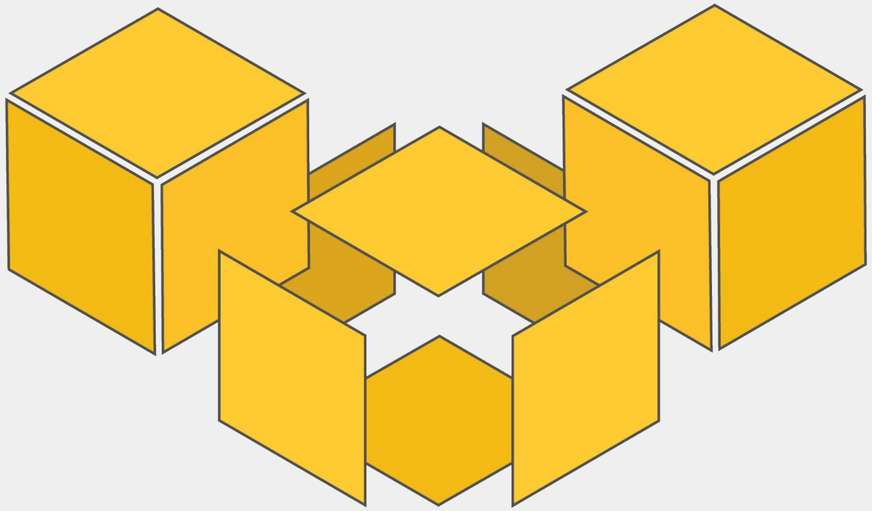


Blockchain
AT BERKELEY

Workshop 3 -

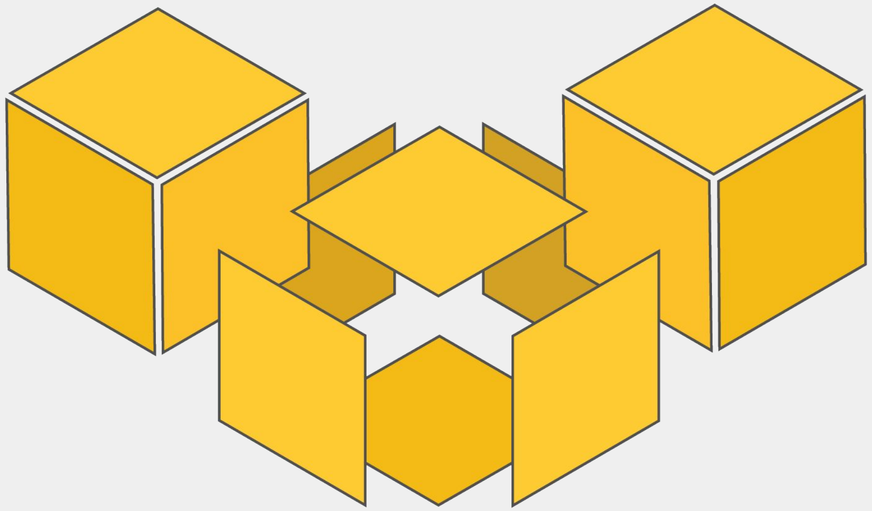
- Blockchain vs. Central Database
- User Cases

Overview

1. Intro
2. IoT Team
3. Healthcare Team
4. Supply Chain Team
5. Finance Team

User Case Discussion

6. Gartner Explanation
7. Hyperledger
8. Slock.it
9. Questions & Closing



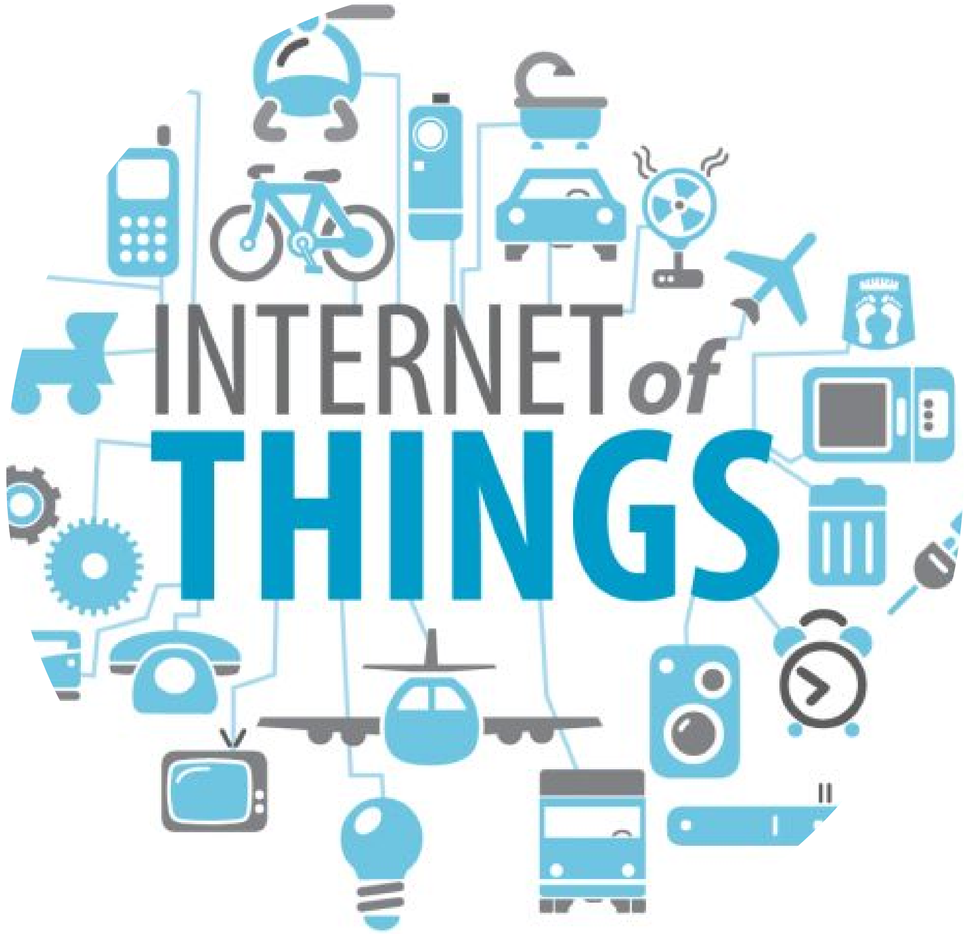
Blockchain
AT BERKELEY

Internet of Things:

Prediction Markets Using Sensors

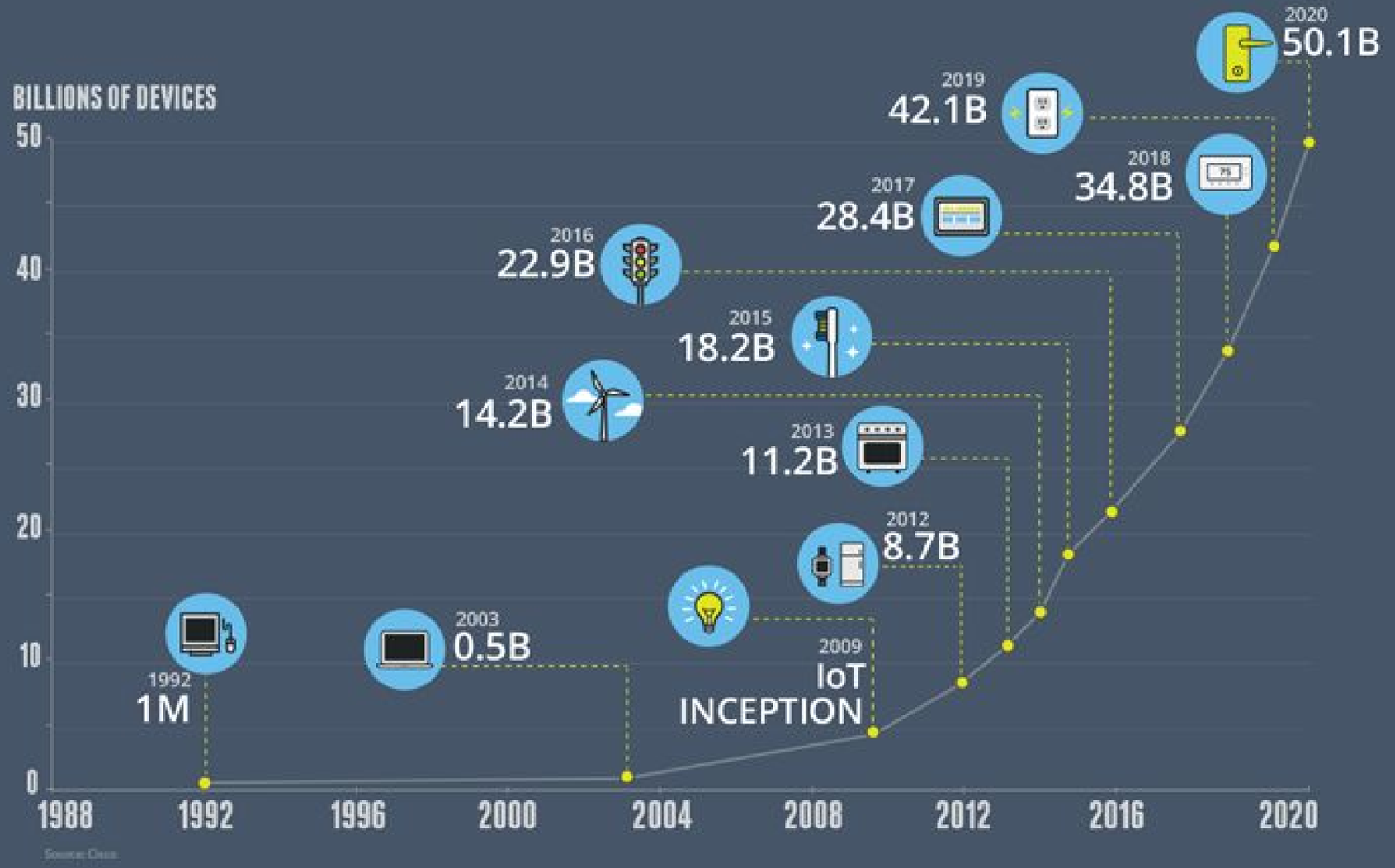
The Internet of Things

The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.



GROWTH IN THE INTERNET OF THINGS

THE NUMBER OF CONNECTED DEVICES WILL EXCEED **50 BILLION** BY 2020



Source: Cisco

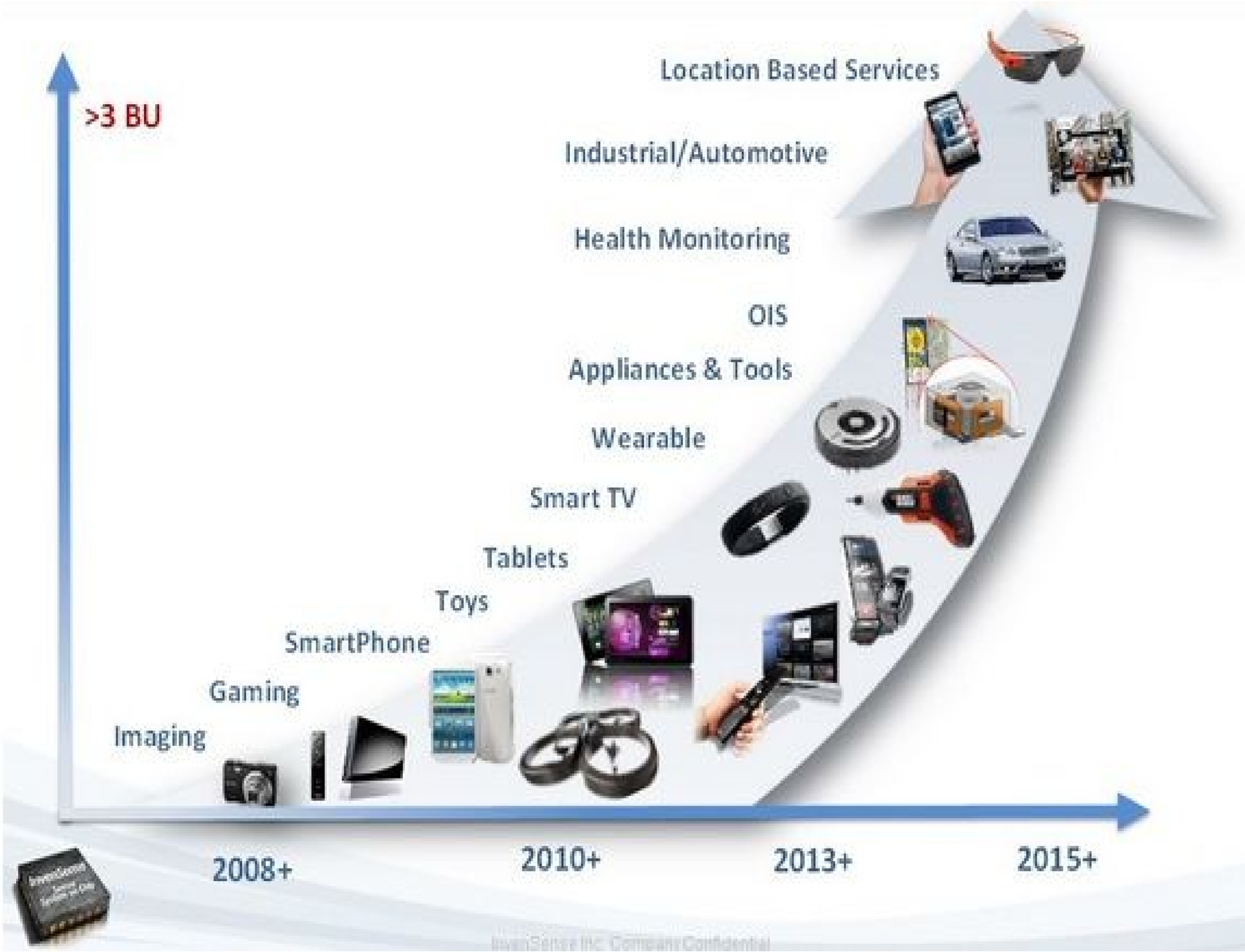
Inspired by Augur:

- Prediction markets
- Decentralized network
- Crowdsourced forecasting tool
- System of Oracles for contract settlement

Growth in Sensors

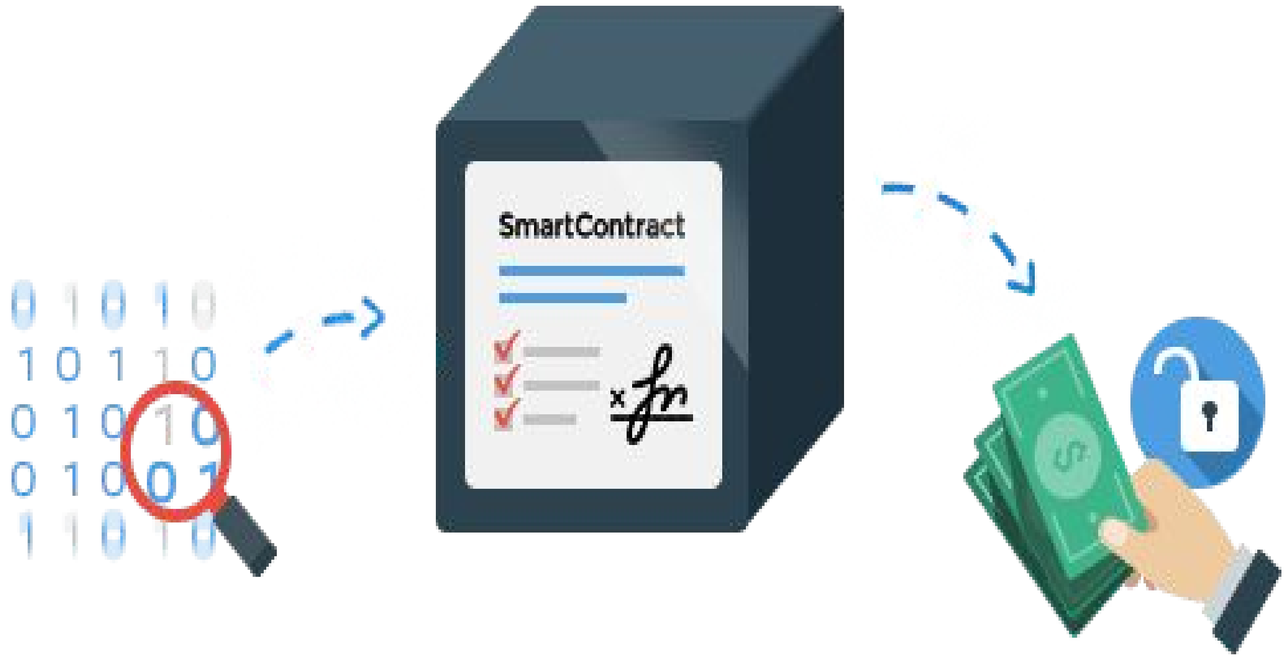
In the coming decade, more and more sensors will become internet connected, enabling remote sensing of:

- Fire detection
- Earthquake detection
- Floods
- Temperature
- Humidity
- Moisture
- And more



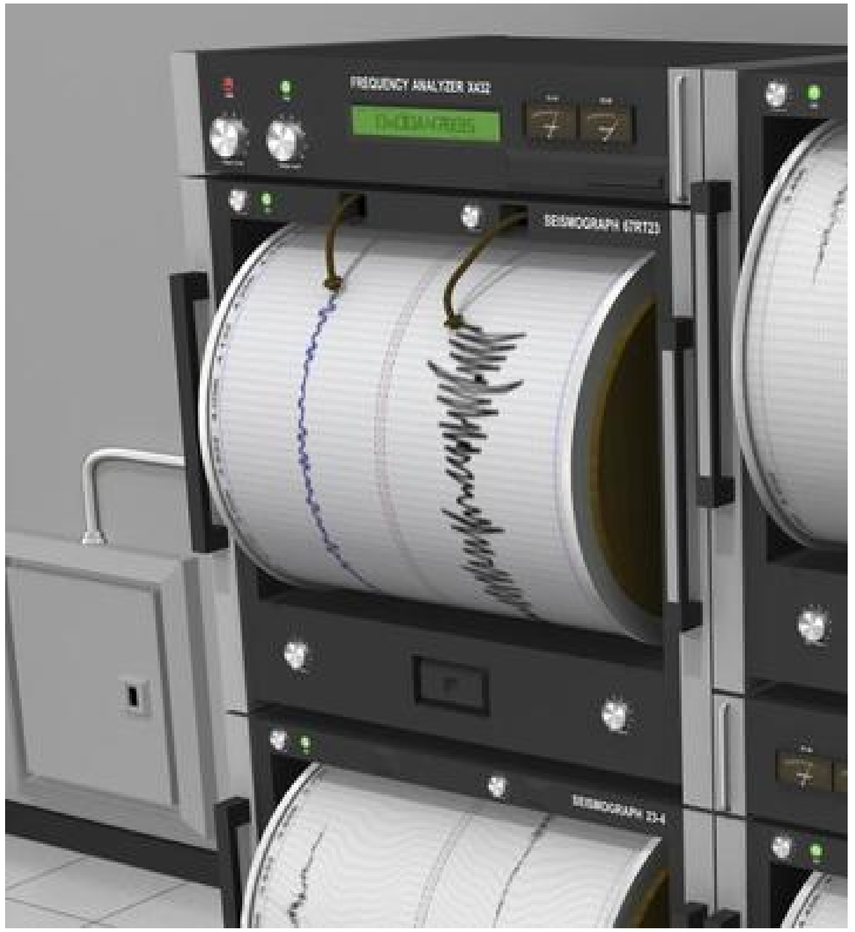
Sensors as Oracles

- What if instead of relying on a system of Oracles, smart contracts could be settled by a network of smart sensors?
- By utilizing sensors used in existing IoT applications, consensus would occur almost instantly
- This would mitigate subjectivity and collusion.



Application - Earthquake Insurance

- Earthquake insurance using networks of seismometers and accelerometers
- Can utilize existing “brownfield sensors”
  - Owners of seismometers can monetize their sensors by adding them to our network
  - Correct predictions reward the owner of the sensor, incentivizing accuracy
- Property owners in earthquake prone areas can hedge against property damage without having to pay for the infrastructure, marketing, sales, etc of an insurance company
  - Results in more efficient and flexible insurance



Why it is better than a centralized database:

Sybil Attacks

- Buying and faking data from multiple locations would be more prohibitively expensive than a subjective decision by an Oracle.
- We would use the same structure of pruning bad sensors as Augur currently uses to consolidate good Oracles.

Supply Chain Presentation

Blockchain@Berkeley

Current Ticket Buying Processes

1. Buy from vendor
2. Need to beat out fast bots
3. End up buying from reseller / waiting in long lines vs. scalpers

1. Buy from reseller online
2. No guarantee of authenticity
3. Buyer may receive invalid ticket

Problem: Ticket resale transactions

- In ticket marketplaces, sellers can refuse to give tickets once paid
- People can pretend they have tickets to transfer to other people.
- Sellers can potentially present a used, stolen or fake ticket as an authentic one.
- Scalping and botting are prevalent
- Customers worry a lot about ticket transaction authenticity.

Solution: Tickets as a Crypto-token

- Implement tickets as a “crypto-token”
- Ticket authenticity guaranteed
- Purchase tickets with Ether
- Smart contract integration in transactions
- “Spend” the ticket @ the physical venue

Benefits of Using a Blockchain

- Customers possess auto-verified tickets via ledger
- Venues and Artists have more oversight
- Greater range of data to analyze
- Custom contracts
- Tickets do not “disappear” after purchase

Further use cases:

- Adaptations for Air/Rail/Bus fares
- Transactions involving rare antiques etc.

Healthcare Blockchain

...

Caring for Health with Chains of Blocks

What is The Problem?

Patient records and information are held in many databases and a great deal of manpower is needed to facilitate the exchange of that information, which is very costly.

- Patient data is stored in “walled gardens” due to privacy concerns (e.g., HIPAA)
- Patient matching/identification is not easy; no common identifier across database systems
    - The same person is recorded differently in different systems (e.g., at the insurance company, hospital, or primary care medical group)

Our Solution

Put patients' medical records on a blockchain.

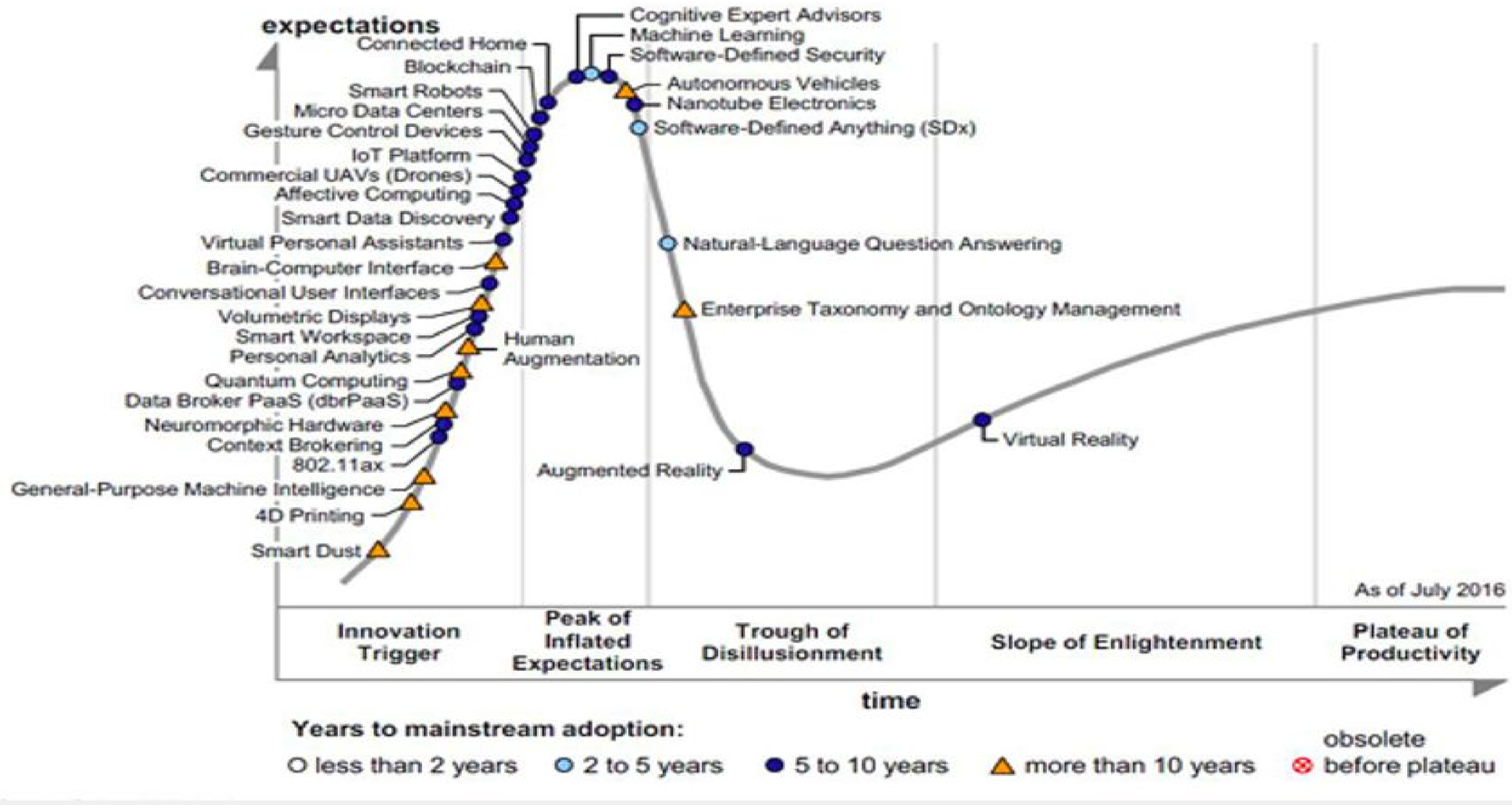
- Rather than having teams of people in one organization call each other and coordinate the transfer of information, each organization could receive the information from a blockchain
- In order to authenticate read and write access to records you need to designate certain people or organizations as administrators to blockchain
- Use a multisig contract
    - BitGo or Hyperledger
    - m of n parties can unlock/add data (e.g., patient and doctor, hospital and health insurer, etc.)
    - Most likely will use consortium blockchain built on Hyperledger

Why is This Better Than a Centralized System?

- **Disintermediation**: removes confusion and manpower, creates common for patient IDs across systems avoids expensive human communication
- **Security**: immutable and more redundant, separates authorization while still reducing manpower
- **Privacy**: data is encrypted and stored on the blockchain; requires multi-party authentication
- **Reduced Errors**: Requirement for multi-party authentication improves data sanity and oversight
- **Robustness**: different databases stay in sync without each organization having to pay a team to manage them
- **Auditability**: a complete, universal log of contract transactions on the blockchain

Blockchain at Berkeley

Figure 1. Hype Cycle for Emerging Technologies, 2016



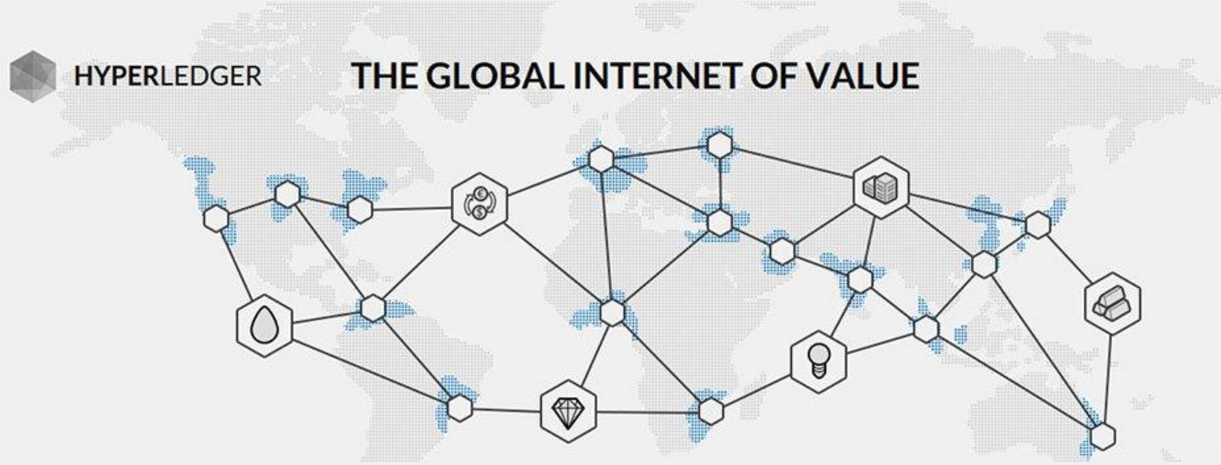
Blockchain at Berkeley

Hyperledger

A collaborative effort created to advance blockchain technology by identifying and addressing important features for a cross-industry open standard for distributed ledgers that can transform the way business transactions are conducted globally.

What is Hyperledger?

HYPERLEDGER PROJECT

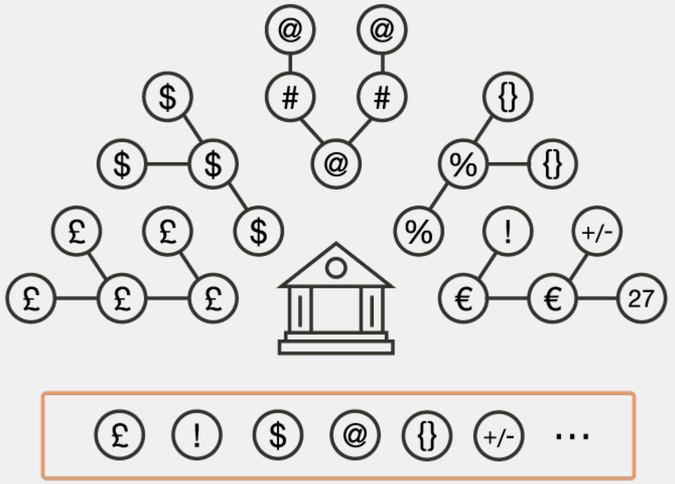


A world of many networks

1. Finance
2. Supply Chain (in progress)
3. Healthcare (future)

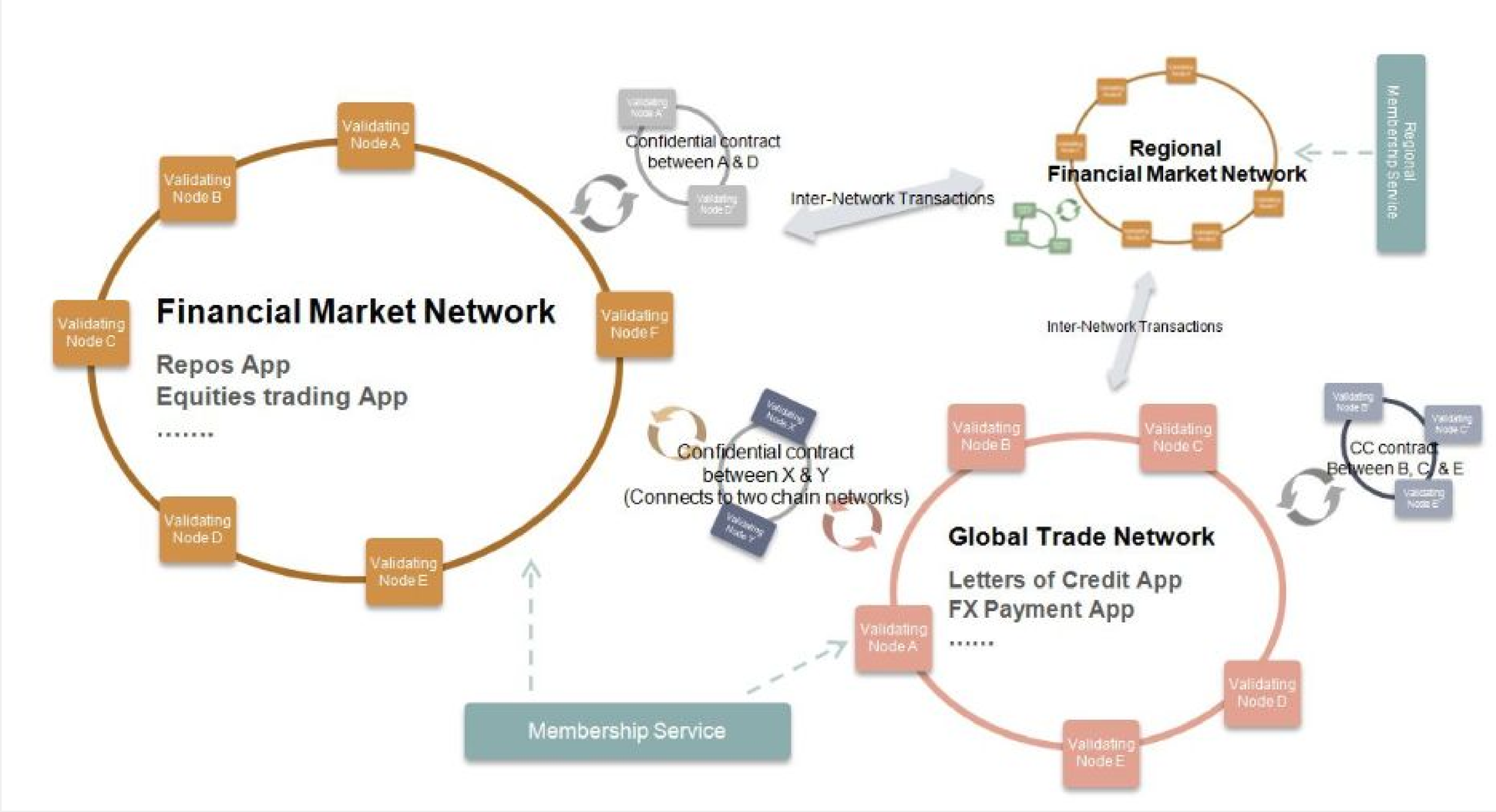
Three main values of Hyperledger (Vision):

- Assuming there will be multiple Blockchain networks across industries
- Increasing demand for permissioned ledgers
- Importance of both privacy and confidentially



Requirements (Hyperledger Architecture)

HYPERLEDGER PROJECT

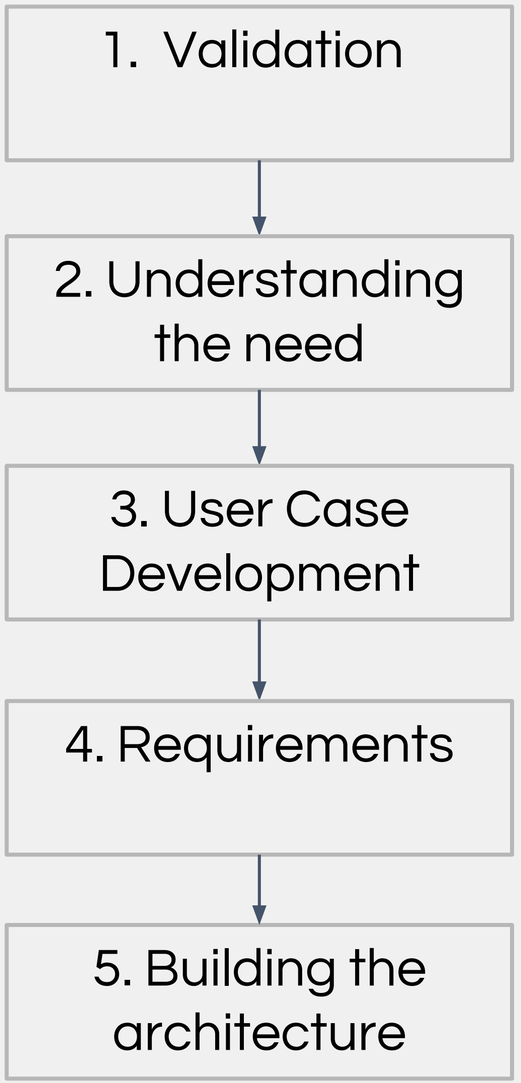


Requirements (Hyperledger Architecture)

HYPERLEDGER PROJECT

Requirements from Industry use cases

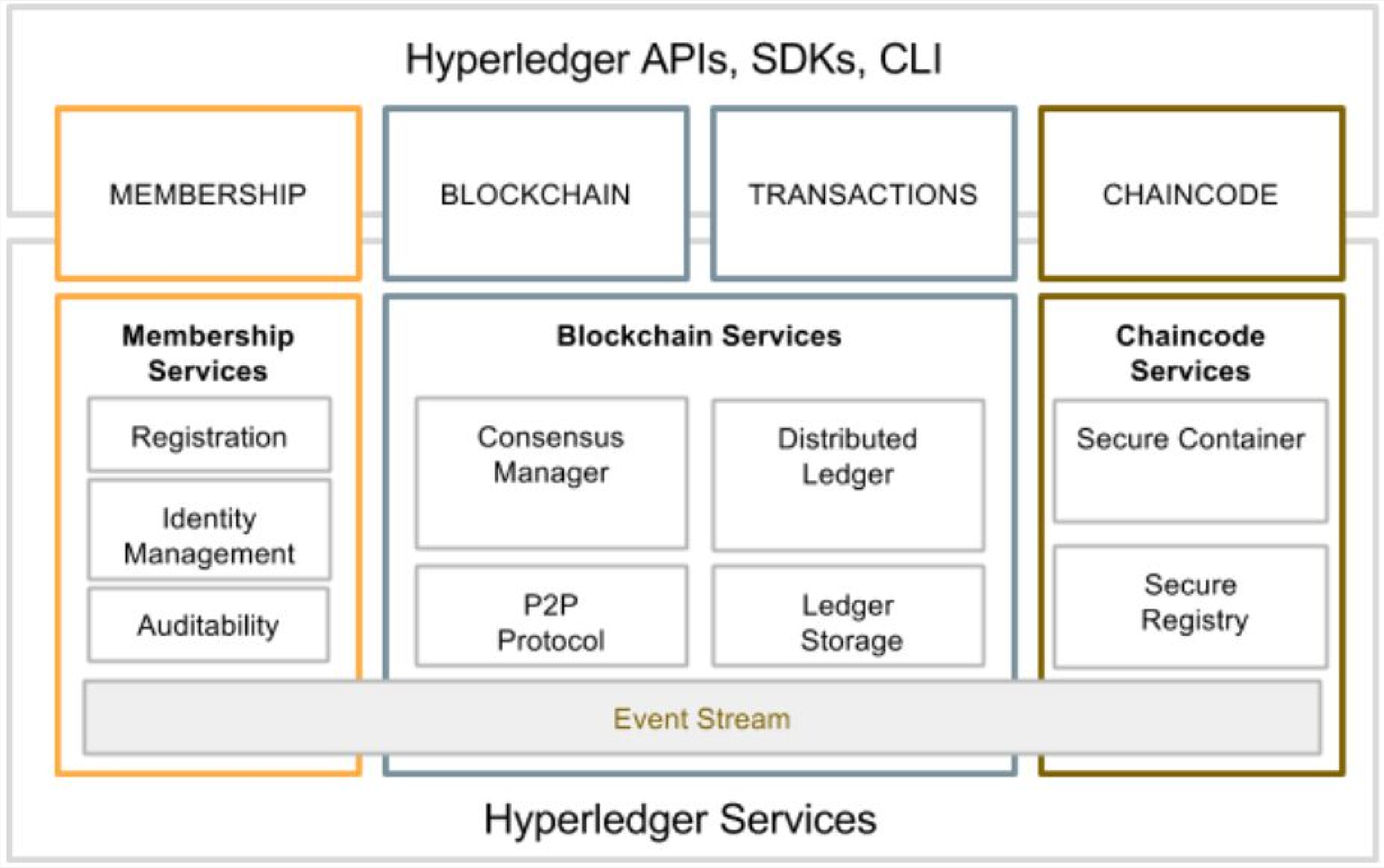
1. Identity and auditability
2. Private transaction and Confidential contracts
3. Modular consensus
4. Logic = *Chaincode = Smart Contracts*
5. Performance and Scalability



Link for Chaincode:
https://github.com/IBM-Blockchain/learn-chaincode

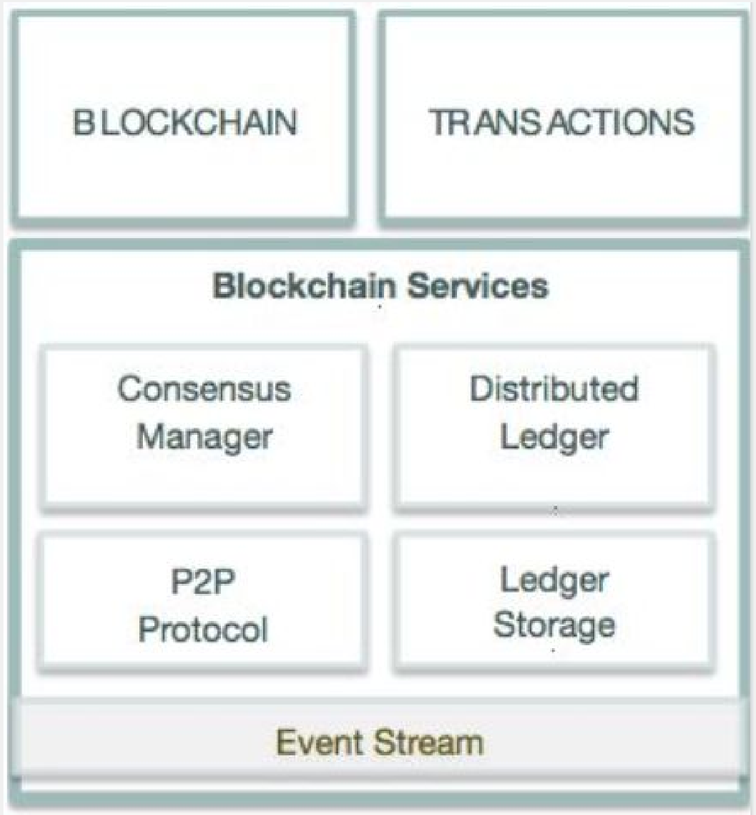
Requirements (Hyperledger Architecture)

HYPERLEDGER PROJECT



Blockchain Layer

HYPERLEDGER PROJECT



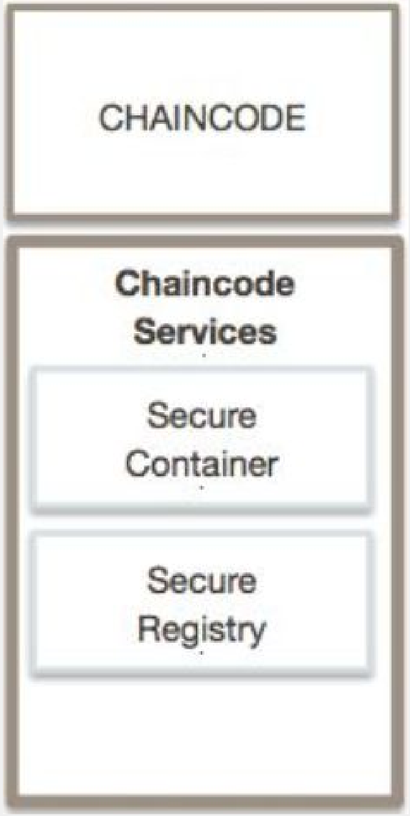
P2P Protocol uses G oogle RPC, which is implemented over HTTP/2 standards, providing many capabilities including bidirectional streaming, flow control, and multiplexing requests over a single connection.

Distributed Ledger manages the blockchain and the world state Distributed Ledger uses R ocksDB to persist the dataset, and builds an internal data structure to represent the state that satisfies the three attributes.

Consensus Manager is an abstraction that defines the interface between the consensus algorithm and the other Hyperledger components. Consensus Manager receives transactions, and depending on the algorithm, decides how to organize and when to execute the transactions. Successful execution of transactions results in changes to the ledger.

Chaincode Layer

HYPERLEDGER PROJECT



Chaincode as defined in the previous sections, a chaincode is a decentralized transactional program, running on the validating nodes.

Chaincode Services uses Docker to host the chaincode without relying on any particular virtual machine or computer language.

Secure Registry Services enables Secured Docker Registry of base Hyperledger images and custom images containing chaincodes.

Blockchain at Berkeley

Smart Contract Banking

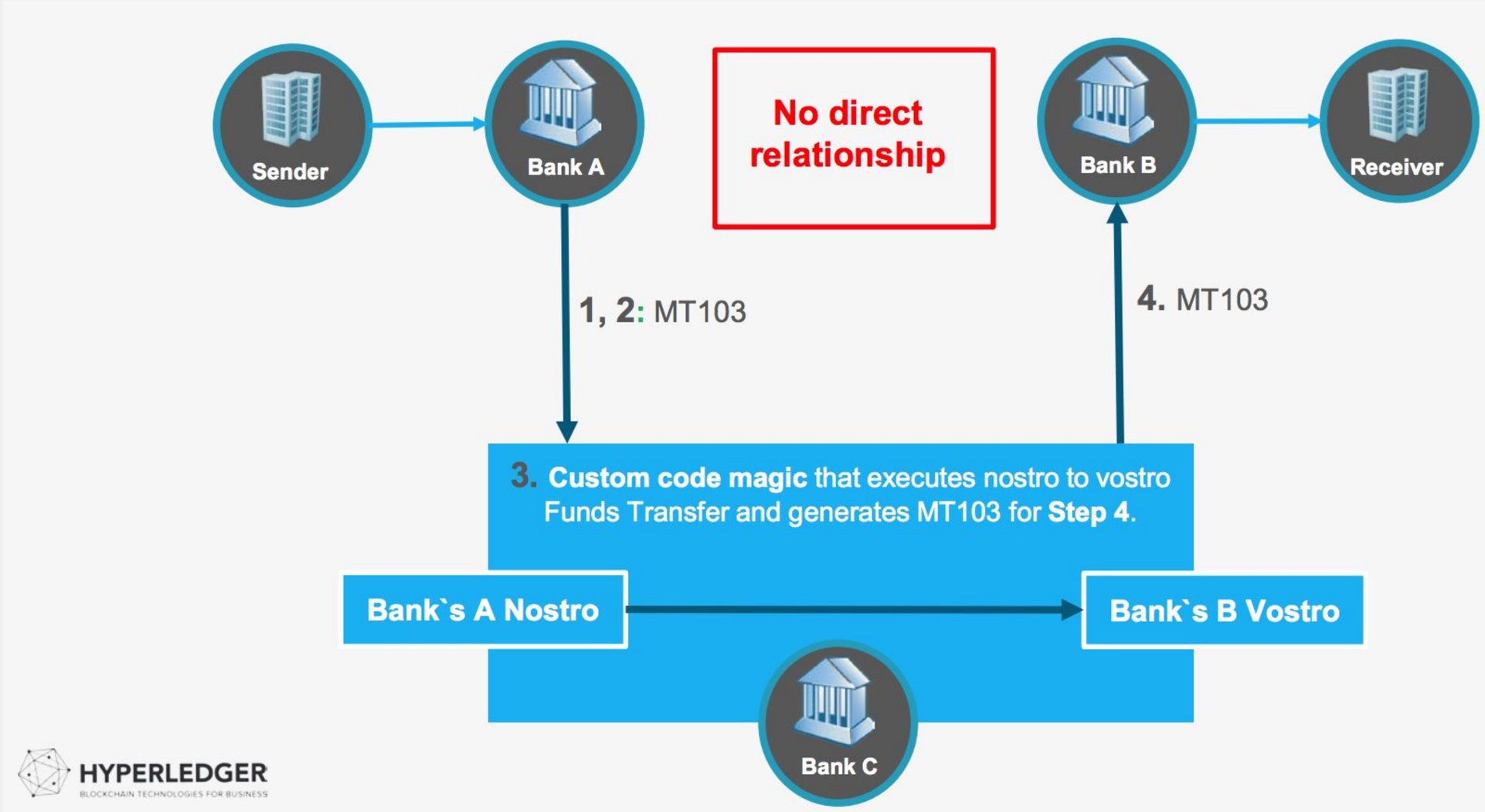
Why Smart Contracts in banking?

HYPERLEDGER PROJECT

- Preserve existing banking ecosystem, but optimize some of its processes
- Get Blockchain benefits today, rather than tomorrow

Traditional banking

HYPERLEDGER PROJECT



Example

HYPERLEDGER PROJECT

- A Smart Contract is the Financial Product served by Bank C to facilitate correspondent banking operations between Bank A and Bank B A MT103 received from Bank A triggers the execution of a chaincode (acting as a Smart Contract) which
- Validates whether bank A’s nostro account can be debited and respective bank B’s vostro can be credited
- Executes Nostro to Vostro funds transfer
- Generates MT103 to Bank B (optionally)

Example

HYPERLEDGER PROJECT

By Blockchain nature: A smart contract can automate business processes in a trusted way by allowing all stakeholders to process and validate contractual rules as a group (under permissioned model)

Goal

HYPERLEDGER PROJECT

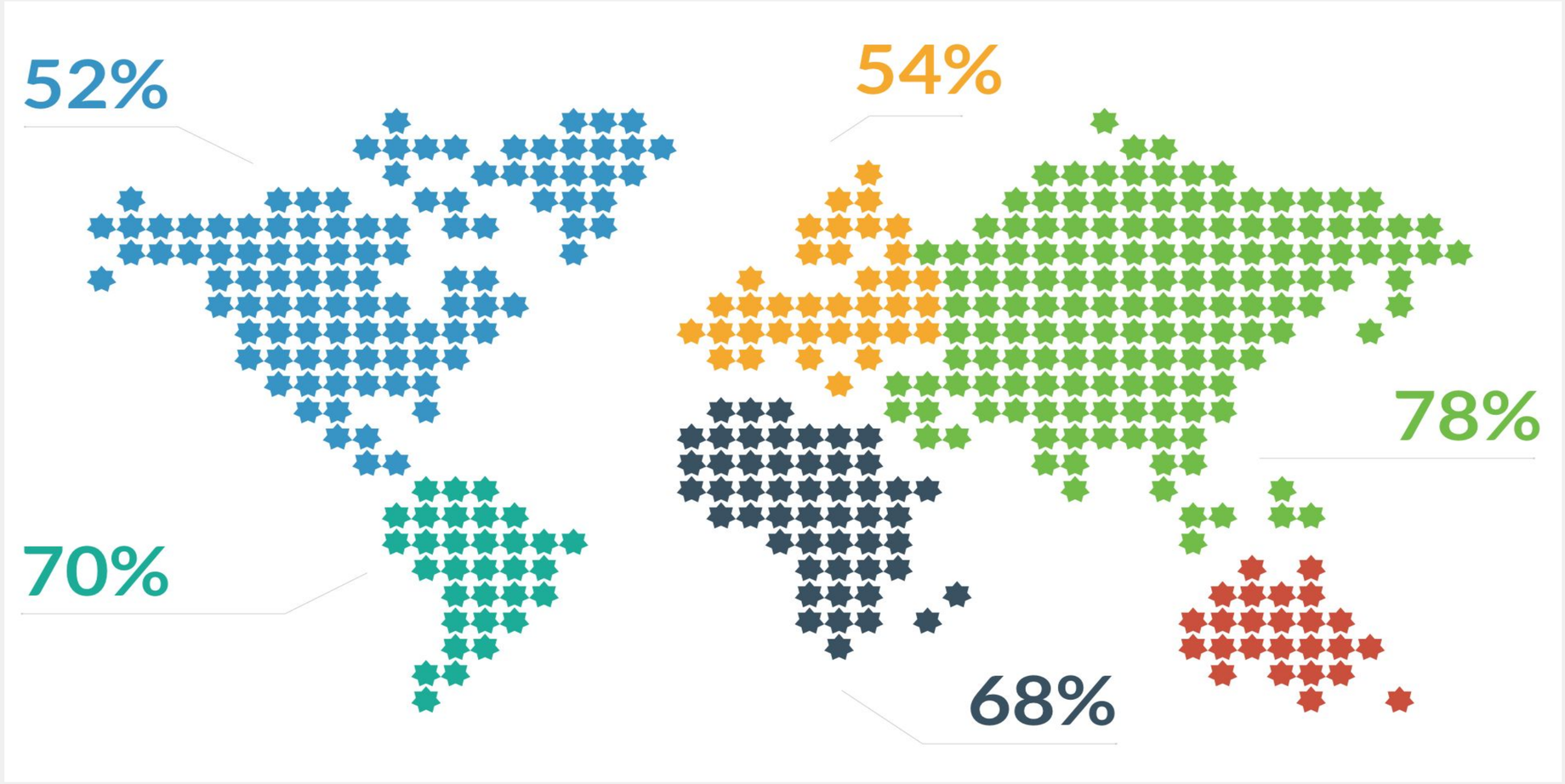
- Make correspondent banking transparent and traceable: chaincode and its execution gets viewed & monitored by all parties (under permission model)
- Minimize technical complexity in correspondent banking solutions: exclude middleware and back-office custom code: rely on smart contracts as a single standard
- Reach semi-peer-to-peer funds transfer eco-system

Blockchain at Berkeley

- Decentralize the sharing economy, empowering anyone to easily rent, share or sell anything that can be locked
- Opportunity to disrupt the disruptors such as Airbnb and other intermediaries that are based around some form of physical access.
- Slock.it is much more than a smart lock. That is simply the first application.

Blockchain at Berkeley

Willingness to share own assets per region



Blockchain at Berkeley

Turning Personal Assets into Income

- Rent access to apartment, houses and garages.
- Smart outlets for electric cars and drones
- Interactions without intermediaries between people and machines

Blockchain at Berkeley

- Slock.it sees the future, one without intermediaries but it starts with smart locks, and smart outlets.

- Autonomous cars, drones, and anything connected to the digital IoT world will be able to execute smart contracts.

Blockchain at Berkeley

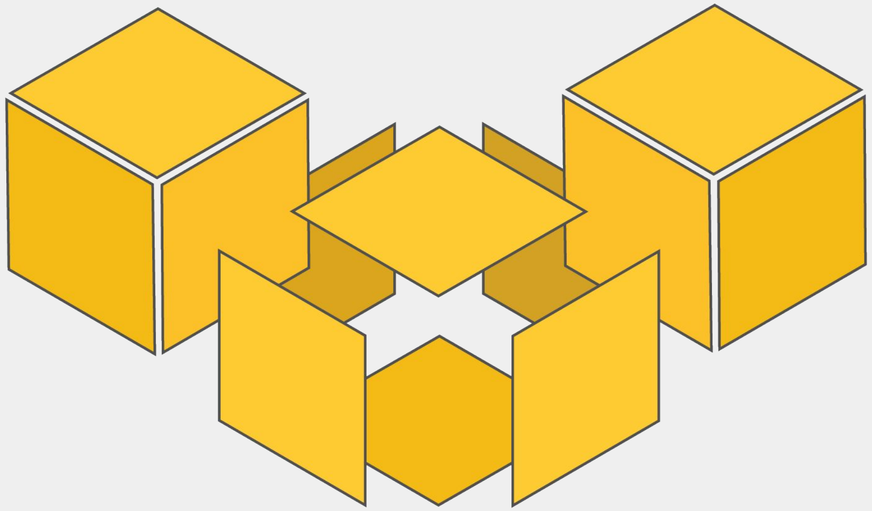
Slock.it realizes that in the Internet of Things:

- Give connected objects an identity.
- Create the ability to receive payments.
- Create the capability to enter complex agreements.

The world is asking for you!

Announcement

1. Presentations for next week
2. Will sent the prompt out tomorrow



Blockchain
AT BERKELEY

Thanks!

We're the world's first university-based blockchain consulting firm.

Like us on Facebook:
@Berkeleyblockchain
https://www.facebook.com/berkeleyblockchain/