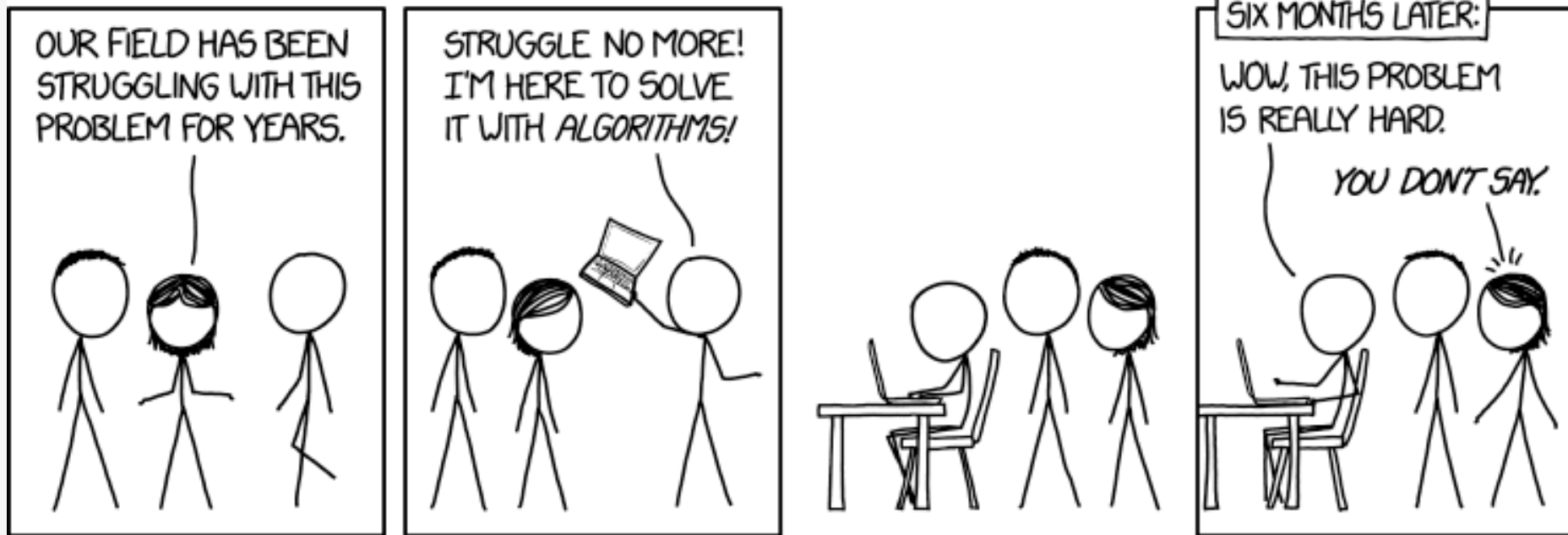# Blockchain Executive Workshop

Marta Piekarska, Director of Ecosystem, Hyperledger

2017

We think that blockchain is magic.

AGENDA FOR TODAY

1. World Before Blockchain

2. Buzzword 1: Decentralization

3. Buzzword 2: Auditability and Traceability

4. Buzzword 3: Immutability

5. Buzzword 4: Public Blockchain

6. Buzzword 5: Business Blockchain

7. Buzzword 6: POC and Pilots

8. No Buzz, just work: where we are, where do we go next?

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Welcome!

Jennifer M. O'Rourke
Illinois Blockchain Business Liaison

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Introduction

Alexandra Prodromos
Bloq, Inc, Research and Marketing Strategist

World Before Blockchain

Marta Piekarska, Director of Ecosystem,
Hyperledger

Beginning of Bitcoin

The roots of Bitcoin are located in the so called "Cypherpunks" movement (see: https://www.wired.com/1993/02/crypto-rebels/), a group of technical-skilled activists, who campaigned for protection of privacy and anonymity in the Cyberspace from the beginning of 1990s onwards (see: "A Cypherpunk's Manifesto" issued by Eric Hughes on March 9, 1993: https://www.activism.net/cypherpunk/manifesto.html). Members of the Cypherpunks were activists like Hal Finney, Nick Szabo, David Chaum, Wei Dai, Phil Zimmermann, Julian Assange and Satoshi Nakamoto, who later developed the Bitcoin.
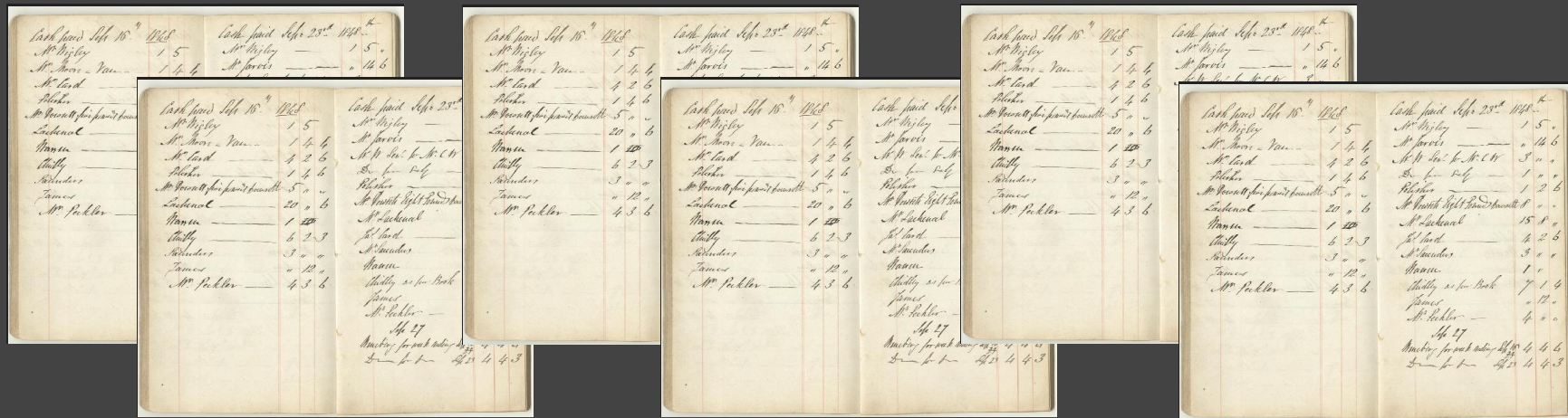
HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

How do we agree on an assets balance?

Traditional Ledgers

In the digital world

There are many copies, that may contain different versions of truth

In the digital world

THE CHALLENGE:
Which one is the real one?!

Now everyone can publish their version
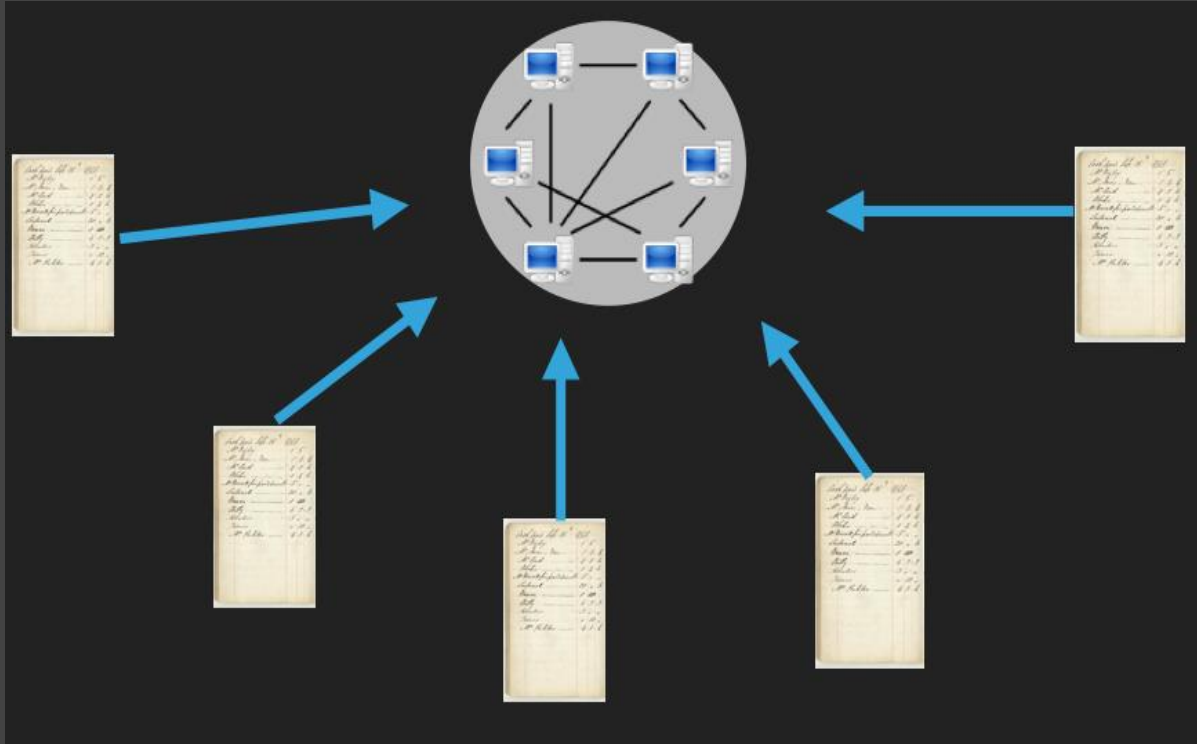
Words you should google

Consensus:
PoW, PoS, POET, Raft, BFT, PBFT

Crypto/Security:
PKI, HASH, SHA-256,
zk-SNARK, HE, ECC,
ECDSA, SGX

Ledger Concepts:
Mining
Blocks
Forks
Parents
Uncles
Merkle Trees

Platform Concepts:
Nodes
Oracles
Notaries
Wallet
Smart Contracts

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Traditional Encryption
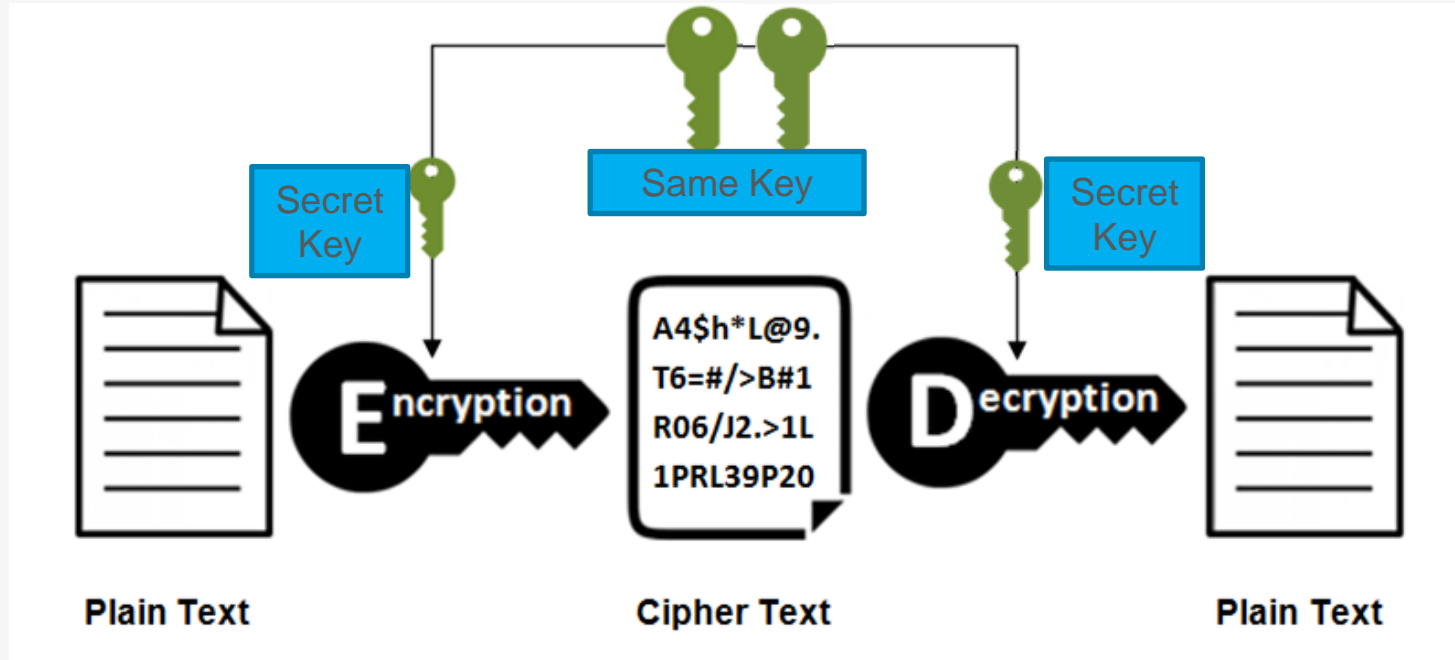
Public Key Cryptography

Plain Text → Encryption → Cipher Text → Decryption → Plain Text

Public Key — Different Keys — Secret Key

A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
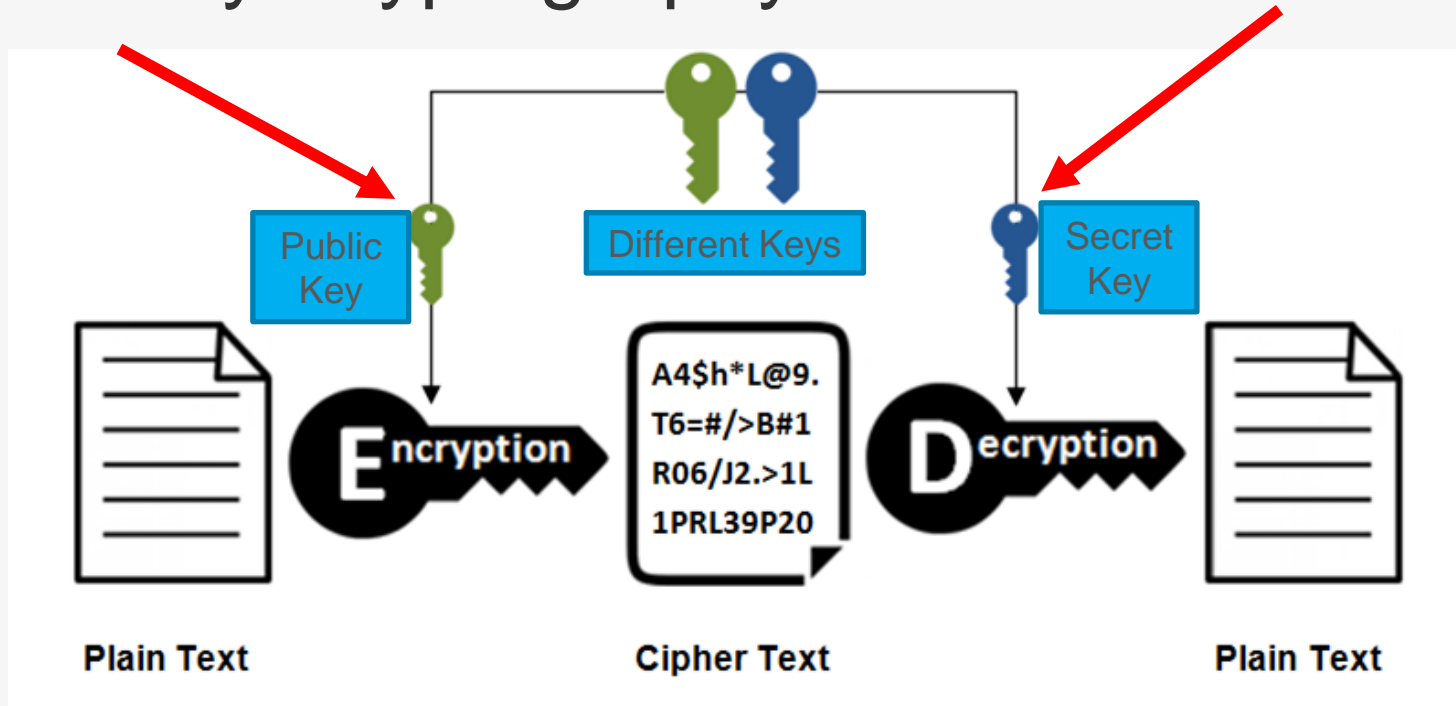
Digital Signatures

Hash Functions

plaintext

hash function

message digest

digest signed with private key

plaintext + signature

private key used for signing
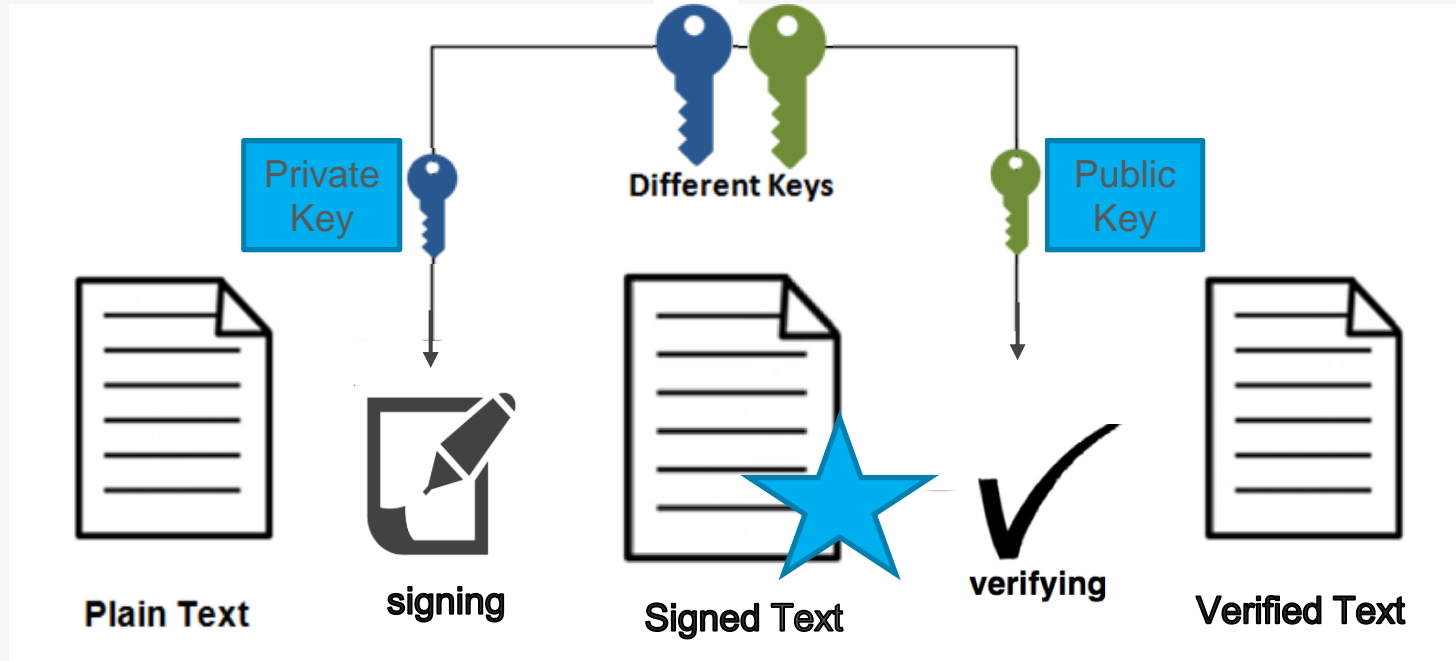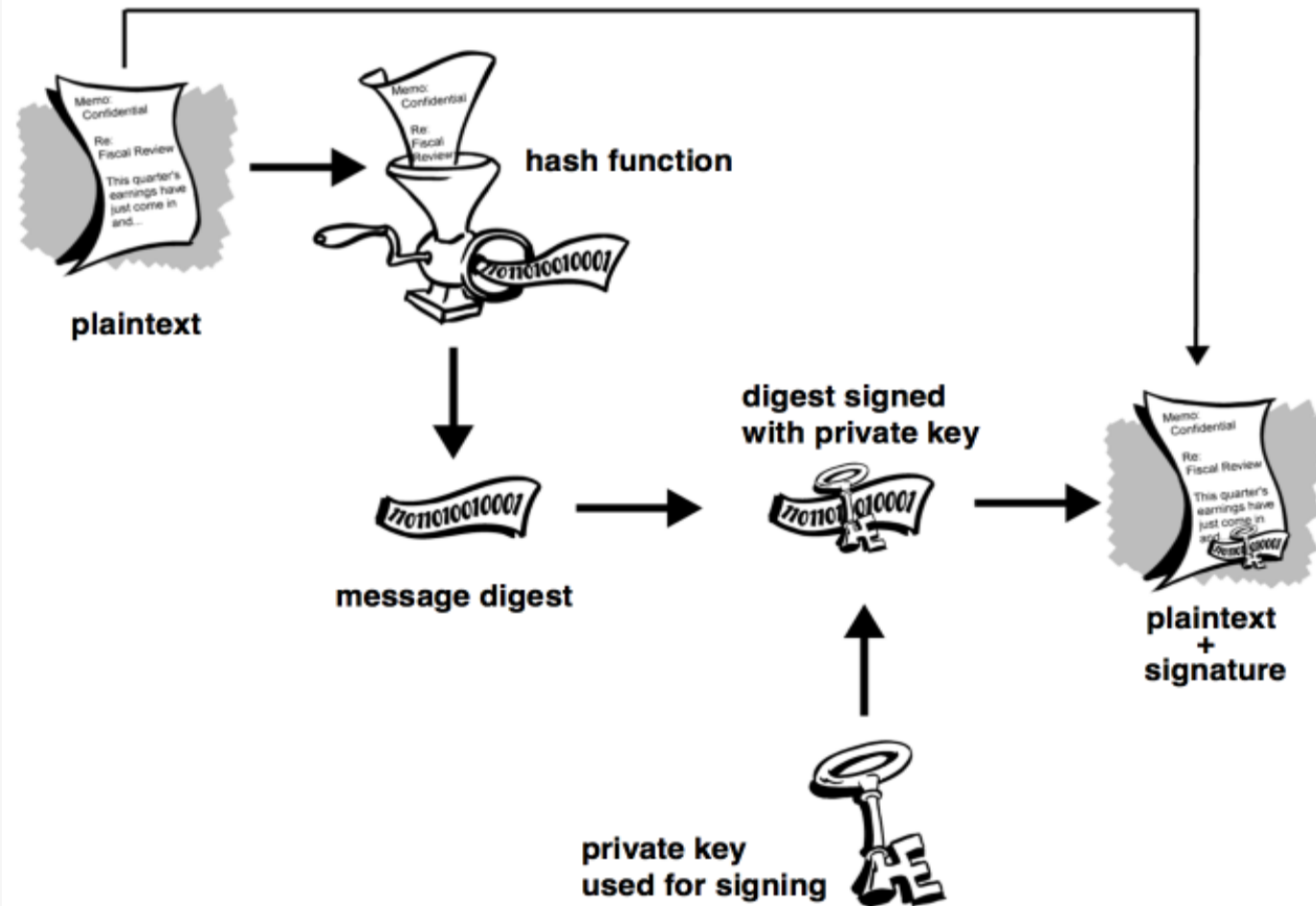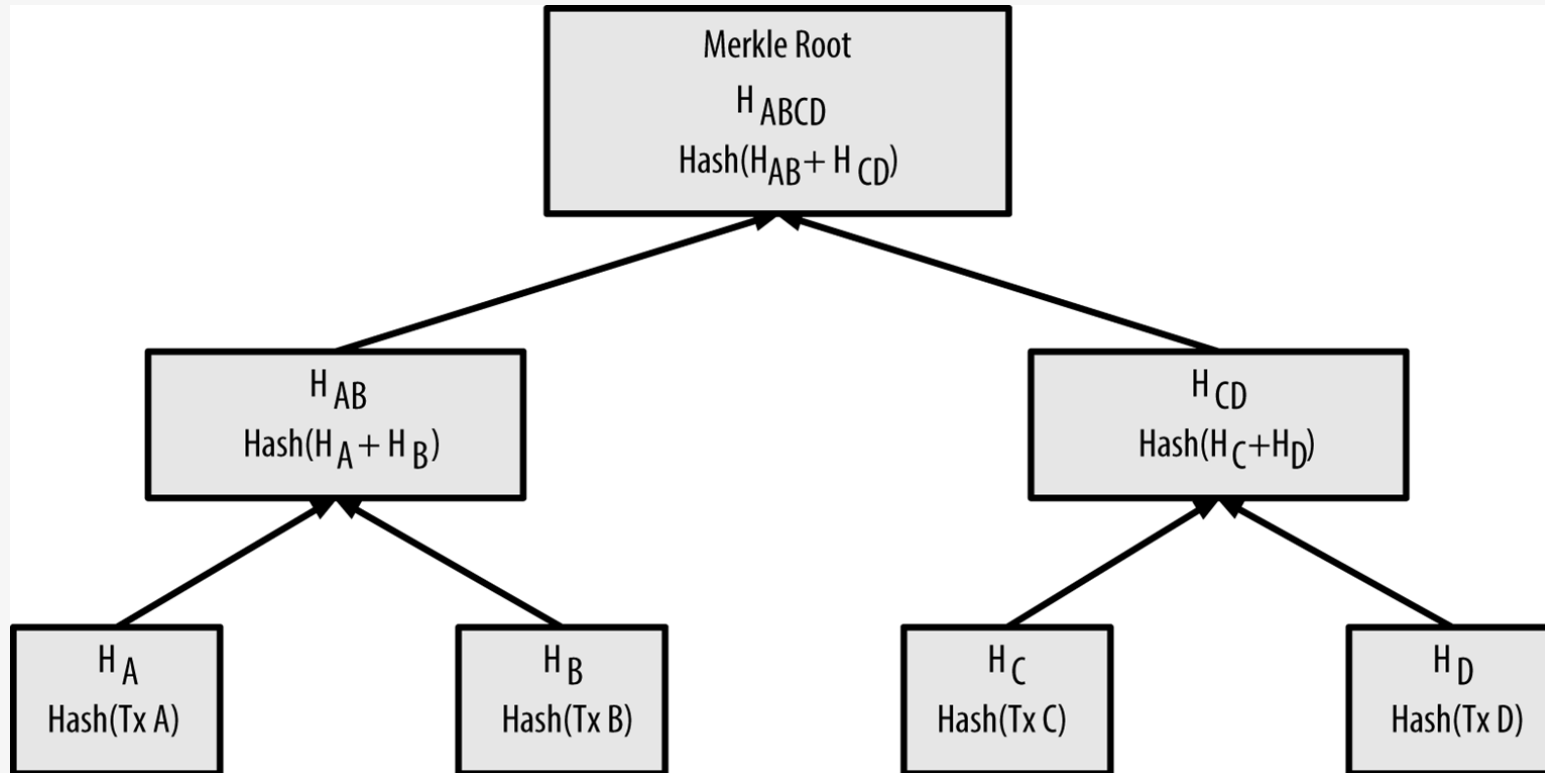
Merkle Tree

Verification of Merkle Tree
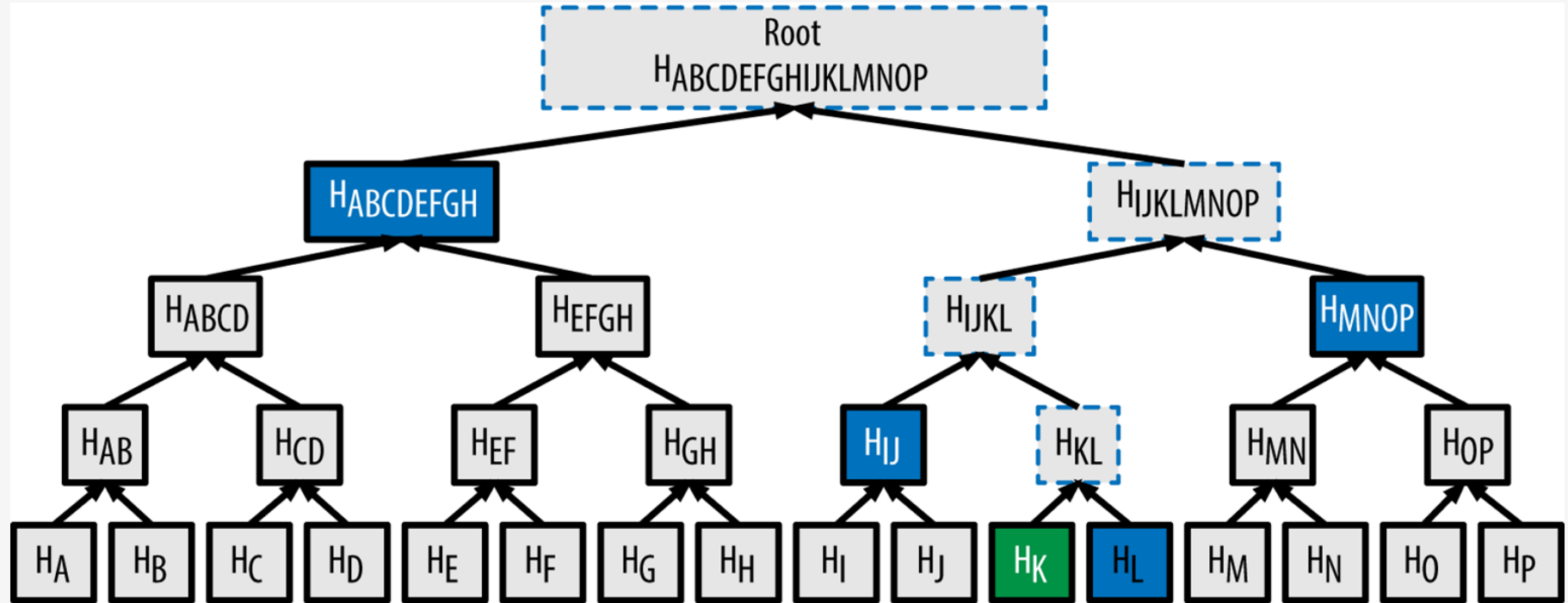
Blockchain, trust and transparency
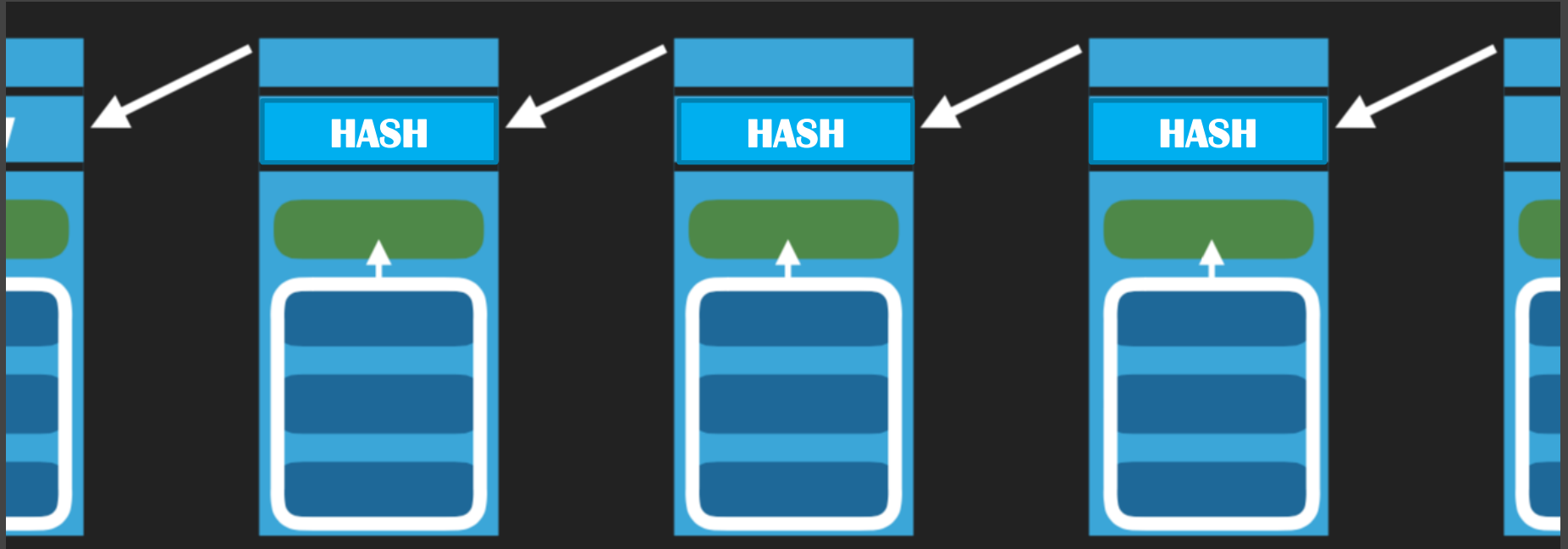
Blockchain, trust and transparency
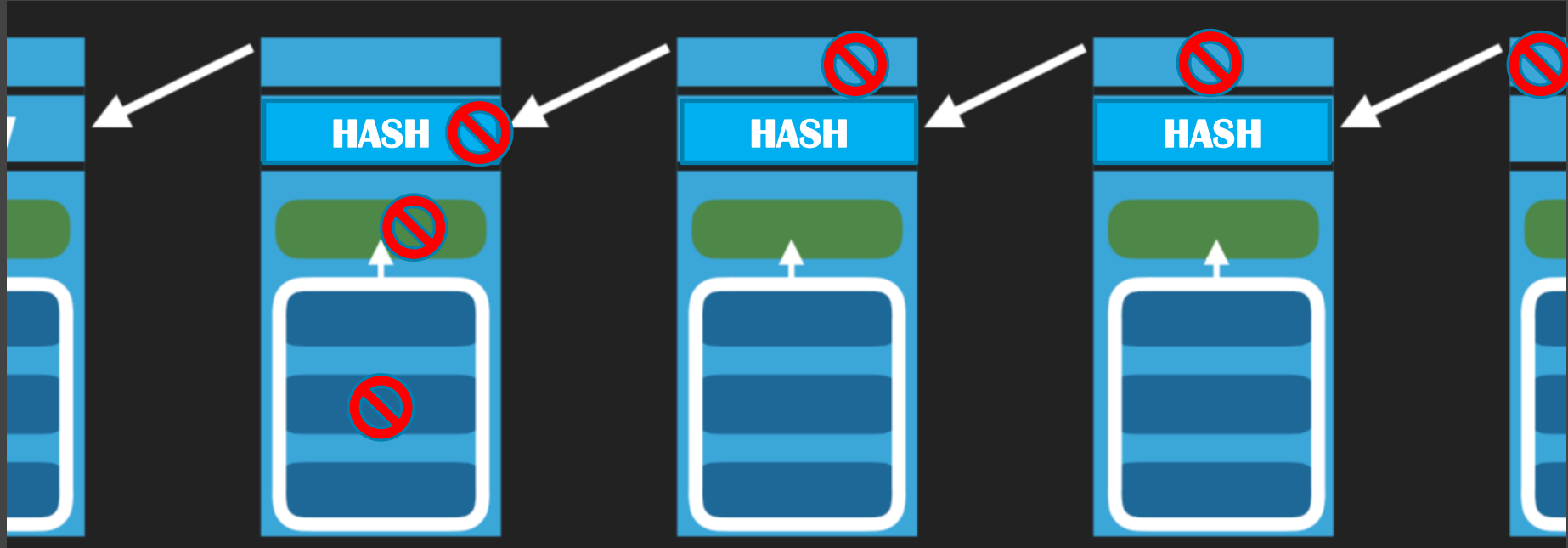
What does it mean to be decentralized?
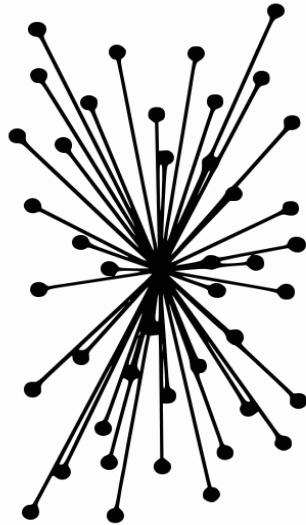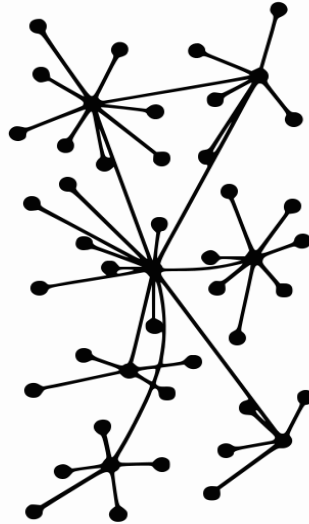
Centralized   Decentralized   Distributed

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS
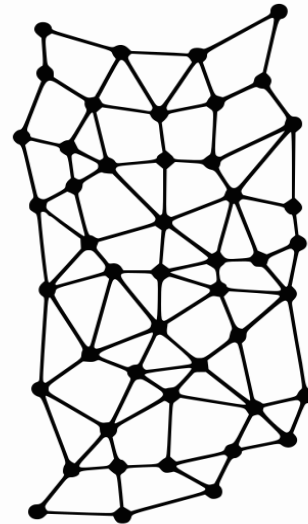
Distributed Ledgers in Action

All business participating in a commercial ecosystem need a ledger to contain a record of transactions. It is vitally important to know that your copy of the ledger is identical to your business partners' and free from discrepancies.

 Example scenario:

1. Everyone in a room has a book with the instructions to write down entries as they get called out.
2. Someone calls out item number one and everyone writes it down.
3. Then two people call out item number two at the same time, but the item number differs.
4. There needs to be a process for who wins, and the loser gets to try to call out item number three.
5. When all agree on the outcome of an entry, the next link in that ledger can be written.
6. Whether this happens in a small scale or the size of the internet, that is the spectrum for how a distributed ledger can work.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Still you need to agree on a common version

PBFT and derivatives

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

What makes a good consensus?

- **Decentralized governance:** A single central authority cannot provide transaction finality.
- **Integrity:** It enforces the validation of the transaction integrity (e.g., mathematically through cryptography).
- **Nonrepudiation:** There are ways to verify the supposed sender really sent the message.
- **Privacy:** There should be ways to ensure that only the intended recipient can read the message.
- **Fault tolerance:** The network operates efficiently and quickly, even if some nodes or servers fail or are slow.
- **Performance:** It considers throughput, liveness, scalability, and latency

Finally, the agreed block is added to the ledger and distributed

Open Sourced

Network Verified

Beyond Borders

Cryptographically Secure

Fast

Decentralized

Myth Debunked: Blockchain ≠ Cryptocurrency

Cryptocurrency is an application that sits on top of blockchain.

Not the other way around.

Blockchain and cryptocurrencies are often discussed in similar contexts, but they are <u>not</u> one in the same.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Permissioned? Private?

Perm.less Public	Perm.less Private	Permi.ed Public	Permi.ed Private

Bitcoin Etherium	Voting System	Land title Medical Records	Bank Trading system
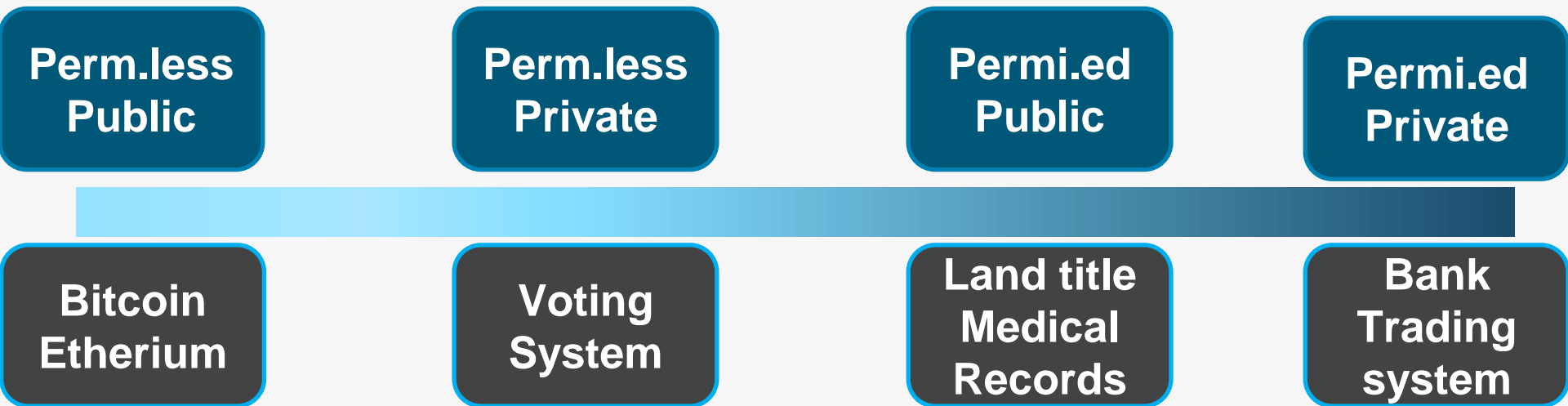
- **Permisioned vs Permissionless: Who can Write to a blockchain (ACCESIBILITY)**
- **Public vs Private: Who can read from a blockchain (VISIBILITY)**

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

30

Why Business Blockchain Technologies

All over the global market there are ledgers that organizations and individuals alike must trust.

Permissioned blockchains differ from what you'll find in Bitcoin or Ethereum.
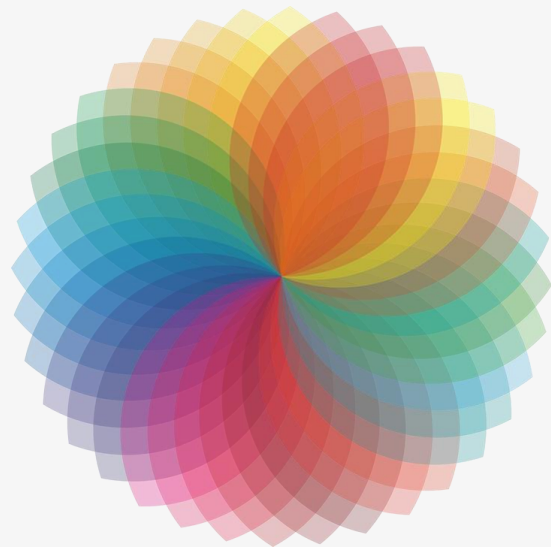
The Spectrum Of Business Blockchain Technologies is huge.
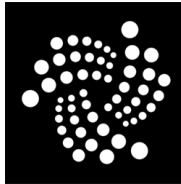
Corda

- **Distributed ledger platform.**
- **Blockchain style P2P network, however it is not a blockchain platform.**
- **Corda only allows information access and validation functions to parties actually involved in the transaction.**
- **Achieves consensus between firms at the level of individual deals, not the level of the system.**
- **Supports various consensus mechanisms.**
- **Has both enterprise and opensource version.**

Quorum

- **Created by JP Morgan,**
- **Fork of the Ethereum public blockchain,**
- **Voting-based consensus algorithm to facilitate an enterprise-focused distributed ledger and smart contract platform.**
- **Data privacy is achieved within the network by allowing data visibility on a need-to-know basis.**
- **Both transaction-level privacy and network-wide transparency.**
- **The network validates all smart contracts and overall system state through the involvement of all running nodes.**

IOTA

- Cryptocurrency, that provides the whole ecosystem based on blockless blockchain to enable machine to machine (M2M) transactions.
- Uses directed acyclic graph technology instead of DLT.
- Also a platform that essentially entails a generalization of the blockchain protocol - the technology called Tangle - that sits at the back end of the IOTA platform.
- Peer-based validation vs minor payment.

A Block DAG. Each block may refer to several predecessor blocks by including their hash in its header.
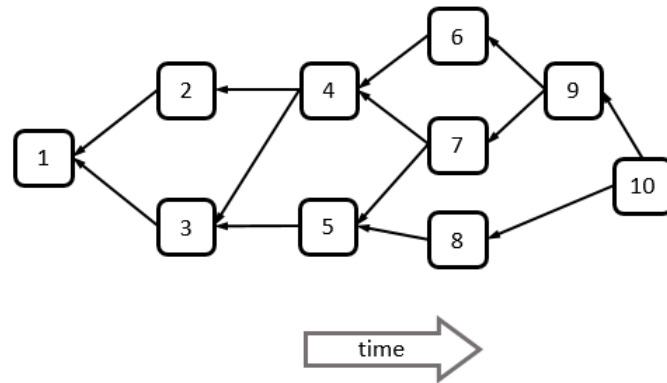
The Linux Foundation is Much More than Linux

Security

We are helping global privacy and security through a program to encrypt the entire internet.

Networking

We are creating ecosystems around networking to improve agility in the evolving software-defined datacenter.

Cloud

We are creating a portability layer for the cloud, driving de facto standards and developing the orchestration layer for all clouds.

Automotive

We are creating the platform for infotainment in the auto industry that can be expanded into instrument clusters and telematics systems.

Blockchain

We are creating a permanent, secure distributed ledger that makes it easier to create cost-efficient, decentralized business networks.

Web

We are providing the application development framework for next generation web, mobile, serverless, and IoT applications.

Let's Encrypt

ONAP OPEN NETWORK AUTOMATION PLATFORM

CLOUD NATIVE COMPUTING FOUNDATION

AUTOMOTIVE GRADE LINUX

HYPERLEDGER

node JS

We are regularly adding projects; for the most up-to-date listing of all projects visit tlfprojects.org

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

The beginning of Hyperledger

HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Hyperledger is a collaborative and global open source software community, hosted by The Linux Foundation, advancing blockchain technologies for business.

Hyperledger Momentum

<2

years since launch

25k+

Commits

4

Tools

5

Frameworks

1

Production Release
**Hyperledger
Fabric v1.0**

180+

Members
(30+ in China)

12

Active Community
Working Groups

80

Meetups
Worldwide

16k

Meetup
Participants

600+

Media Clips Per
Month in 2016

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

The Hyperledger Umbrella

Infrastructure
Technical, Legal, Marketing, Organizational

Ecosystems that accelerate open development and commercial adoption

THE LINUX FOUNDATION

Cloud Foundry	Node.js	**Hyperledger**	Open Container Initiative

Frameworks
Meaningfully differentiated approaches to business blockchain frameworks developed by a growing community of communities

Hyperledger **Indy**	Hyperledger **Fabric**	Hyperledger **Iroha**	Hyperledger **Sawtooth**	Hyperledger **Burrow**

Tools
Typically built for one framework, and through common license and community of communities approach, ported to other frameworks

Hyperledger **Composer**	Hyperledger **Explorer**	Hyperledger **Cello**	Hyperledger **Quilt**

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Hyperledger Blockchain Frameworks

Hyperledger Fabric
Intended as a foundation for developing applications or solutions with a modular architecture, Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play.

Hyperledger Iroha
A business blockchain framework designed to be simple and easy to incorporate into infrastructural projects requiring distributed ledger technology.

Hyperledger Sawtooth
A modular platform for building, deploying, and running distributed ledgers. Hyperledger Sawtooth includes a novel consensus algorithm, Proof of Elapsed Time (PoET), which targets large distributed validator populations with minimal resource consumption.

Hyperledger Burrow
A permissionable smart contract machine. The first of its kind when released in December, 2014, Burrow provides a modular blockchain client with a permissioned smart contract interpreter built in part to the specification of the Ethereum Virtual Machine (EVM).

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

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Hyperledger Modular Approach Benefits

FLEXIBLE MODIFICATION
OF ANY COMPONENT

COMMON FUNCTIONAL
MODULES AND DEFINED
INTERFACES

RE-USE OF
COMMON BUILDING
BLOCKS

EXTENSIBLE
CODEBASES

RAPID
EXPERIMENTATION

DIVERSE DEVELOPER
COMMUNITY
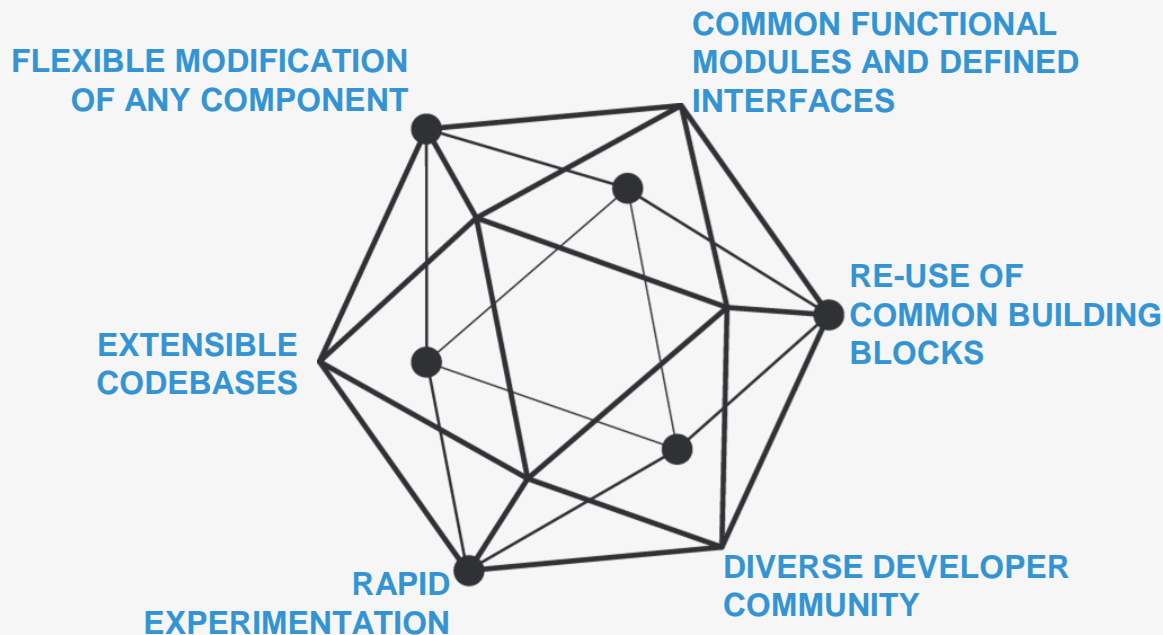
Hyperledger Goals

Where open source teams build diverse approaches for business blockchain technology systems

Create enterprise grade, open source, distributed ledger frameworks & code bases

to support business transactions

Provide neutral, open, & community-driven infrastructures

supported by technical and business governance

Build technical communities

to develop blockchain and shared ledger POCs, use cases, field trials and deployments

Educate the public

about the market opportunity for blockchain technology

Promote our community of communities

taking a toolkit approach with many platforms and frameworks

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

A Few Ways to Participate

Subscribe to Hyperledger Mailing Lists

Attend Hyperledger Hackfests and upcoming blockchain events

Get the **latest development updates** from the wiki

Engage in the discussion on Rocket.Chat

Search for Open Bugs, or Report a New One, in Our Bug Database

Start or join a local Hyperledger Meetup

Participate in the Working Group meetings

Check out all the Hyperledger business blockchain technologies and

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Join Your Industry Peers

Hyperledger Premier Members Serving on the Governing Board

Join Your Industry Peers

General Members

1WorldBlockchain
ABN Amro
Aesthetic Integration
AlphaPoint
Altoros Americas LLC
Aktsiaselts Eurostep Digital
AMIHAN Global
ANNE
ANZ
BBVA
Beijing Botuzongheng Science & Technology Co., Ltd.
Beijing RZXT Technology Development
Belink Technologies
Bitmark
BitSE
Blockchain
BLOCKO Inc.
Blockstream
Bloq
BNP Paribas
BNY Mellon
Broadridge Financial Solutions
BTS
CA Technologies
Calastone
Capgemini

Chain Connected
ChainNova
China Merchants Bank
ChongQin Xichain Technologies
CITIC
Clause, Inc
Cloudsoft Corporation Ltd.
CLS Bank International
Coinplug
CollectorIQ Inc.
Colu
Consensus Base Inc.
ConsenSys
Cuscal Limited
Deloitte Consulting LLP
DLT Labs
Energy Blockchain Labs
Ernst & Young
Factom Foundation
FZG360 Network Co. Ltd
GameCredits
Gem
Gibraltar Stock Exchange (GSX)
Global Peersafe Technology Corp.

Guardtime
Hangzhou Fuzamei Technology
Hashed Health
Huawei
Hyperchain Technologies
IntellectEU
iRootech Technology Co., Ltd
Kaiser Permanente
Korea Exchange
Korea Security Depository
Koscom
Kubique S.p.A.
LedgerDomain
Libra
Loyyal Corporation
Lykke
MadHive
Medicalchain
Milligan Partners
MIRACL UK Limited
Monax Industries Limited
MonetaGo
Montran Labs
Moscow Exchange
Murphy & McGonigle, P.C.
National Stock Exchange of India

Netki
New H3C Technologies
NEX Optimisation
Nokia
Norbloc
NTT Data
Onchain
Oracle
Orange Magic Cube
Paxos
PDX Technologies
RadarWin Cyber Technology
Red Hat
Revelry Labs
Samsung SDS
Sany Heavy Group Co., Ltd
Sberbank
ScanTrust SA
Schroder Investment Management Limited
SecureKey Technologies
Shanghai Ginkoo Financial Technology
Shanghai Onechain Information Technology
Shenzhen Forms Syntron Information

Shenzhen Qianhai Zhaogu Financial Service Co. Ltd
Shenzhen Xinguodu Technology CO., LTD
Sinolending Ltd
Smart Link Lab
Soramitsu
State Street
SWIFT
Swisscom AG
Symbiont
Tai Yi Yun
Tequa Creek Holdings
Patientory
Thomson Reuters
TMX Group Limited (TSX)
TradeIX Limited
VMware
Wells Fargo
Yuphant Blockchain
Zhejiang Shuqin Technology
Beijing Smart Card Technology Research Institute

Associate Members

Accord Project
Bank of England
Blockchain Research Institute
Chamber of Digital Commerce
Cloud Security Alliance
Colored Coins
Federal Reserve Bank of Boston
IC3
IFSE
Mercy Corps
Nxt Foundation
OSCRE
Sovrin Foundation
Taiwan Fintech Association
Tecnalia Research & Innovation
TNO
University of Luxembourg
University of Rome Tor Vergata/Inuit Foundation
VSP Global
Zhejiang University
The Illinois Blockchain Initiative

There will not be a single blockchain that rules them all

Buzzword 6: POC and Pilots

Dev Bharel,
Blockchain Educators Network

Marta Piekarska, Director of Ecosystem,
Hyperledger

Early Adopter Industries

Financial Services

The most immediate business opportunities are to use business blockchains to track and trade stocks and bonds with reduced risk and time, and increased transparency.

Supply Chain

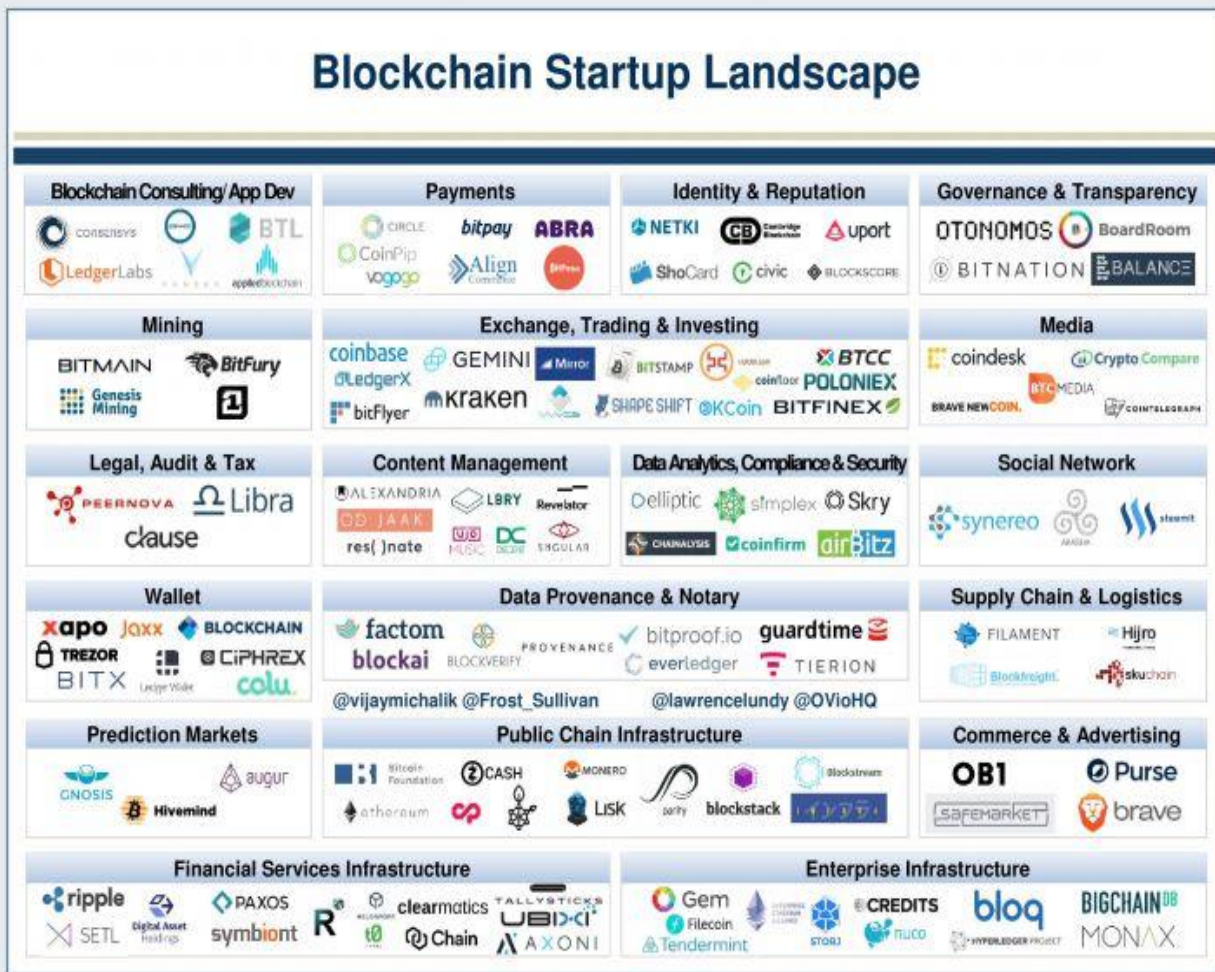Blockchain technologies will lead to greater efficiency, as well as safer and more ethical standards through the ability to prove the veracity of transactions to all stakeholders.

Healthcare

Business blockchains are giving the healthcare industry a chance to reinvent what historically has been a thorny problem: sharing patient data records between organizations.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

How many of you have already tried developing with blockchain?

Blockchain Startup Landscape

Blockchain Consulting/App Dev
consensys, BTL, LedgerLabs, appleblockchain

Payments
CIRCLE, bitpay, ABRA, CoinPip, Align Commerce, vogogo, BitPesa

Identity & Reputation
NETKI, CB Cambridge Blockchain, uport, ShoCard, civic, BLOCKSCORE

Governance & Transparency
OTONOMOS, BoardRoom, BITNATION, BALANCE

Mining
BITMAIN, BitFury, Genesis Mining, 21

Exchange, Trading & Investing
coinbase, GEMINI, Mirror, BITSTAMP, BTCC, LedgerX, coinfloor, POLONIEX, bitFlyer, kraken, SHAPESHIFT, OKCoin, BITFINEX

Media
coindesk, Crypto Compare, BRAVE NEWCOIN, BTC MEDIA, COINTELEGRAPH

Legal, Audit & Tax
PEERNOVA, Libra, clause

Content Management
ALEXANDRIA, LBRY, Revelator, JAAK, MUSIC, DECENT, SINGULAR, res( )nate

Data Analytics, Compliance & Security
elliptic, simplex, Skry, CHAINALYSIS, coinfirm, airBitz

Social Network
synereo, ARANOA, steemit

Wallet
xapo, Jaxx, BLOCKCHAIN, TREZOR, CiPHREX, BITX, Ledger Wallet, colu

Data Provenance & Notary
factom, PROVENANCE, bitproof.io, guardtime, blockai, BLOCKVERIFY, everledger, TIERION
@vijaymichalik @Frost_Sullivan @lawrencelundy @OVioHQ

Supply Chain & Logistics
FILAMENT, Hijro, Blockfreight, skuchain

Prediction Markets
GNOSIS, augur, Hivemind

Public Chain Infrastructure
Bitcoin Foundation, ZCASH, MONERO, Blockstream, ethereum, LISK, parity, blockstack

Commerce & Advertising
OB1, Purse, SAFEMARKET, brave

Financial Services Infrastructure
ripple, Digital Asset Holdings, PAXOS, R3, clearmatics, TALLYSTICKS, UBIXI, SETL, symbiont, t0, Chain, AXONI

Enterprise Infrastructure
Gem, Filecoin, Tendermint, CREDITS, STORJ, nuco, HYPERLEDGER PROJECT, bloq, BIGCHAIN DB, MONAX

FROST & SULLIVAN   OUTLIER·VENTURES

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Cross-Border Payments

After months of work, a global team of developers have completed a cross-border POC built with Hyperledger Fabric. Designed to test whether moving member bank accounts to a distributed ledger could help the inter-bank payments platform Swift reconcile in real time, the blockchain trial is now ready for its next phase of testing with General members ANZ, BNP Paribas, BNY Mellon and Wells Fargo.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Read about the POC in Coindesk.

Hear about the collaboration in the ANZ Community Spotlight video.

Healthcare Records

Hyperledger Composer offers a set of APIs, a modeling language and a programming model to quickly define and deploy business networks and applications that allow participants to send transactions that exchange assets.

Join the Hyperledger Healthcare Working Group (HLHC) to help bring commercial blockchain adoption to the healthcare industry.

Together we can create a blockchain system that disenfranchises the most vulnerable. Lean more here.

Interstate Medical Licensing

Associate Hyperledger Member State of Illinois has implemented a pilot program in collaboration with General member Hashed Health using Hyperledger Fabric to reduce complexity of interstate medical licensing, as well as to improve the veracity of provider directories and claims adjudication processes.

HASHED HEALTH

HEALTHCARE BLOCKCHAIN INNOVATION

The Illinois BLOCKCHAIN Initiative

Read the full announcement. 59

Ethical Seafood Movement

Hyperledger Premier member Intel is collaborating with the Hyperledger community to implement a modern approach to seafood traceability. Leveraging the Hyperledger Sawtooth framework, the seafood journey can now be recorded from ocean to table.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

(intel®)

Watch the explainer video and read the full case study on the Hyperledger Sawtooth project page.

Read about the demo in CoinDesk.

Diamond Supply Chain

In 2003, the Kimberley Process Certification Scheme (KPCS) was established to prevent conflict diamonds. Purchased diamonds now come with a certificate to prove the distributor did not obtain the diamond from rebels, that the mine has been audited, etc. The idea is that paperwork can confirm provenance; however, the process is lengthy and there is a history of fraud from missing paperwork.

To keep blood diamonds from entering the supply chain Hyperledger Premier member SAP Ariba is collaborating with Everledger to pilot a distributed ledger diamond track and trace system using Hyperledger Fabric v1.0 that everyone in the industry can write to from miners, to distributors, to retailers.

Holding a diamond to light creates a unique pattern that may be used to create an ID. When a bag of diamonds changes hands in the supply chain, it forms two entries in the chain: the diamond IDs present upon sending and receipt. Once a diamond ID number is inside the system it provides integrity as any stakeholder can then query and instantaneously verify a diamond's provenance.

This system is empowering whistleblowers, governments, mining companies, retailers, journalists, and human rights organizations to get specific on tracking where conflict diamonds are entering the supply chain and preventing them from entering the market.

Read about the Hyperledger Fabric pilot in *International Business Times.*

Verifiable IDs for Refugees

Blockchain could bring tremendous positive impact to those who live in communities without a strong state actor issuing verifiable identification. The World Bank reports 2 billion people internationally do not have access to financial services. Moreover, the UN reported in 2015 that more than 95 million people have been forcibly displaced, stateless or refugees.

Consider the more than 245,000 refugees living in one of five camps that comprise the Dadaab UNHCR base in northern Kenya, the second-largest such complex in the world. Established 17 years ago, Dadaab is no longer a temporary camp, this is a city struggling to develop.

These refugees are underserved not only by the state, but also by the NGOs who are trying to understand the refugees' histories, both medical and financial. If someone requests a new business loan, for example, what is their financial history? Have they taken out a loan before? A common system of record to track items and actions of a given identity in that network could help the people of Dadaab build something from the ground up that they wouldn't otherwise be able to build.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Identity Management is a core focus of Hyperledger's Blockchain for Good initiatives. If interested in helping write the world using blockchain, join the open Identity WG, which meets every other Wednesday at 9am PST.

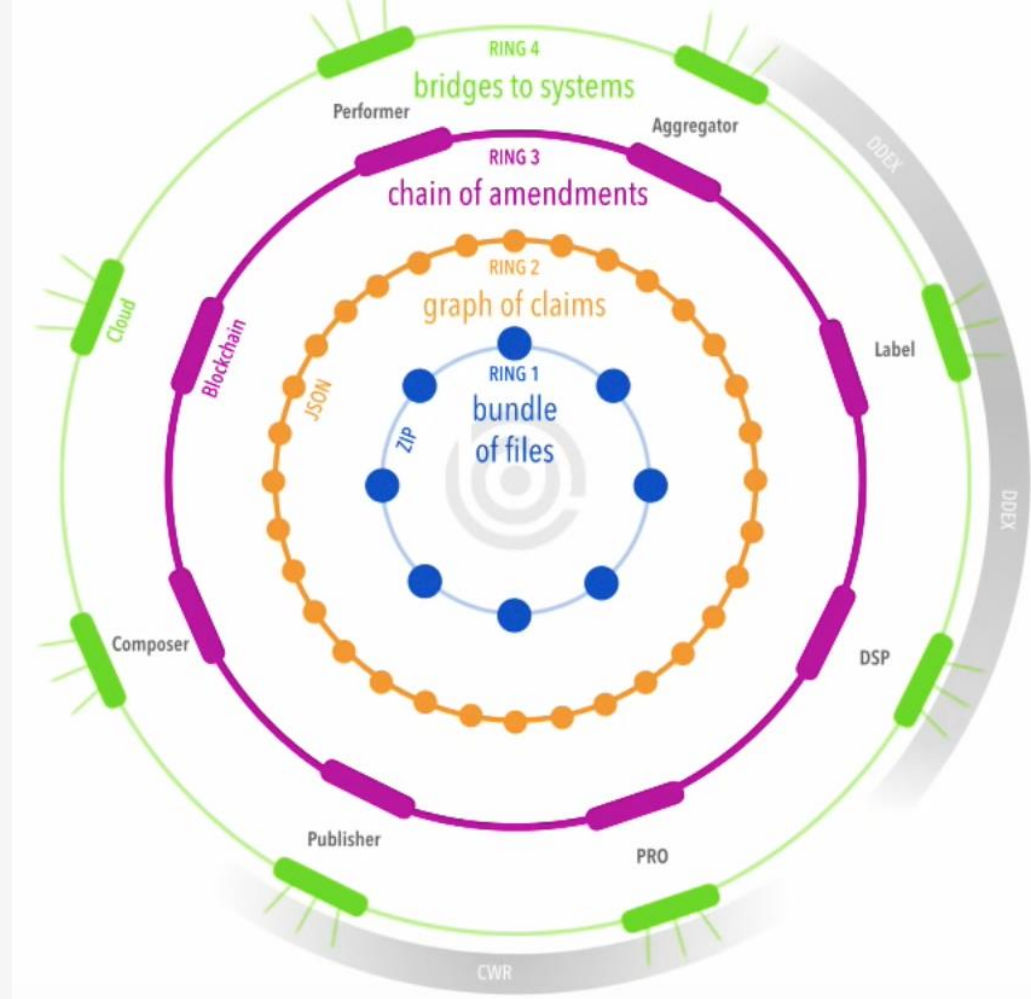**Read more about the impact of blockchain on refugees in *Quartz*.**

Building a music content rights registry that will help musicians express their rights and wishes for commercializing their art in an interoperable file format.

"Hyperledger Sawtooth will enable us to scale rapidly and customize transaction processors specifically for ingesting rights data"

When to use blockchain?

Database & API
– We have decades of experience using databases, use one if you can

Collaborative
– You can only have so much fun on you own with a blockchain

Decentralised
– Avoid replacing one centralised business model with another

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

It is still very early on

Bitcoin will be 10000 days old in May.

That's a car on day 10000

Things I learned today:

Words you should google

Consensus:
PoW, PoS, POET, Raft, BFT, PBFT

Crypto/Security:
PKI, HASH, SHA-256,
zk-SNARK, HE, ECC,
ECDSA, SGX

Ledger Concepts:
Mining
Blocks
Forks
Parents
Uncles
Merkle Trees

Platform Concepts:
Nodes
Oracles
Notaries
Wallet
Smart Contracts

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

71

Choose your blockchain quest.