BLOCKCHAIN TECHNOLOGIES

Different Blockchains

Dhiren Patel
CS423 (Nov 15 and 16, 2022)

WORLD BANK GROUP

VEERMATA JIJABAI TECHNOLOGICAL INSTITUTE
V.J.T.I.
ESTD 1887
MUMBAI 400019

DeLight Chain

HAW
HAMBURG

LEARNING OUTCOMES

- **Know**
  - types and classification of blockchains
  - about foundation of various blockchains
  - security concerns
  - mapping of blockchains to application domains

- **be able**
  - to describe evolution steps and major types of blockchains

WHAT MAKES THE BLOCKCHAINS DIFFERENT FROM EACH OTHER?

- **Openness**
  - **Public**

    Anybody (full node user) can add blocks to the blockchain (e.g. Ethereum, Bitcoin, Litecoin etc.)
  - **Permissioned**

    Only designated trusted nodes can add blocks to the blockchain
    - Consortium based (e.g. R3 Corda, JP Morgan-Quorum)
  - **Private** (e.g. IBM – Hyperledger Fabric, Multichain – Multichain, IOTA - IOTA etc.)

WHAT MAKES THE BLOCKCHAINS DIFFERENT FROM EACH OTHER?

- **Consensus Protocols**
  - Proof of Work – PoW (Ethereum, Bitcoin, IOTA etc.)
  - Proof of Stake – PoS (Peercoin, Ethereum Next Generation Casper etc.)
  - Proof of Elapsed Time – PoET (Hyperledger Sawtooth) (a wait time randomly generated by a trusted execution environment – who creates a new block)
  - Practical Byzantine Fault Tolerance – PBFT (Ripple, Hyperledger Fabric etc.) – reduce influance of faulty nodes (efficient energy and transaction finality)
  - Proof of Authority (blocks are validated by approved accounts: validators)
  - Proof of Burn (miners gain the power to mine a block by “burning” a portion of the tokens they have in their possession – minimizing energy consumption)
  - Solo and Kafka (node to validate a batch of transactions and add them as a new block - used by Hyperledger - SOLO involves a single ordering node, Kafka - the leader does the ordering)

BRIEF CLASSIFICATION OF BLOCKCHAIN TYPES

	Consensus	#node requirement for majority	Transaction/Block Approval Time
Permissionless/Public (Bitcoin, Ethereum)	PoW	High (Thousands)	Long (5-15 sec per tx)
Permissioned/Private (Hyperledger, IOTA, Ripple, R3 Corda, Hashgraph)	PBFT	Low	Short (1 – 5 msec per transaction)
Permissioned/Public (Ethereum after PoS is implemented)	PoS	Moderate	Short (10 – 15 msec per block)

Source/further reading:
IOTA Transactions, Confirmation and Consensus, https://github.com/noneymous/iota-consensus-presentation
Hyperledger White Papers, https://www.hyperledger.org/resources/publications#white-papers
Ethereum, A Next-Generation Smart Contract and Decentralized Application Platform, https://github.com/ethereum/wiki/wiki/White-Paper

APPROACHES FOLLOWED BY DIFFERENT BLOCKCHAIN/DLT ORGANIZATIONS

Blockchain/DLT	Approach	Organization
Bitcoin Blockchain	Financial Payments using Cryptocurrency	Bitcoin
Ethereum Blockchain	Application development using tools provided by the Blockchain (Remix, Metamask, Web3.js, etc.)	Ethereum
Fabric, Sawtooth, Iroha	Using Development Platforms/APIs (configuring nodes, mobile applications, certifying authorities)	Hyperledger
Corda	Develop Industry Specific Solutions (Finance, Legal, Healthcare, etc.)	R3
Ripple	Cross border payments using blockchain	Ripple
IOTA	Directed Acyclic Graph (DAG) based token for IoT - Open, Feeless Data and Value Transfer Protocol	IOTA
Hashgraph	DAG based asynchronous consensus algorithm with guaranteed Byzantine Fault Tolerance - high transaction throughput	Swirlds (harness the power of the cloud without servers)

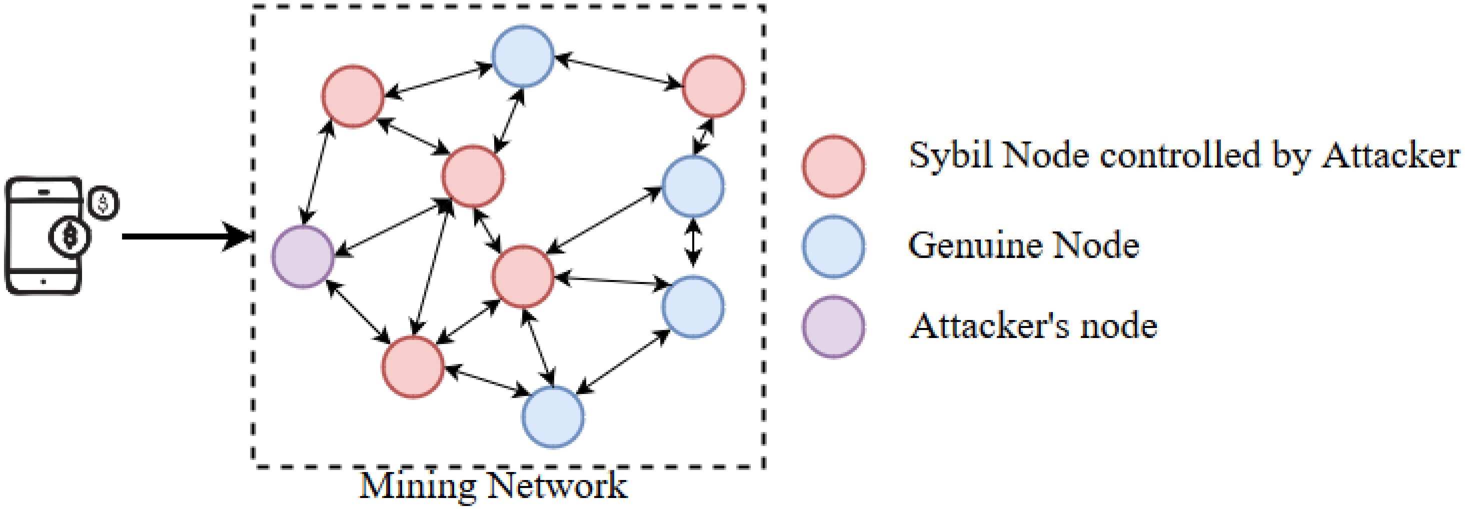
BITCOIN BLOCKCHAIN

- Block creation time: ~10 min
- Average transaction size: 495 bytes
- Maximum block size: 1 MB (2 MB)
- Average number of transactions per block: $\frac{10^6 bytes}{495\ bytes} = 2020$
- Blockchain size: ~197.5 GB – July 2018 (~250 GB – Oct 2019) (~437 GB – Nov 2022)
- increasing

- **Hardware Mining**: to solve Bitcoin blocks
  - started with Field-Programmable Gate Arrays (FPGA)
    - led to the creation of mining farms
  - started with GPU
    - Nvidia GTX 1080 TI can compute around 0.5 GH/s (advanced...)
  - now Application-Specific Integrated Circuits (ASICs) are used
    - capable of computing around 4 – 14 TH/s with a power efficiency of 0.098 – 0.29 W/GH
- **Cloud Mining**
  - to avoid purchasing dedicated mining equipments, creating cooled atmosphere for the hardware, cloud mining became popular
  - Types: hosted, virtual hosted, leased hashing power //Attack landscape (Semantic Report)

SECURITY CONCERNS ABOUT BITCOIN (1/2)

- **Sybil Attack** – Lack of robust identity management
  - Attacker creates multiple identities (maybe virtual) and takes control of the network
  - to forward attackers block faster than the genuine users block
- **DoS/DDoS Attack** – Inherent from the Sybil Attack



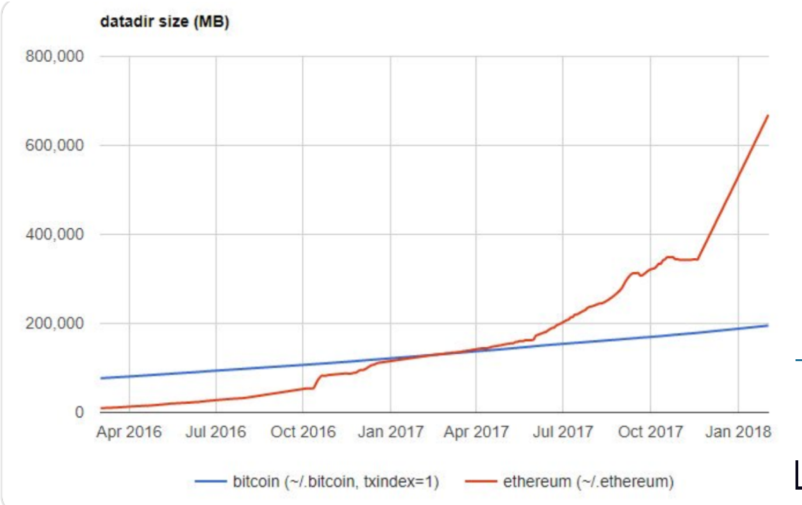
SECURITY CONCERNS IN BITCOIN BLOCKCHAIN (2/2)

- **Majority Attack** – Bitcoin blockchain assumes an honest majority
  - 80 % of mining pools located in China (2019) – Now 20%, 20 % distributed over Iceland, Japan, Czech Republic, India

- **Indentity Theft** – Due to weak password for wallet
  - Stealing of private keys/wallet passwords through phishing attack

ETHEREUM

- Follows the *Blockchain First* approach
  - Developers build their application by using tools provided by the blockchain (Serpent, Solidity, Web3.js, Truffle, etc.)
- Governed by the Core developers
- Currency: Ether, Token system
- Purpose: Run Smart Contracts - Smart Contracts compiled into *bytecode* and executed by nodes using Ethereum Virtual Machine (EVM)
- Consensus: Proof of Work (present), Casper (future) – at Ledger level
- Block time: 15.3 sec
- Block size: 25.93 KB
- Blockchain size: 553.1 GB (2018) (today ~1014 GB = 1 TB)
- Gas limit: 7,999,992 Gas



ETHEREUM: GAS AND PAYMENT REQUIREMENT

- Gas
  - mitigated DDoS attacks
  - **Gas**: all programmable computation is subjected to fees in Ethereum
  - **gasLimit**: every transaction has a specific amount of gas associated with it
    - 20,000 gas is used for storing 8 bytes of data and the current cost is 10 $\frac{gwei}{gas}$ (1 ether = $10^{18} wei$)
      - 1 kB data $\cong \$\ 3$
    - retrieving the data is free
- User sending a transaction will pay (gasPrice*gasUsed)
    - Minimum gas for a single transaction = 21,000 gas
- Miners receive the gasPrice amount as payment for mining the transaction
- A higher gas price on a transaction will cost the sender more in terms of Ether and deliver a greater value to the miner

→ more likely to be selected for inclusion by more miners

STORING DATA ON BLOCKCHAIN: OFF CHAIN

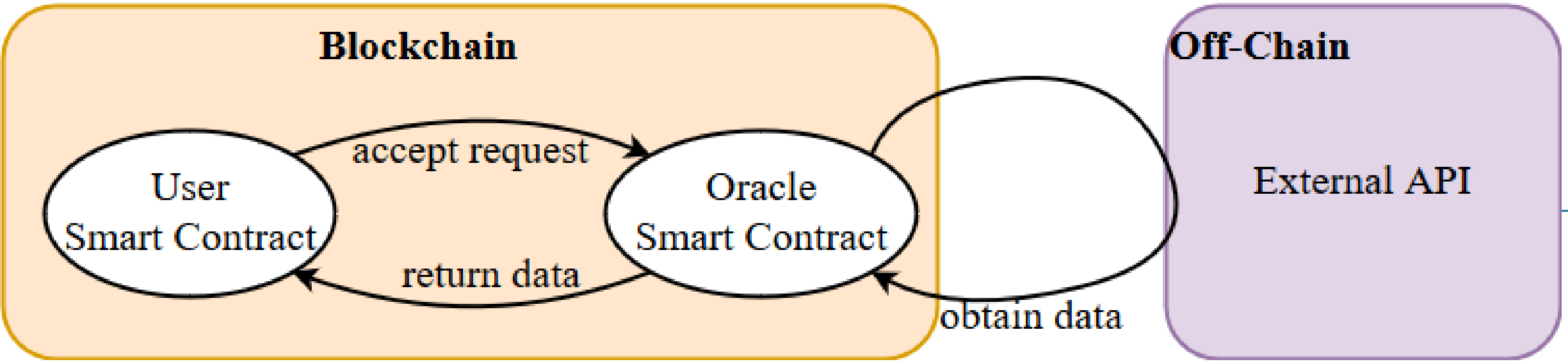
- Decentralized storage: **Inter Planetary File Storage – IPFS** (off chain data storage)
  - Each file is identified by a unique hash – this hash is stored on the blockchain
  - While the data is served through one or more IPFS nodes
  - Keep your own nodes running to keep the content online
  - Or use the **Filecoin** protocol

- Another option for decentralized storage is **Swarm**

ETHEREUM: ORACLES

- A DLT oracle is a trusted service designed to supply external data to a DLT system.
  - E.g. They can be a trusted data feed that sends information into the Smart Contracts, removing the need for Smart Contracts to directly access information outside their network.
  - Usually supplied by third parties and authorized by companies using them.

- They act as data carrier between Web APIs and the Dapps.
- Companies working to create a decentralized Oracle network: LINK, SmartContract.



ETHEREUM: APPLICATION DOMAINS

- Dezentralized Applications (dAapps) Development

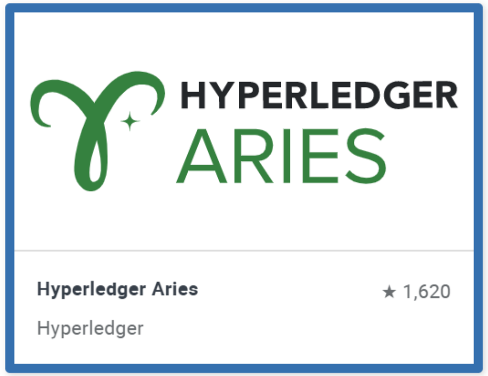
  - Digital signatures
    - Developed by Luxembourg Stock Exchange to ensure authenticity of documents
  - Electric Car charging - RWE (German Energy Provider)
  - Video Games – CryptoKitties
  - Secure Identity Systems – uPort
  - Decentralized Marketplaces

HYPERLEDGER

- The open global ecosystem for enterprise grade blockchain technologies
- Modular, Secure, Interoperable, Crypto-currency agnostic, API library
- bridge permissioned and permissionless networks
- Open source collaborative effort to develop decentralized applications in Finance, IoT, Healthcare, Supply Chain industries
- Governing board headed by Linux Foundation
- 10 academia partners, 25+ industry partners
- support to grow its code base and community on a global level with technical governance that fosters best open development and security practices

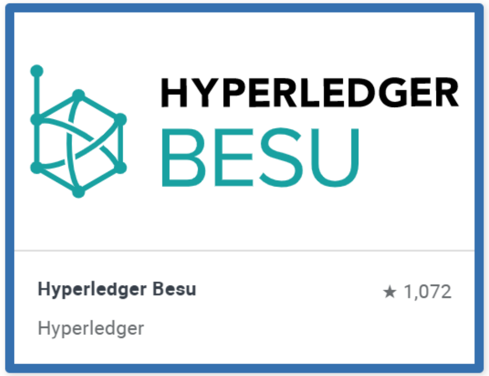
Source/further reading:
Hyperledger, https://www.hyperledger.org/projects

Hyperledger - different Business Blockchain Frameworks (Graduated)



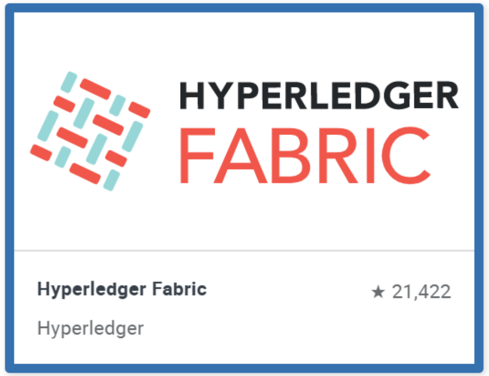
Hyperledger Aries ★ 1,620

Hyperledger



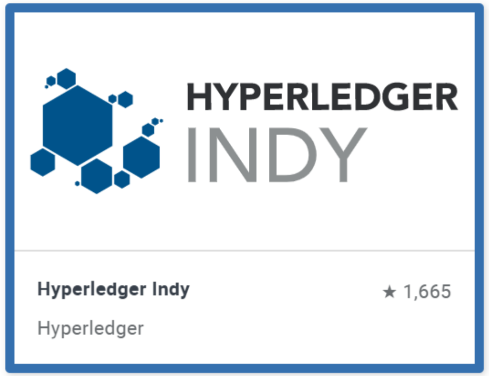
Hyperledger Besu ★ 1,072

Hyperledger



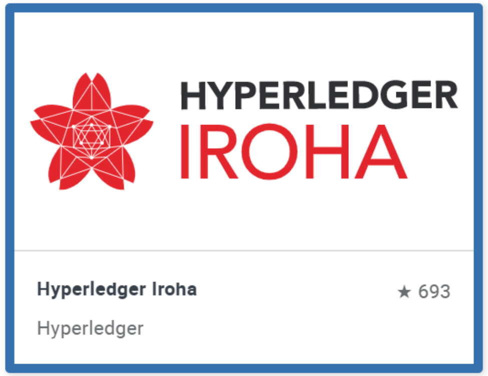
Hyperledger Fabric ★ 21,422

Hyperledger



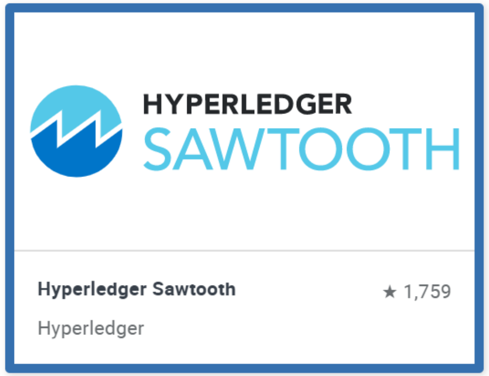
Hyperledger Indy ★ 1,665

Hyperledger



Hyperledger Iroha ★ 693

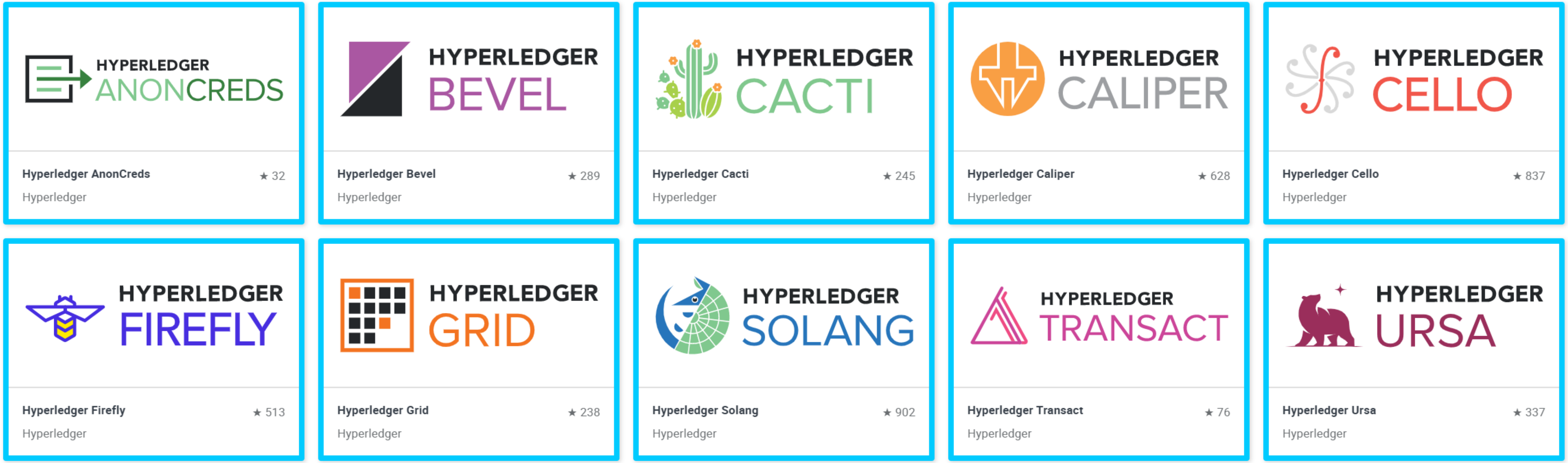
Hyperledger



Hyperledger Sawtooth ★ 1,759

Hyperledger

HYPERLEDGER – INCUBATED PROJECTS



Hyperledger AnonCreds ★ 32
Hyperledger

Hyperledger Bevel ★ 289
Hyperledger

Hyperledger Cacti ★ 245
Hyperledger

Hyperledger Caliper ★ 628
Hyperledger

Hyperledger Cello ★ 837
Hyperledger

Hyperledger Firefly ★ 513
Hyperledger

Hyperledger Grid ★ 238
Hyperledger

Hyperledger Solang ★ 902
Hyperledger

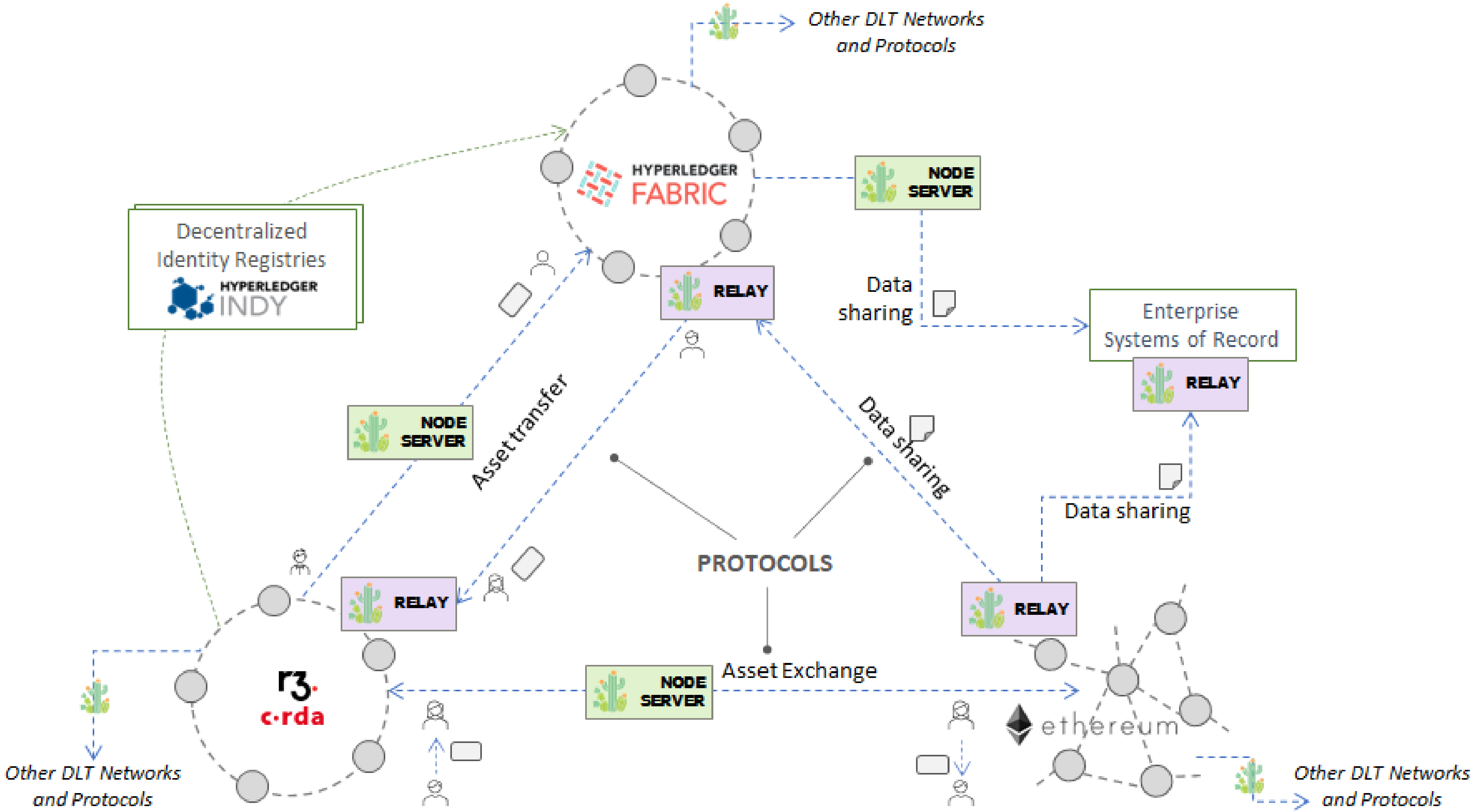
Hyperledger Transact ★ 76
Hyperledger

Hyperledger Ursa ★ 337
Hyperledger

Latest announcements: Nov 2022 - **Hyperledger AnonCreds (**Anonymous Credentials**):** Open Source, Open Specification Privacy Preserving Verifiable Credentials

Hyperledger Cacti, - a pluggable interoperability framework to link networks built on heterogeneous distributed ledger and blockchain technologies and to run transactions spanning multiple networks

HYPERLEDGER CACTI



HYPERLEDGER FABRIC (designed by IBM)

- Platform to build large scale apps on permissioned blockchain networks
- (a go-to protocol for industries like financial services, supply chains, and the insurance industry)
- Implementation of Blockchain technology intended as a foundation for developing blockchain applications
- Permissioned, private (members)
- Chaincodes in Golang or Java
- No native cryptocurrency, can be implemented through chaincode
- Uses PKI, each actor {peers, orderers, client application, administrators} has an identity encapsulated in an X.509 digital certificate.
- **Fabric Certifying Authority – Fabric-CA** serves as a root CA
  - Not capable of issuing SSL certificates
  - A public/commercial root CA can be used instead
- 10,000 transactions per second using BFT consensus at transaction level

FABRIC COMPONENTS

- Validating Peers
  - Transaction Ledger
  - World State
- Pluggable Consensus
  - Practical Byzantine
  - Fault Tolerance
  - None
- Smart Contract
  - Go, Java
  - Key-Value storage
- Membership services
  - Credentials and certifications
  - Users and Peers

TYPES OF PEERS

- PEER
  - Commits transactions – maintains Ledger and World State

- ENDORSING PEER
  - Endorses and executes Chaincode

- ORDERING PEER
  - Includes transactions in blocks
  - Communicates with other peers

FABRIC ARCHITECTURE WORKFLOW (1/2)

1. **Propose:** Client app submits transaction proposal for smart contract to the Endorsing Peer E_0

2. **Execute:** Endorsing Peer executes the transaction and (optionally) „anchors it“ w.r.t the ledger version numbers
   - An „anchor“ contains all data read and written by the contract that is to be confirmed by other endorsers.

3. **Submit:** Client requests further endorsement from other Endorsers (E_1, E_2, …) as per the Endorsement Policy and (may) decide an anchor obtained from any endorsers

4. **Endorse:** Endorsing Peers sign the result and send the Endorsement to the Client

FABRIC ARCHITECTURE WORKFLOW (2/2)

5. **Order:** Client formats transaction and sends it to the Ordering-Service Nodes for inclusion in the ledger

6. **Deliver:** Ordering- Service delivers the next block in the ledger with the endorsed transaction

7. **Validate:** The Peers validate the block received from the Ordering Service and update the Ledger and the World State.

CASE STUDY – HOME DEPOT
HOME IMPROVEMENT RETAILER

2200 stores in USA – each stores have around 35000 products (and Home Depot offers around 1M products on-line)

In a supply chain, there’s a warehouse that vendors stock with product for the retailer (The Home Depot). That product will then ship to stores. Many blind spots lie on a supply chain. If a transaction dispute occurs along the chain, it could take months to pinpoint.

Goal is to resolve Vendor disputes as efficiently as possible for both Home Depot and its vendors.

By design, blockchain creates a permanent, unchangeable record of real-time data — so no one can alter or remove it. Role-based access means that vendors see only what they need to see. No other vendor is going to see another vendor’s information.

IBM Hyperlegder Fabric Blockchain technology provides the real-time visibility, and if a variance occurs at any stopping point on the supply chain, both The Home Depot and its vendors can address the issue right away - bridging the gaps in visibility and communication; and Optimize multiparty workflows around trusted data.

FABRIC: APPLICATION DOMAIN

- Developing enterprise grade transactions based applications
  - B2B contracts
    - Business contracts can be codified to allow two or more parties to automate contractual agreements in a trusted way.
  - Manufacturing Supply Chain Management
  - Cross Border Payments – ANZ, BNP Paribas, BNY Mellon and Wells Fargo
  - Seafood traceability – Intel and Hyperledger
  - Border and Immigration Control
  - **Kaleido Enables Swift's New CBDC Sandbox with Broad Industry Participation** (Nov 2022) - *hosts 18 central banks and commercial banks* - Digital currencies have the potential to quicken settlements across borders, add transparency to global markets, and reach unbanked populations

SECURITY PROBLEMS IN FABRIC (1/3)

- **Problem:** Installation of Malware – Remote Access Trojan (RAT)
  - Chaincode runs on Docker container
  - Chaincode has access to networking – can very easily download and install further software packages (including security tools) and can run for long periods of time
  - Installation of RAT will act as a base from which a threat actor could undertake a more comprehensive attack.
    - A threat actor could create a new ledger with associated malicious chaincode, and persuade others to participate
    - A threat actor could infiltrate an organization responsible for developing and maintaining the chaincode for an existing ledger, then publish an update

Source/further reading:
Graham Shaw, Nettitude

SECURITY PROBLEMS IN FABRIC (2/3)

- **Problem:** Log Injection

  - Unvalidated inputs are written verbatim to a log
  - Indirect threat to the business model
  - Can be used to fabricate log entries to mislead incident response efforts, or corrupt the log to prevent it from being processed by automated monitoring systems.

HYPERLEDGER SAWTOOTH

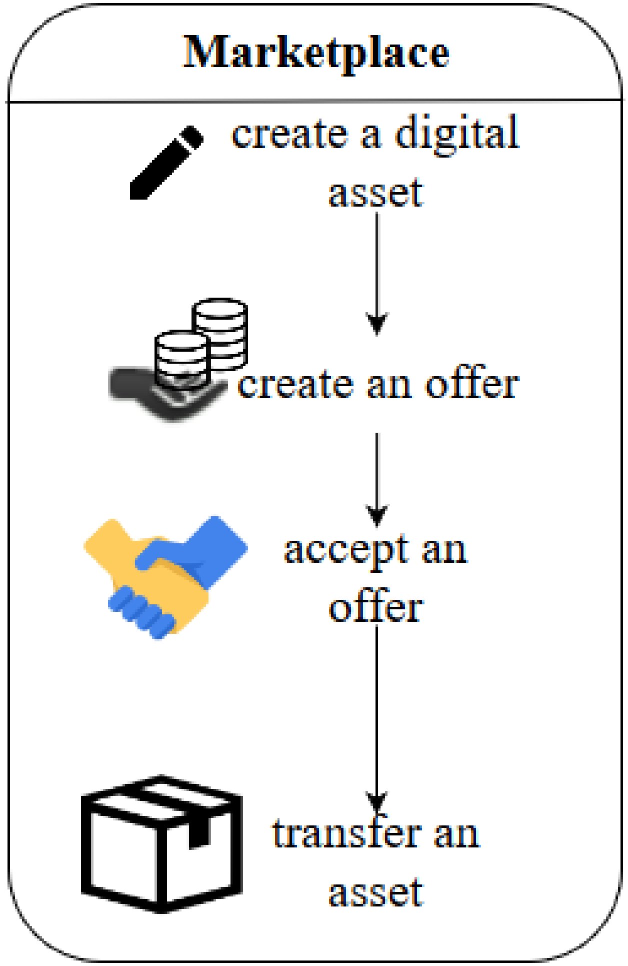
- **Distributed ledger software -** offers a flexible and modular architecture that separates the core system from the application domain, so smart contracts can specify the business rules for applications without needing to know the underlying design of the core system
- Modular Platform for implementing transaction-based updates to data between untrusted parties
  - **Transaction families:** Fix transaction semantics to limit risks

    ➡ e.g. integer key family: only 3 operations (increment, decrement, set) allowed. No looping constructs available

    hard to have intentional or accidental transaction script problems
  - supports a variety of consensus algorithms, including Practical Byzantine Fault Tolerance (PBFT) and Proof of Elapsed Time (PoET)
  - Currently, PoET‘s implementation relies on a Trusted Execution Environment (TEE) e.g. Intel‘s Software Guard Extensions (SGX) which introduces a need for trusted third party
  - SDK available for Python, Go, Javascript, Java and C++

SAWTOOTH: APPLICATION DOMAIN

- Applications for storing digital assets without central authority
  - Digital Asset Exchange – Marketplace
  - Bound Asset Settlement
- Supply Chain Traceability
- ScanTrust used Hyperledger Sawtooth to build a blockchain-enabled traceability function for their existing application
- Music Content Rights Registry



R3 CORDA

- Digital finance - Blockchain platform for the finanacial services industry
- Aims to offer universal interoperability of public networks with the privacy of private networks
- Permissioned (blockchain), private (data sharing)
- Pluggable consensus: ‚Notary Clusters‘ – at transaction level
    - A notary can either sign the transaction or reject and flag the transaction as a double-spent attempt.
- Smart Contracts in Kotlin, Java
    - Smart contract links business logic and business data to associated legal prose to ensure that financial agreements on the platform are rooted firmly in the law and can be enforced in case of ambiguity, uncertainty or dispute.