HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Understanding Hyperledger Fabric

Christopher Ferris, IBM CTO Open Technology

September 2019

Introducing Hyperledger

THE LINUX FOUNDATION PROJECTS

https://hyperledger.org/

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Hyperledger Momentum

3.5
Years since launch

126K+
Commits

9
Tools

6
Frameworks

3
1.0+ Production Releases

260+
Members
(50+ in AsiaPac)

11
Active Community
Working Groups &
Special Interest Groups

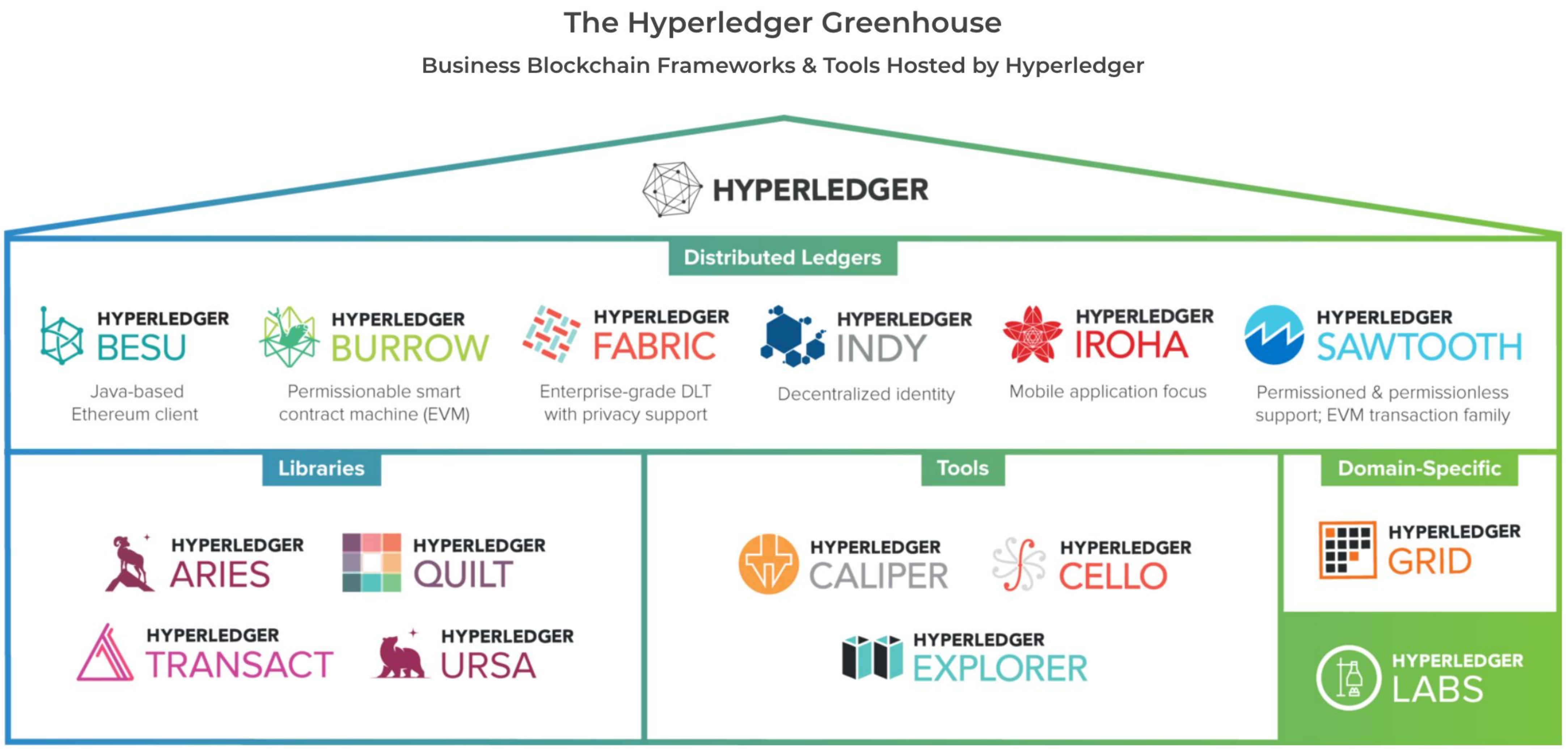
165+
Meetups
Worldwide
(66 countries)

56K+
Meetup
Participants

2,000+
Media Clips Per Month

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

The Hyperledger Greenhouse



The Hyperledger Greenhouse

Business Blockchain Frameworks & Tools Hosted by Hyperledger

Hyperledger Fabric Project News

- Maintaining a quarterly release cadence
- Hyperledger Fabric v1.4.3 released August 2019
- Hyperledger Fabric v2.0.0-alpha released for early access testing
- v1.4.x is our first long term support release

New Features:

- v1.4.1 support for Raft consensus orderer
- v1.4.2 support for Kafka to Raft migration
- v1.4.3 patch release
- v2.0.0-alpha
    - new chaincode lifecycle support
    - Alpine based images
    - StateDB caching

Characteristics

Characteristics

- Permissioned
- Highly modular
- Smart contracts in general purpose languages
- Pluggable consensus
- Privacy
- No “mining” or native crypto-currency required for consensus
- ***Execute-order-validate vs order-execute***

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Permissioned vs Permissionless

- Permissionless
  - Anyone can participate
  - Everyone is anonymous
  - No trust, must treat all entities as adversarial
- Permissioned
  - Participation is selective
  - Identity is known and often vetted
  - Operate under a shared governance model
  - Certain degree of trust can be established

Highly modular platform

- Pluggable *ordering service* establishes consensus
- Pluggable *membership service provider*
- Optional *peer-to-peer gossip service*
- Ledger can be configured to support a variety of DBMSs
    - LevelDB, CouchDB, BerkleyDB*, SAP Hana*
- Pluggable endorsement and validation policy enforcement

Smart Contracts

Highly Modular and Configurable

- Written in traditional programming languages
  - Golang, Java, Javascript, …
  - Implement a language specific shim
- Do not need to be deterministic

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Order-execute

Highly Modular and Configurable

- Most existing smart-contract capable blockchain platforms follow an “***order-execute***” architecture in which the consensus protocol:
  - validates and orders transactions then propagates them to all peer nodes,
  - each peer then executes the transactions sequentially
- Contracts must be deterministic
- Sequential execution limits performance & scale

Execute-order-validate

Highly Modular and Configurable

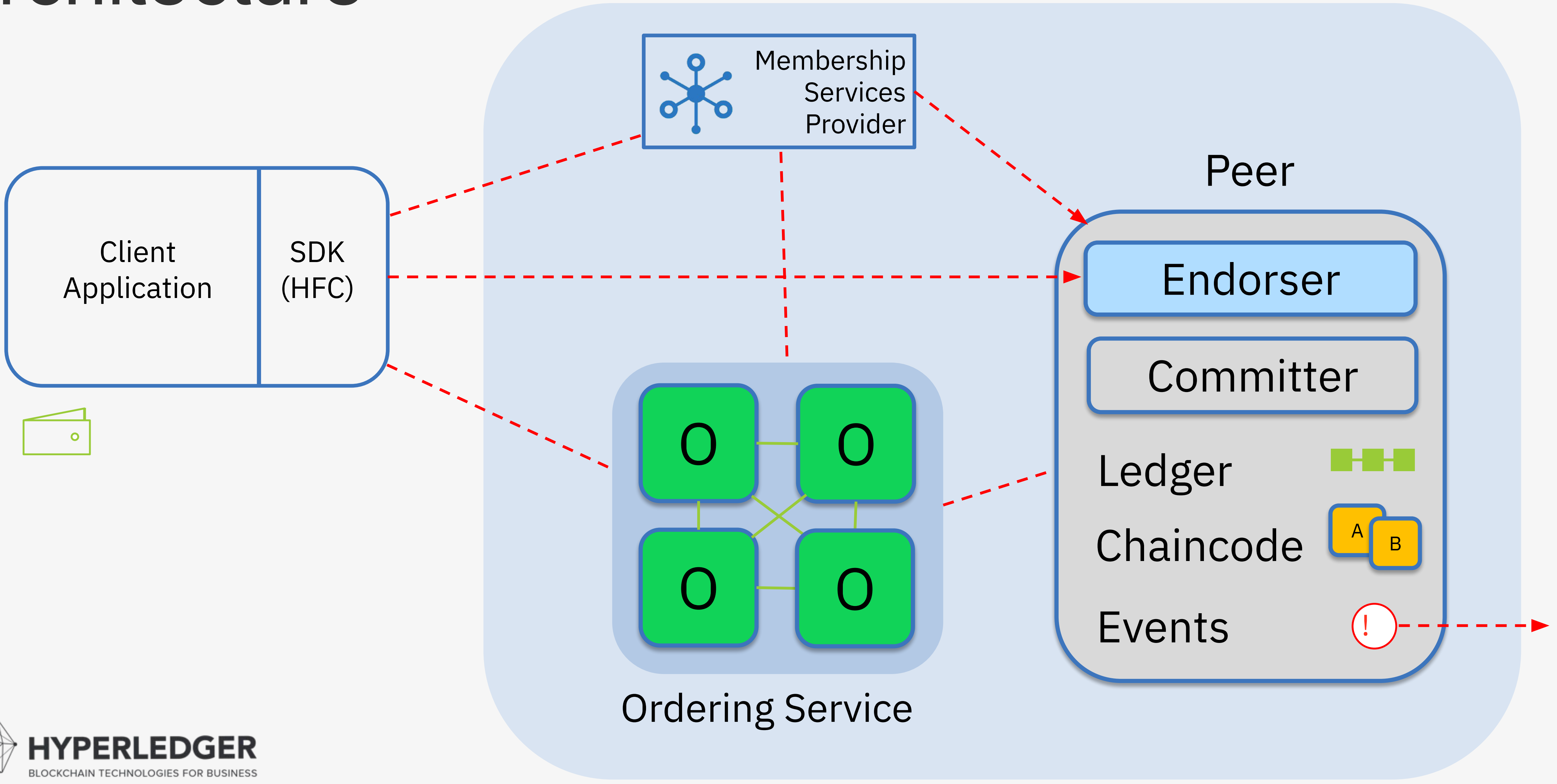
- Separates the transaction flow into three steps:
  - executing a transaction and checking its correctness, and endorsing it;
  - ordering transactions through a consensus protocol; and
  - transactions validated against an application-specific endorsement policy and committed to the ledger
- 1st step eliminates non-determinism
- Allows for parallel execution
- Allows for pluggable consensus

Privacy & Confidentiality

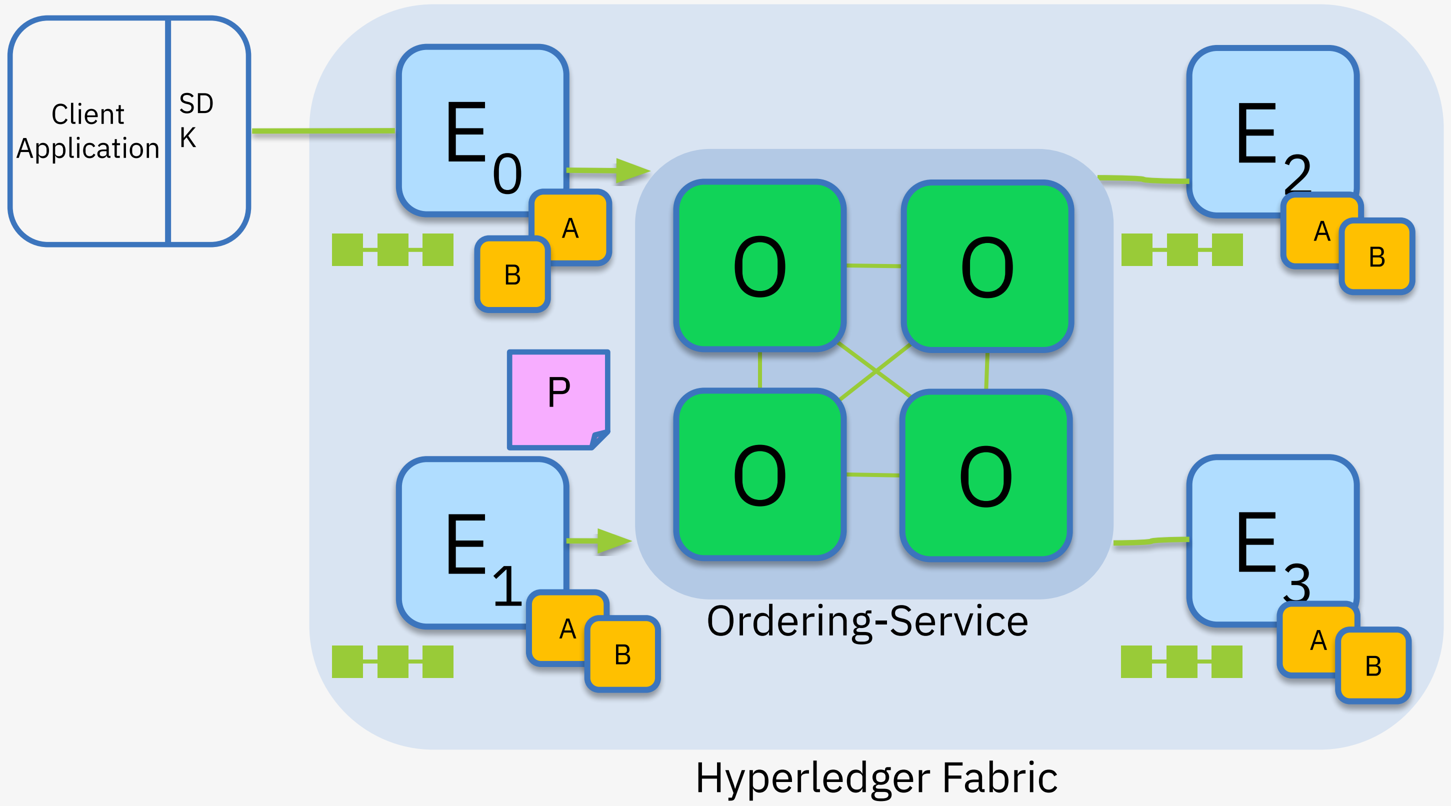
Highly Modular and Configurable

- Channel architecture
- Private data collections
- Zero knowledge proofs
  - Identity mixer
  - ZKAT - coming soon after token capabilities added

Architecture



Channels



- Similar to v0.6 PBFT model
- All peers connect to the same system channel (blue).
- All peers have the same chaincode and maintain the same ledger
- Endorsement by peers E_0, E_1, E_2 and E_3

Key:

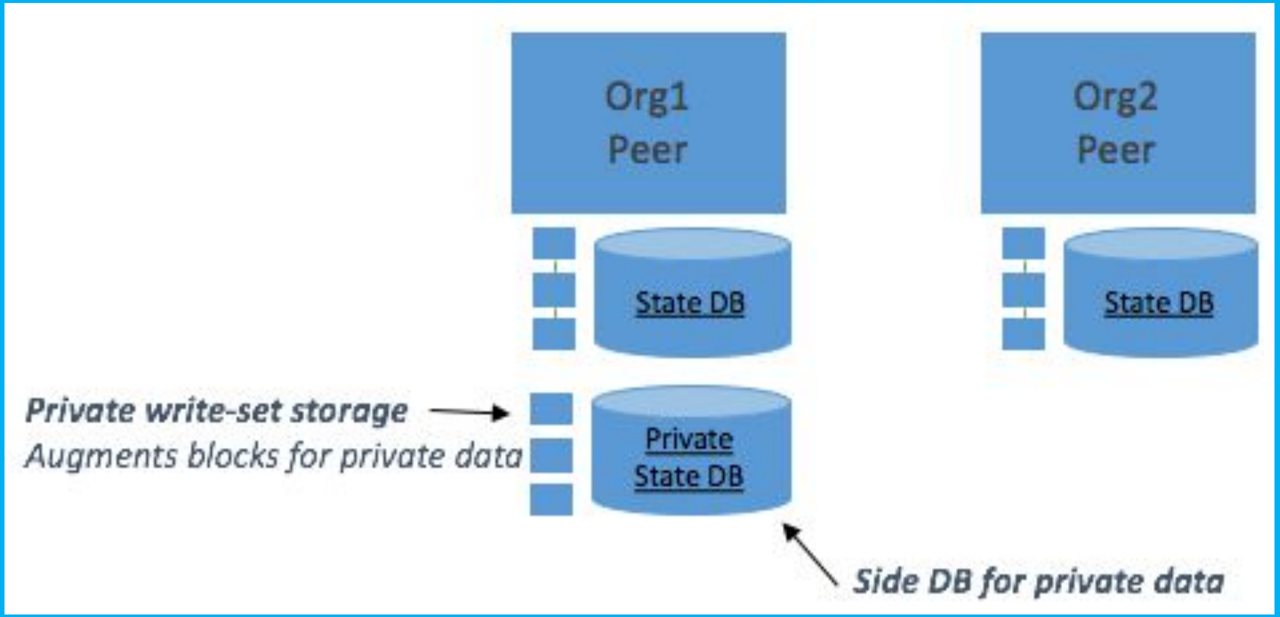
Endorser	🟦	🟩🟩🟩	Ledger
Committing Peer	⬜	⬜	Application
Ordering Node	🟩		
Smart Contract (Chaincode)	🟨	🟪	Endorsement Policy

Private Data Collections

Keep chaincode data confidential among a subset of channel members.

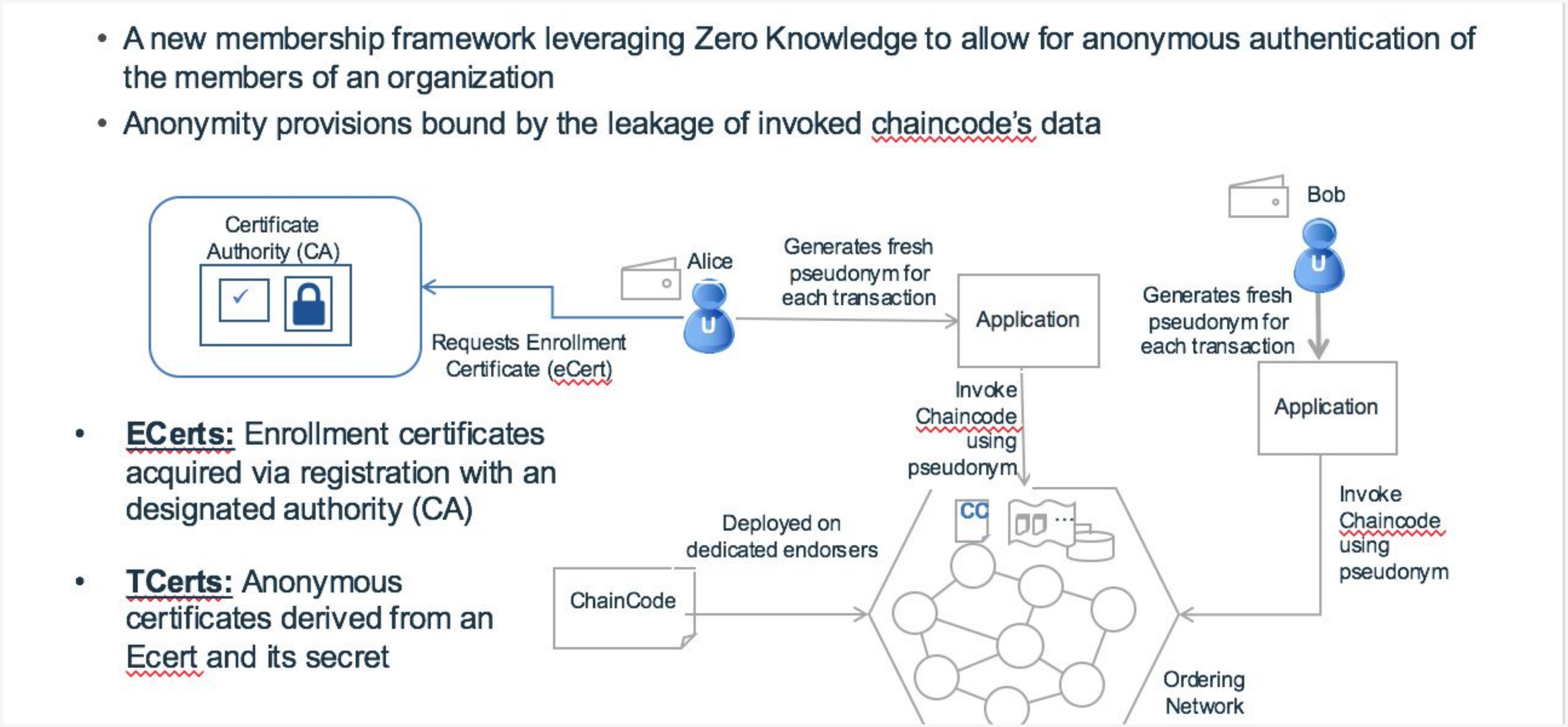
Store private data alongside the public ledger with hashes on the public ledger serving verifiable proof of the data.

- Private data grouped in ***collections*** *having* ***access policies***
- Private data of a collection stored solely to peers who satisfy the collection's access policy



For more details see charts at https://jira.hyperledger.org/browse/FAB-1151

Identity Mixer



- A new membership framework leveraging Zero Knowledge to allow for anonymous authentication of the members of an organization
- Anonymity provisions bound by the leakage of invoked chaincode's data

- **ECerts:** Enrollment certificates acquired via registration with an designated authority (CA)
- **TCerts:** Anonymous certificates derived from an Ecert and its secret

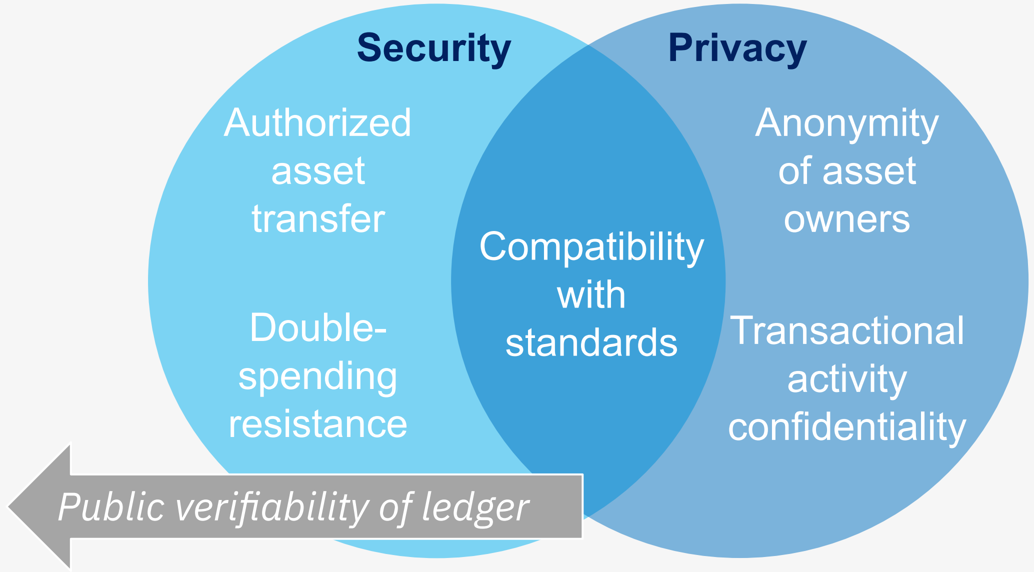
Certificate Authority (CA)
Requests Enrollment Certificate (eCert)
Alice
U
Generates fresh pseudonym for each transaction
Application
Invoke Chaincode using pseudonym
Bob
U
Generates fresh pseudonym for each transaction
Application
Invoke Chaincode using pseudonym
Deployed on dedicated endorsers
ChainCode
CC
Ordering Network

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

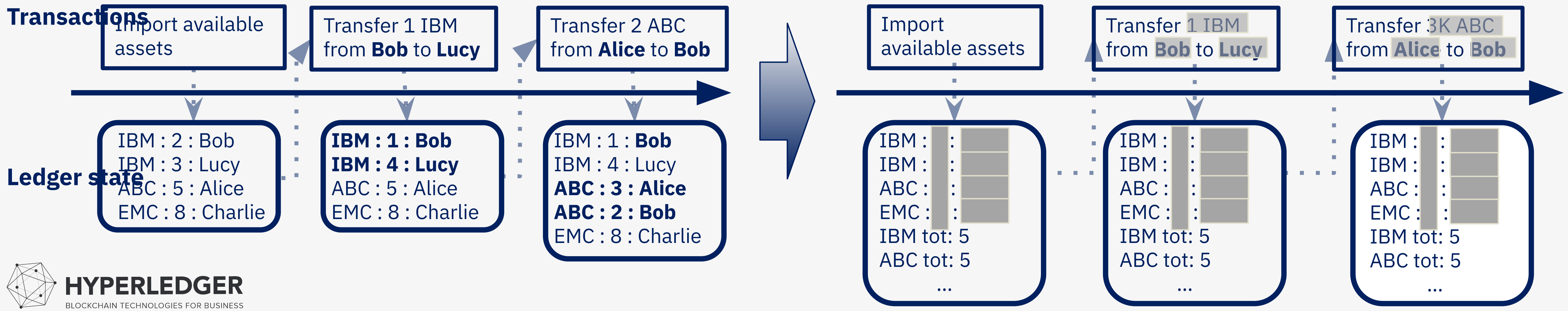
Privacy Preserving Asset Mgt

Relevant in multiple use-cases
- Financial asset transfer
- Securities trading
- Virtual payments

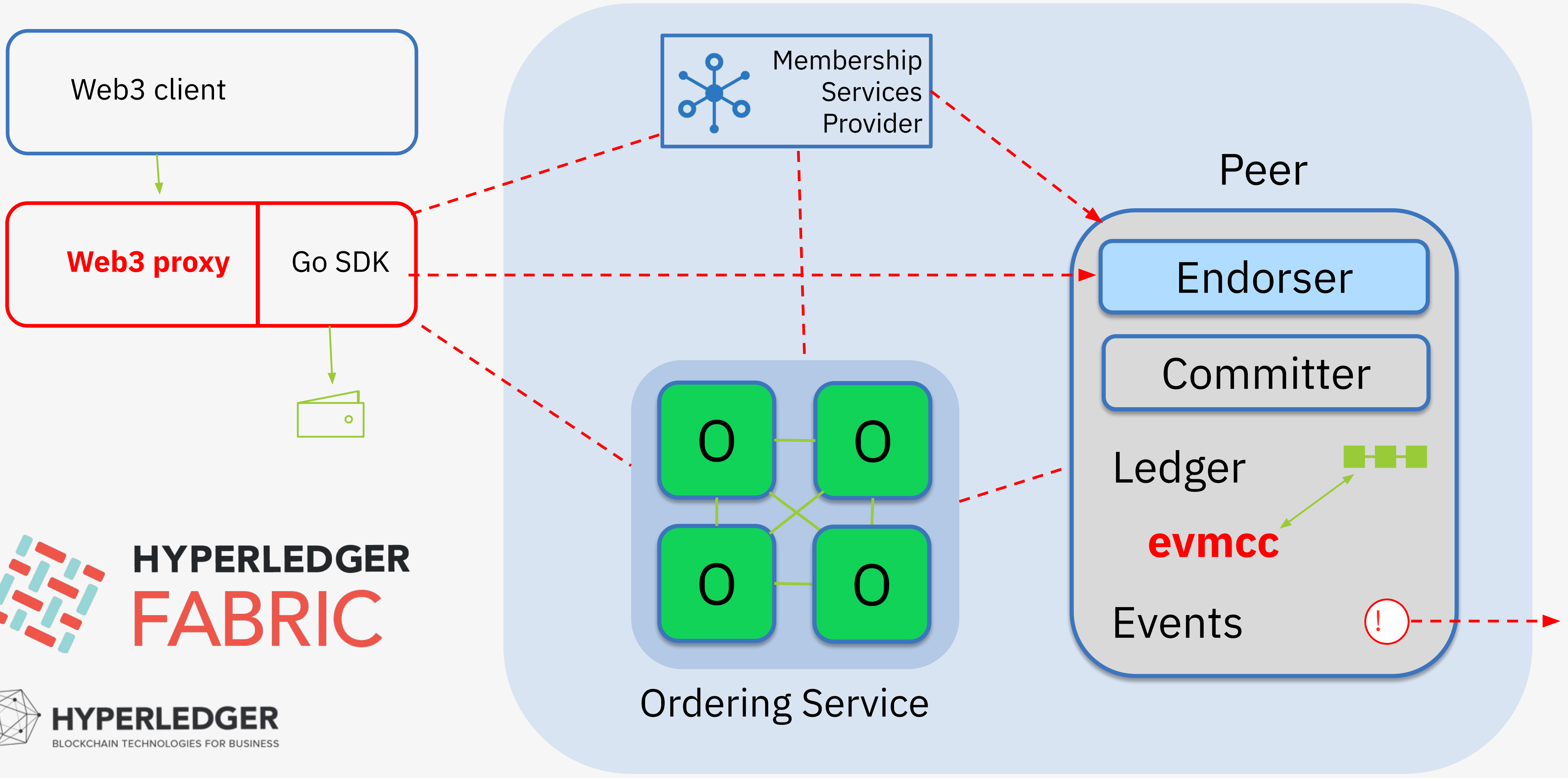
Value: Extend automation, trusted record keeping without the need for trusted mediators


Security
Privacy
Authorized asset transfer
Double-spending resistance
Compatibility with standards
Anonymity of asset owners
Transactional activity confidentiality
Public verifiability of ledger

Shareholder example:



Hyperledger Burrow EVM Integration



HYPERLEDGER FABRIC

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Paving the way for a more powerful Fabric

Concepts we are working to pull into Fabric on an experimental basis

- Pushing transaction functions down into Fabric to provide a “proper” smart contract authoring experience
- Improving the usability of client SDKs
- Modelling of data stored on the ledger and in the world state
- Generation of domain specific RESTful APIs
- Generation of domain and programming language specific SDKs (JavaScript, Java, Go, etc.)
- Skeleton smart contract generation

v2.0 Roadmap (proposed)

Enable further **operational** and **token capabilities**

- RAFT Consensus
- Chaincode Lifecycle
- Local Collections
- Programming model additions
- Sample improvements (advanced commercial paper)
- Alpine images

https://jira.hyperledger.org/secure/Dashboard.jspa?selectPageId=10104

Get Started!

https://wiki.hyperledger.org/projects/fabric

Contribute – become one of the nearly 300 developers working on this critical technology

Consume – leverage the most mature of the emerging enterprise blockchain platforms

HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Thank you!

@christo4ferris

@cbf on rocketchat