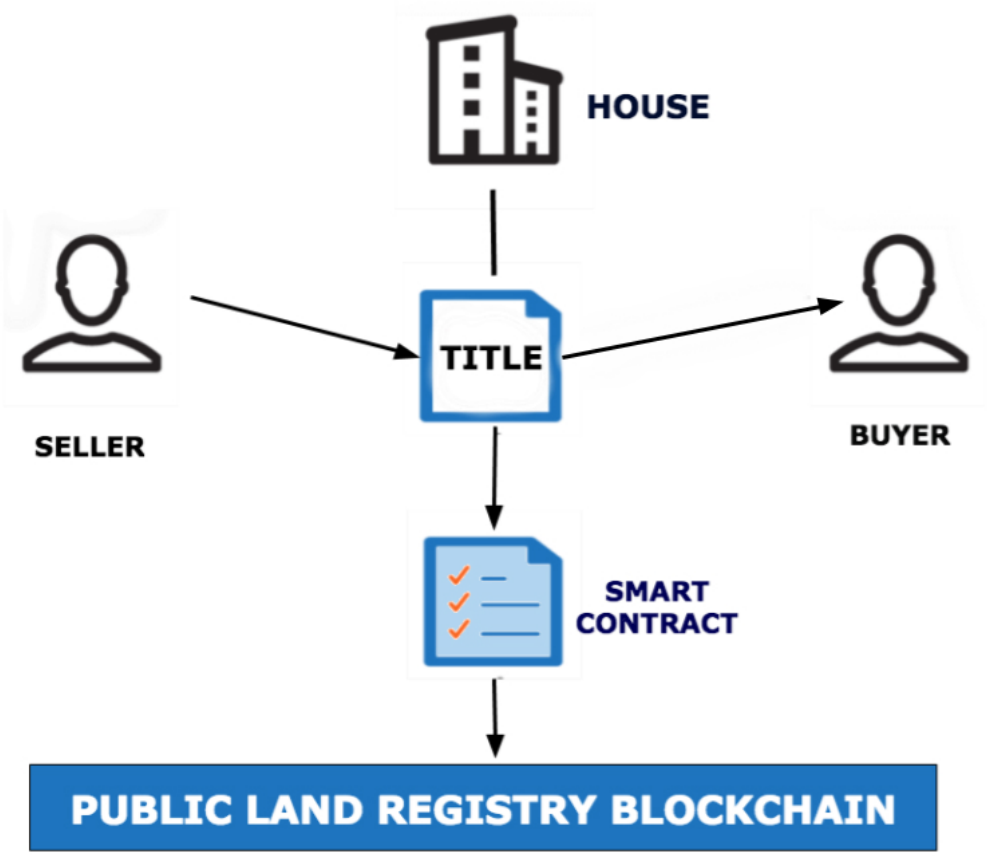
Other examples: Ibm Food with WallMart, CoffeeChain...

6.4 Property Rights

Definition:

- Division of law whereby the rights and responsibilities associated with owning an asset are established
- Rights :
  - use
  - profit
  - exclude others
  - transfer for any assets (partly or completely)
- Reponsabilities:
  - Tax
  - Maintenance and repair costs,
  - Payment for injuries caused by unsafe or defective conditions of the asset.

Link with NFT and tokenization. Intellectual property includes copyright, trademark, and patents alsoon chain



Property Titles on a Blockchain via a Smart Contract

Why DLT in IP?:

- minimize disputes around property rights
- record ownership rights and responsibilities.
- governments have put land registry records on blockchain
- it can provide an immutable, secure, timestamped record for the creation of intellectual propert
- A blockchain may record a hash of a document.
    - As an example, photographers could place a hash of their unique digital photographs on the blockchain.
        - The hash of a digital photograph will be constant so long as the photograph file has not been altered
        - Blockchain can control and track the distribution of the photograph
        - Detect the introduction of counterfeit images
        - Blockchain can be used to resolve disputes as to who first introduced the image

    - -> By placing a hash of intellectual property documents on the blockchain, a party can publicly demonstrate data ownership,
    - -> Prove the existence of certain documents at a given moment in time, without revealing the actual data.
    - -> In addition to the hash, you may also choose to store the location of the file in the blockchain, which could be used for retrieval.

Audience:

Strong brand value in particular

- Such as the fashion industry and luxury good providers

6.4 Provenance

Link with : EU Tax & Customs, EU_IPO, OECD

Definition:

- Provenance is a record of ownership used as a guide to authenticity or quality.

Why:

- data improves insight into products
- OECD aims to improve tracability

Usecases for niches

Consumers who are willing to pay a premium to make sure that they are not funding operations that are not in line with their values

- Authenticity check (should be linked with property rights) - Luxury
- Fair trade and fair labor standards check
- The use or not of harmful chemicals during product manufacturing
- Counterfeit products

6.5 Finances

- Currently, bonds, invoice financing, letter of credit transactions, and interest rate swaps governed by an **ISDA master agreement** have all been recorded on blockchain
- With smart contract technology, a legal agreement can automatically execute clauses within it.

Pains

- Messaged based models
- Slow reconciliation processes
- **Inefficiency of fragmented data stores**.
- **Post trade cycles involve in the trade a series of steps to verify the terms of the trade and to transfer the assets involved by the law to go through a third parties**. Some trades are currently required by law to go through a separate central clearing organization

a complex process known as the post-trade cycle is initiated once parties "execute" a trade. The post-trade cycle involves a series of steps to verify the terms of a trade, and to transfer assets involved in the trade in order to effectuate and settle the trade. Some trades are currently required by law to go through a separate central clearing organization. This organization steps in as the counterparty to each trade, creating two distinct contracts for each trade. These organizations are central securities depositories, whose role is to minimize the risk of trade default, and also to enforce rules against overexposure to certain types of trades.

Opportunities

- Shared data construct,
- Driving down costs
- Increasing efficiency
- Opening up entirely new business models

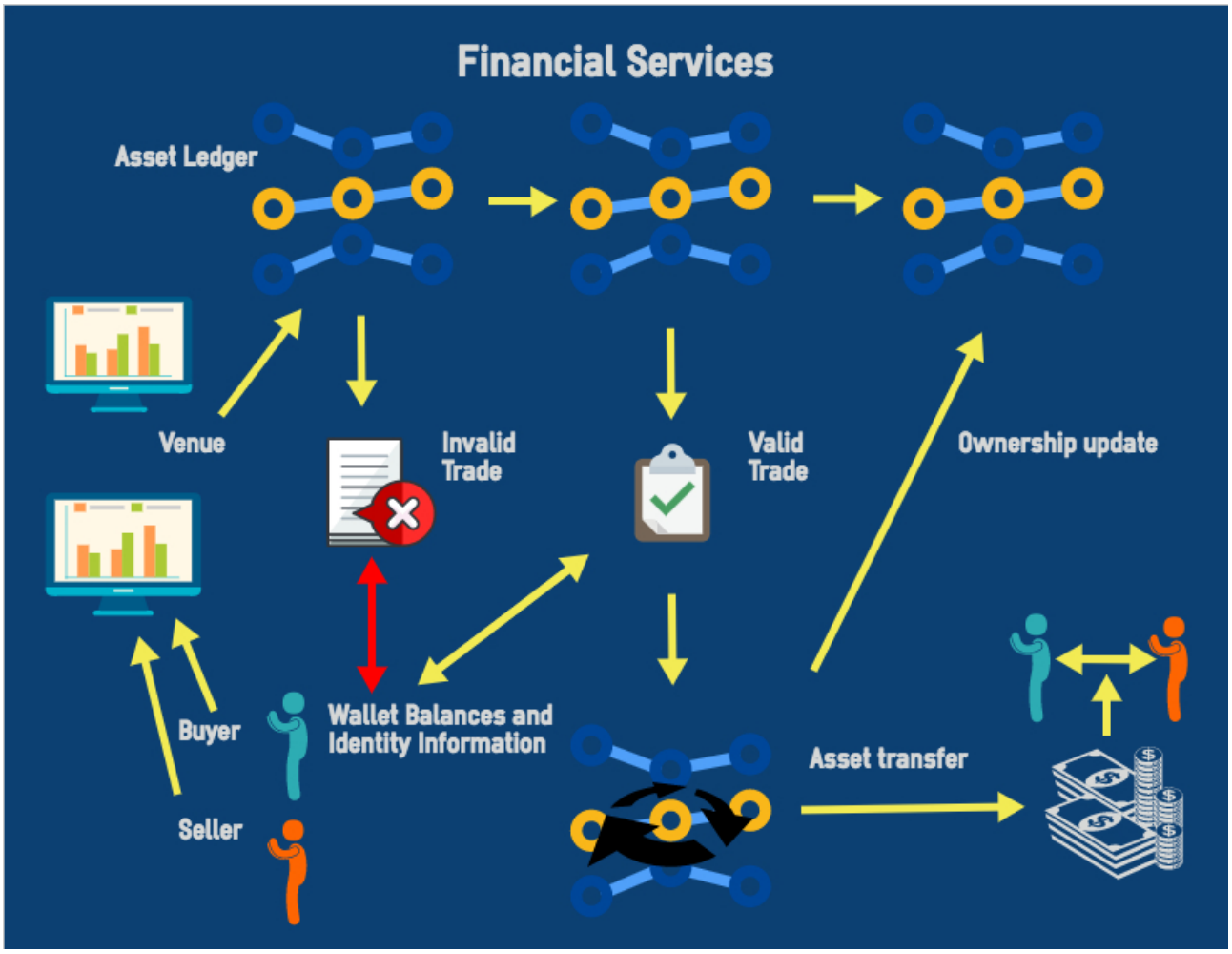
6.6 Trade process

Although every trade has its own lifecycle, generally, the following steps will occur:

- Parties execute a trade. Executing a trade occurs when parties agree on the details of a trade and are willing to enter into the deal.
- One party will draft an inception document, capturing all the terms of the trade, and will send it to the other party to get the trade confirmed.
- The recipient of the inception document will check the details of the trade and confirm the trade by signing and returning the document. Confirmation communication is done often by Fax, SWIFT, or Telex.
- The trade is allocated. For flexibility of profit and loss booking, parties will often allocate the trade to various sub-entities within their organization.

- Each trade will be stored by the party who was allocated the trade on an internal database. For ease of identification, the trade is assigned a unique Trade ID as a standard identifier.
- Post-Trade Changes are sometimes made by the parties. This can occur when:
  - The trade can be amended with consent of both parties
  - One party may assign its position in the trade to a different party
  - A partial termination of the trade may be triggered if a change in the notional of the trade that is not pre-fixed according to the agreement occurs
  - Termination of the deal before maturity of the trade may occur, which may entail a termination fee.
- Payment is made. These payments may be at the close of a trade, or at intermediate stages while a trade is still open. When the payments are made on an open contract, this is known as 'revaluation' and is done to minimize the risk of nonpayment by a counterparty whose position has weakened in the trade due to events that occurred after trade execution.
- Audit of the trade and associated payments is performed by the parties. If a dispute occurs, the parties must communicate and come to a resolution for such discrepancies. This is a manual and costly process.

Example of a Financial Trade Process



The image above shows the automation of back-office processes involved in trade confirmation and post-trade settlement via DLT

- An asset ledger stores ownership and transactions.
- Smart contracts allow the asset ledger to handle collateral management and initiate payments per contract terms.
- Venues (e.g. exchanges, MTFs, bilateral voice conversations) still match trade requests with a counterparty, and provide price discovery.
- Querying information on the asset ledger may assist with price discovery.
- The asset ledger verifies the parties and asset ownership. It will then either accept, or reject the trade.
    - If, for example, the seller does not own the asset in question, or the new trade would result in an illegal overexposure on the buyer side, the trade would be rejected. When a trade is valid and accepted onto the blockchain, the blockchain automates an immediate change in ownership, or a delayed, or contingent asset transfer.
- The changes in asset ownership or contract terms are securely recorded onto the asset ledger.

- The contract is programmed to execute automatically, exchanging payments and other assets per the terms agreed to by the parties.

Control funds on the blockchain

Disadvantages:

- If funds aren't under the control of the smart contract, then there is no way a payment can be guaranteed
- if funds are controlled by the parties' smart contract agreement, then those payments can indeed be guaranteed at the close of the trade

Advantages

- Conducting post-trade settlement in an automated way through smart contracts promises to introduce efficiencies, and reduce friction associated with trades.

Barriers to entry (solved):

- Data Privacy (partially solved with ZKP and DECO)
- TEE : Some regulations in the finance industry will not allow you to share information, or store it on a shared medium, even if it is encrypted. In addition, regulations covering securities professionals specify how ownership of certain assets must be recorded and properly transferred

6.7 Healtcare

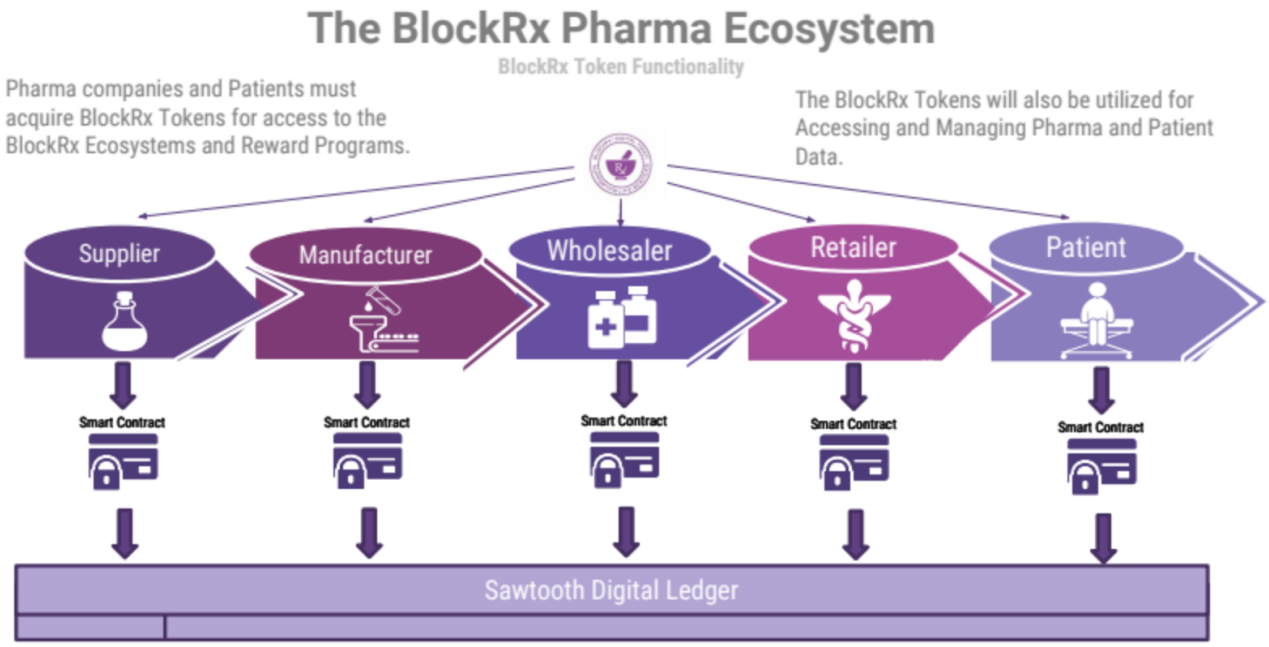
DigitalID

Why Healtcare?

- By streamlining these multi-party processes
- Insurance benefits investigation eligibility checks are performed
- protect data from cybercrime
- online identity management,
- medical history
-

Benefits:

- reduce the time and expense of collecting and verifying multiple pieces



6.8 gi

Benefits:

- Streamlining verification procedures for academic credentials, thus reducing fraudulent claims and bringing more transparency, ease of use, and speed to this process.
- Verifying e-portfolios of digital badges
- Securing and sharing student records
- Identity management
- Sharing security data (from security cameras and sensors, for example) across device networks
- Creating learning marketplaces
- Records management
- Increasing accountability and transparency for charitable school donations
- Streamlining the public assistance system for families and students.

More blockchain education use cases: :
https://www.forbes.com/sites/tomvanderark/2018/08/20/26-ways-blockchain-will-transform-ok-may-improve-education/#6b6198ac4ac9

6.8 Smart Energy Management

6.9 Dubai

- The Dubai Blockchain Strategy aims to enable the execution of all applicable government transactions through blockchain by 2020.
- The Decentralized Data Marketplace leverages blockchain technology to ensure the security and immutability of transactions, tokenization to hide sensitive information, etc. The UAEPASS is the national digital identity platform, giving UAE citizens, residents and visitors access to local and federal government services, as well as those of private companies, all on a single smart application, allowing them to authenticate and sign documents digitally.
- The DubaiNow mobile application is a one-stop shop for smart services, unifying more than 55 key services from 22 government agencies. This application allows users to manage their bills, register their cars, renew licenses, track visa applications, obtain general information in real-time (from weather, to public transport, to health, etc.), and much more. This application also enables the Dubai government to implement various social responsibility-related activities: donations are collected and then distributed to a variety of beneficiaries, in collaboration with charities and government agencies. It also allows you to direct how money collected from fines you pay (e.g. traffic fines) are used, among other things.
- Paperless government by 2020 is another goal of the Smart Dubai initiative, allowing officials and citizens to save time and resources, and protect the environment as well. “Adopting Blockchain technology Dubai stands to unlock 5.5 billion dirhams in savings annually in document processing alone - equal to the one Burj Khalifa’s worth of value every year.”

6.10 Best Practices

Security for the long term

- While blockchain transactions are secure and cryptographically protected when it comes to the current technological advancements, we should always keep in mind that nothing is static, and technology continues to advance at an incredibly fast pace. What is secure today may not be so in the near future. Hackers and other bad actors are constantly focusing on breaking the cryptographic algorithms that protect blockchain data today.

To avoid the potential security disruptions of tomorrow, a critical best practice is that users should never put personally identifiable information, or PII, on their blockchains.

File storage on the blockchain

- Due to the way blockchains work to store data, replicating it on every other node or peer in the network, storage and compute costs can be incredibly high. *To avoid added storage costs, it is recommended that other storage and replication methods to be used* - this includes cloud networks like AWS S3, GCP Filestore, etc. This way, nodes and peers can have pointers or links to the data files kept outside of the blockchain network, instead of the actual data.

Permissioned blockchain for private data

- On public blockchains, anybody has access to the information stored on the network: they can add transactions and read the data that is in it. When it comes to permissioned blockchains, data can be stored, accessed and used only between partners that have access to it. *Permissioned blockchains, such as the Hyperledger technologies, are a great solution for businesses, as they want their data to remain private.*

Blockchain governance structure

- Most blockchain-related challenges are related to the governance model that is chosen. *To keep things straightforward, you should define the governance structure upfront very early in the process*, even before diving into blockchain: decide how new users/organizations are added to a blockchain network, how to determine if a user/organization should be removed from the blockchain network, include a mechanism that deals with and removes bad actors previously allowed in the network, etc. Keep in mind that things change over time, and as such, the governance procedures may change as well.

Performance and scalability requirements

- *Blockchain architects must have a clear understanding of the requirements for their specific use cases, and they must ensure that their blockchains meet those requirements*. Based on these requirements, decisions must be made early on with each deployment and use case in regards to what technologies to use.

Goals of blockchain business cases

- Not every project or solution is successful, unless it is carefully planned, designed and implemented. *A carefully thought out strategy must be designed and implemented for each project, to ensure that goals are achieved.*

6.11 When to use or not blockchain technologies

1. Start with the business need

    i. What are you doing in this entreprise?
    ii. What are you doing with your business, suppliers, customers, competitors
    iii. What are the business processes? provenance tracking problems? registry issues (CINS)?
    iv. Where is there a SC or a decentralized ledger opportunity?
2. Define requirements
    i. #participants ?, tps?, #nodes?, geo? which devs to onboard? What are the rules, risks, and responsibilities of each party?

One way to way to explore that is through industry consortiums where they discuss technical standards, common business processes, poc

It's important to think about an **industry wide approach.**, once you have it think about the **characteristics of that need**

Requirements

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package