University of California, Davis
Webinar, 29 October 2020

# Why Only Permissioned Blockchains Matter: A Realist's Perspective


## C. Mohan

**Distinguished Visiting Professor** (Tsinghua University, Beijing, China)
**Honorary Advisor** (TNeGA, Chennai, India) & **Advisor** (Kerala Blockchain Academy, India)
**Retired IBM Fellow & Former IBM India Chief Scientist**

http://bit.ly/CMbiod

Twitter, WeChat: seemohan


**Links to Videos, Slides, Papers @ http://bit.ly/CMbcDB**

**This Talk's Slides http://bit.ly/UCDmoT**

Keynote at ACM SIGMOD International Conference on Management of Data
Amsterdam, The Netherlands, 3 July 2019

# State of Public and Private Blockchains: Myths and Reality

## C. Mohan

**IBM Fellow**
**IBM Almaden Research Center, San Jose, USA**

**Distinguished Visiting Professor**
**Tsinghua University, Beijing, China**

**Paper**: http://bit.ly/sigBcP **Video**: http://bit.ly/BCamsK **Slides**: http://bit.ly/AMSsBC

**Links to Videos, Slides, Bibliography @ http://bit.ly/CMbcDB**

# Agenda

**Goal:** Introduce basics of blockchains (BCs), bust some myths and discuss **practically useful** permissioned/private BCs, with details of some permissioned BC systems

- Origin of Blockchains (**BC**s) & Blockchain-as-a-Service (**BaaS**)
- Related Distributed Systems/Databases Topics
- Evolution: Smart Contracts, Permissioned BCs, …
- Consortia Approach to Development of Systems & Market Scene
- Applications: Production Deployments, PoCs, …
- Benchmarks and Standards
- Architectural Choices and Relationship to DBMS Replication & Logging
- Technical Details of Representative Systems:
  Hyperledger Fabric, Quorum (Enterprise Ethereum), R3 Corda,
  Hyperledger Sawtooth, AntChain, SAP, Ripple, Libra
- Futuristic Topics

Check out my ACM SIGMOD 2019 **Keynote** paper: http://bit.ly/sigBcP

# Blockchain (BC)

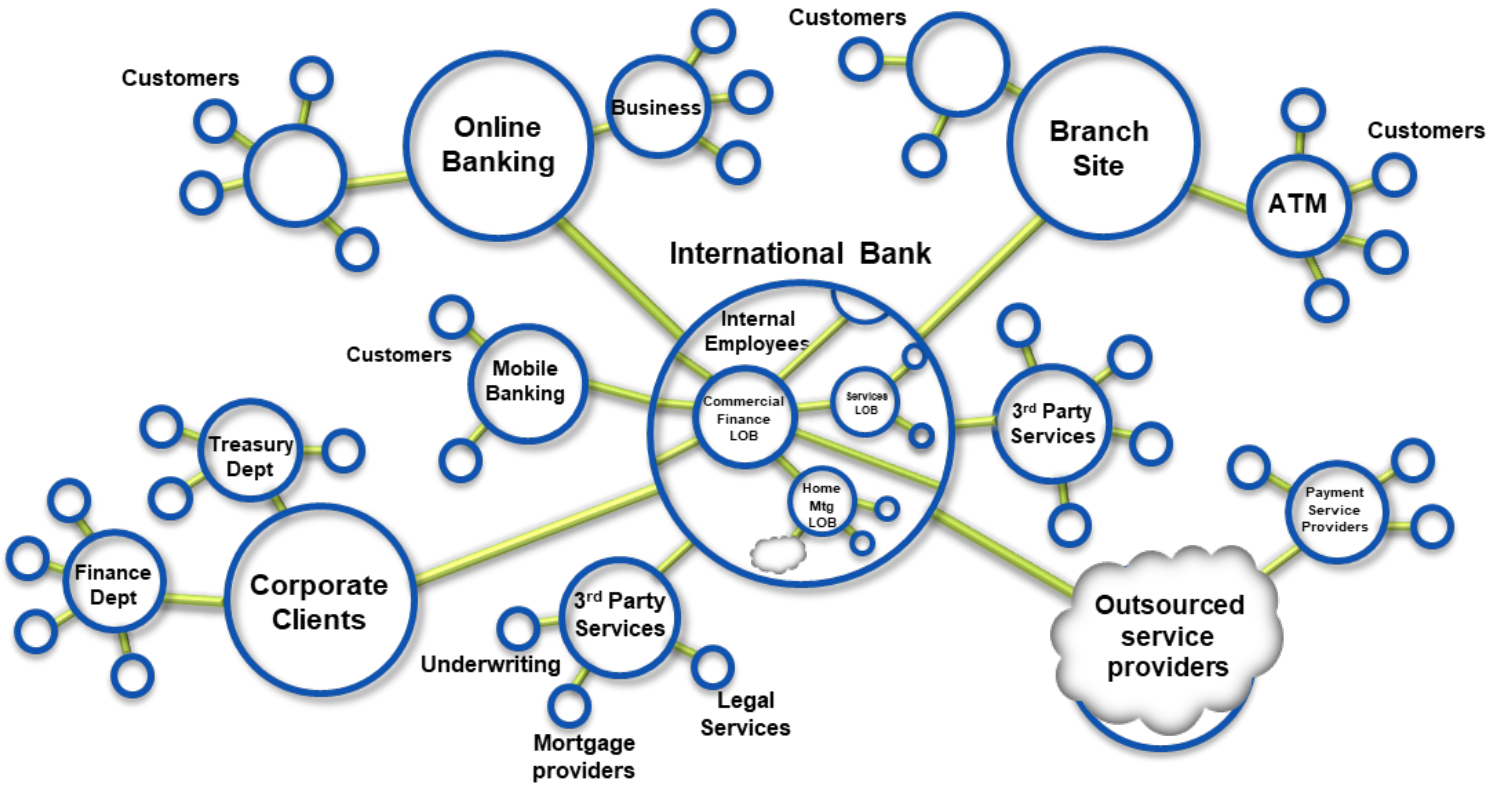
- Origin in cryptocurrencies (Bitcoin - *Satoshi Nakamoto*, 2008)
  (Pseudo) Anonymity, **permissionless/public/open** environment
  Energy wastage via "mining" with associated "reward", awful performance
  (7 TPS, 10 minutes response time)
  Widely-varying transaction fees & enablement of illegal activities
- Numerous organizations across the world working on various aspects of it:
  security, consensus, database, benchmarks, verification, standards, …
- **My focus**: **Permissioned/Private** BC Systems!

  Leverages underlying blockchain data structure of Bitcoin while providing
  - Much better performance/scalability
  - Controlled information sharing among organizations & users
  - Deterministic behavior – no forking, linear blockchain
  - Avoids greedy behavior by not having "rewards" and transaction "fees" (non-Ethereum ones)
  - Byzantine behavior issues significantly reduced

# Permissioned/Private Blockchain

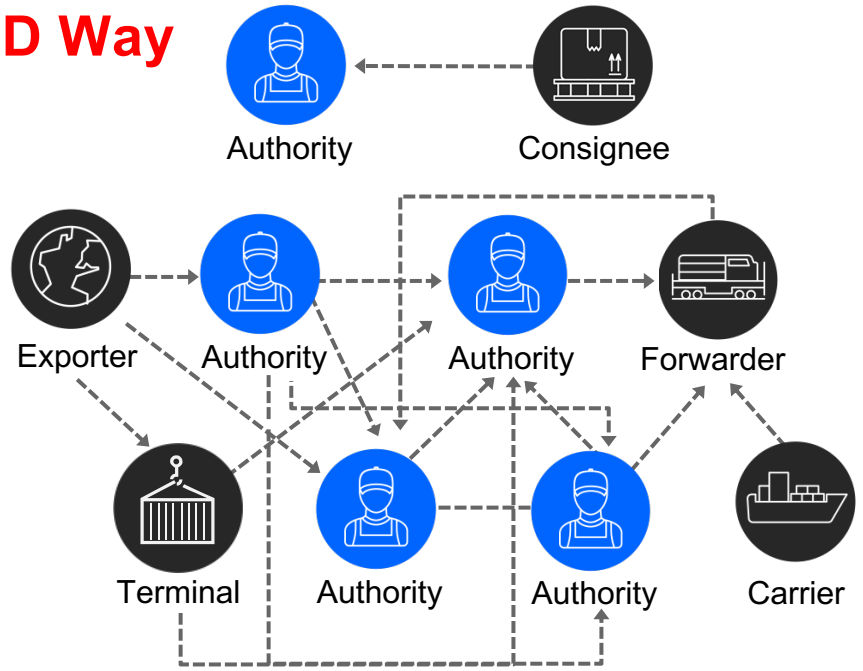
– Blockchain builds on basic business concepts
- Business Networks connect businesses and **people**
- Participants with Identity
- Assets flow over business networks
- Transactions describe exchange or change of states of assets
- Smart Contracts underpin transactions
- Ledger is a log of transactions

– Blockchain is a shared, replicated, permissioned ledger
- Consensus, provenance, immutability, finality



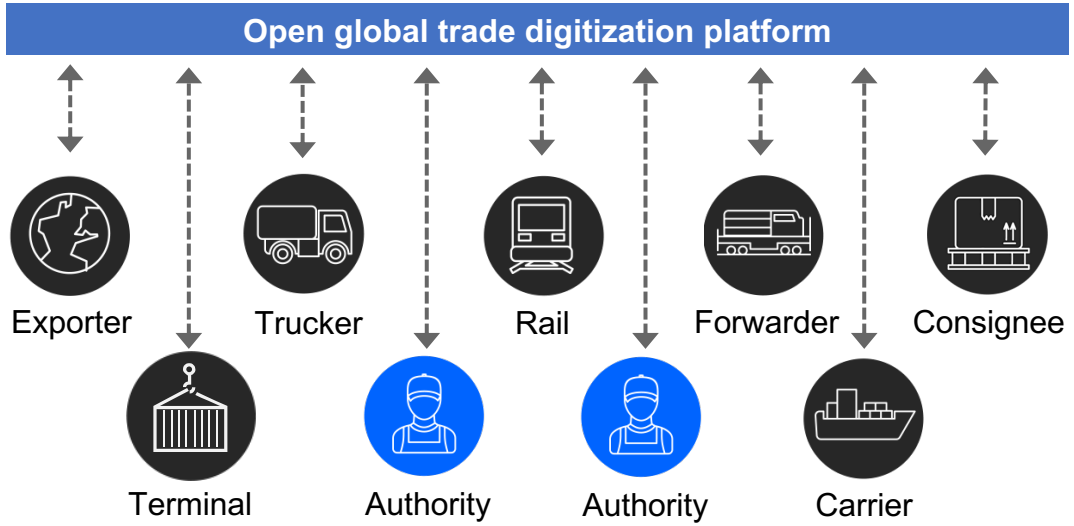
# The Case for a Better Way (Import/Export Use Case)

## OLD Way




- Inconsistent information across organizational boundaries and “blind spots” throughout the supply chain hinder the efficient flow of goods
- Complex, cumbersome, and costly peer-to-peer messaging
- Manual, time-consuming, paper-based processes
- Risk assessments often lack sufficient information; clearance processes subject to fraud
- The administrative cost of handling a container shipment is comparable to the cost of the actual physical transport
- No single source of truth

## Blockchain Way




- Instant, secure access to end-to-end supply chain information; single source of the truth
- Assurance of the authenticity and immutability of digital documents
- Trusted cross-organizational workflows
- Better risk assessments and fewer unnecessary interventions
- Far lower administrative expenses and elimination of costs to move physical paper across international borders

# State of the Blockchain World

- Way too much hype associated with permissionless blockchains –
  "cottage industry" of startups & research papers ("religious" fervor among believers!)
- Non-uniform treatment of cryptocurrencies across countries (e.g., DCEP in China)
- If you believe in gambling/esoterica, you might wish to get into them
- Permissioned systems are like RDBMSs were 35+ years ago: few systems released but users are on their own to figure out how to use them effectively, compare systems, …
- Many interesting issues remain to be solved and new tools to be built
- Standards, benchmarks and interoperability work in progress
- Not just lack of standard APIs but also **different underlying conceptual models in systems**
- Incredible momentum behind Hyperledger Fabric-based BaaS offerings
- Rapid progress in short time - many production deployments of practical use cases
- DBMSs being enhanced to provide blockchain-like features and/or old DB ideas rehashed
- Chinese SW giants very active

# European Union Blockchain Observatory & Forum

- Created as a European Parliament pilot project – 1st Term 2/2018 - 5/2020
- Thematic reports at https://www.eublockchainforum.eu/reports
  - Governance of and with blockchains
  - Blockchain and cyber security
  - Blockchain use cases in healthcare
  - Convergence of Blockchain, AI and IoT
  - Blockchain and the future of digital assets
  - Blockchain in trade finance and supply chain
  - Legal regulatory framework of blockchains and smart contracts
  - Blockchain and digital identity
  - Scalability, interoperability and sustainability of blockchains
  - Blockchain for government and public services
  - Blockchain and the GDPR
  - Blockchain innovation in Europe
  - EU Blockchain Observatory & Forum 2018-2020 Conclusions and Reflections
- Workshop reports & videos: Research priorities, social impact, financial services, healthcare, …

# Other European Union Efforts

- European Blockchain Partnership - created in April 2018
  - Joins at a political level all EU Member States and members of the European Economic Area (Norway and Liechtenstein)
  - Signatories of this declaration will work together towards realizing the potential of blockchain-based services for the benefit of citizens, society and economy
  - Building a European Blockchain Services Infrastructure (EBSI) for delivering EU-wide cross-border public services using blockchain technology
  - Call for tenders for pre-commercial procurement for EBSI to be out by 9/2020
- International Association of Trusted Blockchain Applications (INATBA)
  - Public-private multi-stakeholder organization launched in April 2019
  - Brings together suppliers and users of DLT, representatives of governmental organizations and worldwide standards bodies
  - To promote transparent governance, interoperability, legal certainty and trust in services enabled by blockchain and DLT

# Rapid Progress in Permissioned Blockchains

Banks, regulators, universities, startups, big tech companies, services companies, governments, …

**mostly as part of consortia** (Hyperledger, EEA, R3, FISCO, …)

- 2/2017: 1st **production** deployment of BC system by IBM & Northern Trust for managing private equity – **Fabric 0.6**
- 4/2017: **Tencent** announced **TrustSQL**
- 7/2017: **Hyperledger Fabric 1.0 r**eleased (aka **Production Ready**)
- 8/2007: **Hyperledger Fabric** on IBM Cloud – **BaaS offering** IBM Blockchain Platform on highly secure Linux on mainframes
- 1/2018: **Baidu** announced BaaS offering
- 3/2018: Hyperledger **Caliper** Benchmarking Project initiated
- 4/2018: **Huawei:** Blockchain Cloud Service for China & **AWS:** Blockchain Templates (Fabric/Ethereum)
- 5/2018: **Enterprise Ethereum Client Spec** released by Enterprise Ethereum Alliance (**EEA**)
- 8/2018: **Oracle** released Oracle Blockchain Platform - **Fabric** based, with Berkeley DB & **SQL** support
- 9-10/2018: Financial Blockchain Shenzhen Consortium launched **FISCO** BCOS & **Alibaba** launched BaaS
- 12/2018: **Amazon** announced Quantum Ledger Database (**QLDB**) – available from 9/2019
- 6/2019: Facebook announced controversial Libra cryptocurrency & Libra Core implementation
- 9/2019: **Blockchain table** extension announced in Oracle Database 20c (still in preview)
- 10/2019: **Chinese President** Xi Jinping declares national focus on blockchain innovation
- 1/2020: **Fabric 2.0** released
- 4/2020: Open source smart contract language **DAML** SDK 1.0 released & **Ant Financial** launches OpenChain/AntChain
- 5/2020: Hyperledger **Cactus** starts as Greenhouse project for **blockchain integration**

# Blockchain-as-a-Service (BaaS) Products & Research Work

## Hyperledger Fabric (Incredible Momentum Behind It)

- **IBM** Blockchain Platform (IBP)
- **Oracle** Blockchain Platform
- **Baidu** Blockchain Engine (BBE)
- **Amazon** Managed Blockchain
- **Ant Financial** Cloud BaaS
- **Microsoft** Azure Blockchain Workbench
- **JD** Blockchain Open Platform
- **SAP** Cloud Platform Blockchain
- **Huawei** Blockchain Cloud Service (BCS)
- **Tencent** TBaaS

**Numerous Hyperledger Fabric-based University Research Projects Across the Globe**

# Worldwide Standardization Efforts

- Quite chaotic with numerous entities working on identical and/or overlapping topics
- Recent (17 June 2020) Event
  - "Joining Forces for Blockchain Standardisation" focused on Identity, Interoperability, Governance, Smart Contracts
  - Agenda https://ec.europa.eu/digital-single-market/en/news/joining-forces-blockchain-standardisation
  - Summary report: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68644

# Blockchain Myths (Past & Present)

- **Fiat** currencies are bad, cryptocurrencies are good
- **Bitcoin** will become the universal currency replacing all fiat currencies
- Permissionless blockchains provide trust in a **completely trustless** environment; governments are bad and (pseudo) **anonymity** is good!
- Permissionless blockchains are **completely decentralized**
- Permissioned blockchains are centralized or **centrally controlled**
- Anyone in a permissionless blockchain can **validate** any transaction
- Permissionless blockchains are **more secure** than permissioned blockchains
- **Off-chain** sensitive data storage is better than **on-chain** storage of such data
- **Creating "money"** with algorithms and energy wastage is better than well thought out and controlled printing of fiat currencies in a system with checks and balances (economists, real-world GDP based on goods/services)
- Worrying only about money transfers in Bitcoin networks is sufficient (i.e., without considering the full cycle of receiving goods/services satisfactorily for which payments are made)
- Initial Coin Offerings (**ICOs**) better than **IPOs** since they enable crowdsourcing of capital

# Negative News

Published by Josiah Wilmoth in Bitcoin Op-ed, Bitcoin Opinion, News

## Bitcoin is Erasing 300 Years of Monetary Evolution: Nobel Economist Paul Krugman

Cryptocurrency miners' demand for Nvidia computer chips evaporates, LA Times, 17 Aug 18

Nvidia Corp.'s nine-month crypto gold rush is over. .. Sales of graphics chips to miners of cryptocurrencies such as Ethereum dried up faster than expected, the Santa Clara company said.

The New York Times

## *After the Bitcoin Boom: Hard Lessons for Cryptocurrency Investors*

"After the latest round of big price drops, many cryptocurrencies have given back all of the enormous gains they experienced last winter. The value of all outstanding digital tokens has fallen by about $600 billion, or 75 percent, since the peak in January, according to data from the website coinmarketcap.com." NY Times, 20 Aug 18

The Man Who Solved Bitcoin's Most Notorious Heist, WSJ, 10 Aug 18

In the nine years or so since bitcoin made its debut, cryptocurrency worth more than $15 billion at peak prices has been stolen, much of it in hacks like those that precipitated Mt. Gox's collapse. That tally doesn't include thefts that haven't been publicized, or cryptocurrency used in other illegal activities, like buying stolen credit cards or paying hackers.

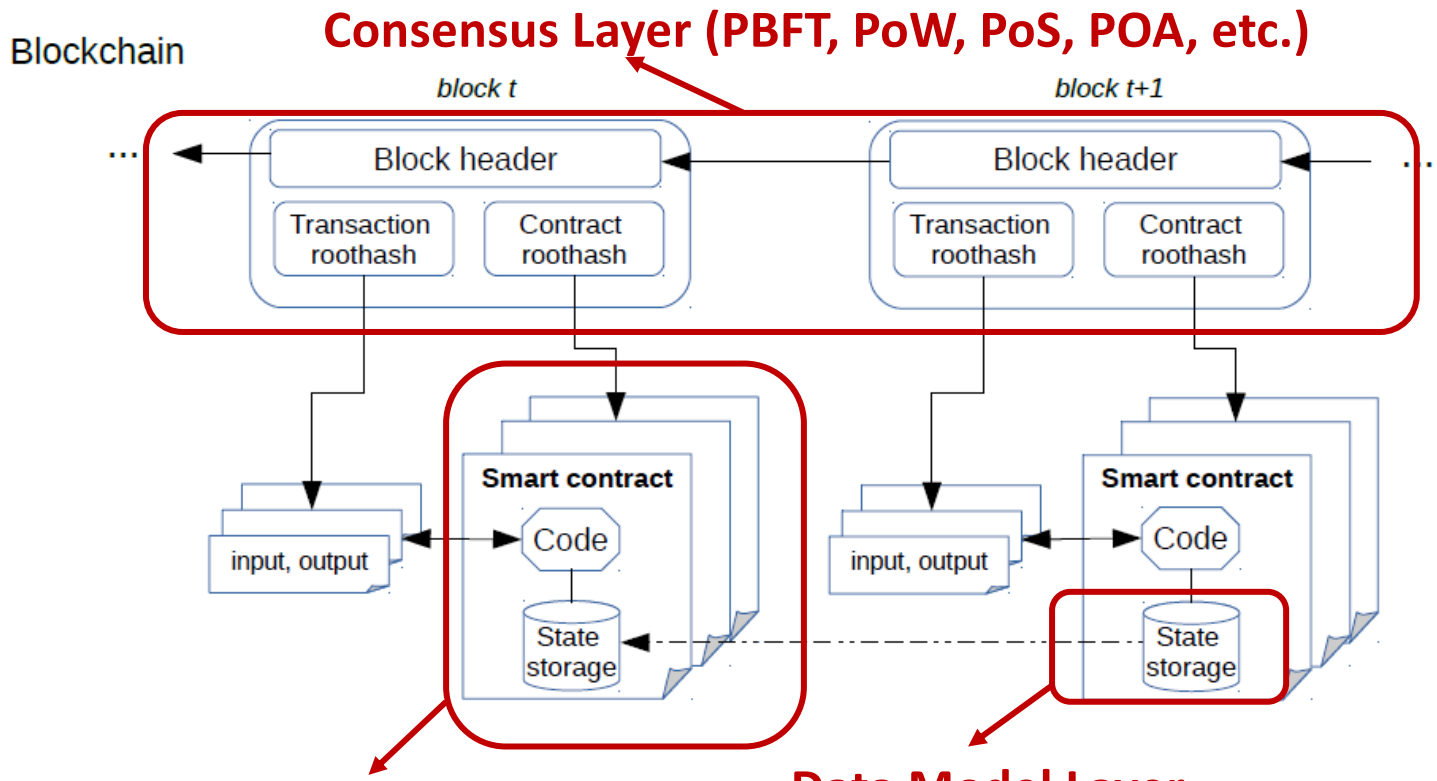
# Distributed Systems

- Distributed operating systems
- Distributed virtual memory
- Message passing in distributed computations and distributed checkpoints
- Clock synchronization and event ordering (e.g., Lamport clocks)
- Byzantine agreement and distributed consensus
- Two phase commit optimizations (e.g., Presumed Abort)
- (Transactional) RPCs and distributed file/object systems
- Asynchronous computation via message queues and pub-sub
- Distributed event-based systems
- Client-server, mobile computing and caching, WWW
- Workflow or business process management systems
- Service Oriented Architecture (SOA)
- Public cloud and hybrid cloud
- ...

# Data Systems

- Relational DBMSs (e.g., System R) and SQL
- Data consistency, degrees of isolation and fault tolerance
- Distributed databases (e.g., R*) and distributed transactions/queries
- Synchronous and asynchronous replication with primary copy
- Update anywhere (multi-master) replication and eventual consistency
- Stored procedures, user-defined types/functions, data provenance, …
- Data warehousing and parallel DBMSs – OLTP vs OLAP
- Shared Nothing Vs Shared Disks
- Object-oriented databases, XML, schema chaos, data integration, …
- Web2.0-inspired NoSQL, sharding & massive scaling (e.g., Spanner), JSON, …
- Big Data: Map-Reduce, Hadoop, Spark, …
- Data privacy, multitenancy and trans-border data flow restrictions
- Multi data centers and disaster recovery
- …

# BC Software Stack




Source: Anh Dinh, et al., SIGMOD 2017

# Blockchain Architecture/Feature Choices

- Cryptocurrencies Vs Generalized Assets
- Permissionless/Public Vs Permissioned/Private
- Byzantine Vs Non-Byzantine fault model
- Consensus approach: PoW, PoA, PoET, PBFT, …
- SQL Vs NoSQL data stores
- Transactional stores Vs Non-transactional stores
- Versioned/Unversioned state database
- On-Chain Vs Off-Chain data
- Parallelism exploitation during different phases of transaction execution
- Pluggable features: consensus protocol, state DB, smart contract language, …

**Good Survey Paper**: Untangling Blockchain: A Data Processing View of Blockchain Systems, A. Dinh et al.

# Blockchain versus DB Recovery Log

- Many similarities
  - Both are append only and hence ever growing
  - Contain transaction related information
- Many differences
  - Contents vary (reads also recorded in blockchain)
  - No use of hashing in recovery log (Byzantine faults not worried about)
  - Recovery log could be truncated after DB backups are taken
  - Multiple transactions' log records interspersed in recovery log

# Database Replication

- Primary log replay at replica – homogeneous systems with full DB replicas, typically done for disaster recovery (DR) backup
- Log capture generates DML statements from what is logged and apply executes those statements (e.g., IBM Q Replication)
  - Can handle non-determinism and partial replicas
  - Requires dependency analysis to leverage parallelism at apply time
  - https://www.ibm.com/developerworks/data/roadmaps/qrepl-roadmap.html
- Capture DML statements as issued by application and re-execute them at replica (e.g., H-Store/VoltDB)
  - Cannot handle non-determinism
  - Typically, serial execution of transactions

**Upfront (fairly random, unoptimized) ordering of transactions in blockchain systems – leads to all sorts of issues!**

# Architectural Differences

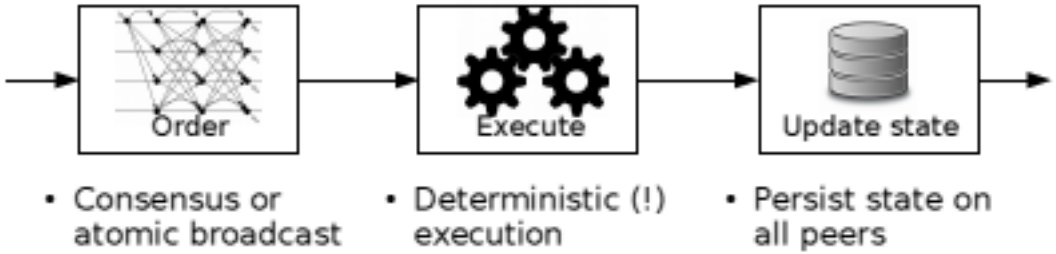



**Figure 1: Order-execute architecture in replicated services.**

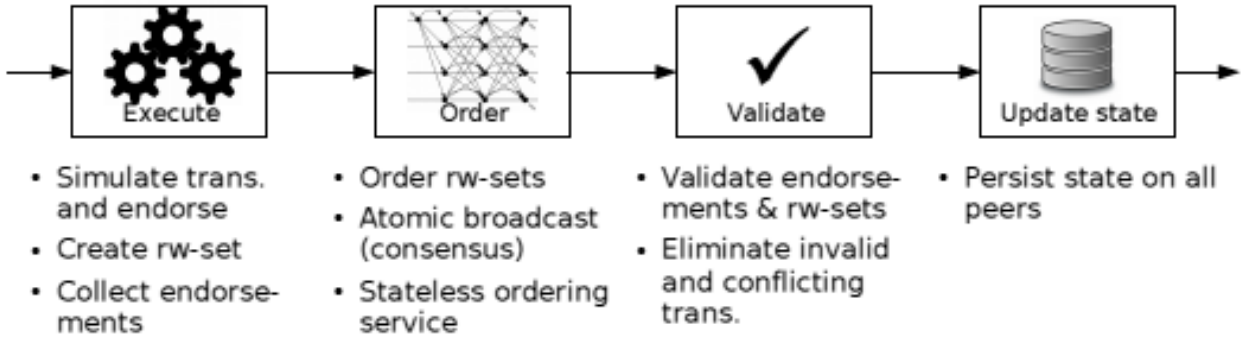
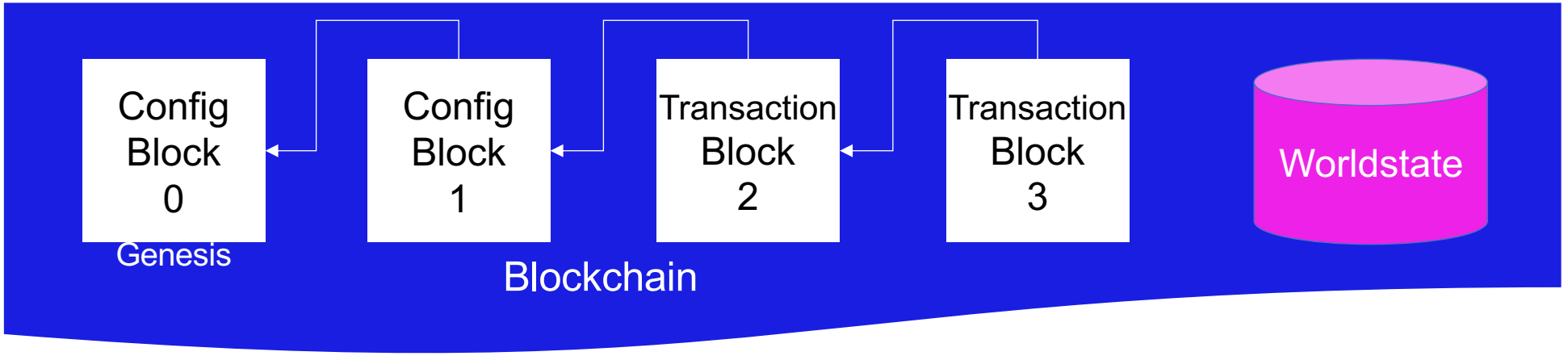



**Figure 2: Execute-order-validate architecture of Fabric (*rw-set* means a readset and writeset as explained in Sec. 3.2).**

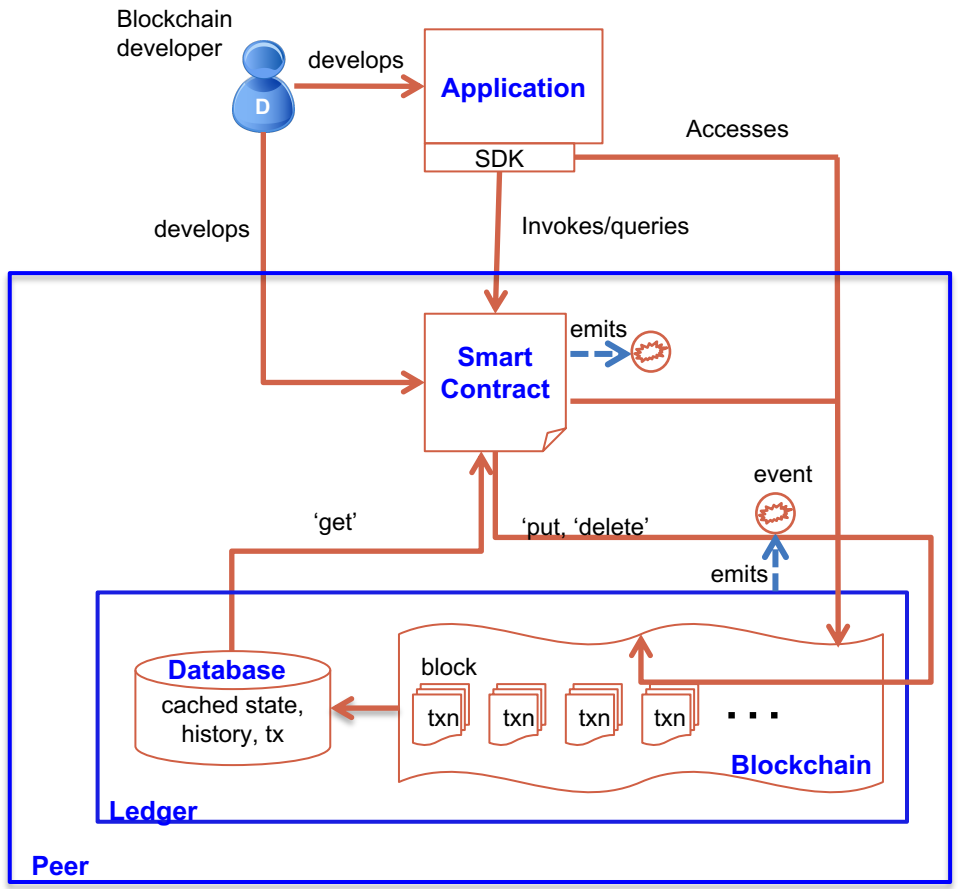
http://bit.ly/HFpapr

# Hyperledger Fabric Ledger

- The ledger is maintained by each peer (party) and includes the blockchain and worldstate
- A separate ledger is maintained for each channel the peer joins
- Transaction read/write sets are written to the blockchain
- Channel configurations are also written to the blockchain
- The worldstate can be either LevelDB (default) or CouchDB
  - LevelDB is a simple key/value store
  - CouchDB is a document store that allows complex queries
- The smart contact decides what is written to the worldstate



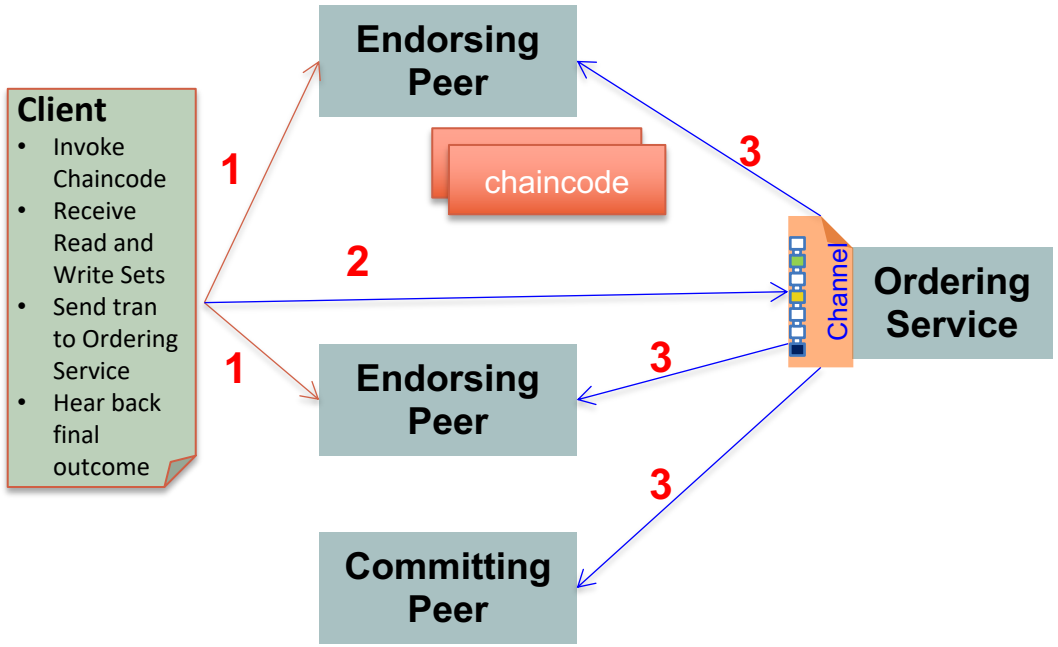
# Overview of Application Flow (Fabric)




- Developers create application and smart contracts (chaincodes)
  - Chaincodes are deployed on the network and control the state of the ledger
  - Application handles user interface and submits transactions to the network which call chaincodes
- Network emits events on block of transactions allowing applications to integrate with other systems

# Transaction Execution Overview Fabric V1

## Endorsement, Ordering, Validation/Commit




- Transaction is sent to the counter-parties represented by Endorsing Peers on their Channel
- Each Peer simulates transaction execution by calling specified Chaincode function(s) and signs result (Read-Write Sets)
- Each Peer may participate in multiple channels allowing concurrent execution
- Ordering Service accepts endorsed transactions and orders them according to the plug-in consensus algorithm then delivers them on the channel
- All (Committing) peers on channel receive transactions: on successful validation, commit to ledger. No chaincode execution.

Channel.SendTransactionProposal (Step 1) and channel.SendTransaction (Step 2)

# Transaction Flow Architecture Fabric V1

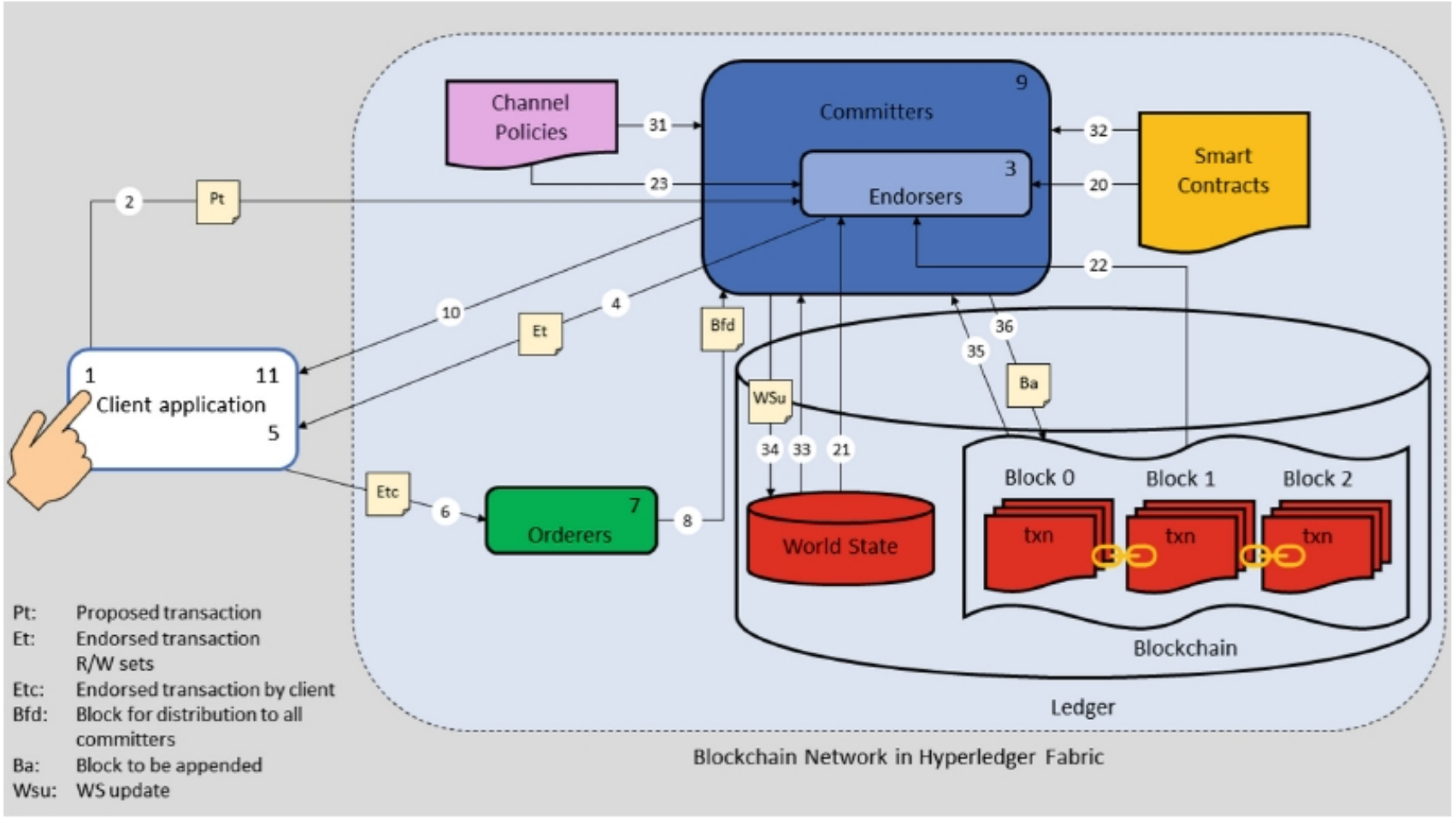



**Fig. 1.** Conceptual transaction flow architecture

Sjir Nijssen, Peter Bollen

# DBMS Implications

- Simulation concept requires layer between smart contract and State DB having to analyze DBMS calls
  - Update statements split into two: read part and write part
  - Read alone sent to DBMS with modifications to retrieve version #s for items read
  - Writes not sent to DBMS but processed and cached locally – doesn't allow for read your own write by chaincode transaction
- During Commit phase, read sets validated by retrieving each item's version # individually and then, if validation succeeds, writes also done one at a time
- Dealing with phantoms requires reexecution of query during commit phase to be sure simulation read set same as read set at Commit time
- Smart contract portability across different State DBMSs hard to do
- Lots of open questions and research issues in this area

# FastFabric (U of Waterloo)

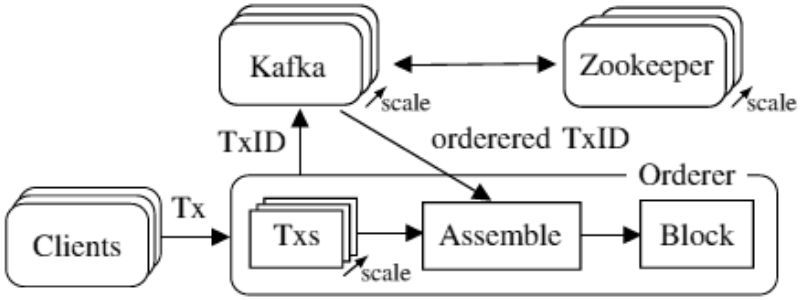



Fig. 1. New orderer architecture. Incoming transactions are processed concurrently. Their TransactionID is sent to the Kafka cluster for ordering. When receiving ordered TransactionIDs back, the orderer reassembles them with their payload and collects them into blocks.

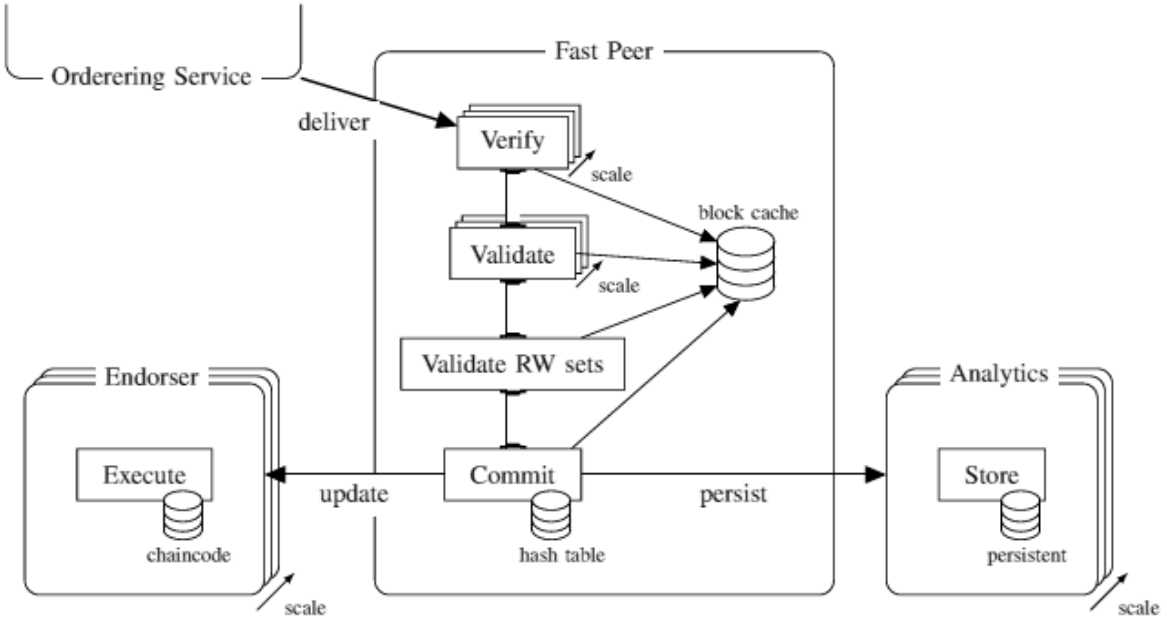
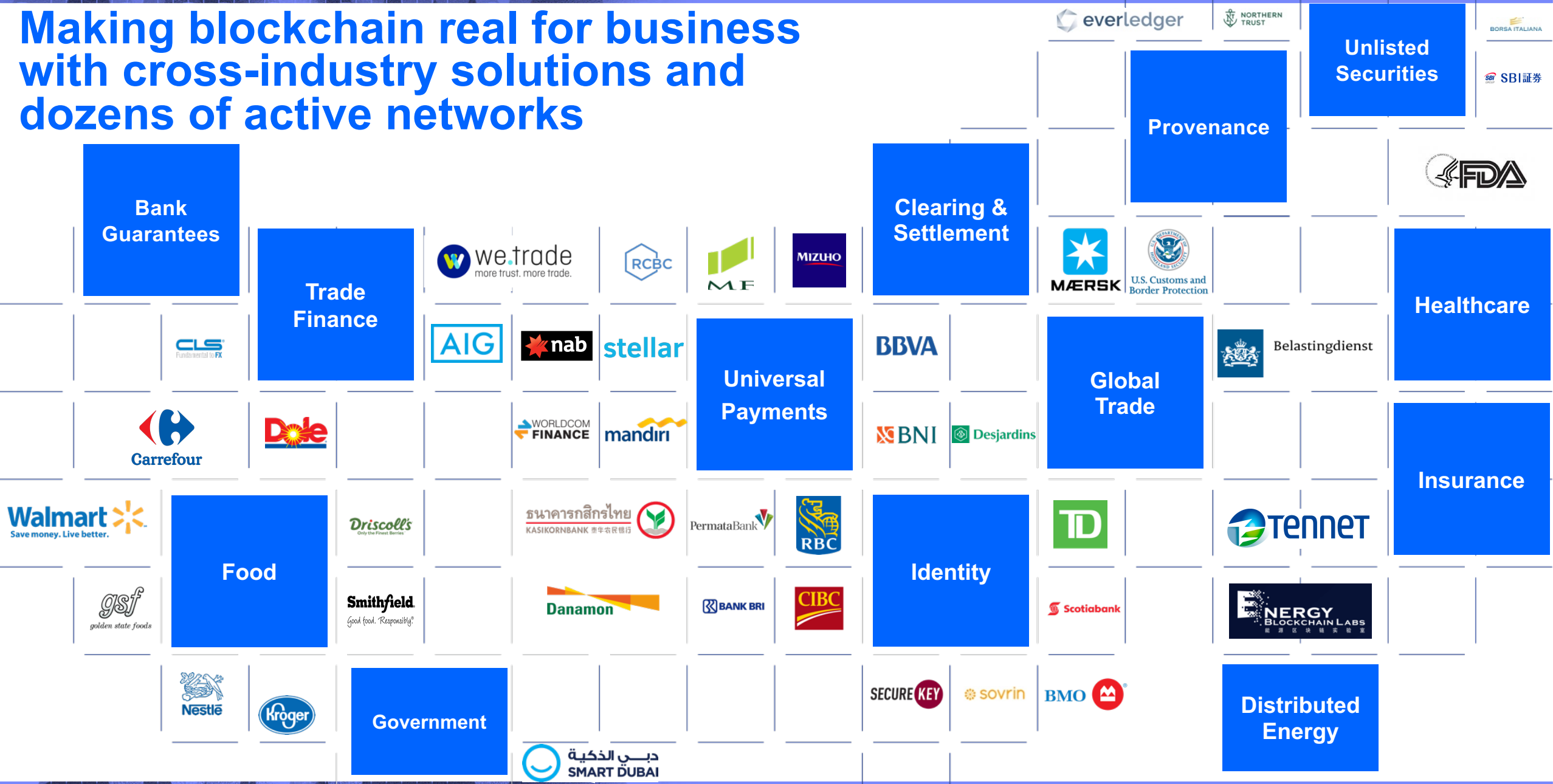



Fig. 2. New peer architecture. The fast peer uses an in-memory hash table to store the world state. The validation pipeline is completely concurrent, validating multiple blocks and their transactions in parallel. The endorser role and the persistent storage are separated into scalable clusters and given validated blocks by the fast peer. All parts of the pipeline make use of unmarshaled blocks in a cache.

Christian Gorenflo, Stephen Lee, Lukasz Golab, Srinivasan Keshav: **FastFabric: Scaling Hyperledger Fabric to 20 000 Transactions per Second.** International Journal of Network Management. Vol. 30, No. 5, September/October 2020. https://doi.org/10.1002/nem.2099

# Making blockchain real for business with cross-industry solutions and dozens of active networks

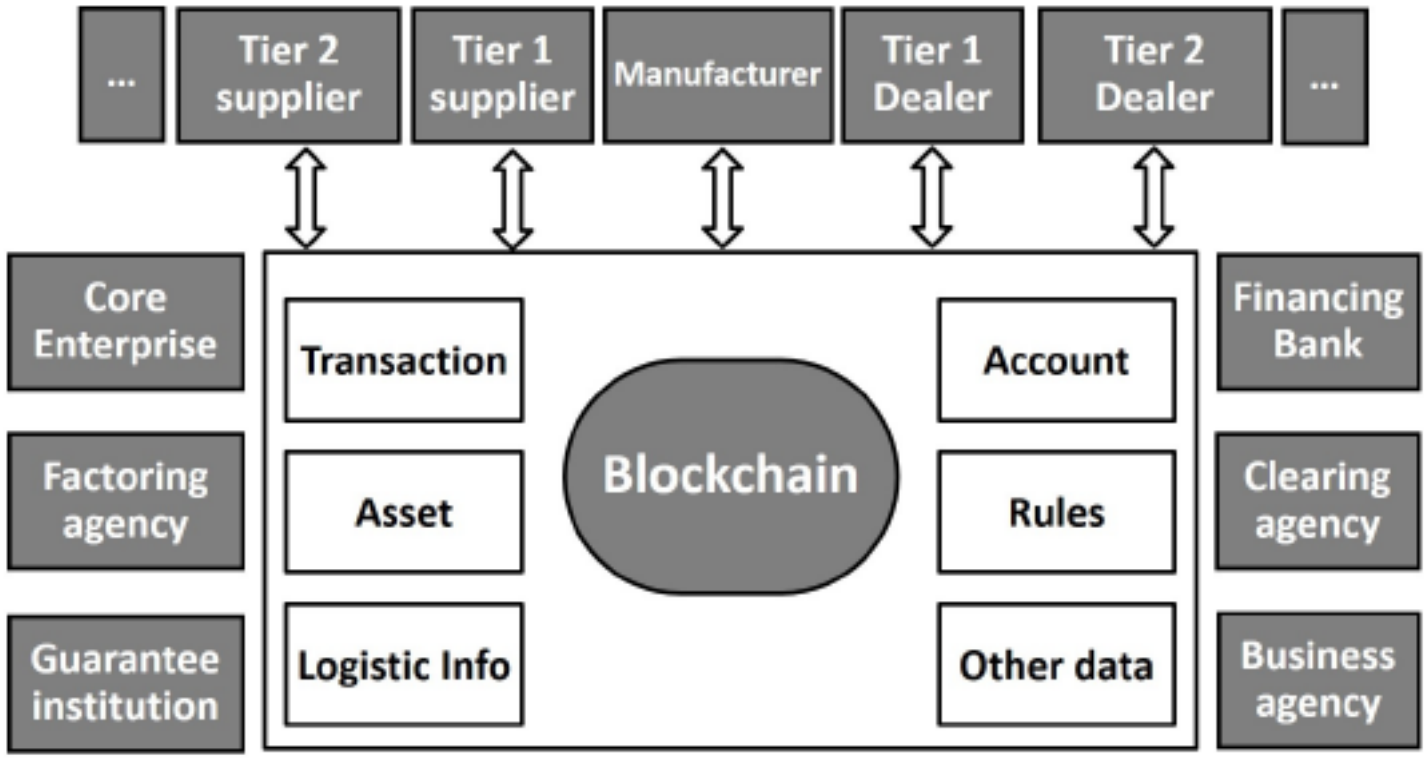


# Global Blockchain Industry Snapshot EqualOcean 3-2020

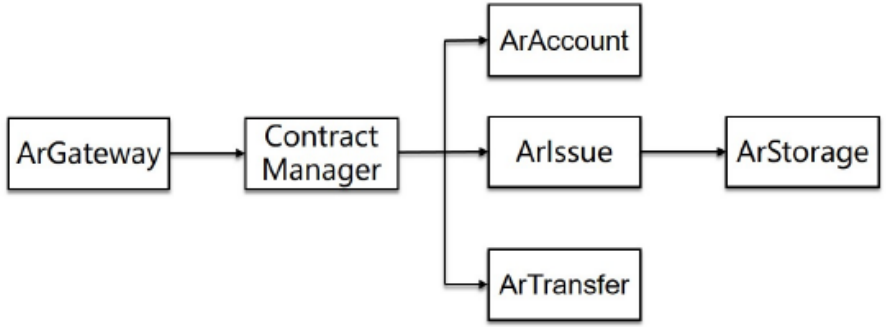
| | Category | Chinese companies | Companies from the rest of the world | |
|---|---|---|---|---|
| | BaaS | Ant Financial, Huawei, Tencent | Amazon, IBM, Microsoft, SAP | Enterprise services |
| | Data service | Chaindigg, CovenantSQL, Yunphant | CryptoMove, Factom | |
| | Security | Chains Guard, PeerSafe | Acronis, StrongSalt | |
| | Solutions | 33.cn, Consensus Datatrust | BlocWatch, Ionixx | |
| | Charity | China Everbright Bank, ICBC | BitGive, Citi | Industry applications |
| | Supply chain | Hyperchain, Wanxiang Blockchain | Blocko, DHL | |
| | Energy | Energy Blockchain Labs, YGSoft | Shell, Xage | |
| | Legal affairs & e-government | Fadada, Thunisoft | CrimsonLogic, Procvis | |
| | Finance | CITIC, Hundsun, PingAn, ZhongAn | B3i, Figure | |
| | Healthcare | Neusoft, TAI | Chronicled, HealthCombix, SimplyVital | |
| | Protocol | Conflux, Ultrain | Bitcoin, EOS, Ethereum, Hyperledger | |
| | Hardware | Bitmain, Canaan | Bitfury | |

# Ant Duo-Chain – Supply Chain Finance (SCF)

SCF on Blockchain




Smart Contract Workflow
SCF Accounts Receivable




Source: Ant Financial

**Other Ant Financial Apps: Cross-Border Remittance, Trusted Evidence Preservation, Product Genuineness Traceability**

# Food Trust/Safety

## What?

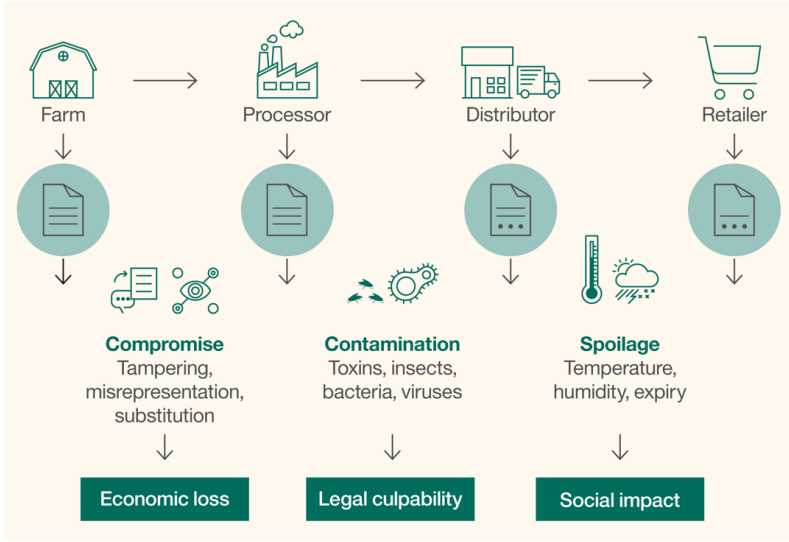
- Provide trusted source of information and traceability to improve transparency and efficiency across food network

## How?

- Shared ledger for storing digital compliance documentation, test results and audit certificates network

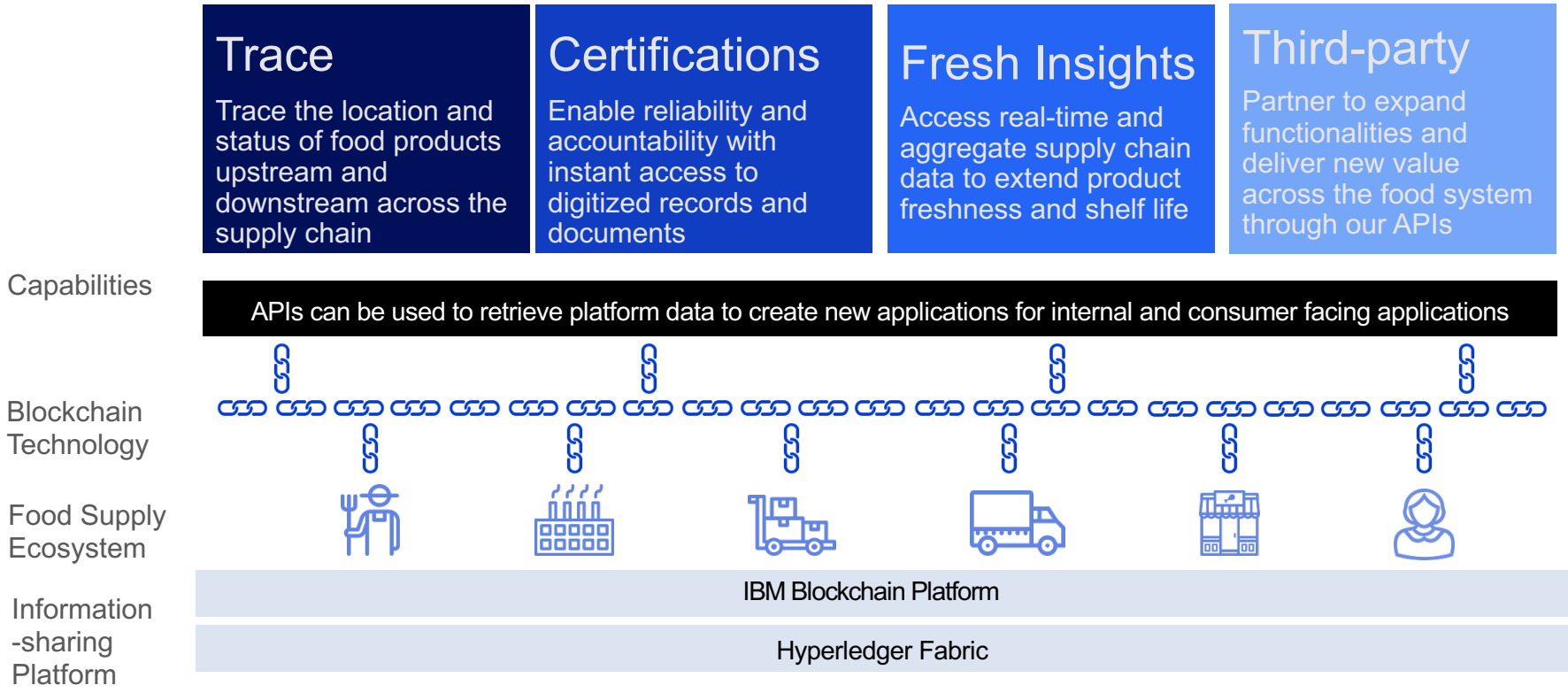
## Benefits

- Reduce impact of food recalls through instant access to end-to-end traceability data to verify history in food network & supply chain
- Help address 1 in 10 people sickened and 400K fatalities worldwide which occur every year from food-born illnesses



# IBM Food Trust

## Built on a blockchain platform, IBM Food Trust offers industry-specific functionality targeted at key pain points



# IFT Effectiveness Demoed via Walmart Mango Pilot

## *Pilot Test Case*

**How long does it take to trace a package of sliced mangoes back to the farm?**


## *Supply Chain*


## *Results*

**Typical manual, mixed digital and paper-based method**

**6 days**
**18 hours**
**26 minutes**

---

**IBM Food Trust digital solution**

**2.2 seconds**

# Dubai Blockchain Strategy

- Aims for Dubai to become the first blockchain-powered city by 2020
- For Dubai government to become paperless by shifting all transactions to Blockchain, and empower Dubai Smart city experience for all
- Based on Three pillars:
  - ✓ Government Efficiency: implementing blockchain technology in government services
  - ✓ Industry Creation: supporting the creation of a blockchain industry through empowering start ups and businesses
  - ✓ International Leadership: leading global thinking on blockchain techonolgy
- the Smart Dubai Office SDO launched Blockchain Challenge in partnership with global accelerator 1776
  - aims to identify the most innovative blockchain ideas from startups around the world and bring them to Dubai
- SDO launched a city-wide effort to implement blockchain in city services
- Partnerships with IBM as a Blockchain Lead Strategic Partner, and Consensys as Blockchain City Advisor.

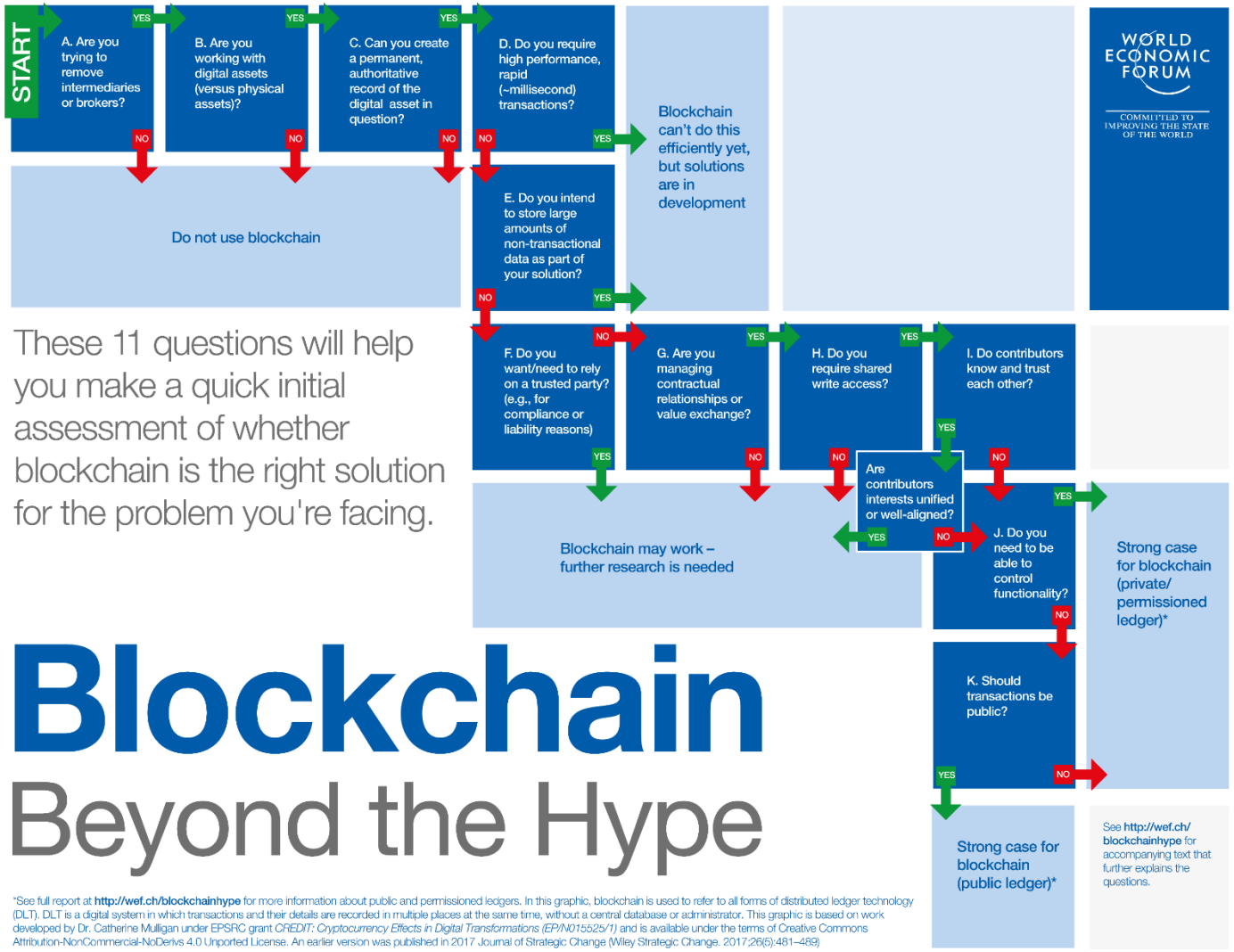

Dubai launches Blockchain strategy to become paperless by 2020

Hamdan unveils ambitious plan to save 25 million work hours annually through paperless transactions

GULF NEWS

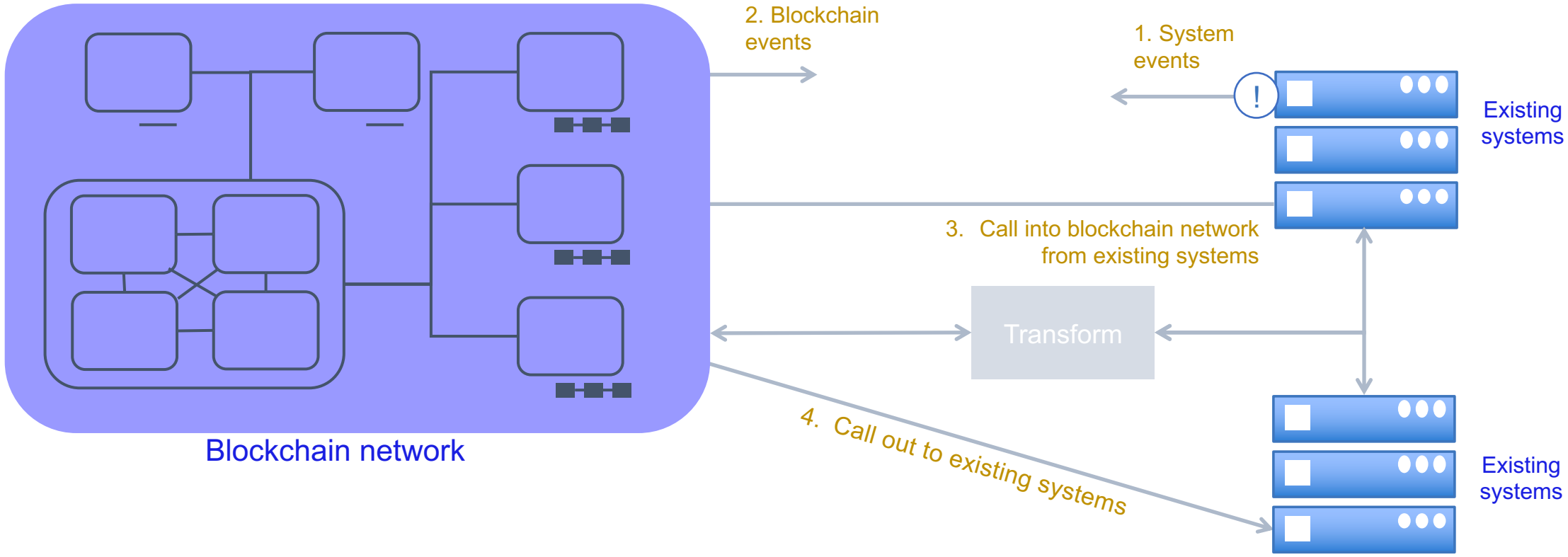

Source: Saeed Al Dhaheri, Etisalat Academy 3/2017

# Which Use Case Needs Blockchain? World Economic Forum 4/18




**Notes: Incorrect Recommendation about use of blockchains for managing physical assets**

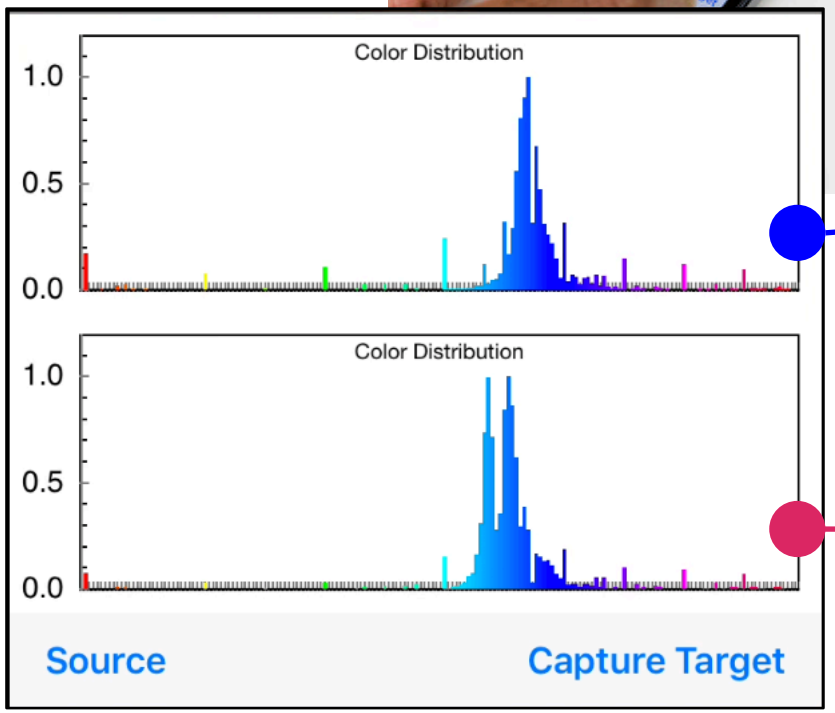
# Integrating with Existing Systems – Possibilities



# Crypto-Anchor Verifier

**5/2018: IBM Introduced Crypto Anchor Verifier –**
special lens added to mobile phone camera
Microscopic details of an object's surface are measured – e.g., optical characteristics such as shape, viscosity, saturation value, spectral values (AI + optical imaging)

- **Nobody likes knockoffs.**
- Within the next five years, cryptographic anchors and blockchain technology will ensure a product's authenticity -- from its point of origin to the hands of the customer.
- In certain countries, nearly 70% of certain life-saving pharmaceuticals are counterfeit. Digital profiles of legitimate pharmaceuticals can be stored in a blockchain to detect counterfeits.




REAL

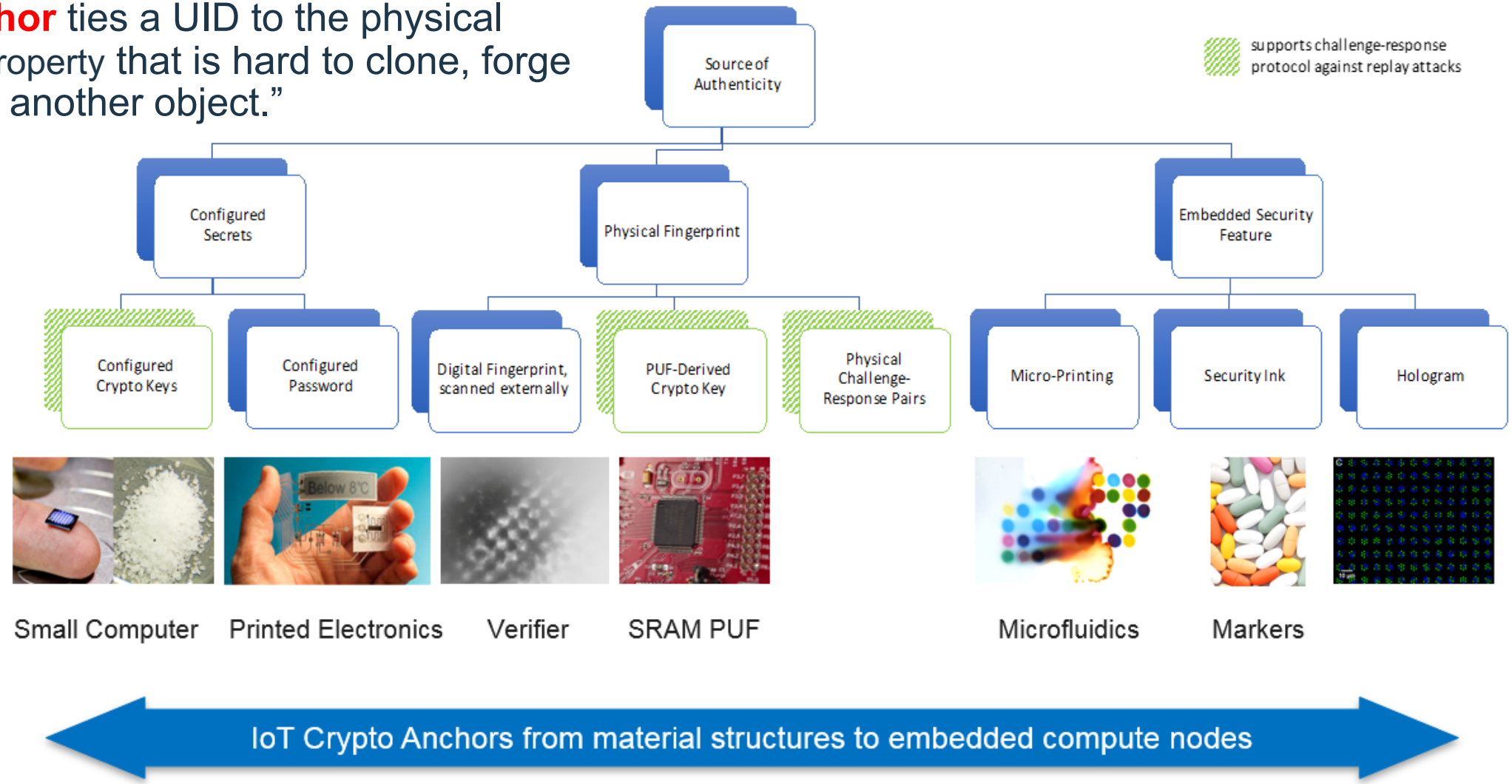
*Wavelength AI models shows differences between pills*

FAKE

"Crypto Anchors", V. Balagurusamy et al. **IBM Journal of R&D**, Vol. 63, No. 2/3, March/May 2019

# Securing Against Counterfeiters with Crypto Anchors

"A **crypto anchor** ties a UID to the physical object with a property that is hard to clone, forge and transfer to another object."



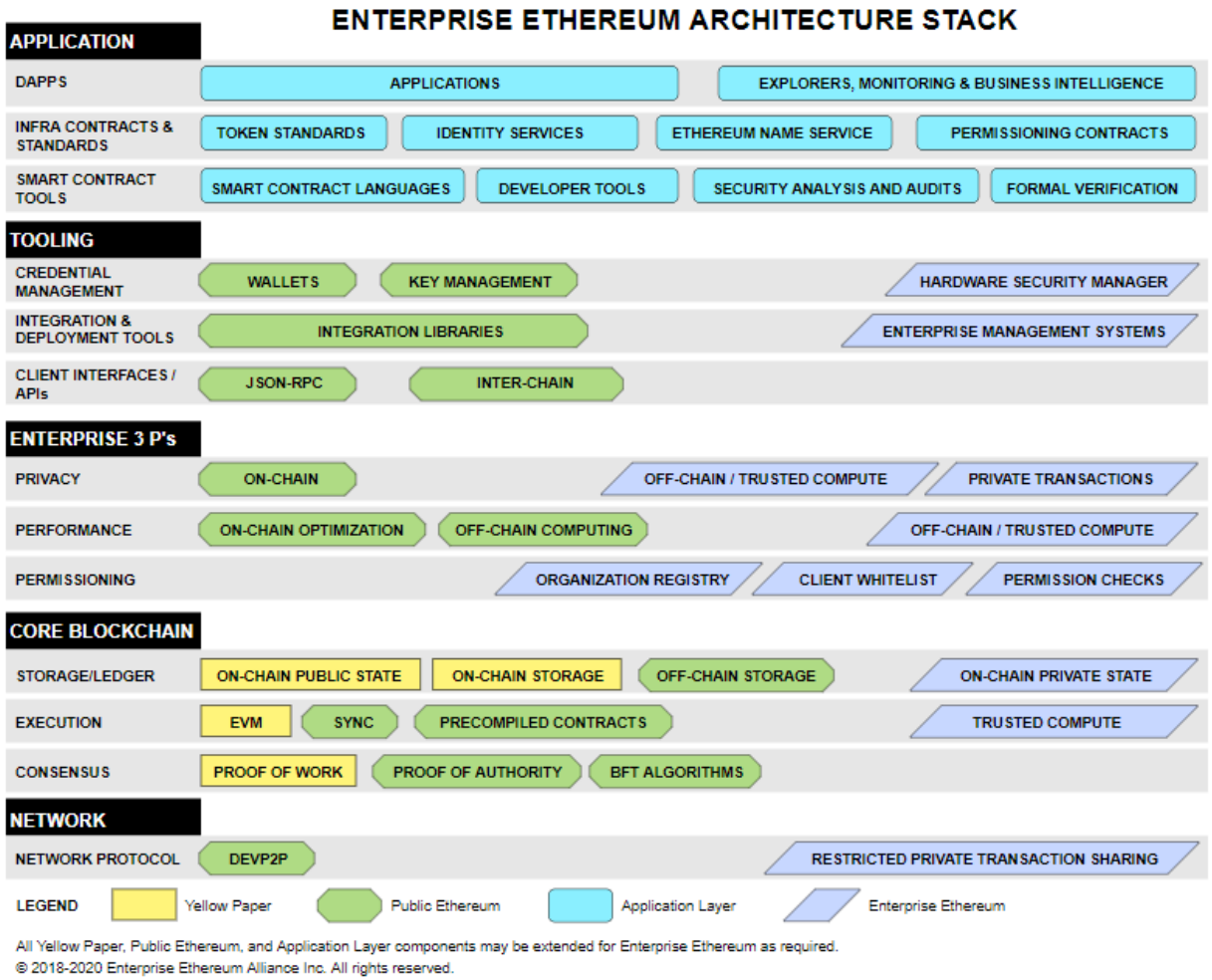
# Ethereum

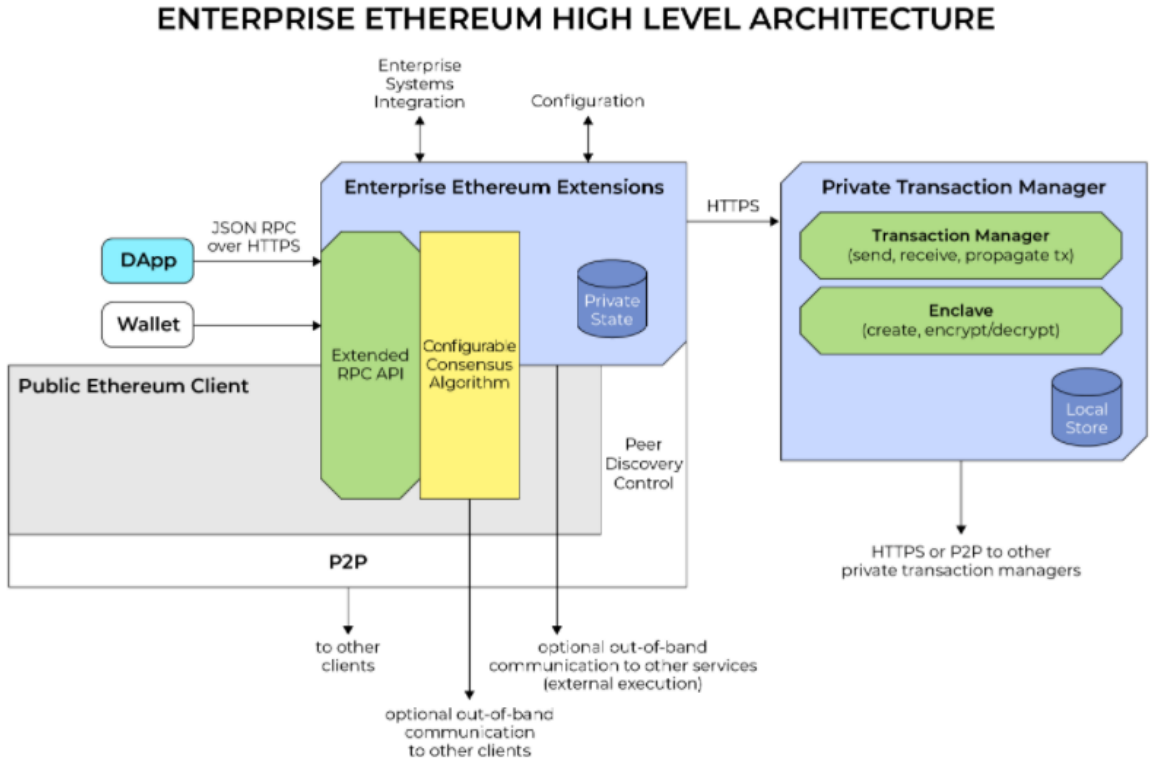
- Public blockchain system like Bitcoin
  - Extends it with Smart Contracts
  - Cryptocurrency Ether
  - Uses PoW for consensus
  - Own machine language (Solidity) & virtual machine (EVM)
  - *Gas:* virtual charging mechanism for transactions and smart contracts!
- Most apps relate to its currency Ether
- Ethereum client implements Ethereum Protocol by providing the following:
  - Execution environment for processing transactions in the Ethereum blockchain
  - Storage for persisting data related to transaction execution
  - P2P networking for communicating with the other Ethereum nodes to synchronize state
  - APIs for app developers to interact with the blockchain

# Enterprise Ethereum

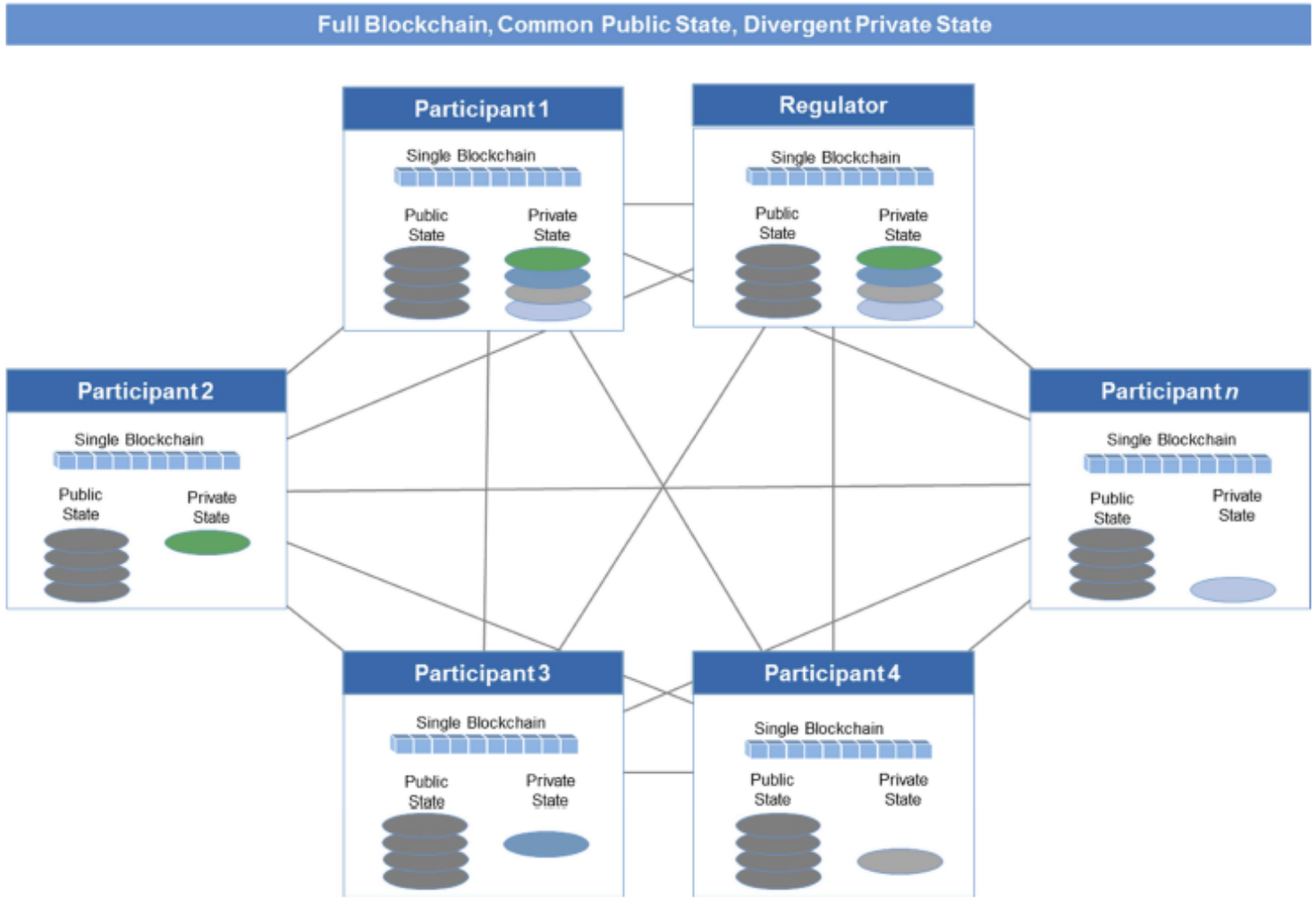
- *Enterprise Ethereum Alliance* (**EEA**): JPMorgan Chase, Microsoft, Intel, Accenture, Banco Santander, BNY Mellon, ConsenSys, Credit Suisse, ING, Thomson Reuters, UBS, Wipro
  - EEA will add confidentiality (Quorum), scalability (pluggable consensus) and permissioning to Ethereum
  - Focus on specification, **EntEth** 1.0 with Python reference client, benchmarking, compliance testing and tools
  - Develop standards for Ethereum: best practices, security, privacy, scalability, interoperability
    - V1 EEA **Client** spec released in 5/2018; V1 EEA **Permissioned Blockchains** spec released in 5/2020
- **Quorum** developed by JPMorgan
- JPMorgan used Quorum to implement JPM Coin and Interbank Information Network (IIN) payments messaging network
- ConsenSys used Quorum for trade finance blockchain komgo, agribusiness consortium Covantis, and LVMH Aura for luxury goods

# EEA Client Specification & High Level Architecture (8/2020)



# Quorum Network J.P. Morgan



# Ethereum and Quorum Sale to ConsenSys

MICHAEL KAPILKOV 1 HOUR AGO Source: CoinTelegraph 2020-08-26

## Quorum's creator says the project was going nowhere, JPMorgan wanted rid of it


**ConsenSys plans to merge Go-based Quorum and Java-based Hyperledger Besu**

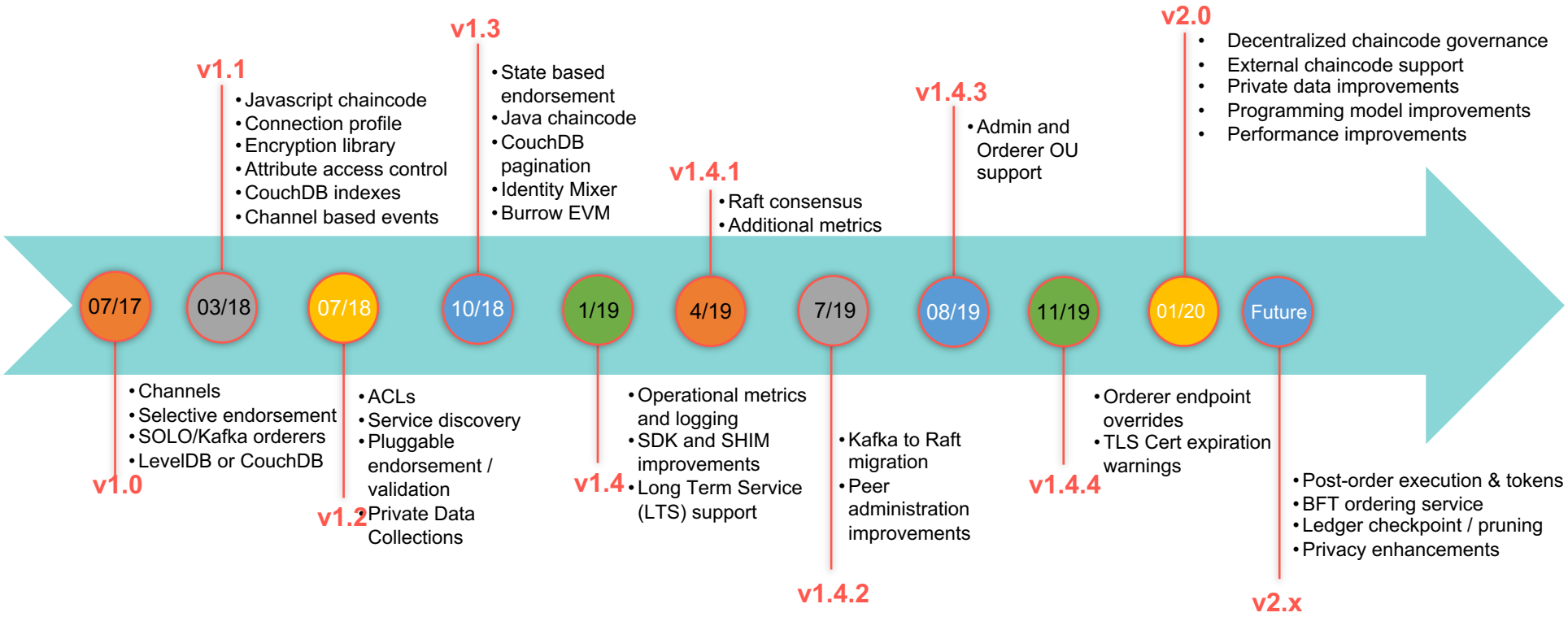
"If JPMorgan, one of the biggest companies ever, can't drive adoption, even when they have a great internal use case, you have to ask yourself 'why'? And my answer to that is the technology is just fundamentally limited. And if you go and talk to other large system integrators, large consultancies, you'll hear very, very similar things. So long as you don't have someone who holds a lot of the Ethereum tokens as the head of Blockchain for the company, you're going to find that people say: 'We have tried using Ethereum, it just doesn't work'."

**Will Marino, Former Quorum Lead @ JPMorgan**

# Hyperledger Besu

- Incubated by ConsenSys and originally called Pantheon
- Joined Hyperledger in August 2019
- First Hyperledger project to operate on a public blockchain
- Java-based Ethereum client for public and private permissioned use cases – Apache 2.0 license
- Can be run on test networks like Rinkeby, Ropsten, Gorli
- Modularity and clean interfaces between elements within client (networking, storage, EVM, …) to enable easier configuration and allowing other Hyperledger projects to integrate and use elements of Besu's codebase
- For consensus supports PoW and PoA (IBFT, IBFT 2.0, Etherhash, Clique)
- Implements EEA client specification

# Hyperledger Fabric Roadmap




Based on https://wiki.hyperledger.org/display/fabric/Hyperledger+Fabric+Roadmap - Dates determined by the Hyperledger community - (*) Subject to change

# Fabric V2 (1/2020)

- 1st Hyperledger project to reach 2.0 stage
- External smart contract support
- Decentralized governance for smart contracts

Improvements to smart contract lifecycle

| Fabric v1.x | Fabric v2.x |
|---|---|
| Single organization instantiates and controls smart contract (endorsement policies, upgrades, etc). | LifecycleEndorsement channel policy specifies which organizations or how many organizations must agree on a smart contract. |
| Must re-install entire smart contract to update endorsement policy or private data collections. | Manage smart contract logic and smart contract definition separately. |
| Smart contract must be identical on all organization's peers. | Organizations can extend smart contract, for example, perform additional org-specific verifications before endorsing. |

# Libra Blockchain (Facebook)

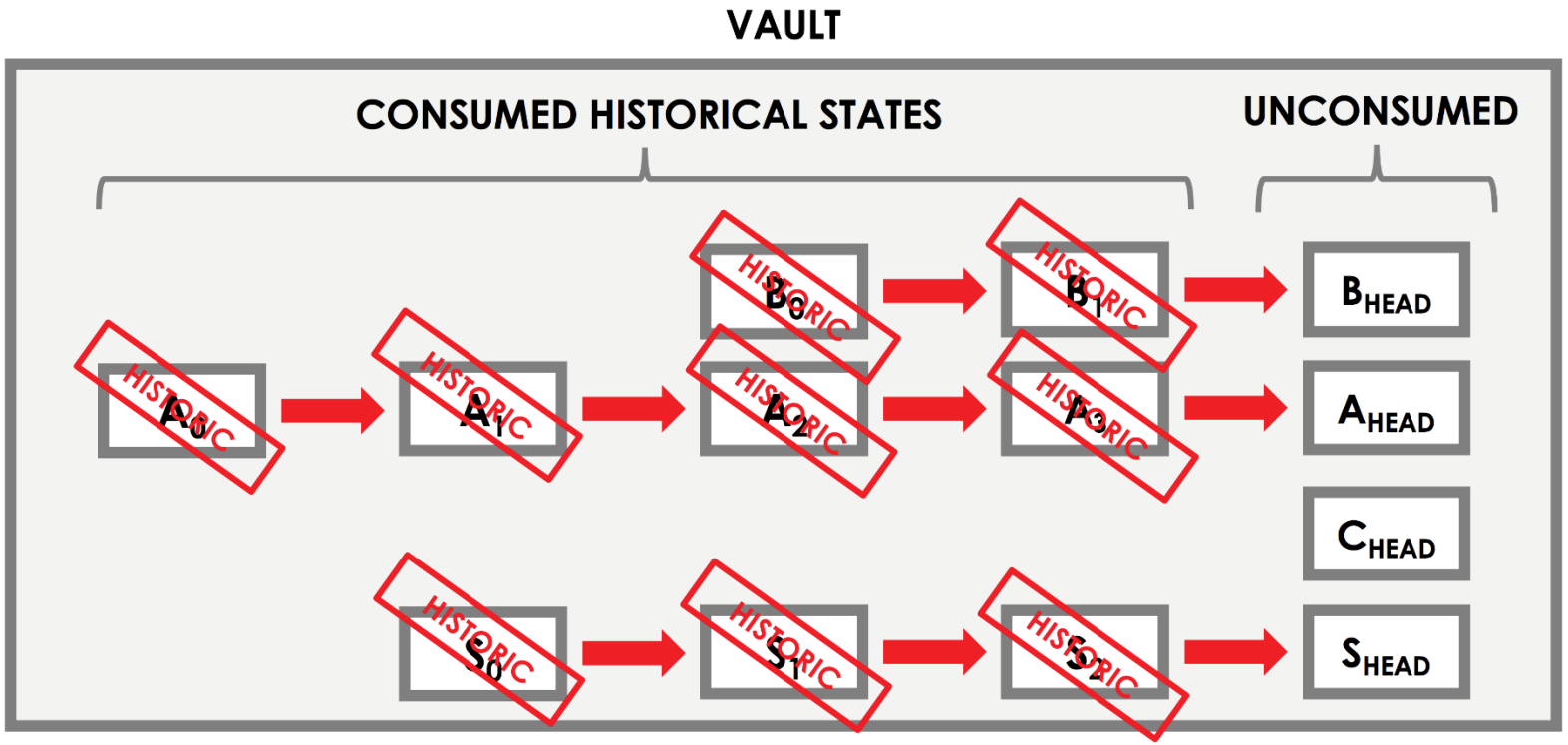
- Facebook initiated but followed up with Libra Association of others also (libra.org)
- Libra cryptocurrency with intrinsic ***stable*** value based on association membership dues (*reserve of assets)* and a competitive network of exchanges
- Initial implementation by Facebook to be followed by Association built system
- **Founding members** from following industry segments: Payments, Technology & marketplaces, Telecom, Blockchain, Venture capital, Nonprofits/academia/multilateral orgs
- Target launch: 1H 2020 along with digital wallet Calibra
- Move language, LibraBFT consensus
- All data stored in a versioned DB
- Has Gas Price concept, Max Gas Amount, Expiration time for transactions
- Partly permissioned and partly permissionless
- Very controversial across geographies
- Many initial members have backed out: PayPal, eBay, Visa, Mastercard, Stripe, …
- Latest news (3/2020): Will support **fiat currencies** also!

# R3 Alliance & Corda

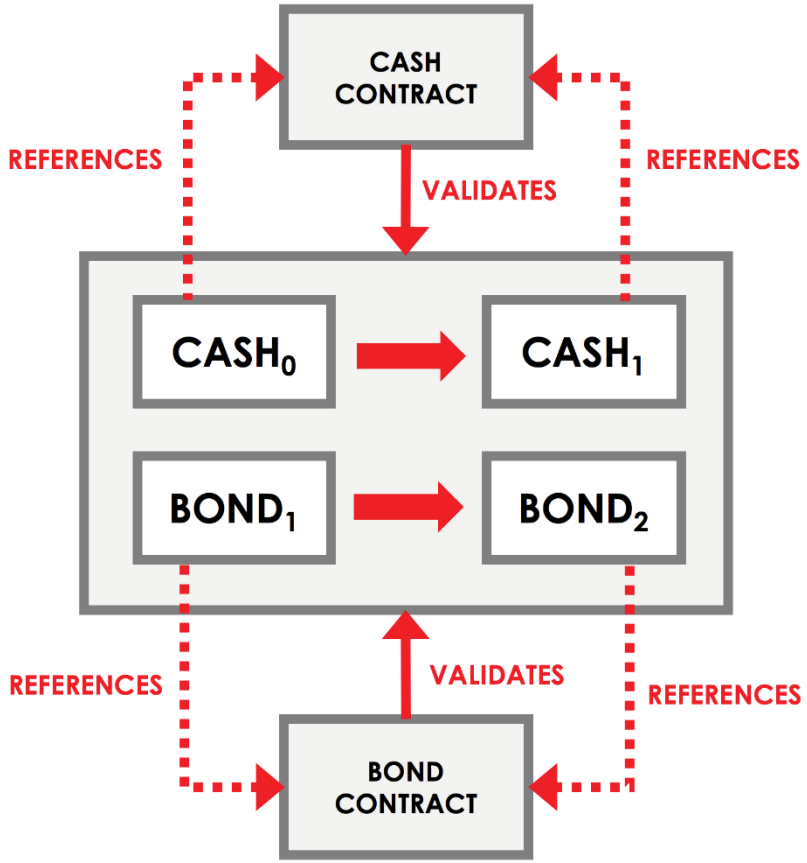
- Barclays, BBVA, Commonwealth Bank of Australia (CBA), Credit Suisse, J.P. Morgan, State Street, Royal Bank of Scotland, UBS
- Special features for JVM to guarantee deterministic behavior
- Nodes backed by RDBMS, ledger data SQL queryable and joinable with private tables
- Corda written in Kotlin (simpler Scala with much better Java interoperability) from JetBrains – contracts in Kotlin/Java
- Contract execution is deterministic and its acceptance of a transaction is based on the transaction's contents alone. A transaction is only valid if the contract of every input state and every output state considers it to be valid
- Consensus over transaction validity performed only by parties to transaction in question
- Given actor sees only subset of overall data managed by system as a whole

# Corda Vault and State

Each node on the network maintains a *vault* - a DB where it tracks all the current and historic states that it is aware of, and which it considers to be relevant to itself



# Corda Contract Validity




A transaction is only valid if it is digitally signed by all required signers. However, even if a transaction gathers all the required signatures, it is only valid if it is also **contractually valid**.

# Ant Financial BaaS


## Product Portfolio

BaaS Marketplace & Solution

On-chain finance: Cross-border payment; Supply chain financing; Exchange; Ticket; Insurance

On-chain retail: Cross-border logistics; Product traceability; Drug tracing; Advertising

On-chain lifestyle: Healthcare; House renting/rental; Copyright; Ticket; Charity; Contract

Security management

Real-name authentication

Anti-DDoS

Key management service

Access control

IoT security

Operation auditing

BaaS Plus: Trusted evidence preservation; Universal tracing; In-person verification; Enterprise authentication; Cross-chain service; Smart contract security check

BaaS Core: Consortium management; Smart contract management; SGX/TEE; Security and privacy; Browser and monitoring; Business view; Node management; User management; Certificate key management; Logging and auditing; Off-chain data synchronization; Large file processing; Hyperledger Fabric; AntChain-Self-developed financial blockchain platform of Ant: Contract tool; Cloud IDE; Privacy protection; Cryptography security; Trust execution environment; FDMT storage; Asynchronous consensus; Contract and virtual machine; Cross-chain technology; Enterprise Ethereum Quorum; Container cluster Kubernetes

Cloud resource layer: Elastic IP Address; Server Load Balancer; ApsaraDB; Container Registry; Alibaba Cloud DNS; Cloud Enterprise Network; Elastic Compute Service; ECS Bare Metal Instance; Apsara Block Storage; Network Attached Storage; Virtual Private Cloud; Express Connect; Cloud resource management platform (Alibaba Cloud Apsara platform); Computing resource; Storage resource; Network resource

Infrastructure layer: Public cloud and private cloud

O&M management

CloudMonitor

Resource orchestration

OpenAPI Explorer

Log Service

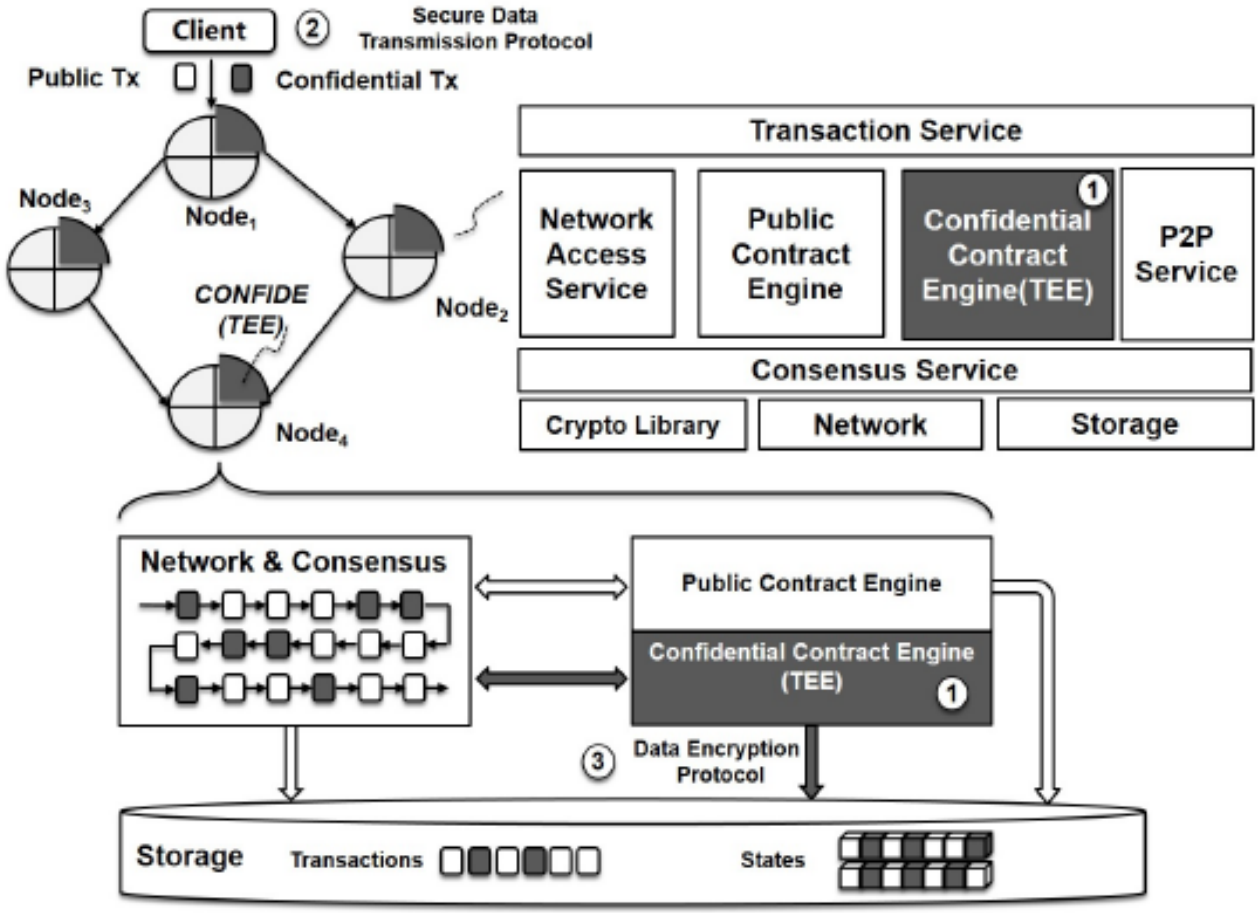
Database management

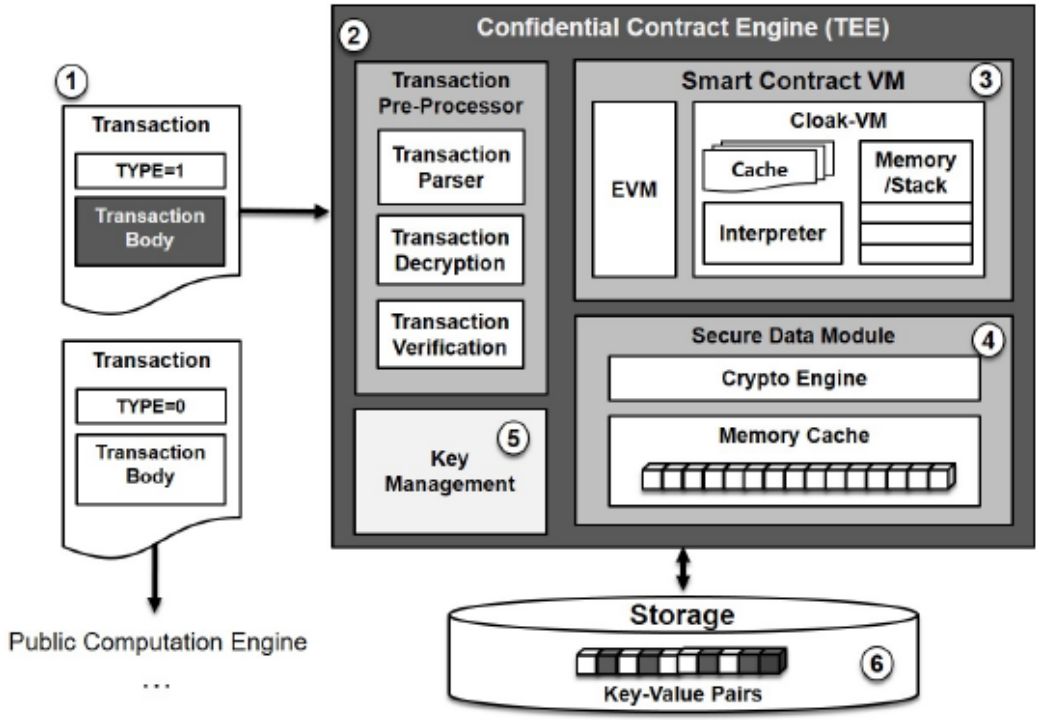
Billing management

# Ant Financial Blockchain (AntChain) Features

- Supports Trusted Execution Environment (TEE) – e.g., Intel SGX
- Max 25K notary blockchain TPS; PBFT for Byzantine fault tolerance
- WebAssembly (Wasm) based contract engine – not EVM
- Standardized Services: trusted evidence preservation, universal tracing and in-person verification, enterprise authentication, cross-chain service, smart contract security check
- Private/public data/transactions/smart-contracts without using expensive zero knowledge proofs (ZKP) - CONFIDE plugin, SIGMOD 2020 paper
- Envelope transaction and private transaction
- Transaction type includes link notary, content notary, hash notary, ciphertext notary, privacy sharing notary, and ciphertext-only notary
- **AntChain Station**: HW encryption acceleration for privacy-preserving computation, enhanced security algorithms, rapid deployment

# Architecture of AntChain + CONFIDE

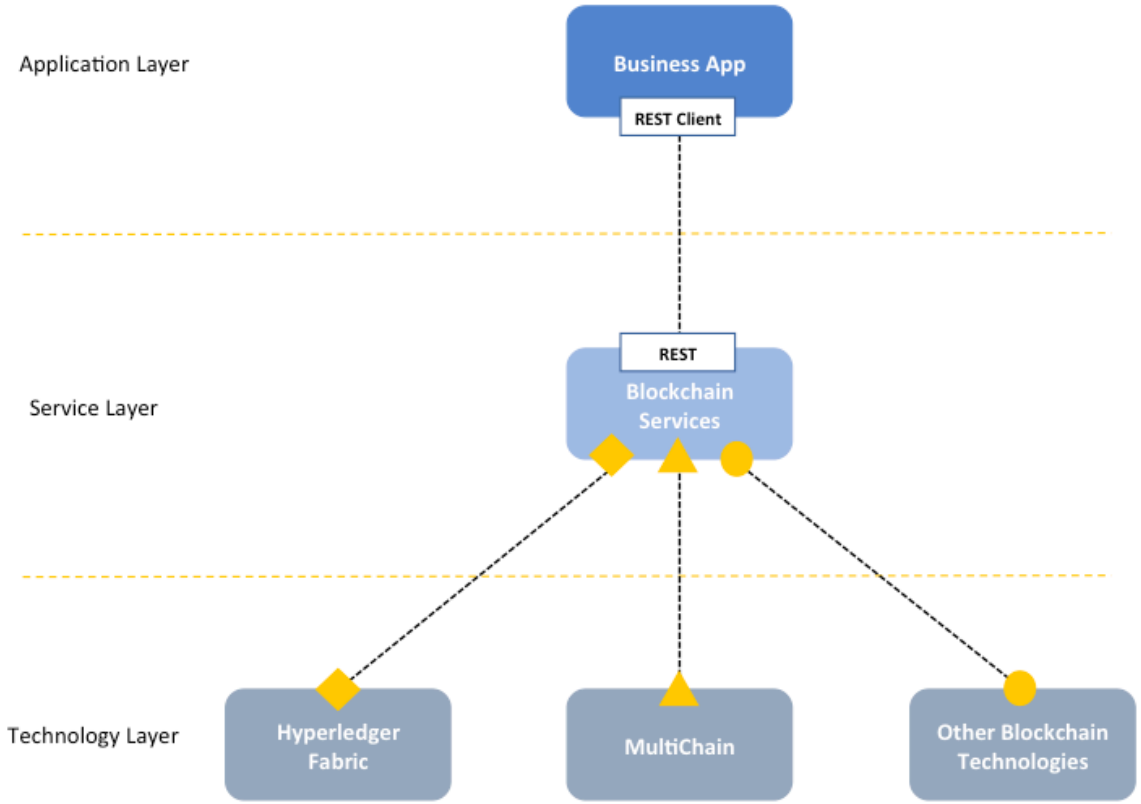


# Sawtooth (Intel)


- Project of Hyperledger; 1.0 release ("Production Ready") announced in 1/2018
- Proof of Elapsed Time (PoET) – Consensus Protocol
  - Every validator requests a wait time from a trusted function
  - Validator with shortest wait time for a particular transaction block is elected leader
  - Guaranteed wait time
  - Randomness in leader election (~ to lottery algorithm)
- Intended to run in a Trusted Execution Environment (TEE), e.g., Intel's Software Guard Extensions (SGX)
- Concept of Transaction Family and Transaction Dependencies
- Transaction Scheduling: Serial or Parallel
- Same block can contain multiple transactions which modify same value!
- Support for Ethereum
- On-Chain Governance: Utilize smart contracts to vote on blockchain configuration settings such as the allowed participants and smart contracts
- https://sawtooth.hyperledger.org/docs/core/releases/latest/contents.html

# SAP Blockchain Application Enablement



# Smart Contracts

- Deterministic versus non-deterministic contracts
- Different languages and restrictions on allowed operations
- Evolution of contracts over time
- Portability of contracts across BC systems
- 4/2020
  - Open source smart contract language **DAML** SDK 1.0 released
  - Portable contracts across Besu, Fabric and Sawtooth

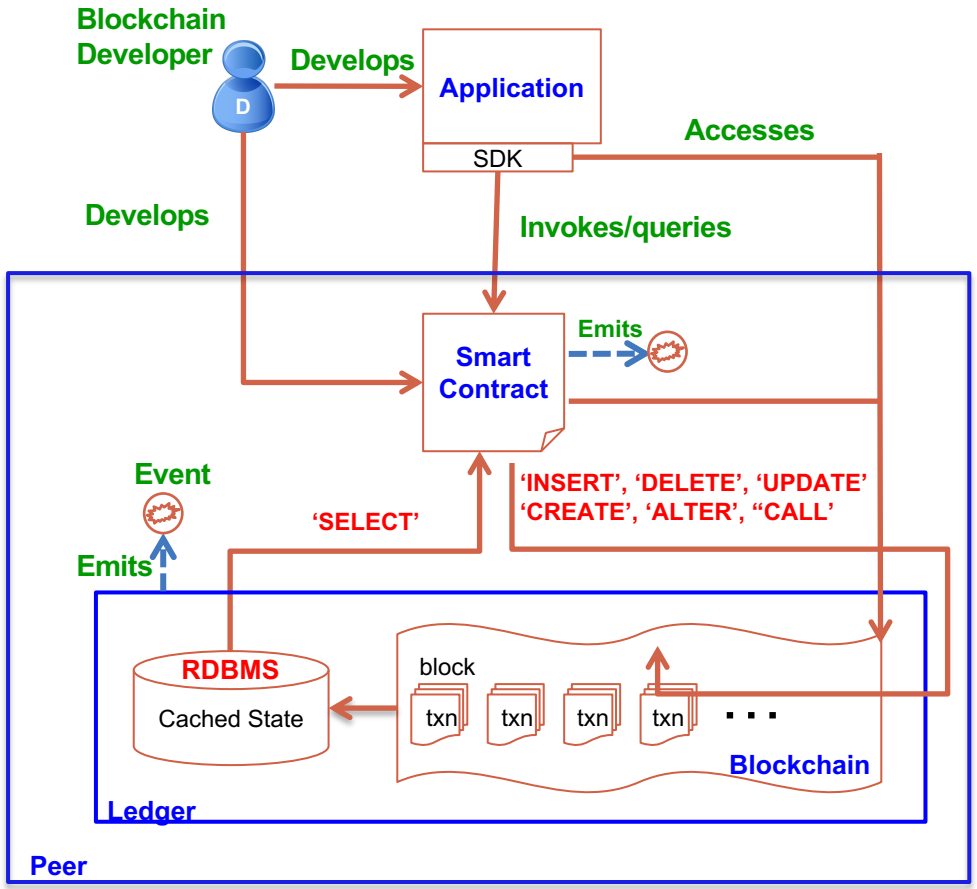
# Hyperledger Cactus

- Blockchain Integration Framework contributed by Accenture & Fujitsu
- Moved from Labs (11/2019) to Greenhouse (5/2020) status
- Pluggable architecture
- Execution of ledger operations across multiple blockchain ledgers, including Hyperledger Besu, Hyperledger Fabric, Corda, and Quorum available now
- Developers continually adding support for new blockchains

# Hyperledger Caliper

- Allows users to measure performance of a specific blockchain implementation with a set of predefined use cases
- Will produce reports containing a number of performance indicators, such as TPS (Transactions Per Second), transaction latency, resource utilization, …
- Intent is for Caliper results to be used by other Hyperledger projects as they build out their frameworks, and as a reference in supporting the choice of a blockchain implementation suitable for a user's specific needs
- Initial contributors: Developers from Huawei, Hyperchain, Oracle, Bitwise, Soramitsu, IBM and Budapest University of Technology and Economics
- https://www.hyperledger.org/projects/caliper

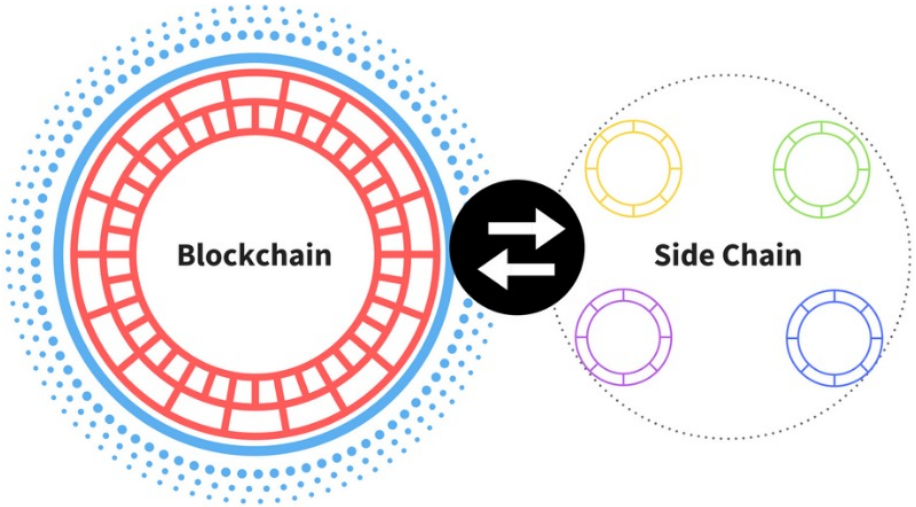
# Application Flow with RDBMS (Abandoned at IBM Research!)




- Developers create application and smart contracts (chaincodes)
  - Chaincodes are deployed on the network and control the state of the ledger
  - Application handles user interface and submits transactions to the network which call chaincodes
- Network emits events on block of transactions allowing applications to integrate with other systems

# Futuristic Topics

- Smart Contract portability & power of data APIs
- DBMS enhancements to add BC features
- Standards across BC systems
- Cross-channel transactions
- Non-deterministic actions
- Analytics on BC assets' data – present & past
- Many app design issues (e.g., how many endorsing peers to send transaction to)
- Design tools for endorsement decisions
- NL contracts -> formal contracts -> executable contracts
- GDPR & PII Implications




**Numerous research possibilities for database and distributed systems people in this New Era of Distributed Computing!**

# More Information

## Links to Videos, Slides, Bibliography, Twitter Handles

http://bit.ly/CMbcDB (blockchain)  http://bit.ly/CMgMDS (database)

## Follow me on

Telegram, Twitter, WeChat, Instagram: @seemohan

Facebook: http://bit.ly/CMFace

LinkedIn: http://bit.ly/CMlink

Biodata: http://bit.ly/CMbiod

Resume: http://bit.ly/CMoRes