Institute for Advanced Study (IAS), City University of Hong Kong (CityU)
Hong Kong, China, 11 January 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

LinkedIn/Telegram/Twitter/WeChat: seemohan
Facebook: cmohan

Links to Videos, Slides, Bibliography & Twitter Handles @ http://bit.ly/CMbcDB

Agenda

Goal: Discuss basics about blockchains (BCs), bust some myths and discuss practically relevant private/permissioned BCs, including details of some private BC systems

- Origin of Blockchains (BCs) & Blockchain-as-a-Service (BaaS)
- Related Distributed Systems/Databases Topics
- Evolution: Smart Contracts, Private BCs, …
- Consortia Approach to Development of Systems
- Applications: Production, PoCs, …
- Market Scene
- Benchmarks and Standards
- Architectural Choices and Relationship to DB Replication
- Technical Details of Representative Systems:
  Enterprise Ethereum, Hyperledger Fabric & Composer, R3 Corda, Sawtooth, Ripple
- Futuristic Topics

Blockchain (BC)

- Origin in digital currencies (Bitcoin - *Satoshi Nakamoto*, 2008)
  Anonymity, **open/public/permissionless** environment
  Energy wastage via "mining" & 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, …
- ResearchAndMarkets.com: Global BC Tech Market **US$19.9B** by 2023 (CAGR 42.8%, 2018-23)

- **My focus**: **Private/Permissioned** BC Systems!

  Leverages underlying blockchain data structure of Bitcoin while providing
  - Much better performance/scalability
  - Controlled information sharing among organizations & users
  - Deterministic behavior

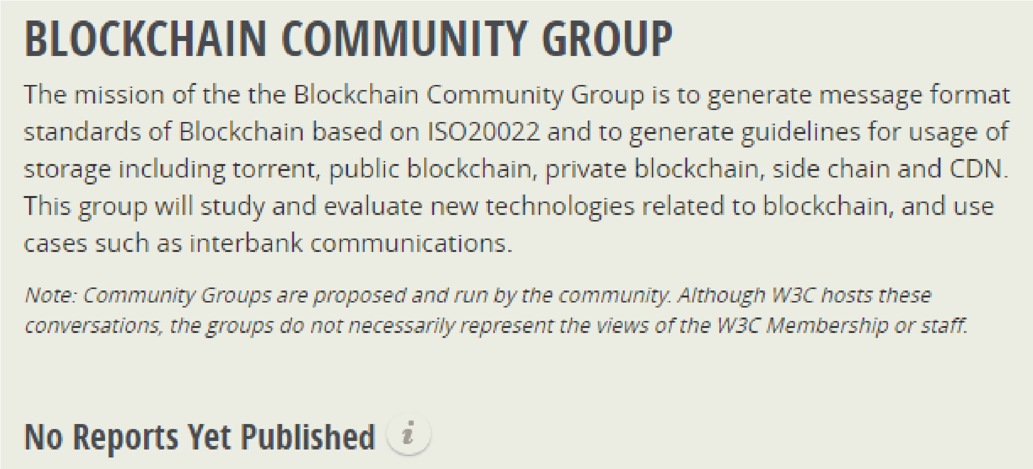
Blockchain (BC)

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

mostly as part of consortia

- 2/2017: First **production** deployment of BC technology by IBM & Northern Trust in Guernsey for managing **private equity fund** by Unigestion – **Hyperledger Fabric 0.6**
- 4/2017: China's **Tencent** announced **TrustSQL**
- 7/2017: **Hyperledger Fabric 1.0** released (aka **Production Ready**)
- 8/2007: **Hyperledger Fabric** on IBM Cloud – **BaaS offering** IBM Blockchain Platform on highly secure Linux on mainframes
- 10/2017: China's **Baidu** joined Hyperledger as a **Premium Member** & 1/2018: Announces 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)
- 7/2018: IBM announces work on **Stablecoin** (pegged to US$) Stronghold USD
- 8/2018: **Oracle** released Oracle Autonomous Blockchain Cloud Service (OABCS) - **Fabric 1.1** based with Berkeley DB & **SQL** support
- 10/2018: Hyperledger and **EEA** decide to collaborate

Blockchain Standards (W3C & IEEE)



BLOCKCHAIN COMMUNITY GROUP

The mission of the the Blockchain Community Group is to generate message format standards of Blockchain based on ISO20022 and to generate guidelines for usage of storage including torrent, public blockchain, private blockchain, side chain and CDN. This group will study and evaluate new technologies related to blockchain, and use cases such as interbank communications.

Note: Community Groups are proposed and run by the community. Although W3C hosts these conversations, the groups do not necessarily represent the views of the W3C Membership or staff.

No Reports Yet Published

IEEE BLOCKCHAIN™

BLOCKCHAIN FOR AGRICULTURE

BLOCKCHAIN FOR CLINICAL TRIALS

PHARMA SUPPLY BLOCKCHAIN

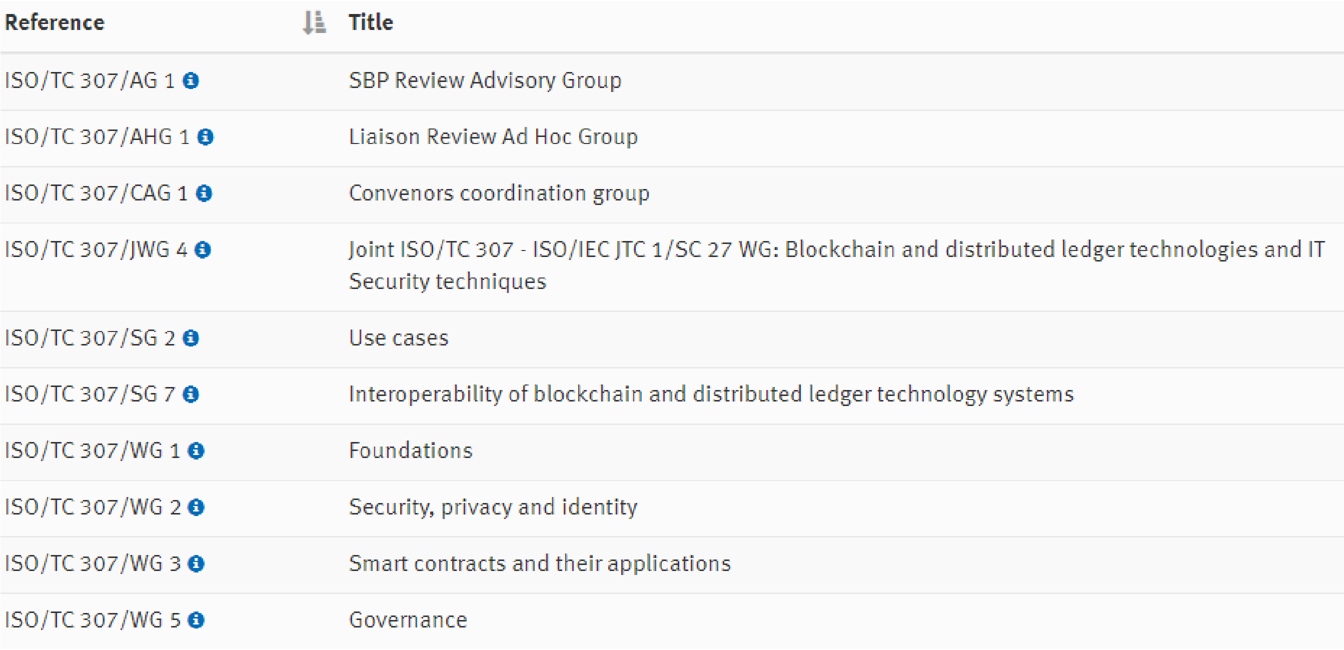
Active Standards Projects:

- P2418.1 - Standard for the Framework of Blockchain Use in Internet of Things (IoT)
- P2418.2 - Standard Data Format for Blockchain Systems
- P2418.3 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Agriculture
- P2418.4 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Connected and Autonomous Vehicles (CAVs)
- P825 - Guide for Interoperability of Transactive Energy Systems with Electric Power Infrastructure (Building the Enabling Network for Distributed Energy Resources)

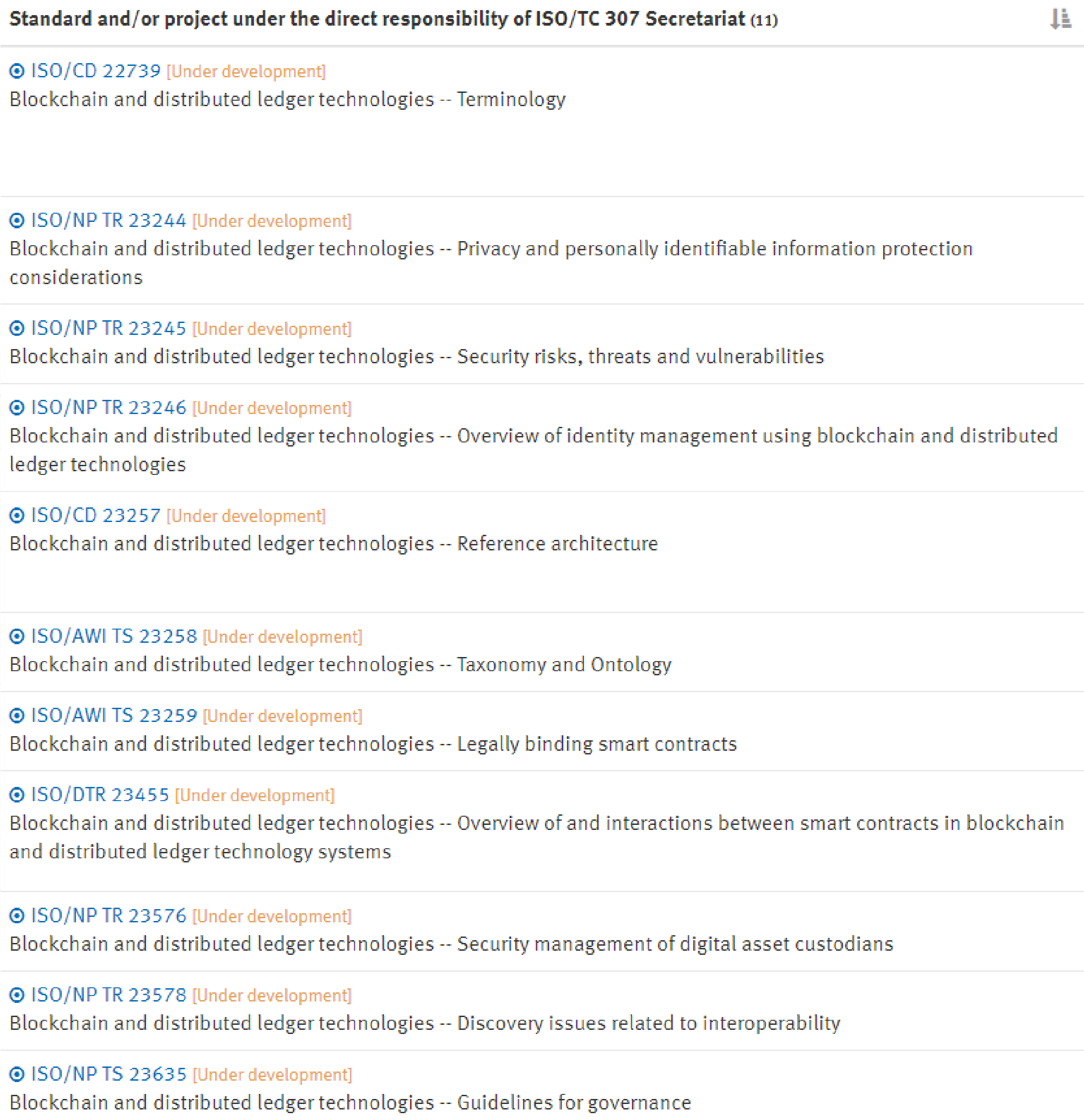
Blockchain Standards (ISO)

ISO/TC 307 (driven by Australian body – from 2016)

Blockchain and distributed ledger technologies



Reference	Title
ISO/TC 307/AG 1	SBP Review Advisory Group
ISO/TC 307/AHG 1	Liaison Review Ad Hoc Group
ISO/TC 307/CAG 1	Convenors coordination group
ISO/TC 307/JWG 4	Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques
ISO/TC 307/SG 2	Use cases
ISO/TC 307/SG 7	Interoperability of blockchain and distributed ledger technology systems
ISO/TC 307/WG 1	Foundations
ISO/TC 307/WG 2	Security, privacy and identity
ISO/TC 307/WG 3	Smart contracts and their applications
ISO/TC 307/WG 5	Governance



Standard and/or project under the direct responsibility of ISO/TC 307 Secretariat (11)

ISO/CD 22739 [Under development]
Blockchain and distributed ledger technologies -- Terminology

ISO/NP TR 23244 [Under development]
Blockchain and distributed ledger technologies -- Privacy and personally identifiable information protection considerations

ISO/NP TR 23245 [Under development]
Blockchain and distributed ledger technologies -- Security risks, threats and vulnerabilities

ISO/NP TR 23246 [Under development]
Blockchain and distributed ledger technologies -- Overview of identity management using blockchain and distributed ledger technologies

ISO/CD 23257 [Under development]
Blockchain and distributed ledger technologies -- Reference architecture

ISO/AWI TS 23258 [Under development]
Blockchain and distributed ledger technologies -- Taxonomy and Ontology

ISO/AWI TS 23259 [Under development]
Blockchain and distributed ledger technologies -- Legally binding smart contracts

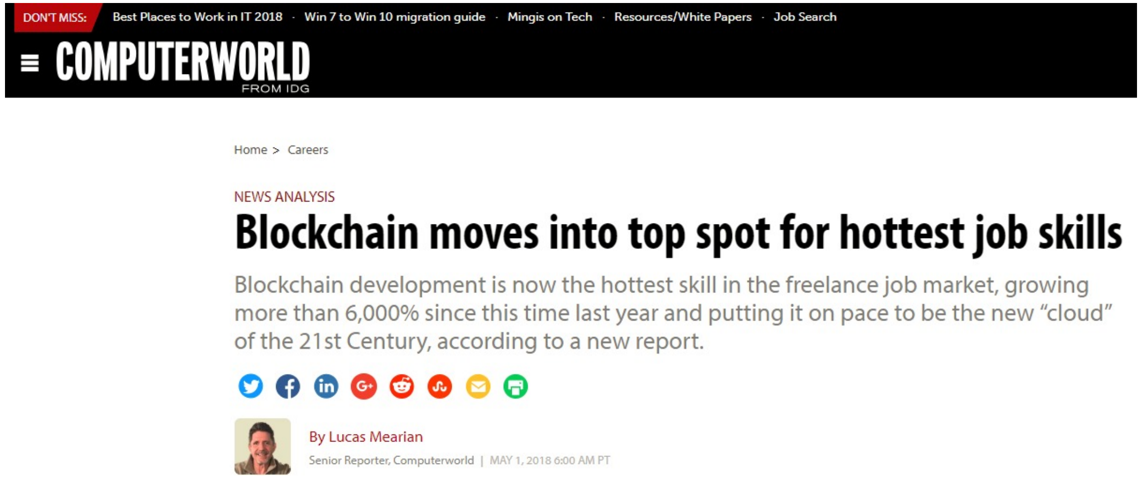
ISO/DTR 23455 [Under development]
Blockchain and distributed ledger technologies -- Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems

ISO/NP TR 23576 [Under development]
Blockchain and distributed ledger technologies -- Security management of digital asset custodians

ISO/NP TR 23578 [Under development]
Blockchain and distributed ledger technologies -- Discovery issues related to interoperability

ISO/NP TS 23635 [Under development]
Blockchain and distributed ledger technologies -- Guidelines for governance

Blockchain Jobs



DON'T MISS: Best Places to Work in IT 2018 · Win 7 to Win 10 migration guide · Mingis on Tech · Resources/White Papers · Job Search

≡ COMPUTERWORLD FROM IDG

Home > Careers

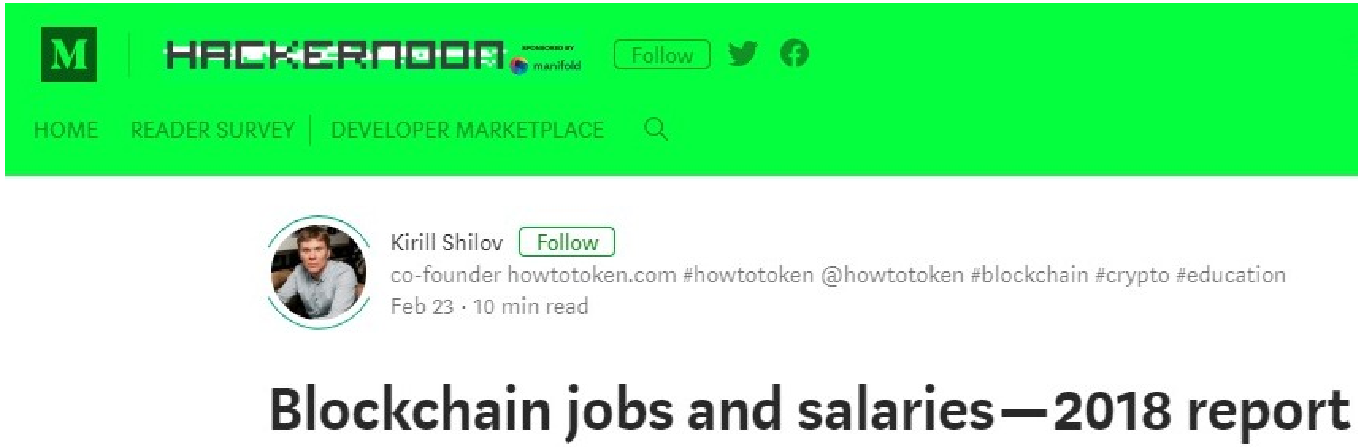
NEWS ANALYSIS

Blockchain moves into top spot for hottest job skills

Blockchain development is now the hottest skill in the freelance job market, growing more than 6,000% since this time last year and putting it on pace to be the new "cloud" of the 21st Century, according to a new report.

By Lucas Mearian

Senior Reporter, Computerworld | MAY 1, 2018 6:00 AM PT



M HACKERNOON manifold Follow

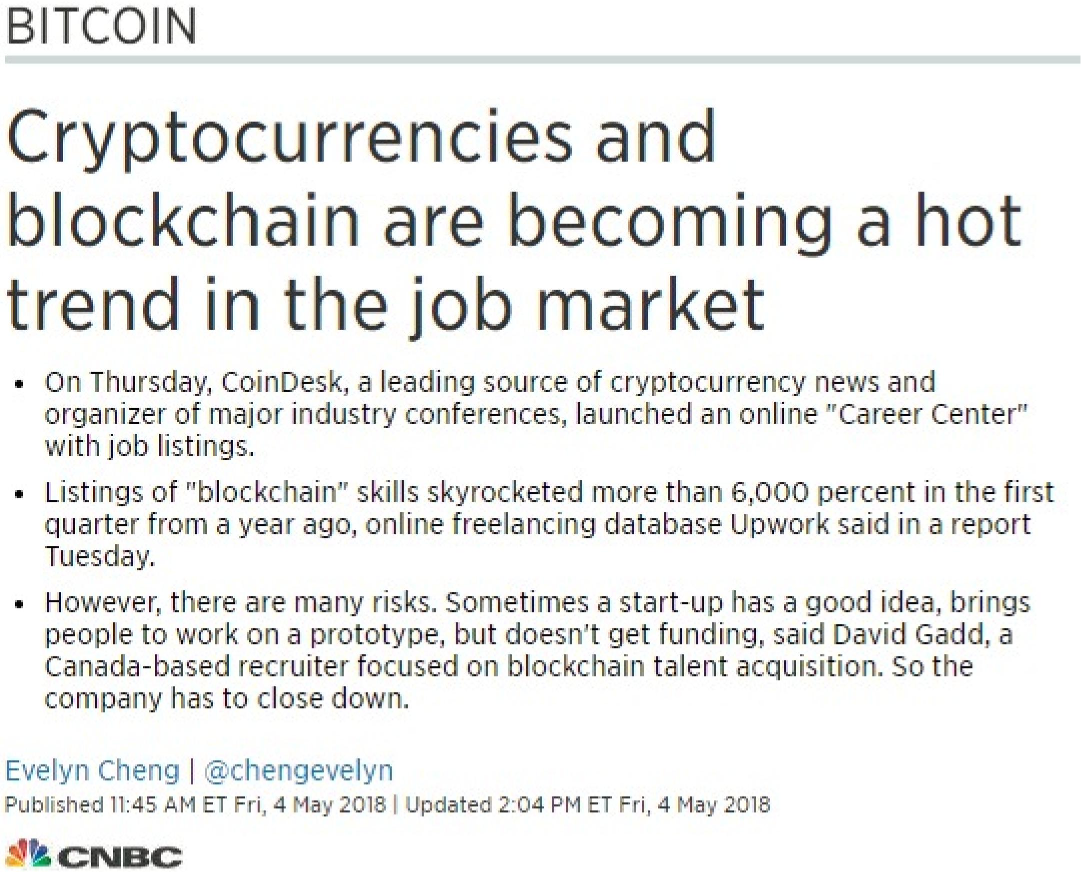
HOME READER SURVEY DEVELOPER MARKETPLACE

Kirill Shilov Follow

co-founder howtotoken.com #howtotoken @howtotoken #blockchain #crypto #education

Feb 23 · 10 min read

Blockchain jobs and salaries—2018 report



BITCOIN

Cryptocurrencies and blockchain are becoming a hot trend in the job market

- On Thursday, CoinDesk, a leading source of cryptocurrency news and organizer of major industry conferences, launched an online "Career Center" with job listings.
- Listings of "blockchain" skills skyrocketed more than 6,000 percent in the first quarter from a year ago, online freelancing database Upwork said in a report Tuesday.
- However, there are many risks. Sometimes a start-up has a good idea, brings people to work on a prototype, but doesn't get funding, said David Gadd, a Canada-based recruiter focused on blockchain talent acquisition. So the company has to close down.

Evelyn Cheng | @chengevelyn

Published 11:45 AM ET Fri, 4 May 2018 | Updated 2:04 PM ET Fri, 4 May 2018

CNBC

Horizon 2020 Existing EU Projects on Blockchain

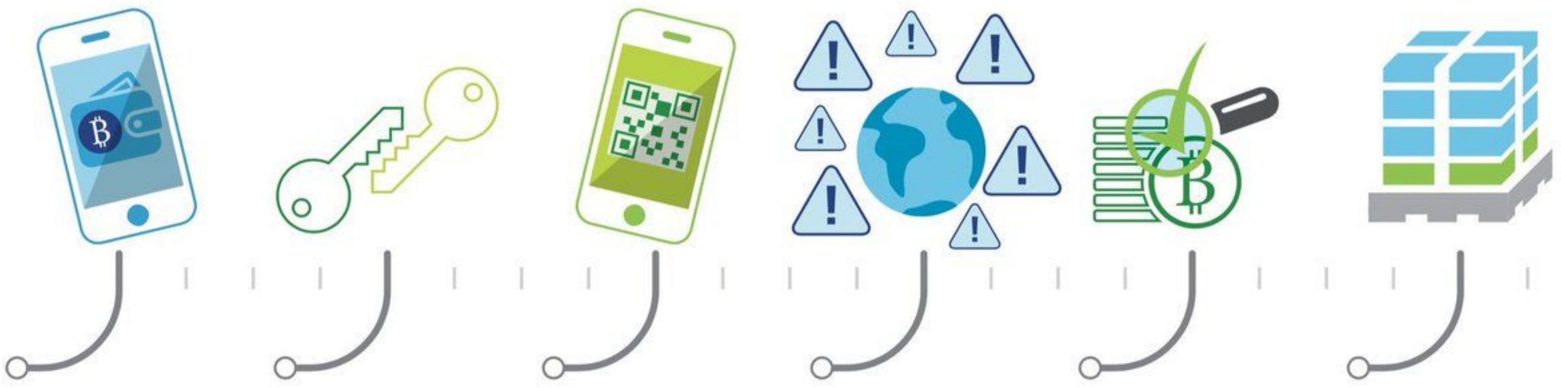
* D-CENT (social money for democratic societies)/EU-funding ended in May 2016- https://dcentproject.eu/
* DECODE (decentralised management architecture)- https://www.decodeproject.eu/
* MyHealthMyData (blockchain for health and patient-centric system)- http://www.myhealthmydata.eu/
* Bloomend (blockchains for social media)- http://cordis.europa.eu/project/rcn/211092_en.html
* SUnFISH- http://www.sunfishproject.eu
* Symbiote- https://www.symbiote-h2020.eu
* GHOST- http://cordis.europa.eu/project/rcn/210233_en.html
* BlockchainKYC (Iceland)- http://cordis.europa.eu/project/rcn/211172_en.html
* Signaturit (Spain)- http://cordis.europa.eu/project/rcn/205049_en.html
* Billon (Poland)- http://cordis.europa.eu/project/rcn/212243_en.html
* BROS- http://cordis.europa.eu/project/rcn/209037_en.html
* DLInnociate- http://cordis.europa.eu/project/rcn/209748_en.html
* DEFENDER- http://cordis.europa.eu/project/rcn/210231_en.html
* TITANIUM- http://cordis.europa.eu/project/rcn/209948_en.html
* INTERLACE- http://cordis.europa.eu/project/rcn/209089_en.html
* STOP-IT- http://cordis.europa.eu/project/rcn/210216_en.html
* CHARIOT- http://cordis.europa.eu/project/rcn/212490_en.html

Blockchain Myths (Past & Present)

- Fiat currencies are bad, cryptocurrencies are good
- Bitcoin will become the universal currency replacing all fiat currencies
- Public blockchains provide trust in a completely trustless environment
- Public blockchains are completely decentralized
- Private blockchains are centralized or centrally controlled
- Anyone in a public blockchain can validate any transaction
- Public blockchains are more secure than private 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 for which payments are made)
- Initial Coin Offerings (ICOs) better than IPOs since they enable crowdsourcing of capital

Bitcoin Blockchain

Figure 1. How the Bitcoin blockchain works



Bob owes Alice money for lunch. He installs an app on his smartphone to create a new Bitcoin wallet. A wallet app is like a mobile banking app and a wallet is like a bank account.

To pay her, he needs two pieces of information: his private key and her public key.

Bob gets Alice's public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.*

The app alerts Bitcoin 'miners' around the world of the impending transaction. 'Miners' provide transaction verification services.

The miners verify that Bob has enough bitcoins to make the payment.

Many transactions occur in the network at any time. All the pending transactions in a given timeframe are grouped (in a block) for verification. Each block has a unique identifying number, creation time and reference to the previous block.

*Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.

Graphic: Deloitte University Press. Source: American Banker[20]

Worries ONLY about money transfers being valid (money exists to send and no double spend)

without considering the full cycle of receiving goods/services for which payments are made!!

Bitcoin & Other Cryptocurrencies

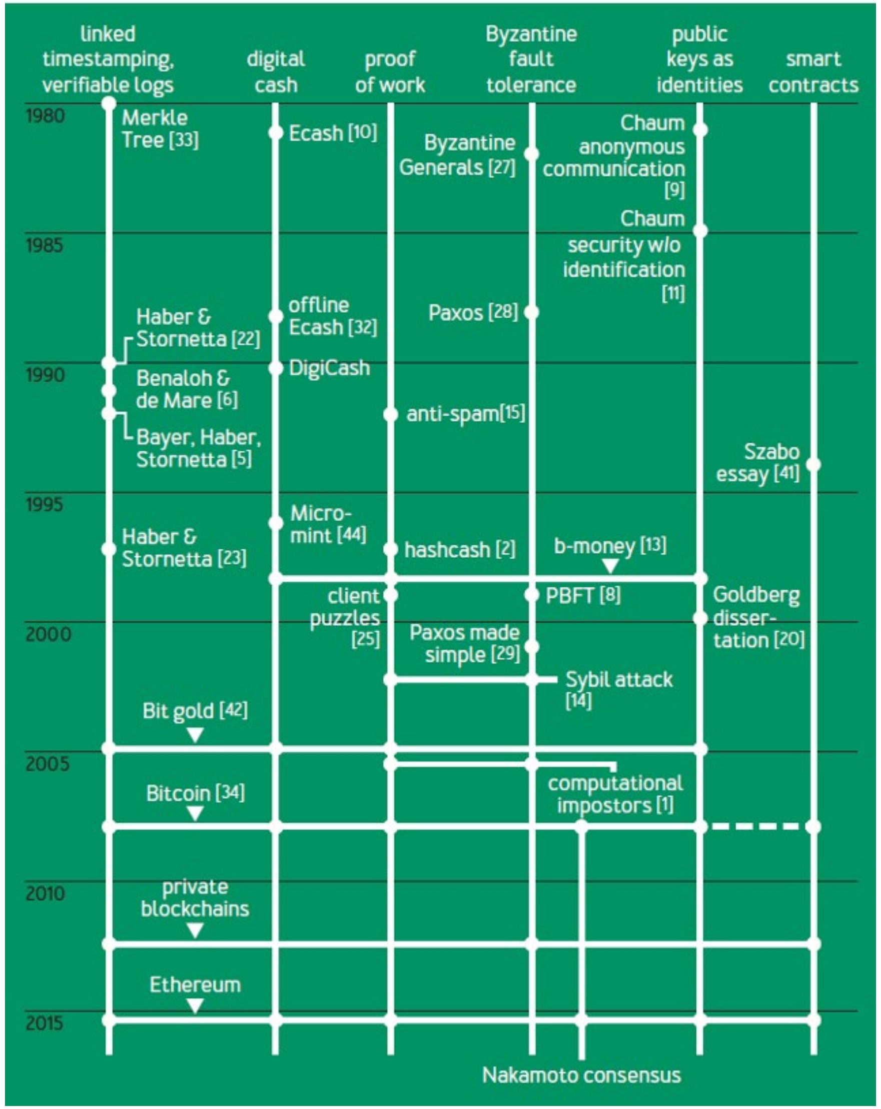
http://bit.ly/HFpapr

UTXO Cryptocurrencies

- **Unspent Transaction Output (UTXO)**: Data model introduced by Bitcoin - also used by many other cryptocurrencies and distributed applications (**DApps**)
- UTXO represents each step in the evolution of a data object as a separate atomic state on the ledger
- Such a state is created by a transaction and destroyed/consumed by another unique transaction occurring later
- Every given transaction destroys a number of **input states** and creates one or more **output states**
- A “coin” in Bitcoin is initially created by a **coinbase transaction** that rewards the “miner” of a block. This appears on the ledger as a coin state designating the miner as the owner.
- Any coin can be spent in the sense that the coin is assigned to a new owner by a transaction that atomically destroys the current coin state designating the previous owner and creates another coin state representing the new owner
- Value in the UTXO model is transferred through transactions that refer to several input states that all belong to the entity issuing the transaction
- An entity owns a state because the **public key** of the entity is contained in the state itself
- Every transaction creates one/more output states in the KVS representing the new owners, deletes the input states in the KVS, and ensures that the sum of the values in the input states equals the sum of the output states’ values
- There is also a policy determining how value is created (e.g., coinbase transactions in Bitcoin or specific mint operations in other systems) or destroyed

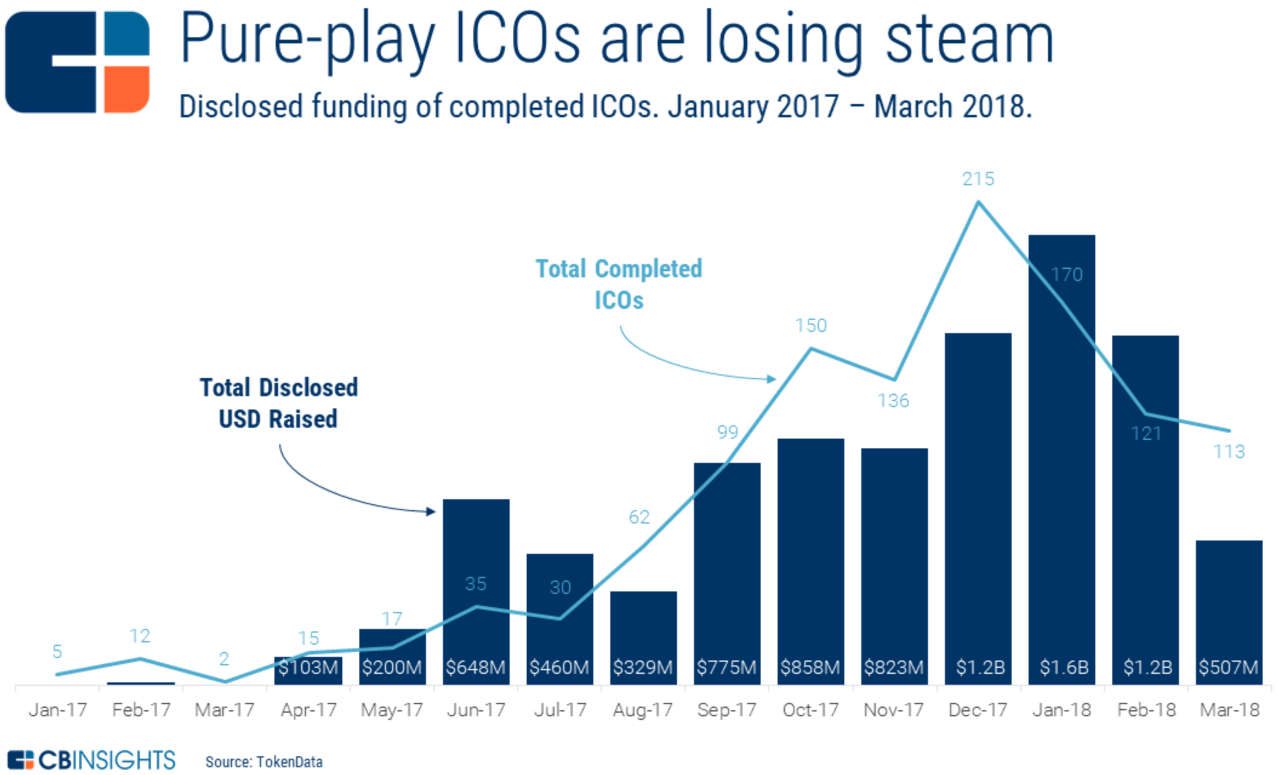
Bitcoin’s Academic Pedigree

FIGURE 1: CHRONOLOGY OF KEY IDEAS FOUND IN BITCOIN



Arvind Narayanan, Jeremy Clark
ACM Queue, August 2017

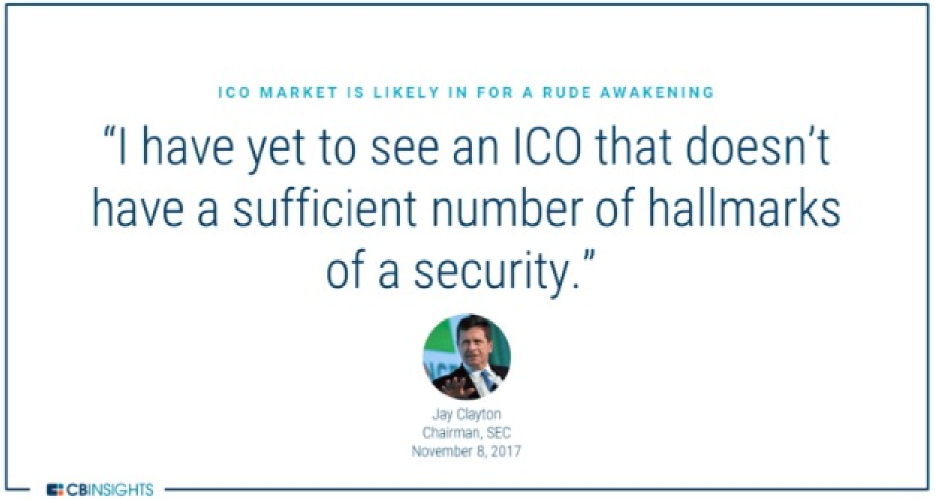
Cryptoassets & ICOs



Pure-play ICOs are losing steam

Disclosed funding of completed ICOs. January 2017 – March 2018.

CBINSIGHTS Source: TokenData



ICO MARKET IS LIKELY IN FOR A RUDE AWAKENING

"I have yet to see an ICO that doesn't have a sufficient number of hallmarks of a security."

Jay Clayton
Chairman, SEC
November 8, 2017

CBINSIGHTS

- CFTC considers cryptoassets to be commodity
- FinCEN as money
- SEC as security (Bitcoin/Ether excepted)
- IRS as property

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

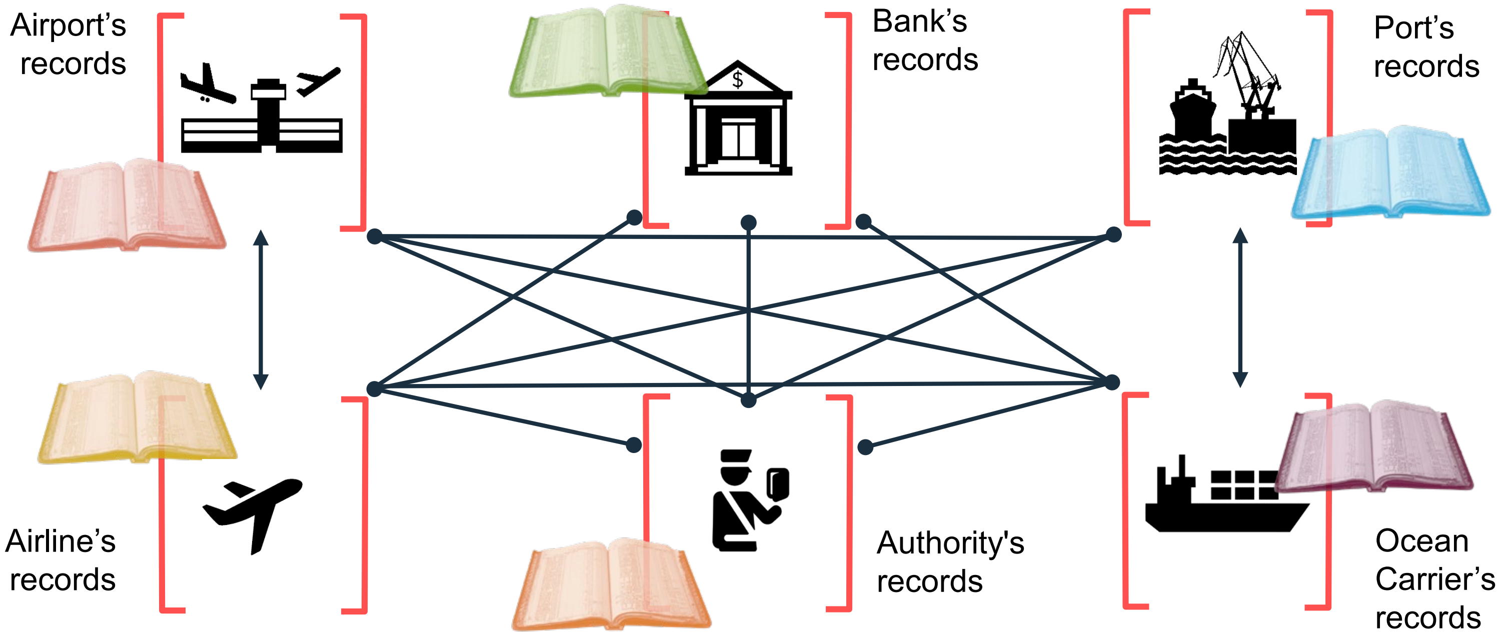
- Distributed operating systems
- Distributed virtual memory
- Message passing in distributed computations and distributed checkpoints
- Clock synchronization and event ordering (e.g., Lamport clocks)
- Byzantine agreement and distributed consensus
- Two phase commit optimizations (e.g., Presumed Abort)
- (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
- …

Problem Being Solved (e.g., Export Import Scenario)

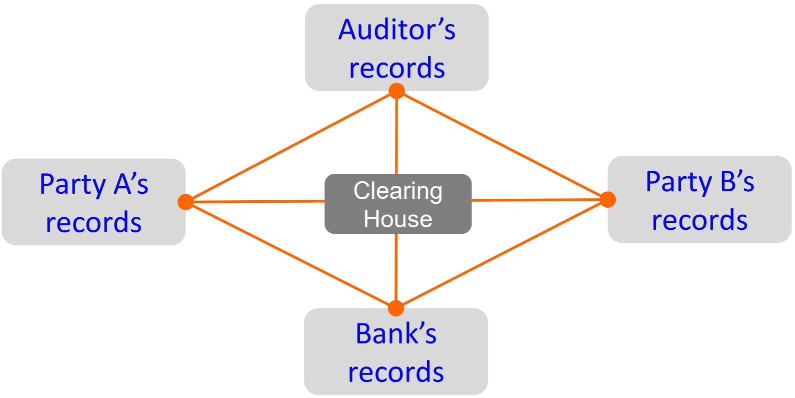
Recording of events is becoming much more complex…



… Inefficient, expensive, vulnerable, lack of transparency

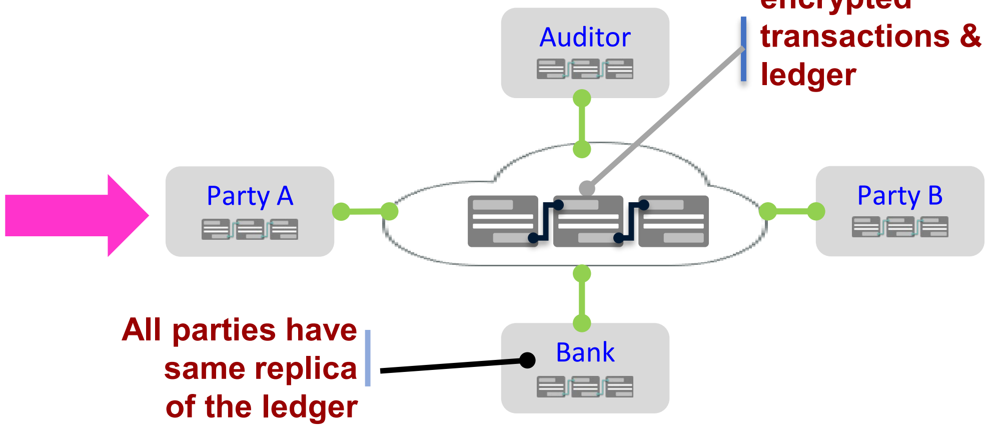
Basic Change to Business Processes

Traditional Way



… Inefficient, expensive, vulnerable

Blockchain Way

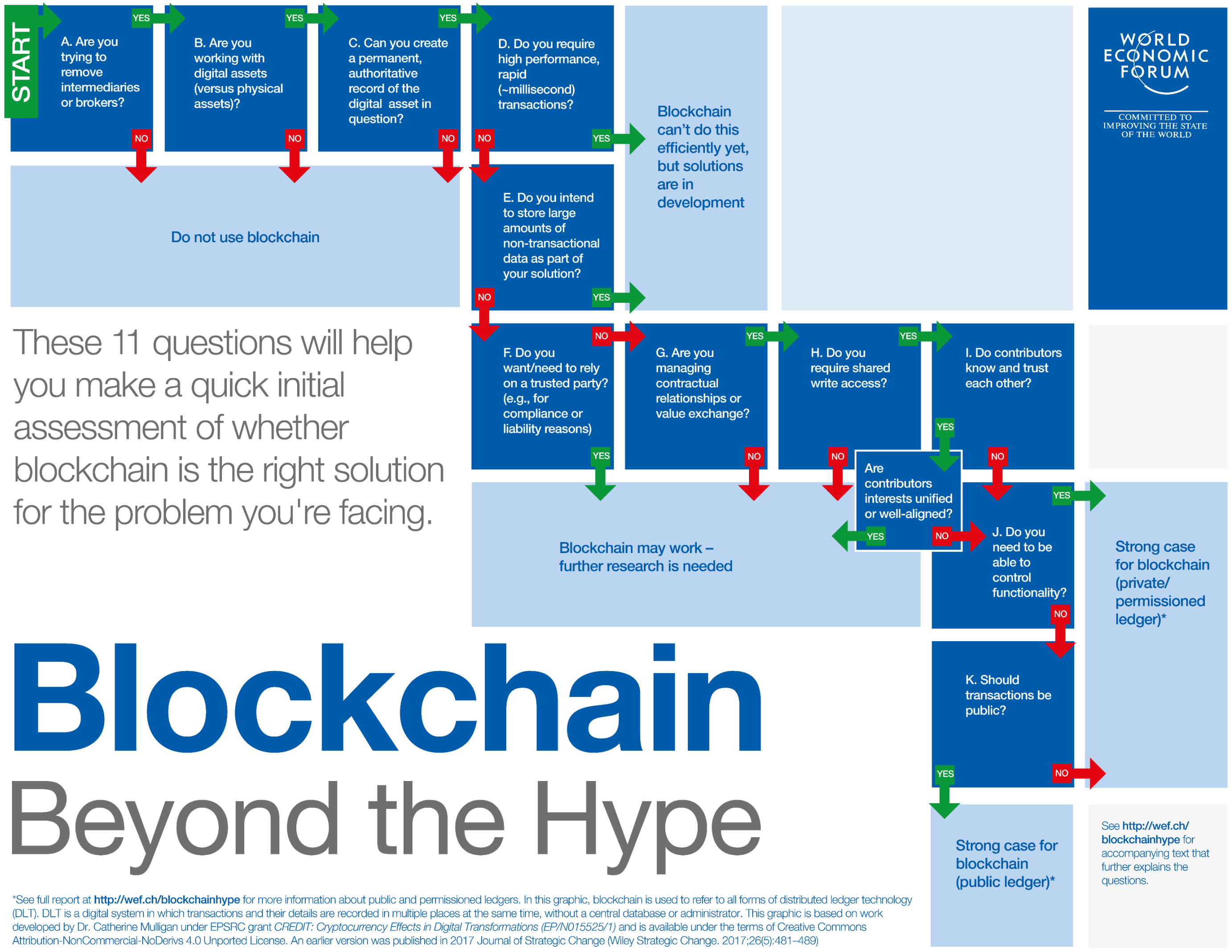


Digitally signed, encrypted transactions & ledger

All parties have same replica of the ledger

… Consensus, provenance, immutability, finality

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



START

A. Are you trying to remove intermediaries or brokers?

B. Are you working with digital assets (versus physical assets)?

C. Can you create a permanent, authoritative record of the digital asset in question?

D. Do you require high performance, rapid (~millisecond) transactions?

Blockchain can't do this efficiently yet, but solutions are in development

Do not use blockchain

E. Do you intend to store large amounts of non-transactional data as part of your solution?

F. Do you want/need to rely on a trusted party? (e.g., for compliance or liability reasons)

G. Are you managing contractual relationships or value exchange?

H. Do you require shared write access?

I. Do contributors know and trust each other?

Are contributors interests unified or well-aligned?

J. Do you need to be able to control functionality?

K. Should transactions be public?

Blockchain may work – further research is needed

Strong case for blockchain (private/ permissioned ledger)*

Strong case for blockchain (public ledger)*

These 11 questions will help you make a quick initial assessment of whether blockchain is the right solution for the problem you're facing.

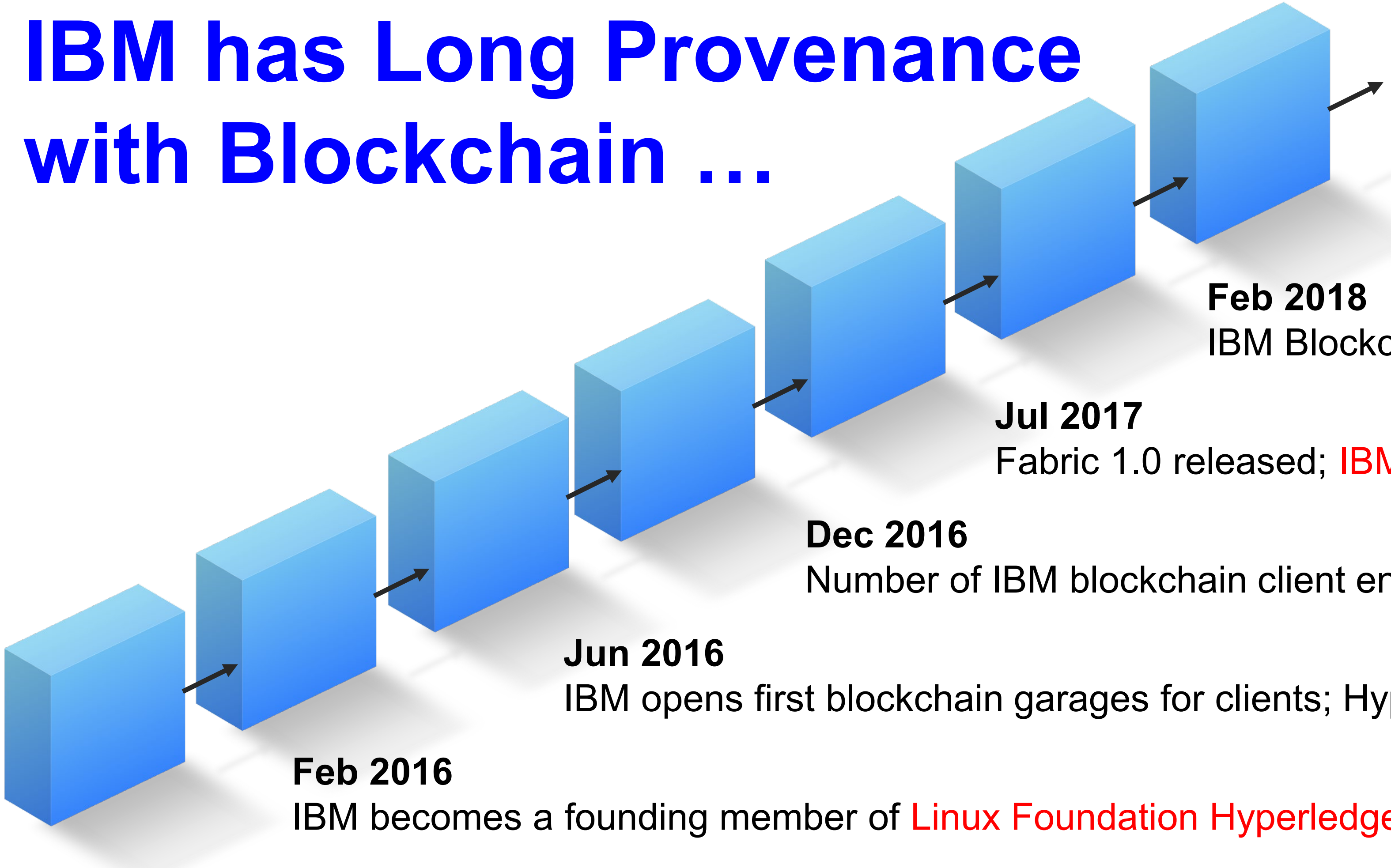
See http://wef.ch/ blockchainhype for accompanying text that further explains the questions.

Blockchain
Beyond the Hype

*See full report at http://wef.ch/blockchainhype for more information about public and permissioned ledgers. In this graphic, blockchain is used to refer to all forms of distributed ledger technology (DLT). DLT is a digital system in which transactions and their details are recorded in multiple places at the same time, without a central database or administrator. This graphic is based on work developed by Dr. Catherine Mulligan under EPSRC grant *CREDIT: Cryptocurrency Effects in Digital Transformations (EP/N015525/1)* and is available under the terms of Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Unported License. An earlier version was published in 2017 Journal of Strategic Change (Wiley Strategic Change. 2017;26(5):481–489)

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

IBM has Long Provenance with Blockchain …



Aug 2015
IBM starts developing first prototype of blockchain technology (Open Blockchain); first client engagements

Feb 2016
IBM becomes a founding member of Linux Foundation Hyperledger; donates code and IP

Jun 2016
IBM opens first blockchain garages for clients; Hyperledger Fabric v0.6 released

Dec 2016
Number of IBM blockchain client engagements now totals over 400

Jul 2017
Fabric 1.0 released; IBM Blockchain Platform announced soon after

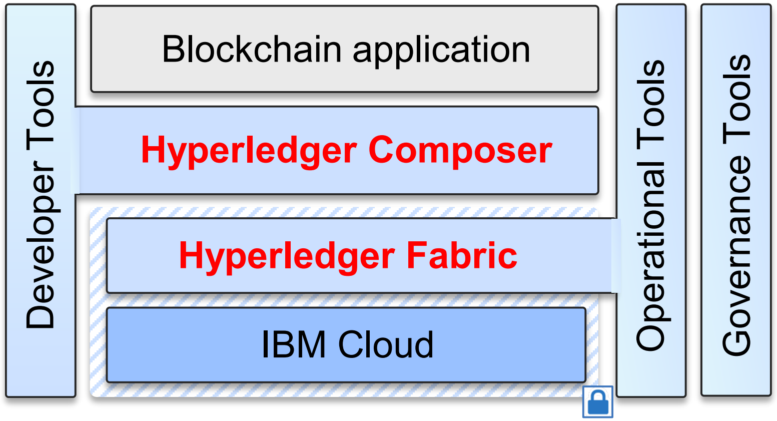
Feb 2018
IBM Blockchain Platform Starter Plan announced @ **THINK**

Jun 2018
IBM Blockchain Platform updated to Fabric 1.1

BaaS: IBM Blockchain Platform (IBP)

IBM Blockchain Platform is a fully integrated enterprise-ready blockchain platform designed to accelerate the development, governance, and operation of a multi-institution business network

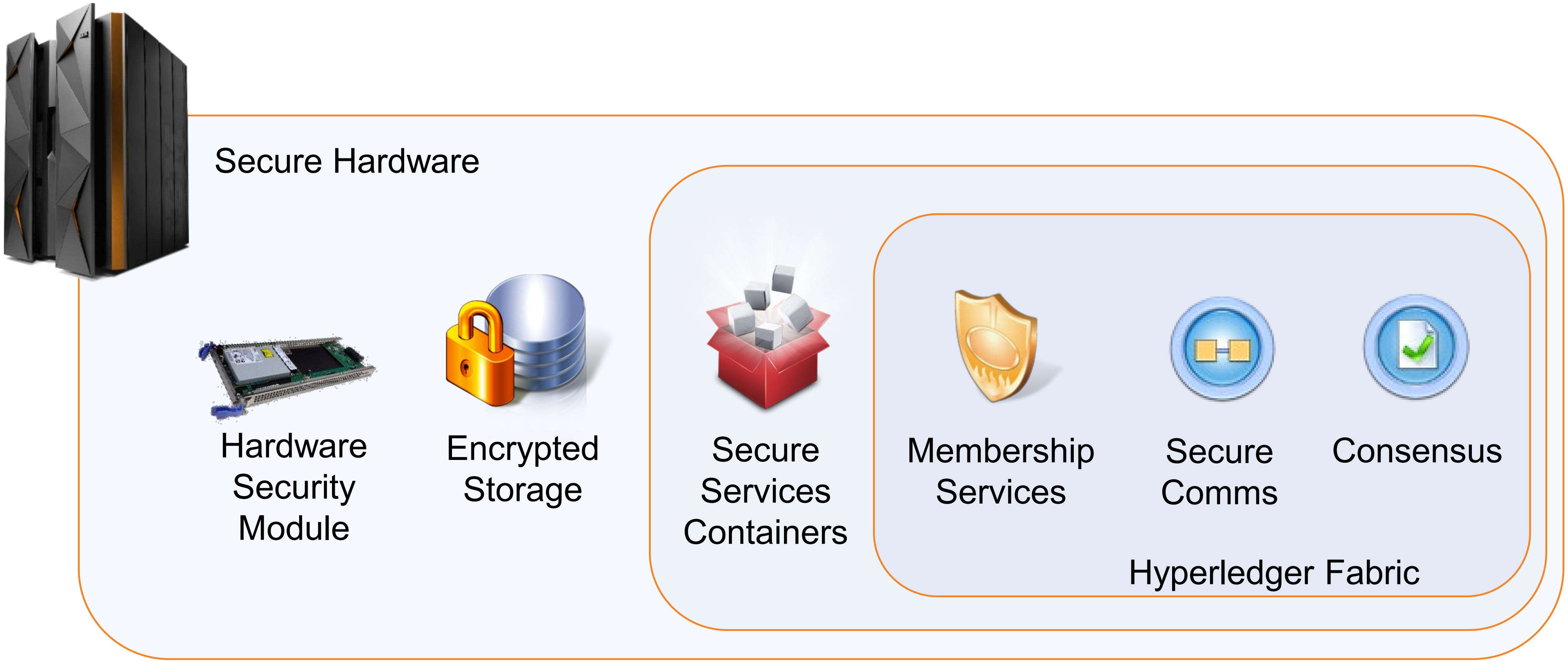
- **Developer tools** that make use of Hyperledger Composer to quickly build your blockchain application
- Hyperledger Fabric provides the ledger; managed through a set of intuitive **operational tools**
- **Governance tools** for democratic management of the business network
- Flexible deployment options, including a highly secure and performant **IBM Cloud** environment



5/2018: IBM Introduces 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)

IBP: Security at Each Architecture Layer



Secure Hardware

Hardware Security Module

Encrypted Storage

Secure Services Containers

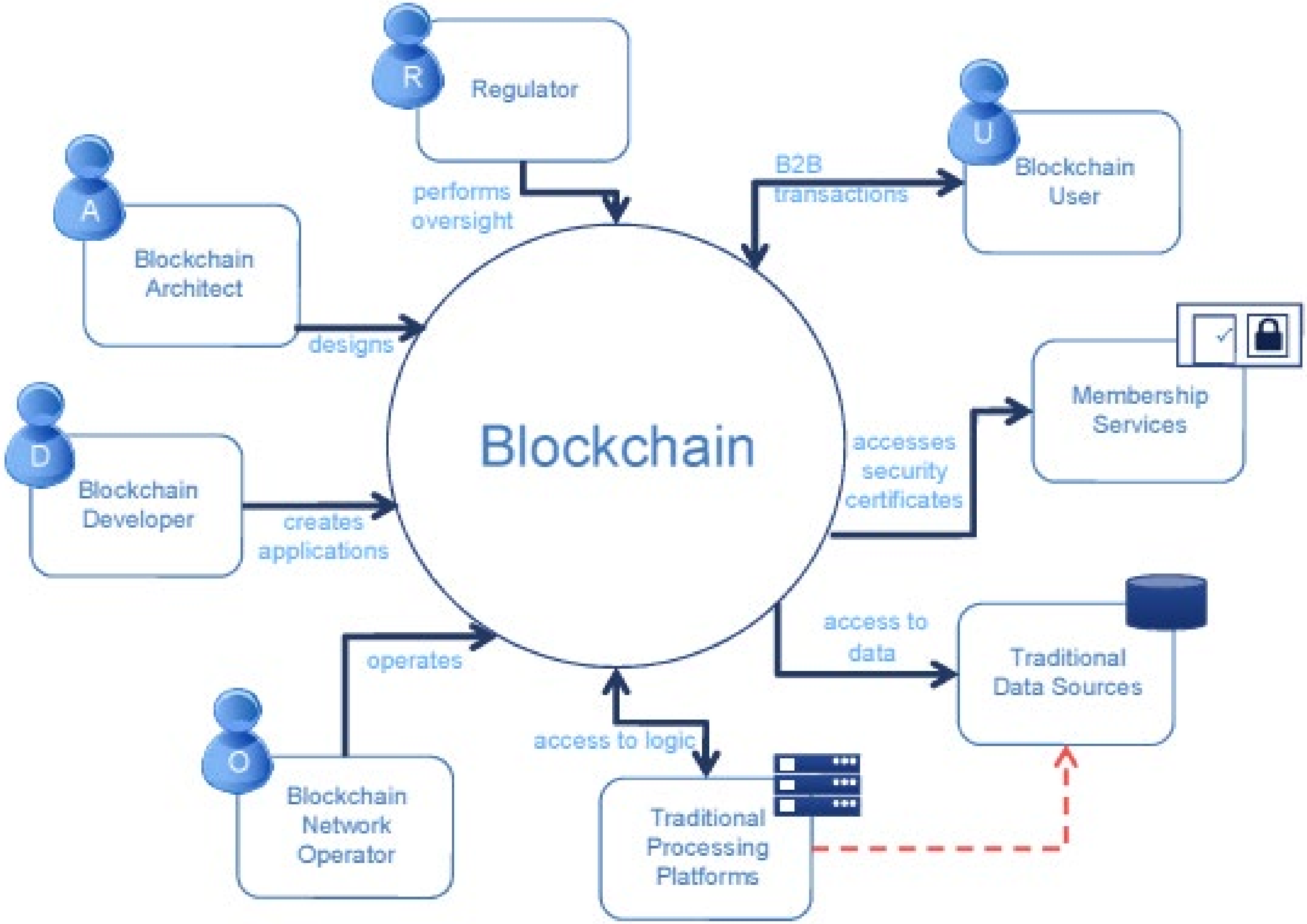
Membership Services

Secure Comms

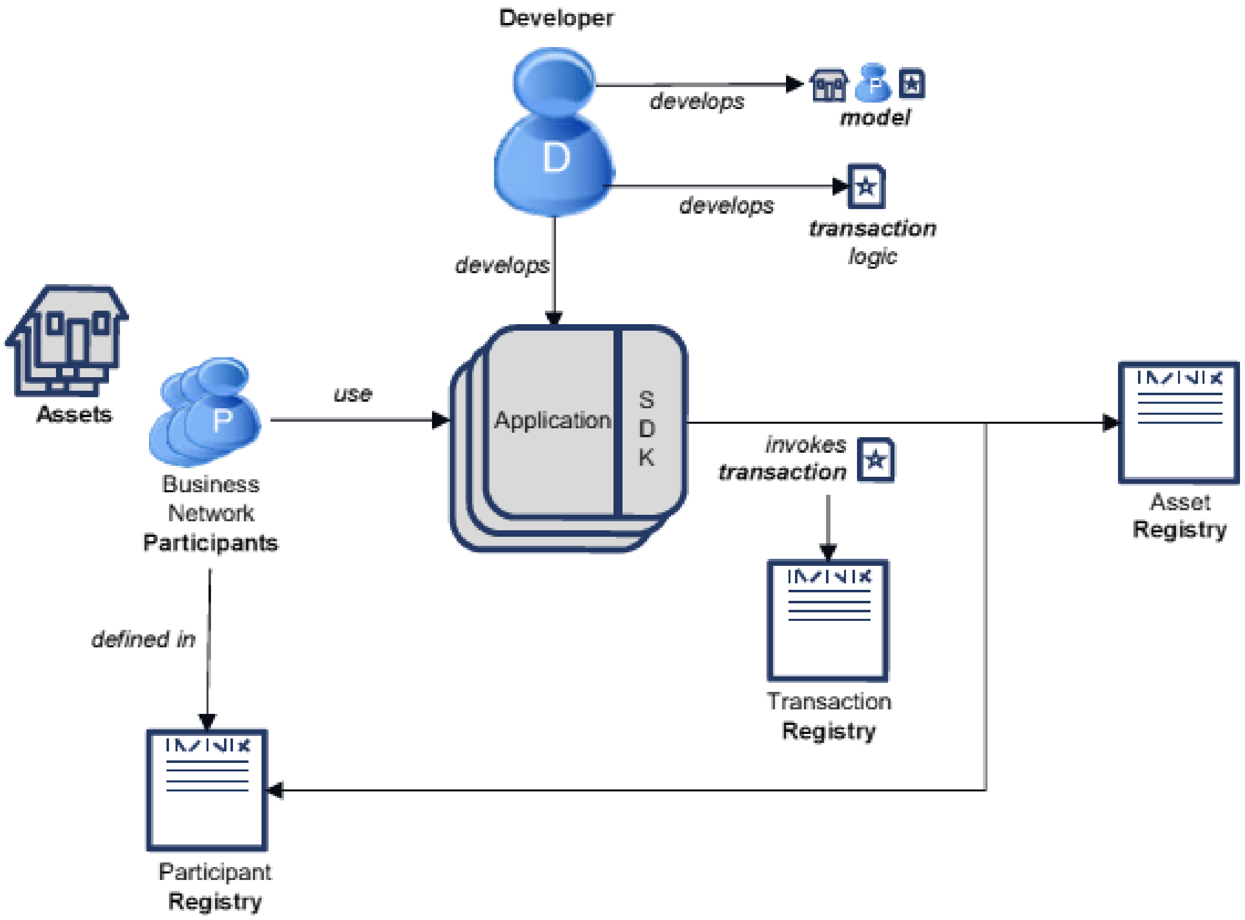
Consensus

Hyperledger Fabric

Actors in a Blockchain Solution



Composer: Workflow of Building a Model



IBM Blockchain Engagements

Making Blockchain Real for Business with > 400 Engagements & Multiple Production Networks

Trade Finance

Digital Trade Chain
MIZUHO
NATIXIS
TRAFIGURA

Pre and Post Trade

DTCC
CLS Fundamental to FX
Bolsa Comercio SANTIAGO
JPX

Complex Risk Coverage

AIG
Standard Chartered

Identity/ Know your customer (KYC)

SECURE KEY
Crédit Mutuel ARKEA
DIACC

Unlisted Securities/ Private Equity Funds

NORTHERN TRUST
BORSA ITALIANA
SBI GROUP SBI証券

Loyalty Program

UnionPay 银联

Medicated Health Data Exchange

FDA

Fraud/ Compliance Registry

دبـــي الذكية
SMART DUBAI

Distributed Energy/ Carbon Credit

TenneT
ENERGY BLOCKCHAIN LABS

Supply Chain

MÆRSK
PSA The World's Port of Call

Food Safety

Walmart
Driscoll's Only the Finest Berries
Tyson
McLANE
Dole
Kroger
Nestlé
Unilever
gsf golden state foods
Mc

Provenance/ Traceability

everledger

Food Trust/Safety

What?

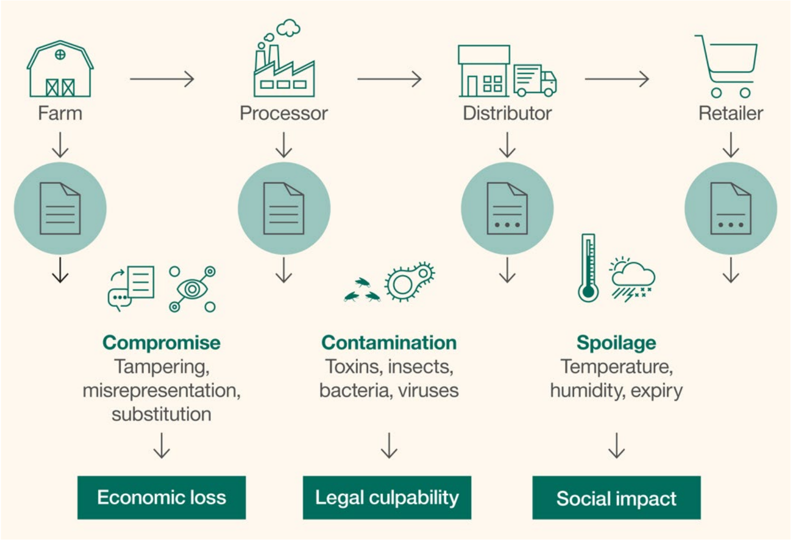
- Provide trusted source of information and traceability to improve transparency and efficiency across food network

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



TradeLens: Global Trade Digitization

What?

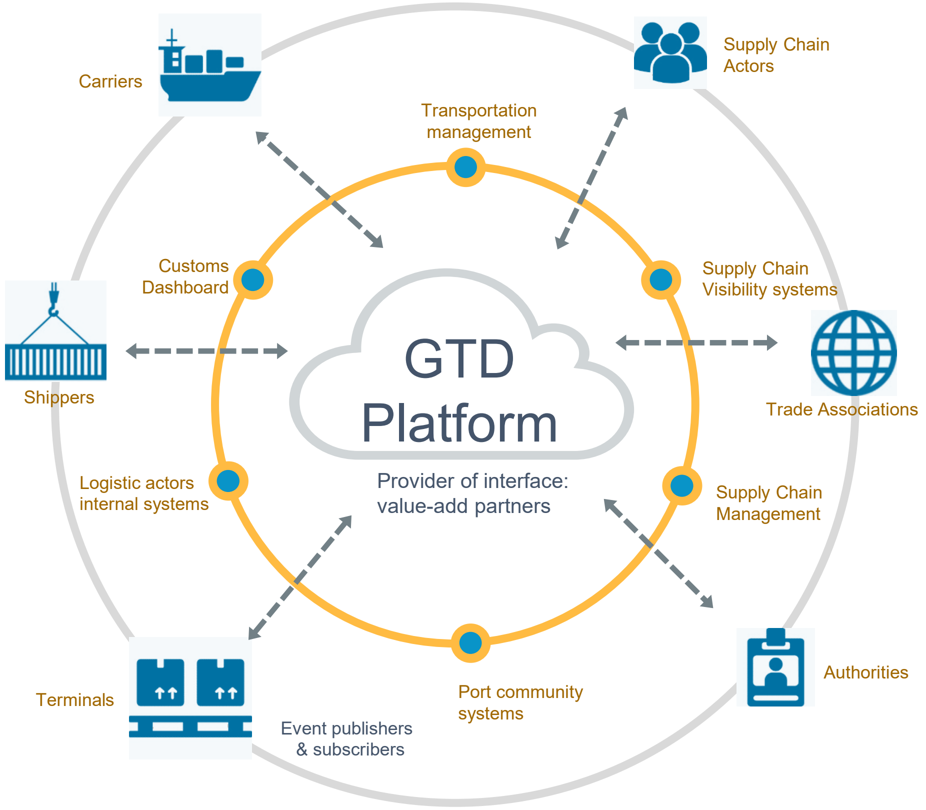
- An open, extensible platform for sharing shipping events, messages, and documents across all the actors and systems in the supply chain ecosystem.

How?

- Providing Shared Visibility and Shared State for Container Shipments

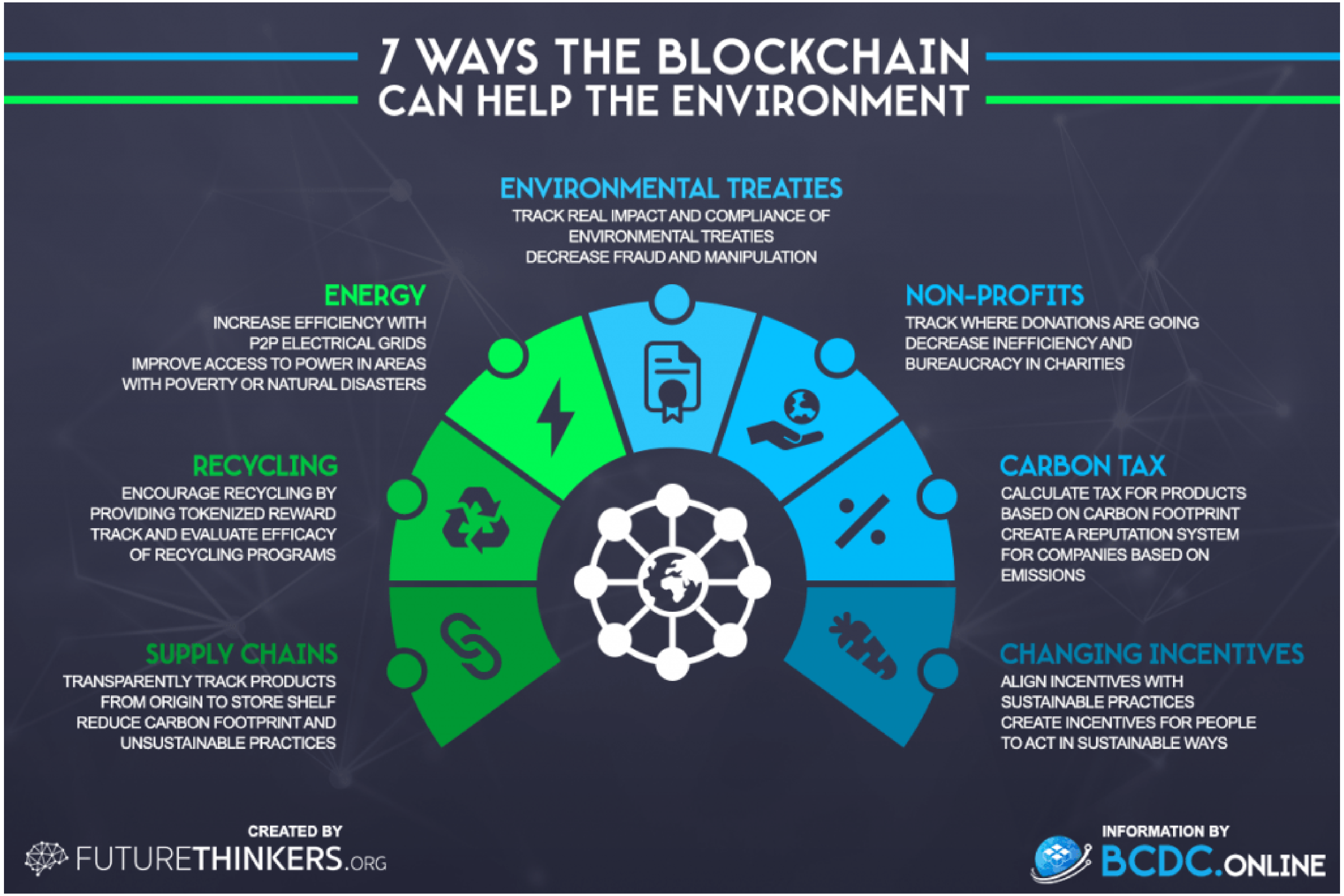
Benefits

- Increase speed and transparency for cross border transactions through real time access to container events.
- Reduced cost and increased efficiency through paperless trade



Carriers
Supply Chain Actors
Transportation management
Customs Dashboard
Supply Chain Visibility systems
Shippers
GTD Platform
Trade Associations
Provider of interface: value-add partners
Logistic actors internal systems
Supply Chain Management
Terminals
Event publishers & subscribers
Port community systems
Authorities

Blockchain & The Environment



7 WAYS THE BLOCKCHAIN CAN HELP THE ENVIRONMENT

ENVIRONMENTAL TREATIES

TRACK REAL IMPACT AND COMPLIANCE OF ENVIRONMENTAL TREATIES
DECREASE FRAUD AND MANIPULATION

ENERGY

INCREASE EFFICIENCY WITH P2P ELECTRICAL GRIDS
IMPROVE ACCESS TO POWER IN AREAS WITH POVERTY OR NATURAL DISASTERS

NON-PROFITS

TRACK WHERE DONATIONS ARE GOING
DECREASE INEFFICIENCY AND BUREAUCRACY IN CHARITIES

RECYCLING

ENCOURAGE RECYCLING BY PROVIDING TOKENIZED REWARD
TRACK AND EVALUATE EFFICACY OF RECYCLING PROGRAMS

CARBON TAX

CALCULATE TAX FOR PRODUCTS BASED ON CARBON FOOTPRINT
CREATE A REPUTATION SYSTEM FOR COMPANIES BASED ON EMISSIONS

SUPPLY CHAINS

TRANSPARENTLY TRACK PRODUCTS FROM ORIGIN TO STORE SHELF
REDUCE CARBON FOOTPRINT AND UNSUSTAINABLE PRACTICES

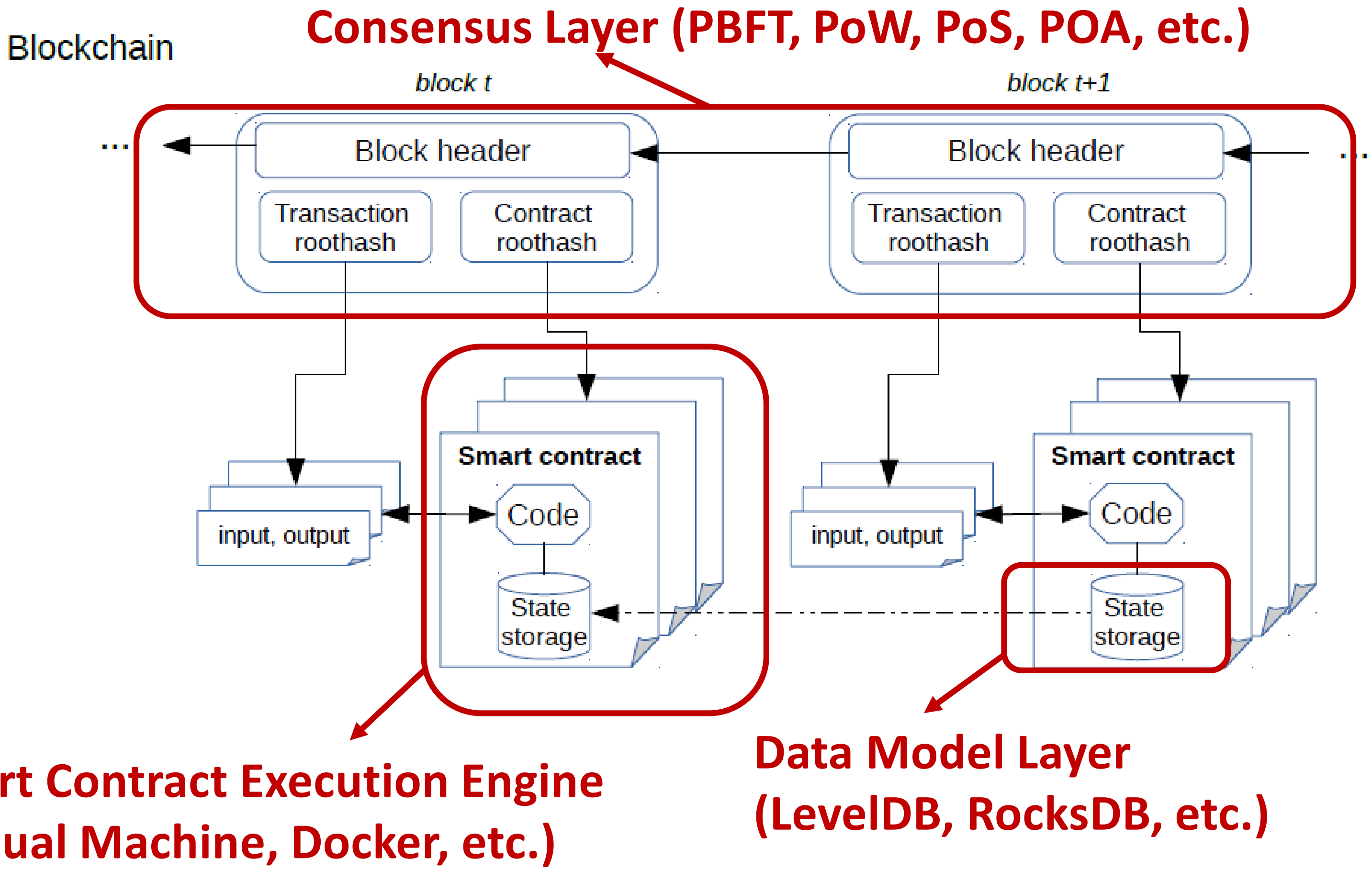
CHANGING INCENTIVES

ALIGN INCENTIVES WITH SUSTAINABLE PRACTICES
CREATE INCENTIVES FOR PEOPLE TO ACT IN SUSTAINABLE WAYS

CREATED BY FUTURETHINKERS.ORG

INFORMATION BY BCDC.ONLINE

BC Software Stack



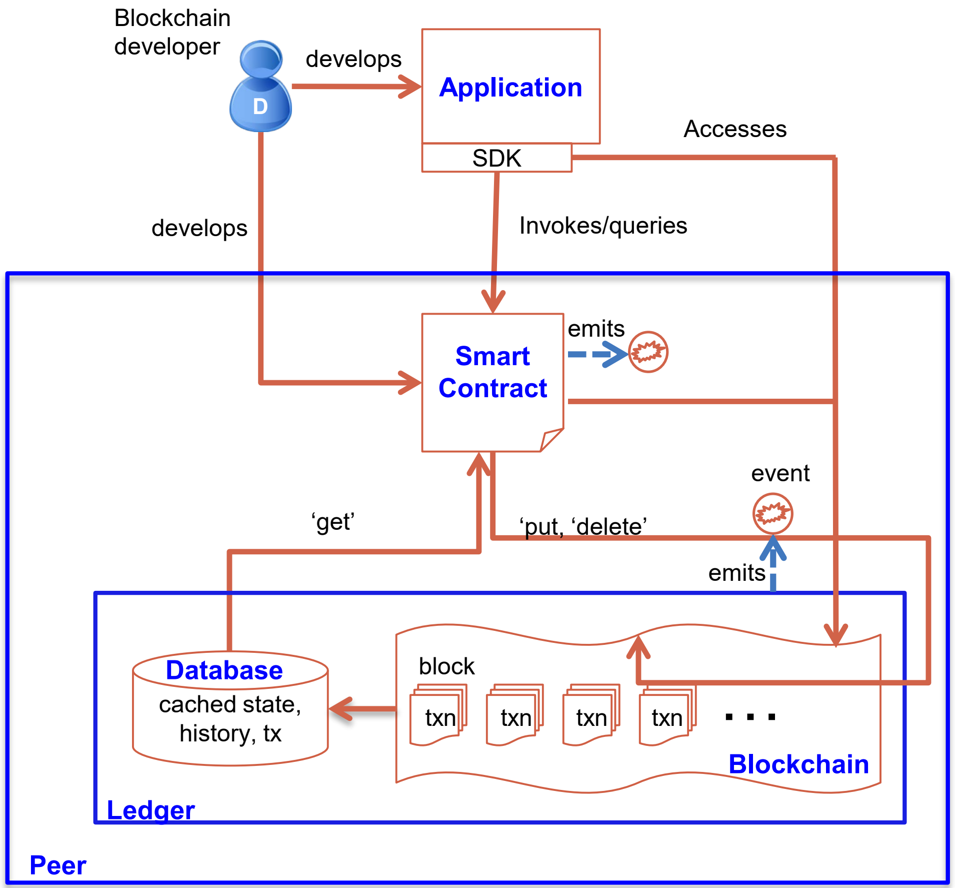
Source: Anh Dinh, et al., SIGMOD 2017

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.

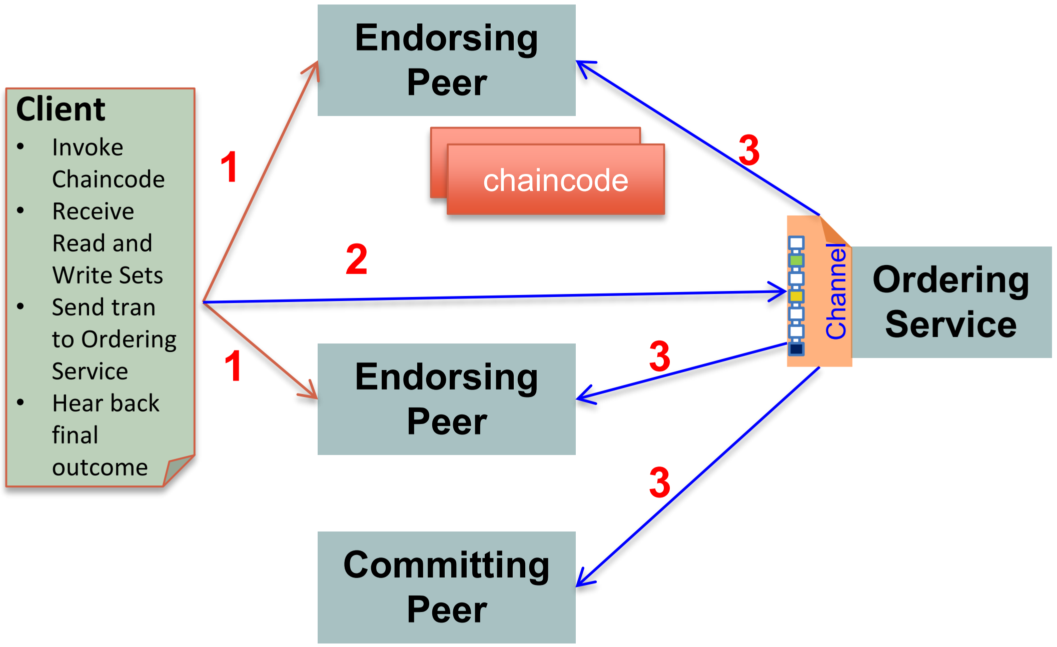
Overview of Application Flow (Fabric)



- 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

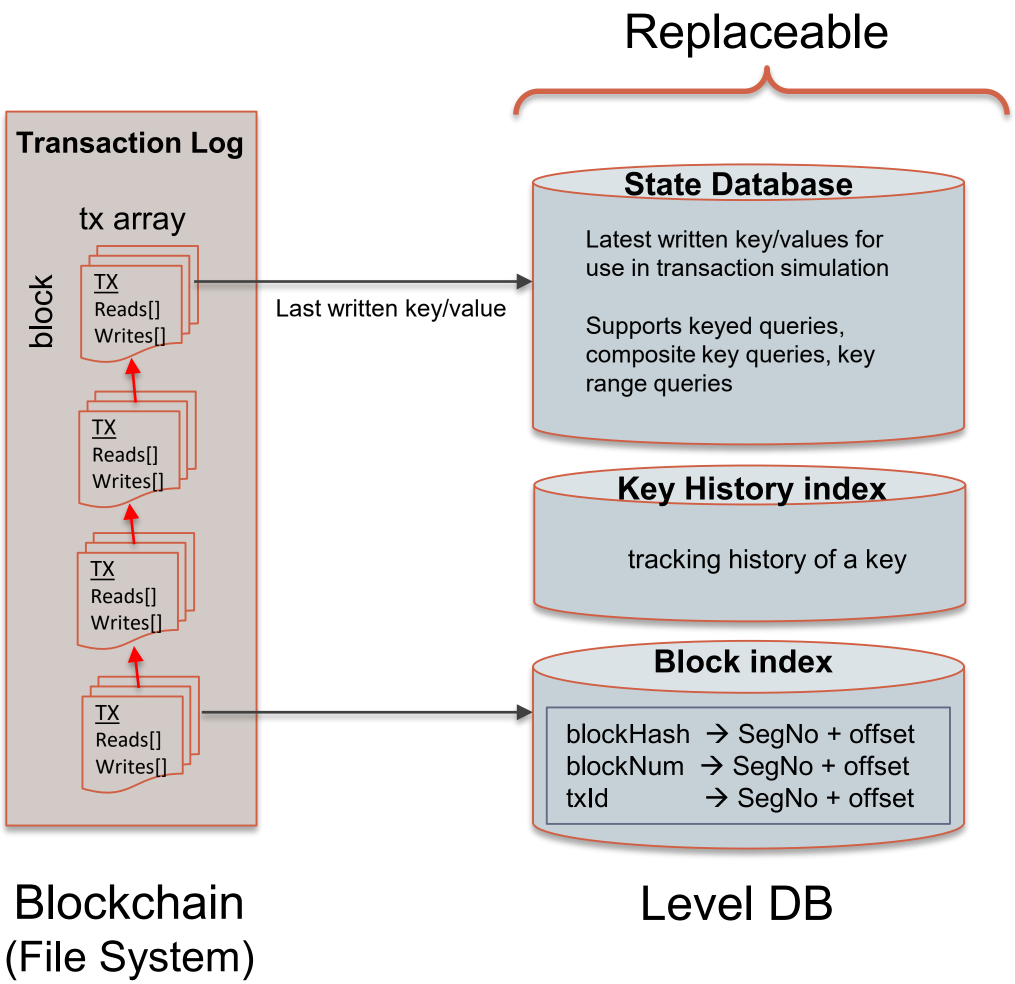
Endorsement, Ordering, Validation/Commit



- 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)

Fabric V1 Ledger



CouchDB (external option) supports keyed queries, composite key queries, key range queries, plus full data rich queries (beta in 1.0)

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

Ethereum

- Public blockchain system like Bitcoin
  - Extends it with Smart Contracts
  - Uses PoW for consensus
  - Own machine lang & VM
  - *gas* charging!
- Most apps relate to its currency Ether
- *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
- **Quorum** from JPMorgan; Support for PBFT added in 7/2017 by AMIS

Hyperledger: A Linux Foundation Project

- A collaborative effort created to advance cross-industry blockchain technologies for business
- Founded February 2016; now more than 230 member organizations
- Open source, open standards, open governance
- Five frameworks and five tools projects
- IBM is a premier member of Hyperledger

Hyperledger Momentum

2 years since launch

47k+ Commits

5 Tools

5 Frameworks

2 Production Releases **Hyperledger Fabric v1.1 Sawtooth v1.0**

230+ Members (30+ in China)

12 Active Community Working Groups

110+ Meetups Worldwide

30k+ Meetup Participants

500+ Developers

HYPERLEDGER SAWTOOTH

HYPERLEDGER FABRIC

HYPERLEDGER IROHA

HYPERLEDGER INDY

Hyperledger Burrow

HYPERLEDGER QUILT

Hyperledger Composer

Hyperledger Cello

Hyperledger Caliper

HYPERLEDGER EXPLORER

www.hyperledger.org

Hyperledger Fabric Project

- Initiated by IBM with IBM open source ledger contribution (Feb 2016)
  http://hyperledger-fabric.readthedocs.io/en/latest/
- Significant change in architecture from V0.6 to V1
  - Smart contract trust flexibility
  - Channel concept for Scalability & Confidentiality enhancement
  - Consensus modularity
  - Pluggable State DB APIs
  - 2 types of peer nodes: Endorsing, non-endorsing/committing
- Used PBFT for consensus before V1
- Other Hyperledger Projects: Iroha, Sawtooth, Composer, Quilt, …

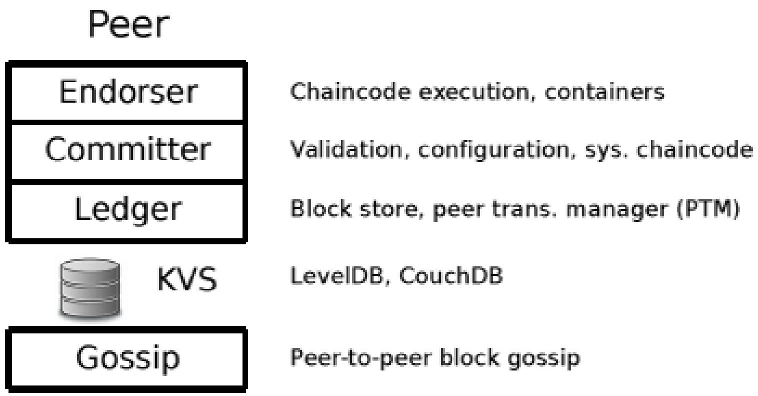

Peer
Endorser
Chaincode execution, containers
Committer
Validation, configuration, sys. chaincode
Ledger
Block store, peer trans. manager (PTM)
KVS
LevelDB, CouchDB
Gossip
Peer-to-peer block gossip

Figure 5: Components of a Fabric peer.

Hyperledger **Premier** members include: Accenture, Airbus, American Express, Baidu, Change Healthcare, Cisco, CME Group, Deutsche Bank, Deutsche Borse Group, Daimler, Digital Asset, DTCC, Fujitsu, Hitachi, IBM, Intel, J.P. Morgan, NEC, R3, SAP, Tradeshift and Wanda FFan Technology

Hyperledger Fabric V1 Contributors - Engineers from: Arxan, Cloudsoft, CLS, d20 Technical Services, Depository Trust & Clearing Corporation (DTCC), Digital Asset, Fujitsu, GE, Gemalto, HACERA, Hitachi, Huawei Technologies, Hyperchain, ImpactChoice, IT People, Knoldus, Linux Foundation, Netease, Passkit, State Street Bank, SecureKey, IBM, SAP, Thoughtworks and Wanda Group. There were also contributions from 35 unaffiliated individuals. In total, 159 developers have contributed.

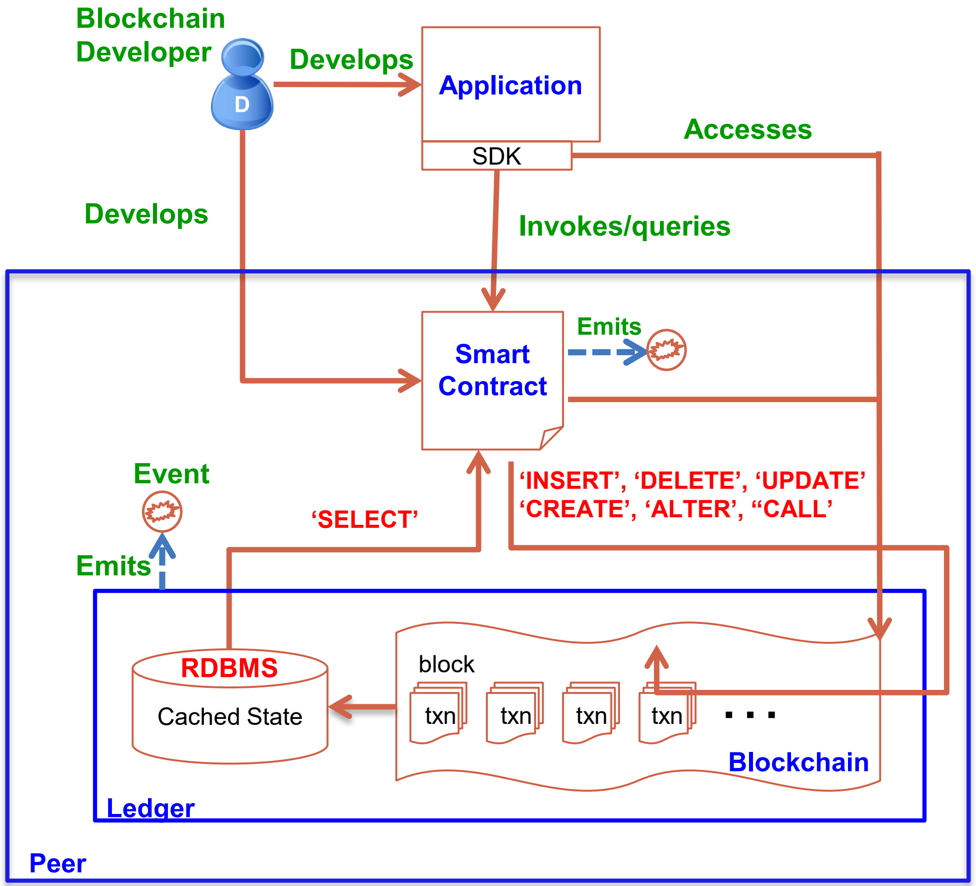
R3 Alliance & Corda

- 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
- Hearn, M. Corda: A distributed ledger, Version 0.5, November 2016. https://docs.corda.net/_static/corda-technical-whitepaper.pdf
- 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

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
- https://sawtooth.hyperledger.org/docs/core/releases/latest/contents.html

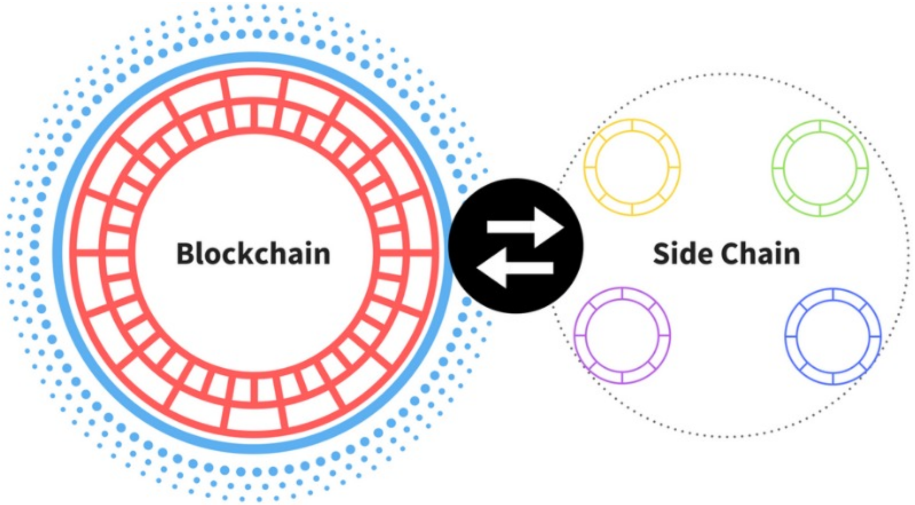
Application Flow with RDBMS (In Progress)



- 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
- 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