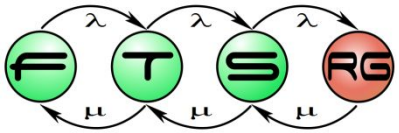
Blockchain
Technologies and Applications

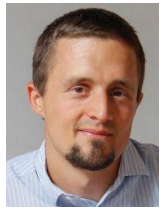
Prof. András Pataricza, pataric@mit.bme.hu
Dr. Imre Kocsis, ikocsis@mit.bme.hu
2020.02.13

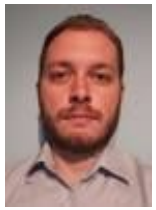
Budapest University of Technology and Economics
Fault Tolerant Systems Research Group



Blockchain@FTSRG

- **2016 IBM Faculty Award** (Prof. Pataricza András)
  - Teljesítménymodellezés és –elemzés, Duke kooperáció
- **Linux Foundation Hyperledger: associate membership**
- Kocsis Imre: **ISO/TC 307** nemzeti delegált
- Hyperledger Caliper
- Hyperledger Summer Internship-ek (!)
- **European Institute of Technology (EIT) Professional School:** “*Blockchain for the decision maker*”





A kurzusról

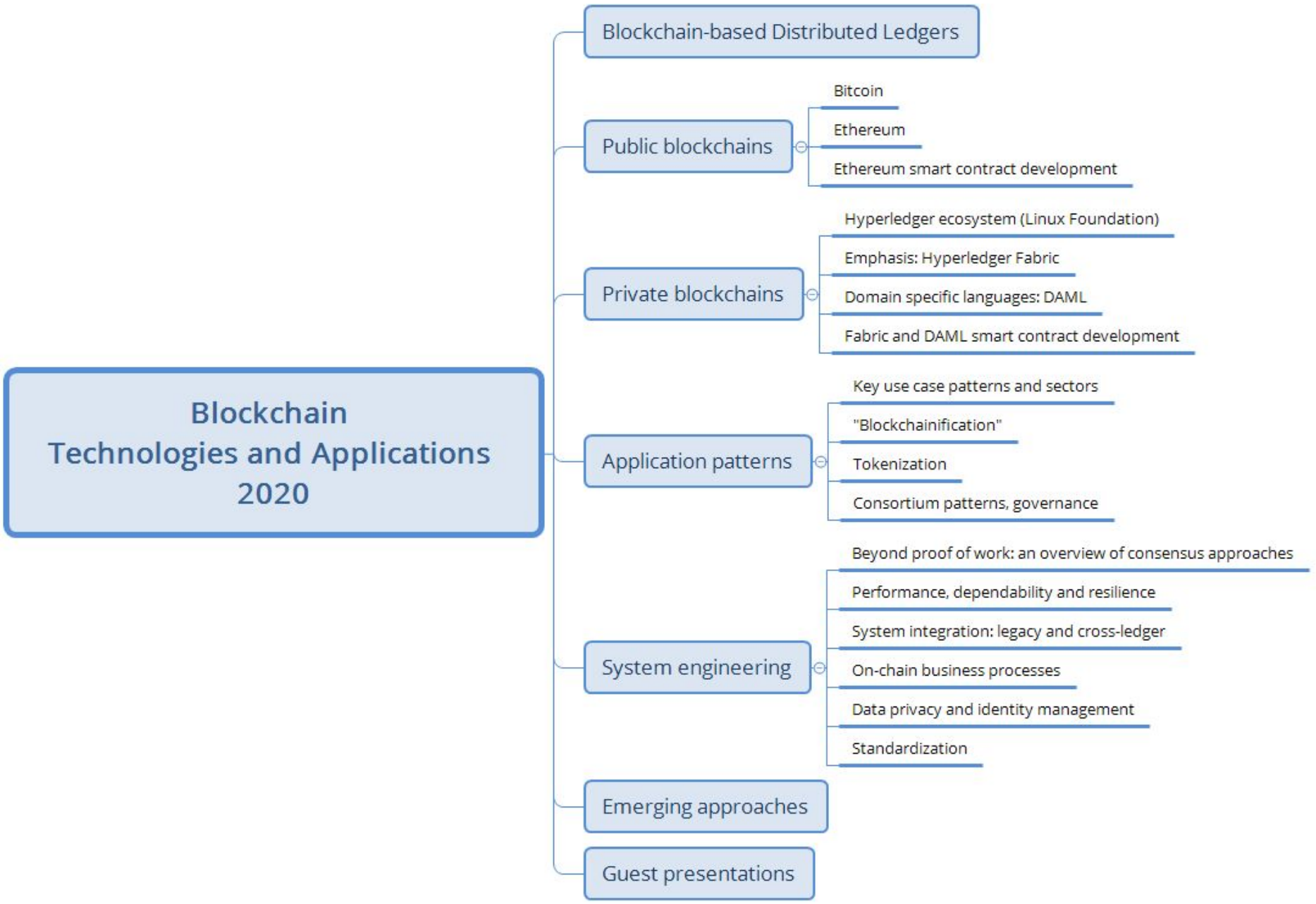
- **Nem (csak) Bitcoin – Blockchain**
  - A mai előadás témája

- Fő oktatási célok
  - Blockchain-ek rendszerszemlélete
  - Nem kripto, “Distributed Ledger Technology”
  - Alapvető alkalmazási esetek megismerése
  - Önálló alkalmazásfejlesztés megalapozása

- Választható tárgy; CS/CE csak mértékkel (~)

- Tárgykövetelmény: házi feladat

Topics we plan to cover during the course



DISTRIBUTED LEDGER TECHNOLOGY

Ledgers

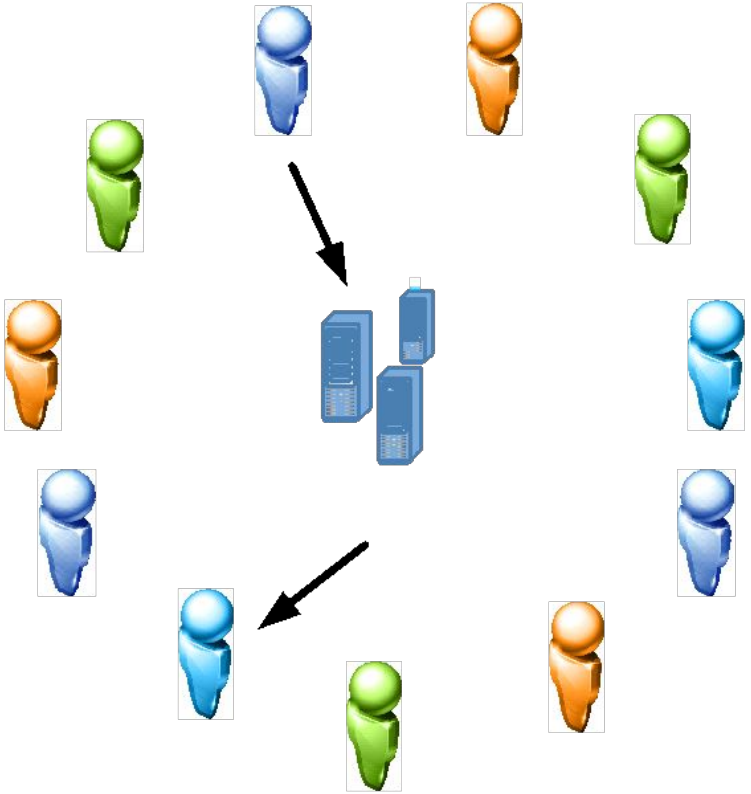
- Principal book of account
- Records transactions
- Append-only
- “Checksums”

- … but really, just a Tx log based “paper DB”

Based on: https://en.wikipedia.org/wiki/Ledger

Distributed ledgers: eliminating trusted 3rd parties

Centralized



Distributed ledger

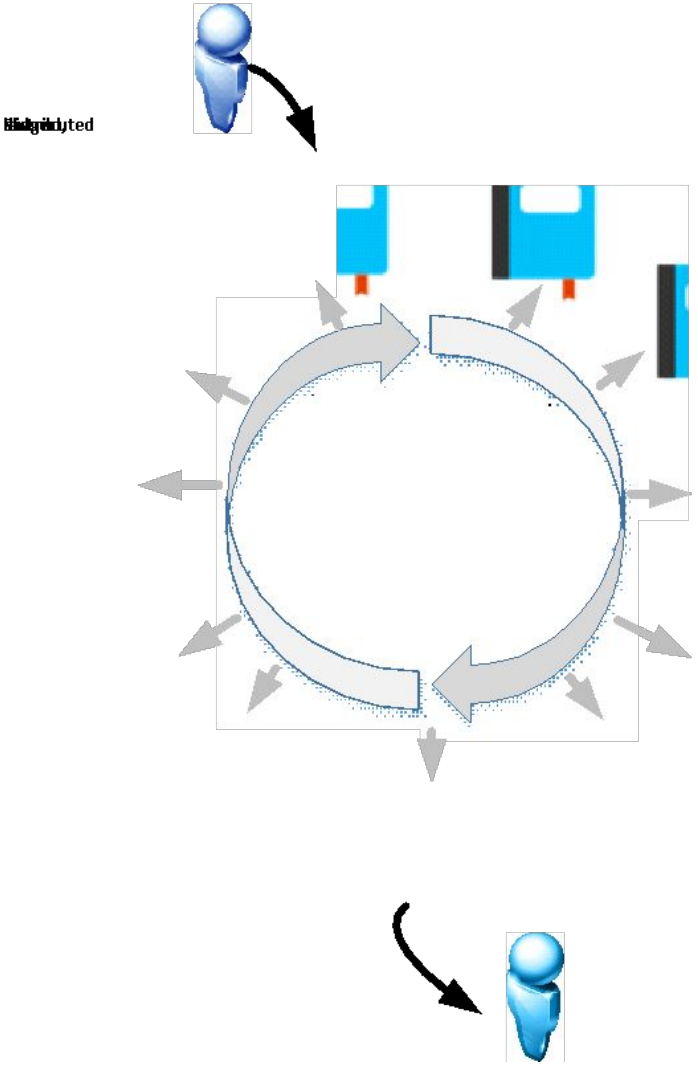
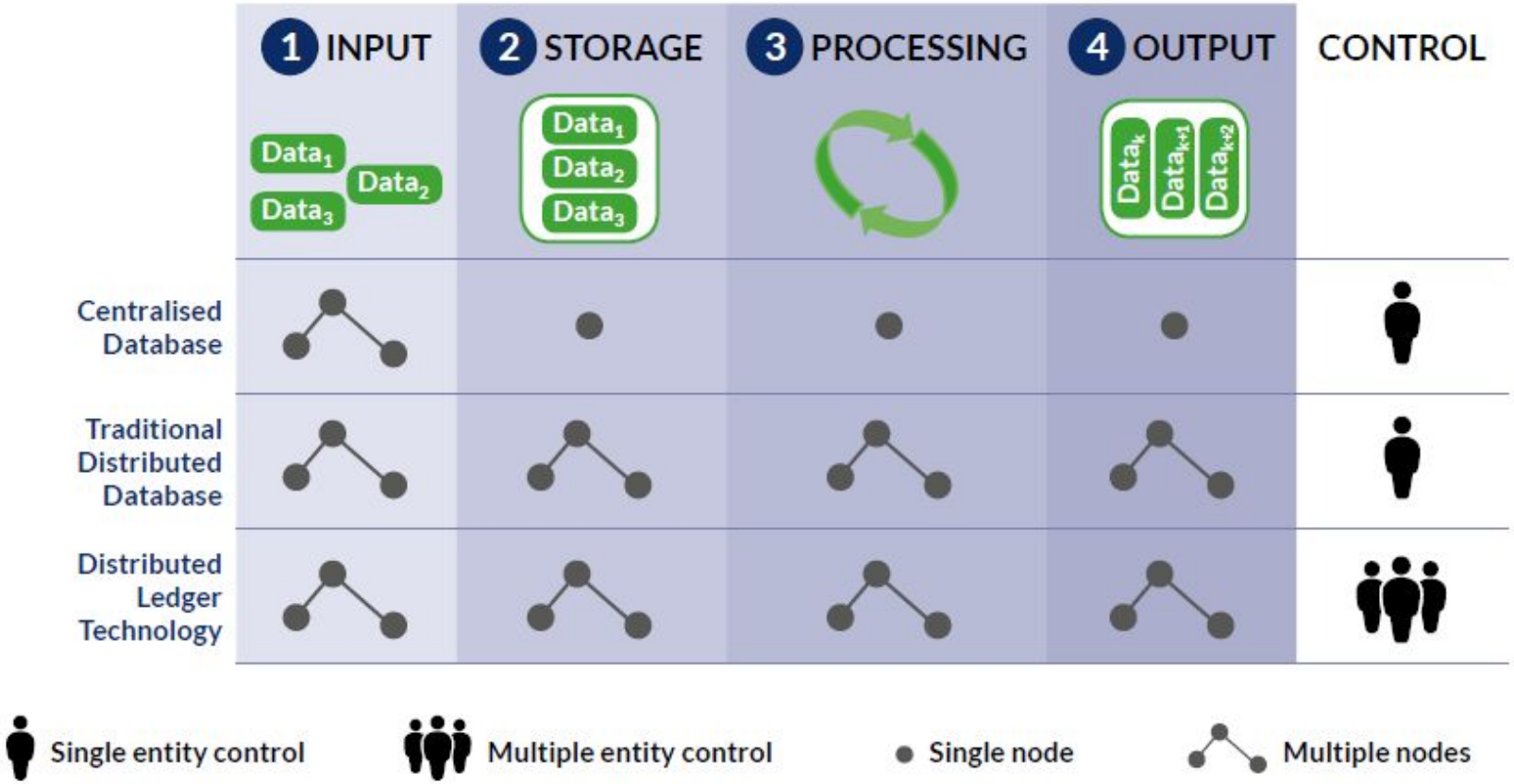


Figure 1: From Centralised Databases To Distributed Ledgers



Note: a traditional distributed database consists of multiple nodes that collectively store and process data, however, the nodes are generally controlled by the same entity as opposed to DLT systems where there are multiple controllers.

A DLT system is a system of electronic records that enables independent entities to establish a consensus around a shared 'ledger' - without relying on a central coordinator to provide the authoritative version of the records

M. Rauchs *et al.*, "Distributed Ledger Technology Systems: A Conceptual Framework," *SSRN Journal*, 2018, doi: 10.2139/ssrn.3230013.

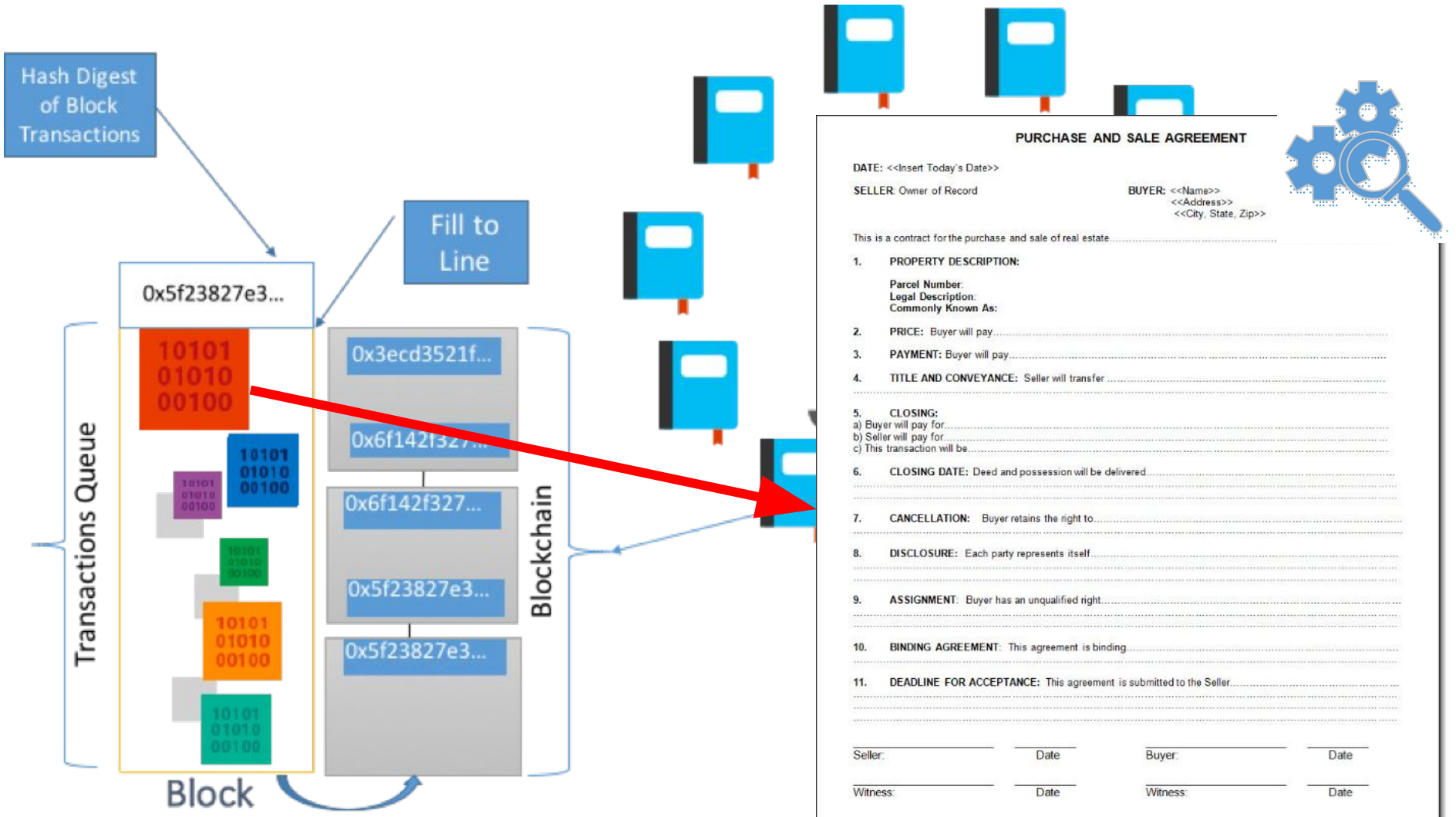
Trusted 3rd parties everywhere

- Communication: e.g. SWIFT
- Marketplaces: exchanges, eBay
- Auth. information: DNS, land registry
- Risk sharing: insurance
- Democracy: ele
- …

Leitmotif: "getting rid of the central party" … but not trust!

…hen have their price
…3rd party making the rules

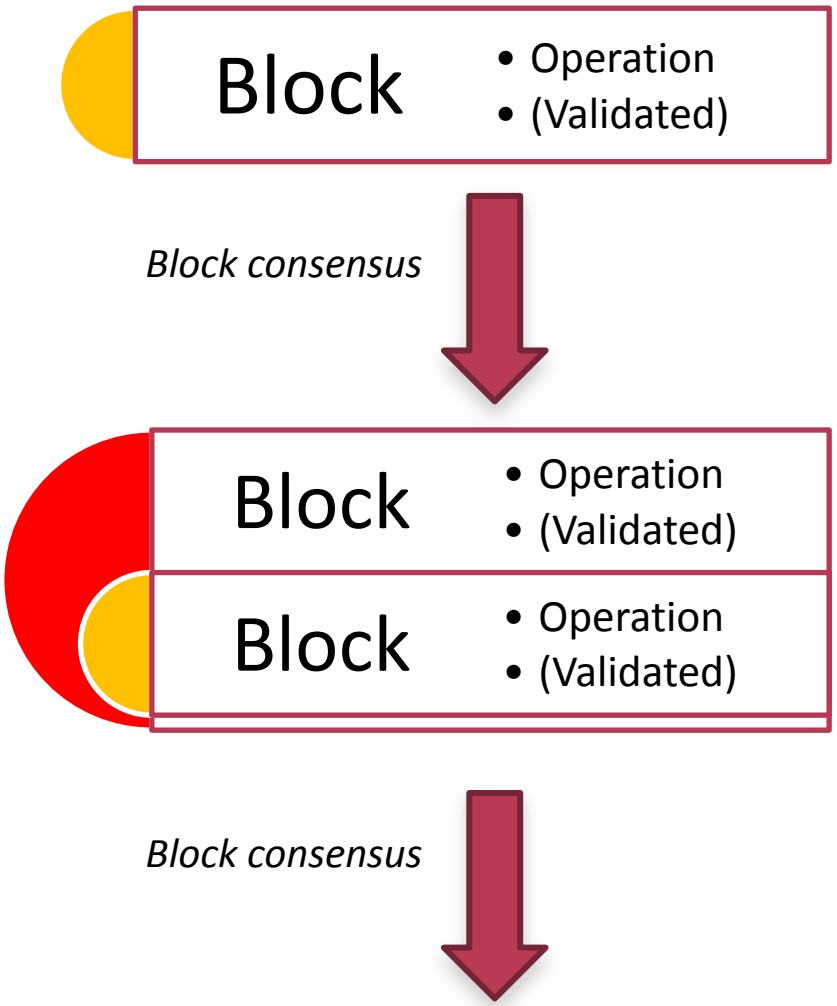
Blockchain technologies: a DLT approach



[1] Source: Marley Gray, Principle Architect PM – Microsoft: Introducing Project Bl

Replacing the middleman with the group

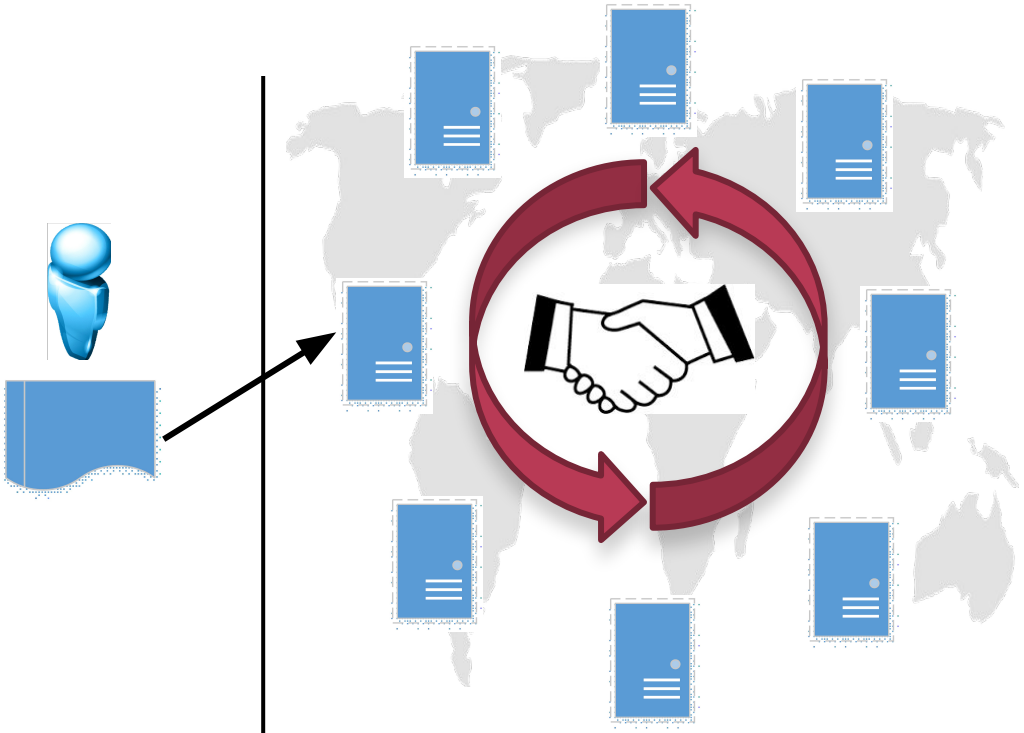
- **P2P network** of nodes
- Each peer: **same ledger**
  - Append-only Tx log
  - Hash-**chained block list**
- **Group consensus**
  - On Tx blocks
  - While certain % honest
- Client != peer

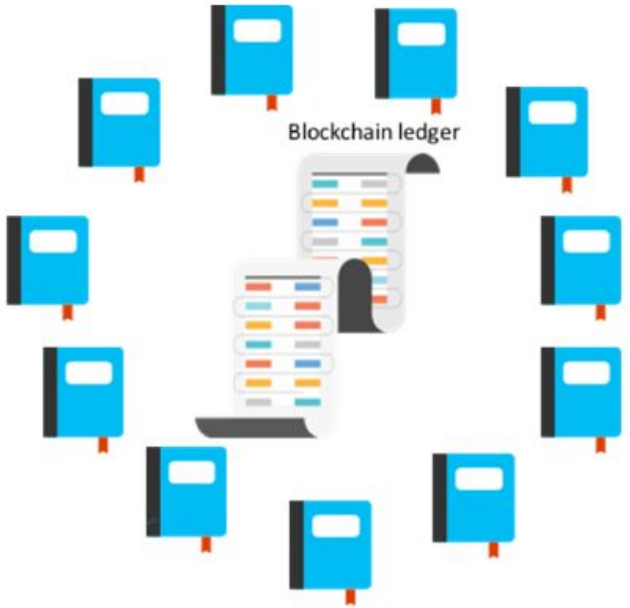


Blockchain properties

- **Ledger**: immutable Tx log; not (just) cryptocurrency!
- **Smart contracts**: programmed Tx logic over ledger state
- **Shared**: across pa
- **Distributed**: replication
- **Cryptographically authentic**: non-repudiable (secure identities), tokenization, signed Txs
- **Trust**: fault/attack tolerant group consensus

Basic transaction logic





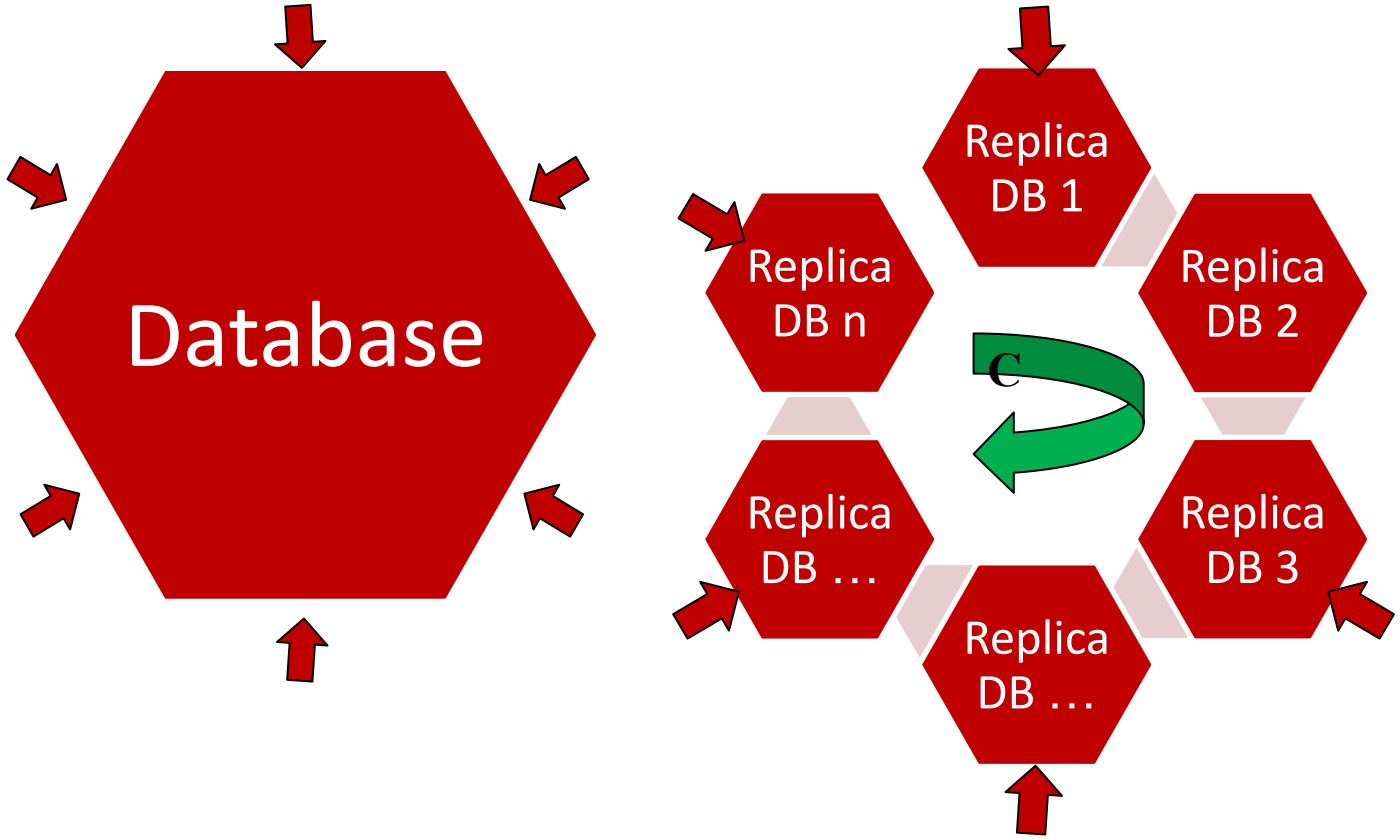
Client **request**

Order, contract exec result, acceptance: **consensus**

All **ledgers updated**

Batch processing < Blockchain latency < hard real-time

But when you peel off the complexity…



Main differences: *extra-functional*

Fully Decentralised System

Fully Centralised System

High censorship resistance	Low censorship resistance
High tamper resistance	Low tamper resistance
Low trust requirement	High trust requirement
Long confirmation time	Low confirmation time
Low throughput capacity	High throughput capacity
High overhead	Low overhead
Highly inefficient use of resources	Highly efficient use of resources

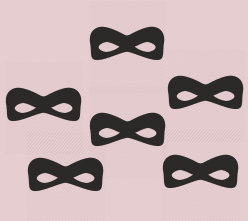
!!! Properties to be understood in an "as a rule" manner

ss desirable

M. Rauchs *et al.*, "Distributed Ledger Technology Systems: A Conceptual Framework," *SSRN Journal*, 2018, doi: 10.2139/ssrn.3230013.

SAME NAME, TWO(?) WORLDS

Public vs private/permissioned/consortium/…

	Network	Participants	Consensus	Transactions
(Bit/alt)coin				
Private/ permissioned blockchain				

„Not true, but a very, very good lie!"
(T. Pratchett, Nightwatch)

Some key points

- **(Cryptocurrency-based) public Blockchains**
  - Ledger *based on* some "unit of value"
  - Peer honesty incentive: "getting more of that"
    - "Mining", Tx fees + possibly deterrents
  - Bitcoin, Ethereum, Monero, Litecoin, …
  - Smart contracts
    - *defined on* and
    - *fueled by* cryptocurrency

We discuss all these in detail in later lectures

- **Private Blockchains**
  - Ledger: some data model
  - Peer honesty
    - A&A and real-world ramifications
    - Value intrinsic to cooperation
  - Smart contract: ledger is essentially a DB
  - **Hyperledger**, Enterprise Ethereum Alliance, Chain Core, …

Public example 1: Bitcoin

1. We fill in the details in the next lecture
2. Politics, “money” aspects, exchanges, …: coming lectures

- **“Ground zero” for Blockchains**
- **Ledger**: “who” has how many “coins”
- **P2P network**: open, global (but not your closet anymore)
- **Tx**: coin transfers
- **Client**: anybody (pseudonymous!)
- **New coins**: probabilistic, work-proportional peer reward

Figure: bitnodes.21.co

Public example 2: Ethereum

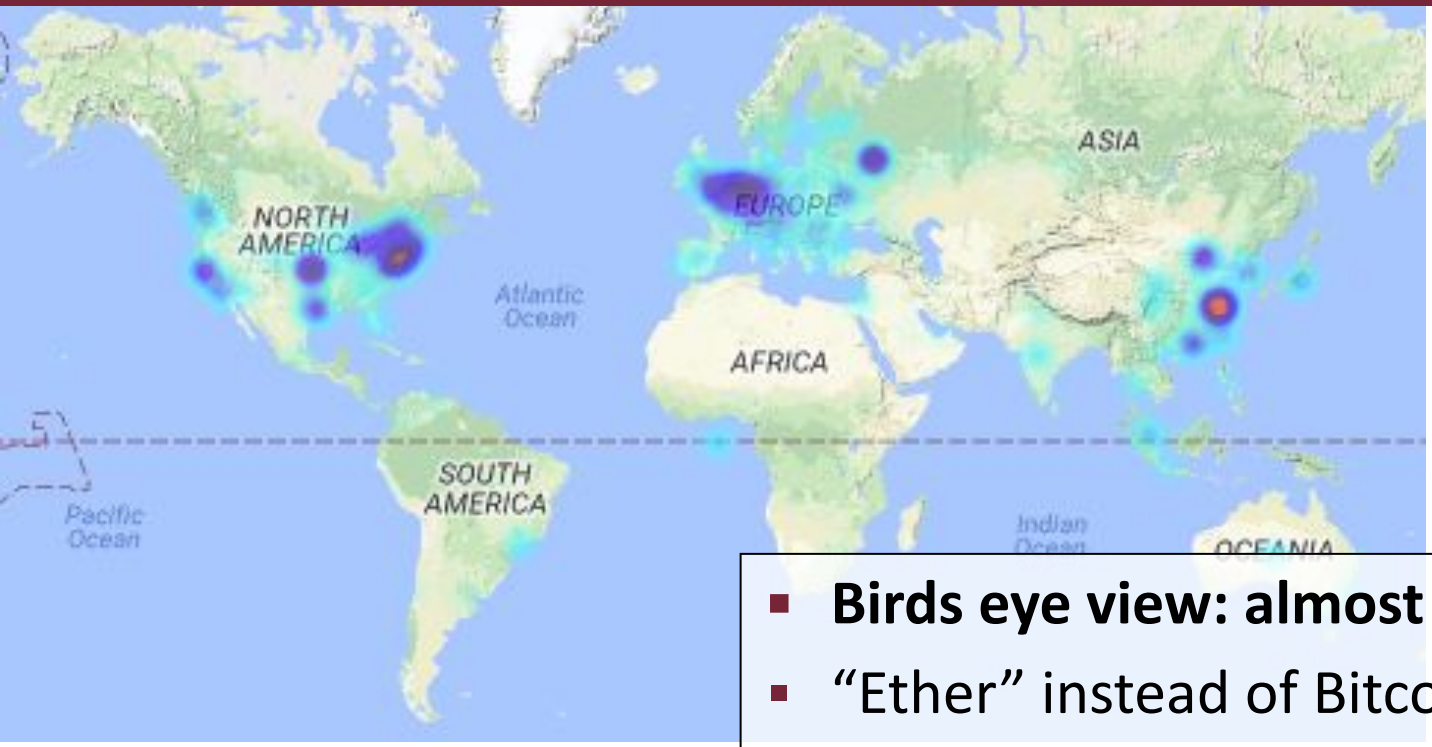


Figure: ethernodes.org

- **Birds eye view: almost like Bitcoin**
- "Ether" instead of Bitcoin

- **But**: you can attach code to an account
  - Fuel its execution with your crypto-funds
  - Have it collect/distribute Ether
  - Define your own "token" in a contract

Slight detour: Bitcoin price

coinbase Prices Products Company Earn crypto up to $186 Sign in Get started

In the last 24 hours

Market is down 0.52%

Search all assets... 24h All assets

#	Name	Price	Change	Market Cap	Trade
1	Bitcoin BTC	HUF 3,164,139.26	-0.82%	HUF 57.6T	Trade
2	Ethereum ETH	HUF 81,315.87	+3.70%	HUF 8.9T	Trade
3	XRP XRP	HUF 96.27	+7.98%	HUF 4.2T	Trade
4	Bitcoin Cash BCH	HUF 143,920.30	-1.70%	HUF 2.6T	Trade
5	Bitcoin SV BSV	HUF 109,919.80	-4.26%	HUF 2.0T	
6	Litecoin LTC	HUF 24,530.95	+1.03%	HUF 1.6T	Trade
7	EOS EOS	HUF 1,627.56	-1.55%	HUF 1.5T	Trade
8	Tether USDT	HUF 311.43	+0.01%	HUF 1.4T	
9	Binance Coin BNB	HUF 7,820.48	-1.91%	HUF 1.2T	
10	Tezos XTZ	HUF 944.91	-6.63%	HUF 654.6B	Trade
11	Cardano ADA	HUF 20.95	+4.57%	HUF 541.3B	
12	Stellar Lumens XLM	HUF 25.55	+6.02%	HUF 512.3B	Trade
13	Monero XMR	HUF 28,682.26	+1.21%	HUF 500.6B	

Ethereum: the very basics of token mechanics

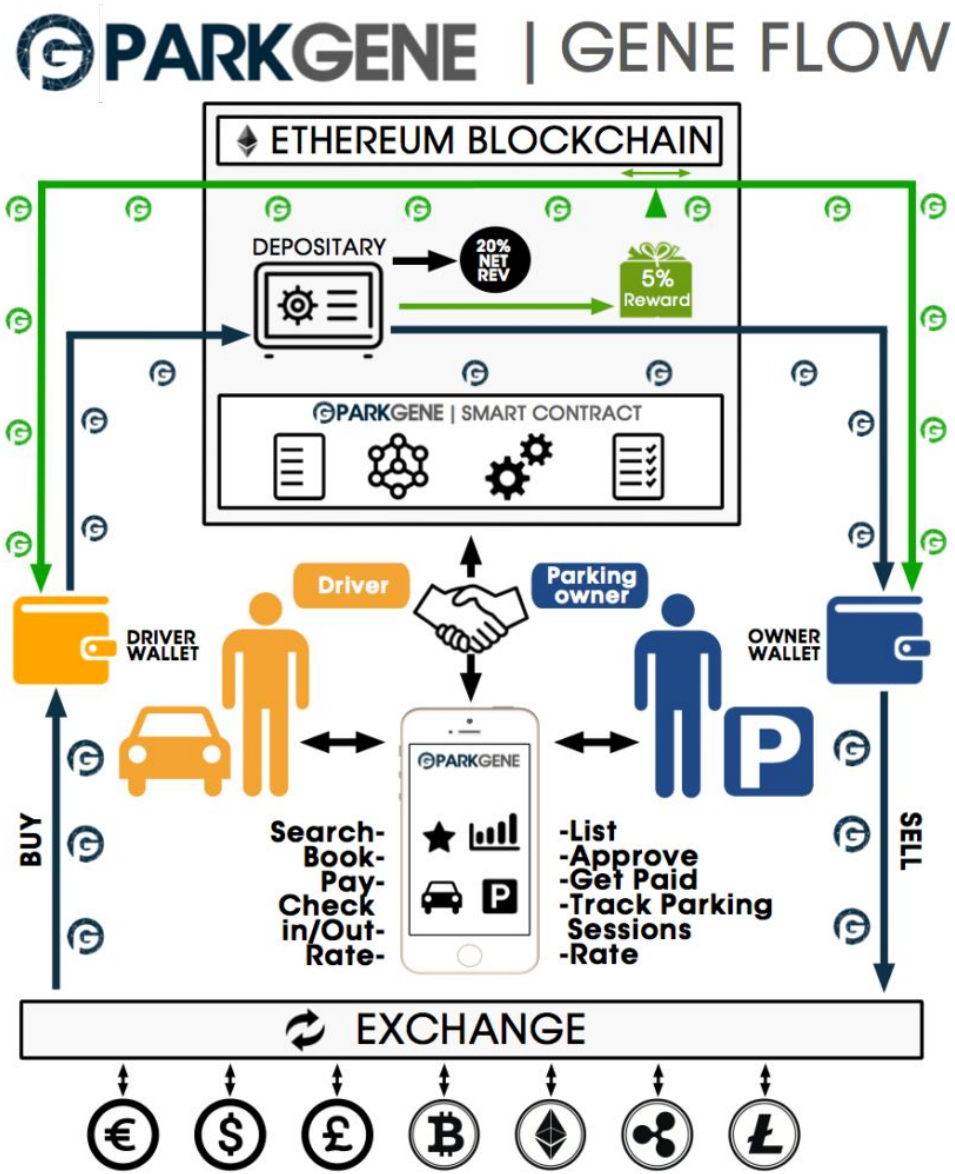
```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
}
```

You pay a little Ether for function calls
But can also sell the token
Contract state and logic “is your business”

Some Ethereum smart contracts

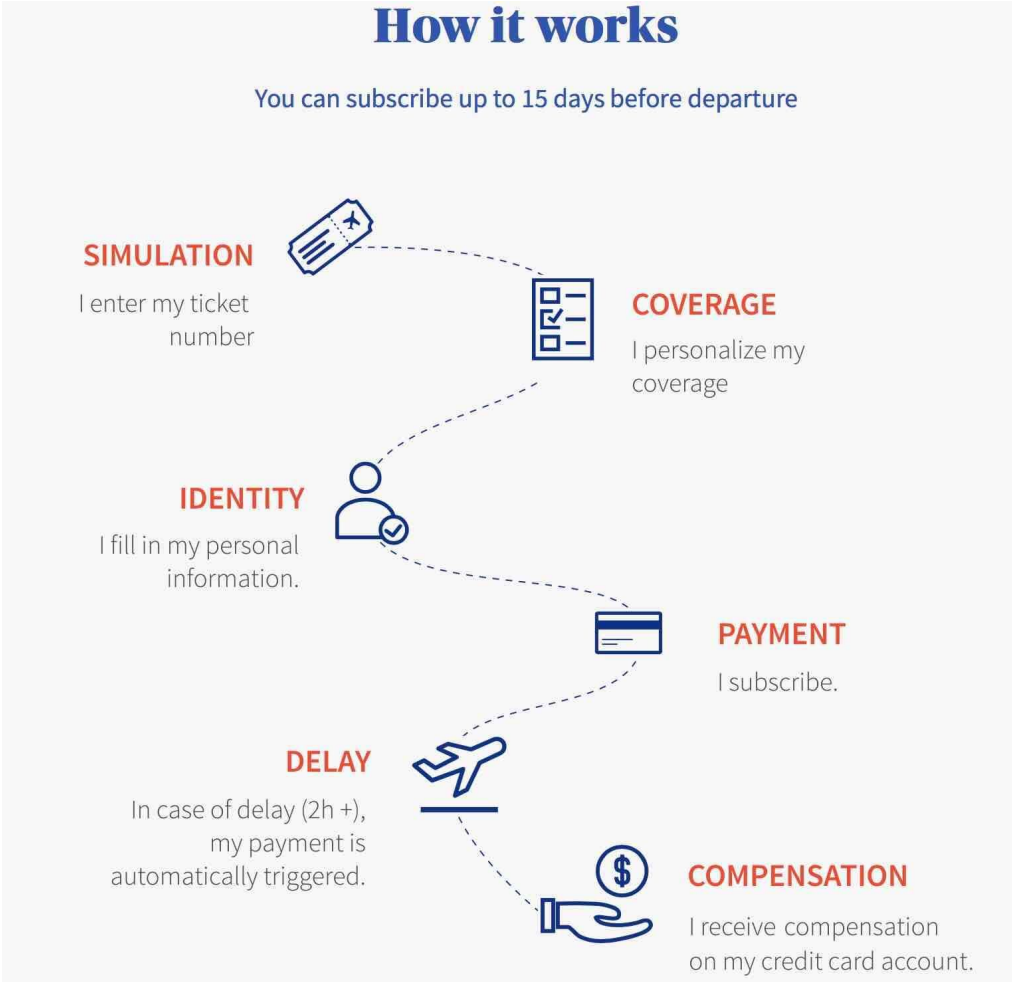


Source: https://parkgene.io/

Some Ethereum smart contracts

- On-chain, “programmed” claim assessment
- Long, closed, manual process transformed into transparent automatism
- Ethereum
  - Privacy?

- But: risk ownership and management not crowd/consortium-sourced
  - Could be; many startups!
- Claim assessment is “only” automated, too



Source: https://fizzy.axa/

Zug Citizens Begin Digital ID Registration on an Ethereum Blockchain

Uport, a self-sovereign identity and user-centric data platform on the Ethereum blockchain, has made its platform available to the citizens of Zug, Switzerland.

The first official Zug identification registered on the Ethereum blockchain before a live audience, Uport recently announced in a Medium blog.

Access To E-Services

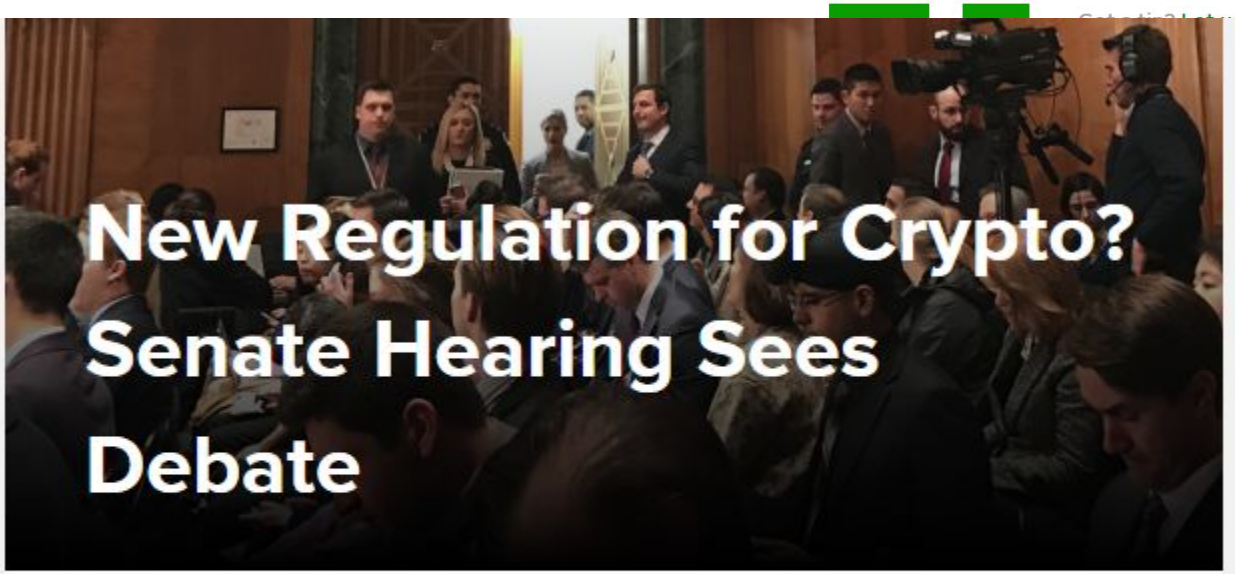
Uport partnered with Zug, commonly known as the "Crypto Valley" for hosting a number of industry startups, on the program to register residential IDs on the blockchain, enabling access to e-services such as proof of residency and online voting. Uport has been developing the platform in cooperation with ti&m, its Swiss partner.

Ethereum

- *Decentralized autonomous organizations?*
  - Well… We will talk about the DAO hack

- ICO: “buying into” an idea
  - Business share, stake, right to use, …
- Many “Initial Coin Offerings” are (were) scams
- Look around!
  - https://icotracker.net/
  - http://www.icocountdown.com/
  - …

Cryptocurrencies: uncertain future



336 49 1

FORTUNE

Bitcoin Might Soon Face Tougher Regulatio

money, though this risk is expected to grow," the Treasury said. "Tha is why these regulations will help."

Two Nobel economics laureates denounced Bitcoin last month. Joseph Stiglitz said it should be outlawed, and doesn't serve "an socially-useful function." Robert J. Shiller said the attraction of

know.

o Events Crunchbase Message Us

s reportedly moving to clamp dov

8 by Jon Russell (@jonrussell)

China banned bitcoin, ICOs and now it appears to be clamping down on Chinese miners, an important group estimated to produce some three-quarters of the world's supply of bitcoin.

On the other hand: DLT enjoys universal support.

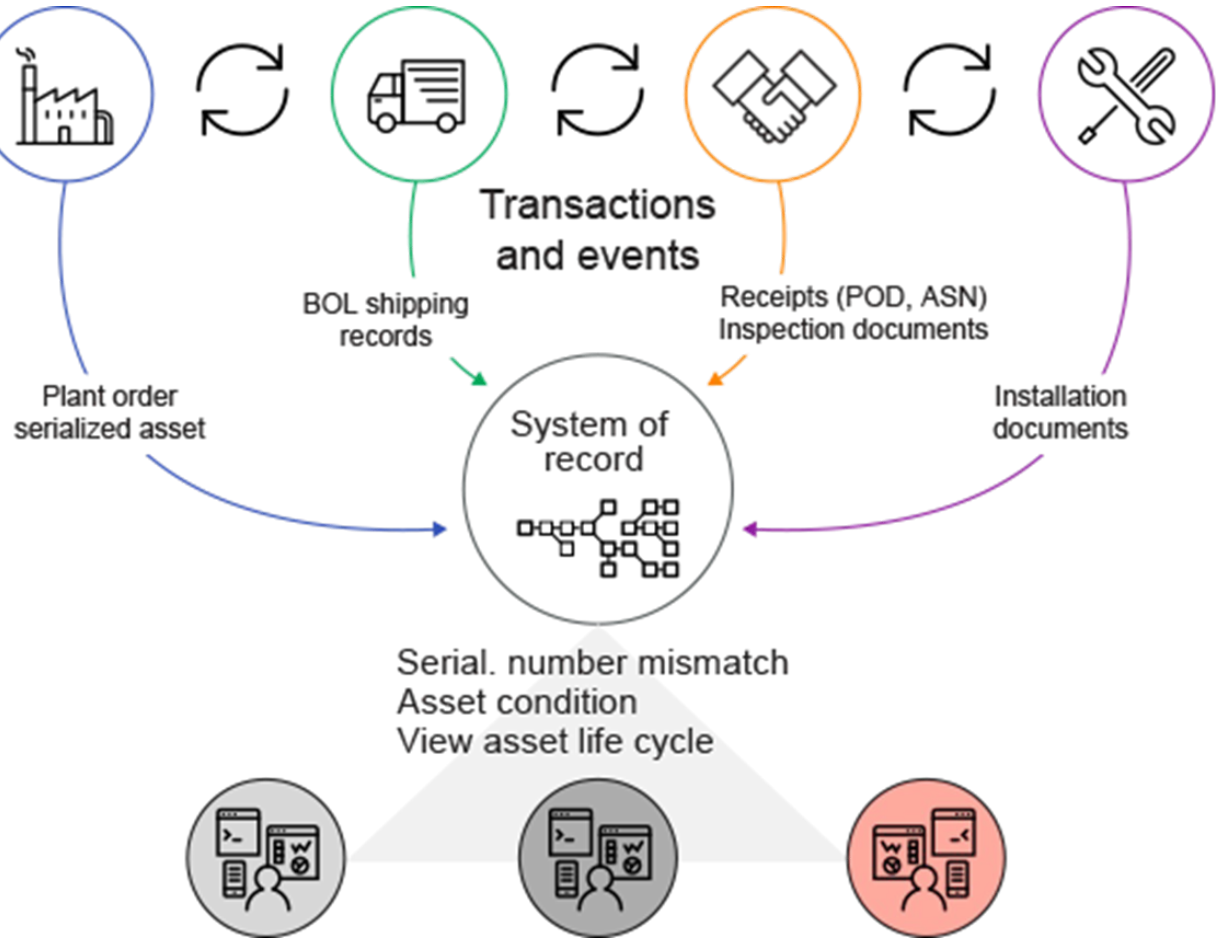
Private Blockchains: asset/supply management

- “Small”, closed network
- Peer + client A&A
- “Weighted” voting
- Arbitrary Tx logic

These are intended!

You can have (asset) tokens

But don’t have to



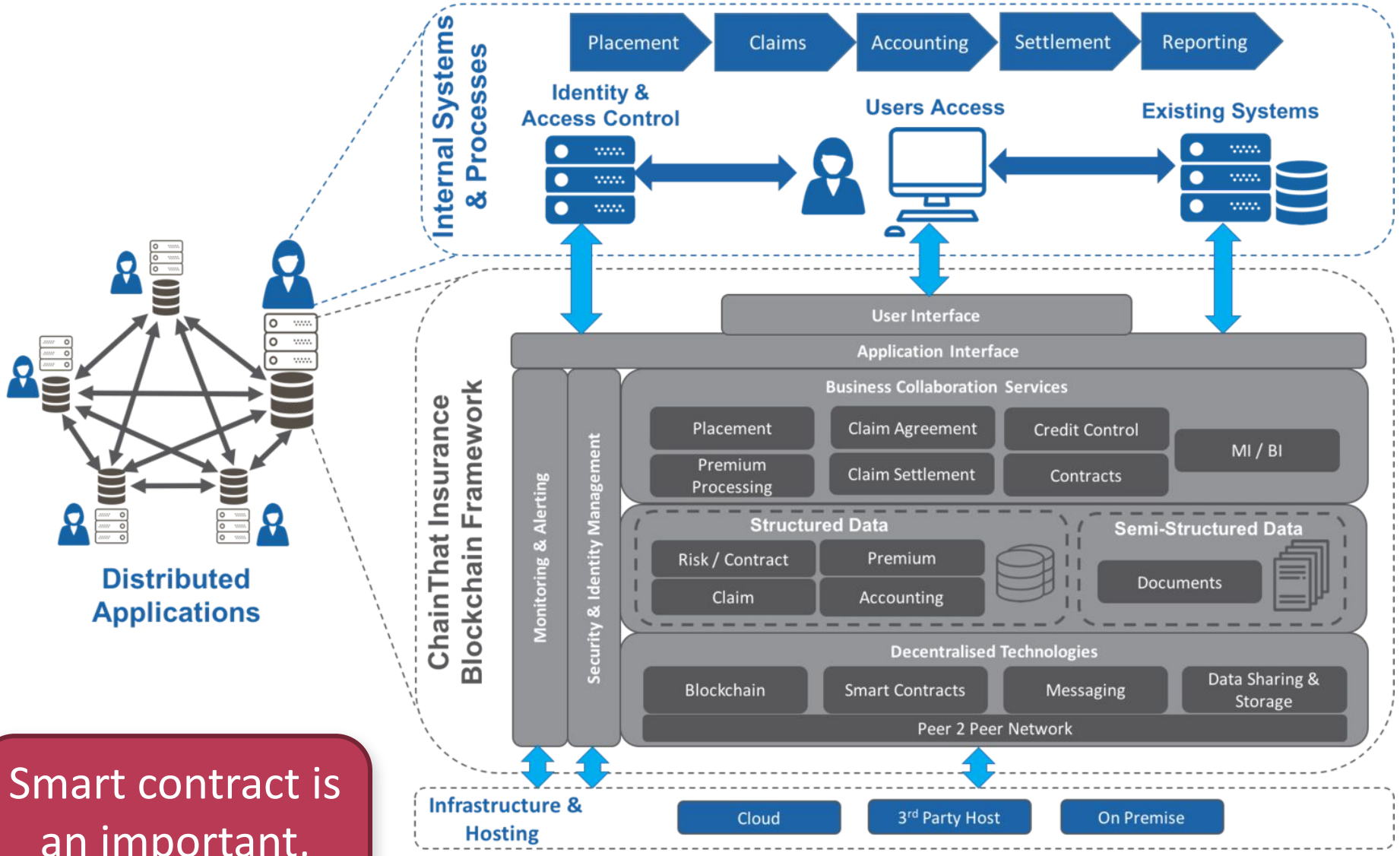
Ábra: IBM: Adopting Blockchain for enterprise asset management (EAM)

A success story: MAERSK and IBM

Ports and Terminals	**Provide** information about the disposition of shipments within the boundaries of the port / terminal **Benefit from** pre-built connections to shipping lines and other actors, end-to-end visibility across shipping corridors, and real-time access to more information to enrich port collaboration and improve terminal planning
Ocean Carriers	**Provide** information about the disposition of shipments across the ocean leg **Benefit from** pre-built connections to customers and ports / terminals around the world and real-time access to end-to-end supply chain events
Customs Authorities	**Provide** information about the export and import clearance status for shipments into and out of the country **Benefit from** more informed risk assessments, better information sharing, less manual paperwork, and easier connections to national single window platforms
Freight Forwarders / 3PL	**Provide t**he transportation plan, inland transportation events, information on intermodal handoffs, and document filings **Benefit from** pre-built connections to the ecosystem, improved tools for customs clearance brokerage function, and real-time access to the end–to-end supply chain data to improve effectiveness of track-and-trace tools
Intermodal Transport	**Provide** information on the disposition of shipments carried on trucks, rail, barges, etc. **Benefit from** improved planning and utilization of assets (e.g., less queuing) given real-time access to end-to-end supply chain events for shipments
Shippers	**Engage** with the solution as a consumer of the shipping information events and paperless trade capabilities **Benefit from** a streamlined and improved supply chain allowing for greater predictability, early notification of issues, full transparency to validate fees and surcharges, and less safety stock inventory

Both examples over Hyperledger fabric (Linux Foundation)

Closed markets: reinsurance



http://www.chainthat.com/framework/

Smart contract is an important, but small part!

Not only enterprise/business!

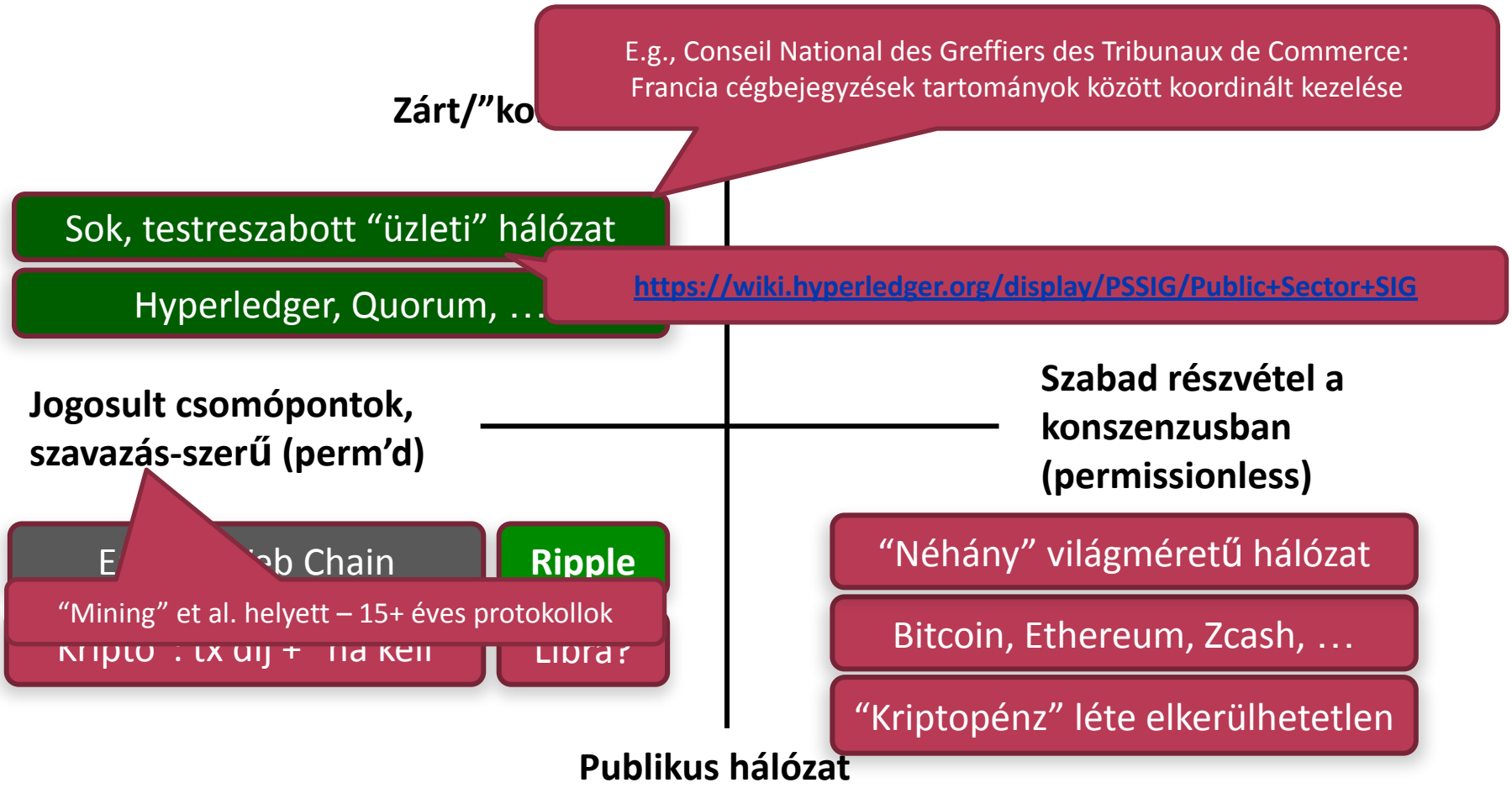
Government services that survey respondents would like to see using blockchain technologies to improve efficiencies and public access

Land Transfers and Property Title registrations	72.1%
Personal Identification and Passport Documentation	68.9%
Management of Health Records	65.6%
Vehicle Registrations	54.1%
Welfare Distribution and Monitoring	37.7%
Urban planning; wider pedestrian sidewalks, increased times for crossings	21.3%
Public Transport Scheduling	16.4%

Source: Blockchain survey, Standards Australia analysis

Note: it is situational, whether the public or private model fits better

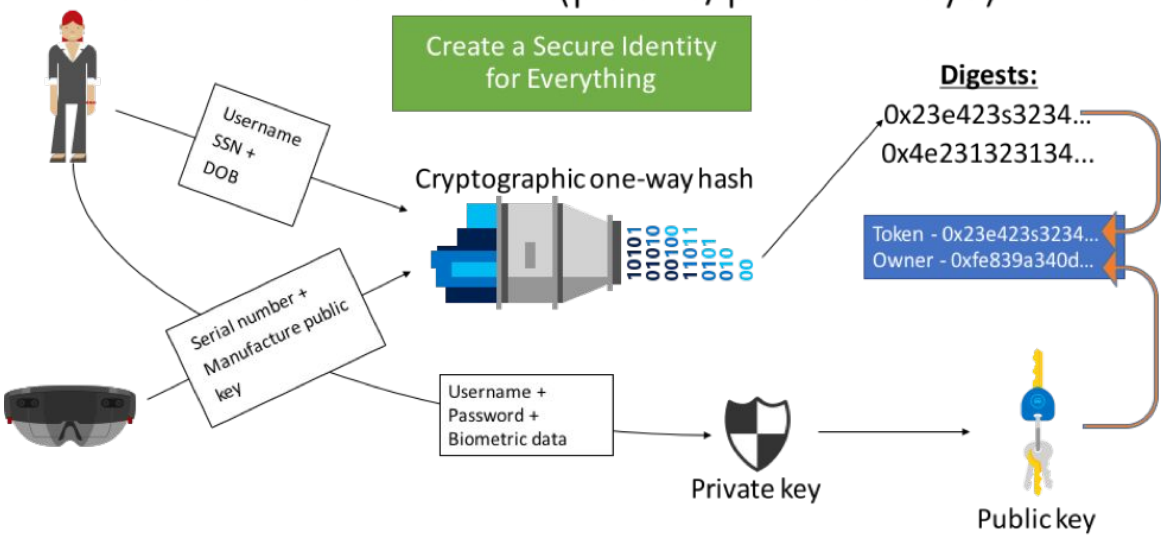
Egy teljesebb taxonómia



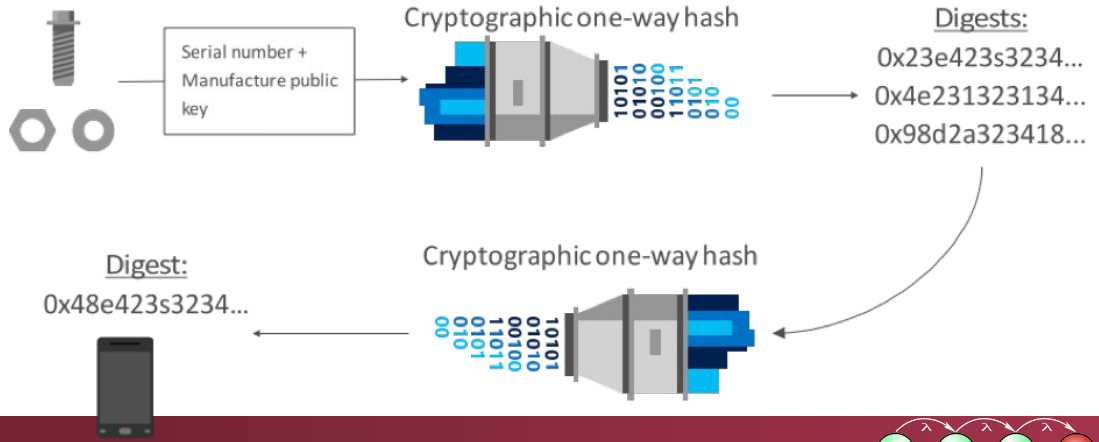
DIGITAL ASSETS AND TOKENIZATION

Cryptographic tokenization of assets

Basics – Tokenization (public/private keys)

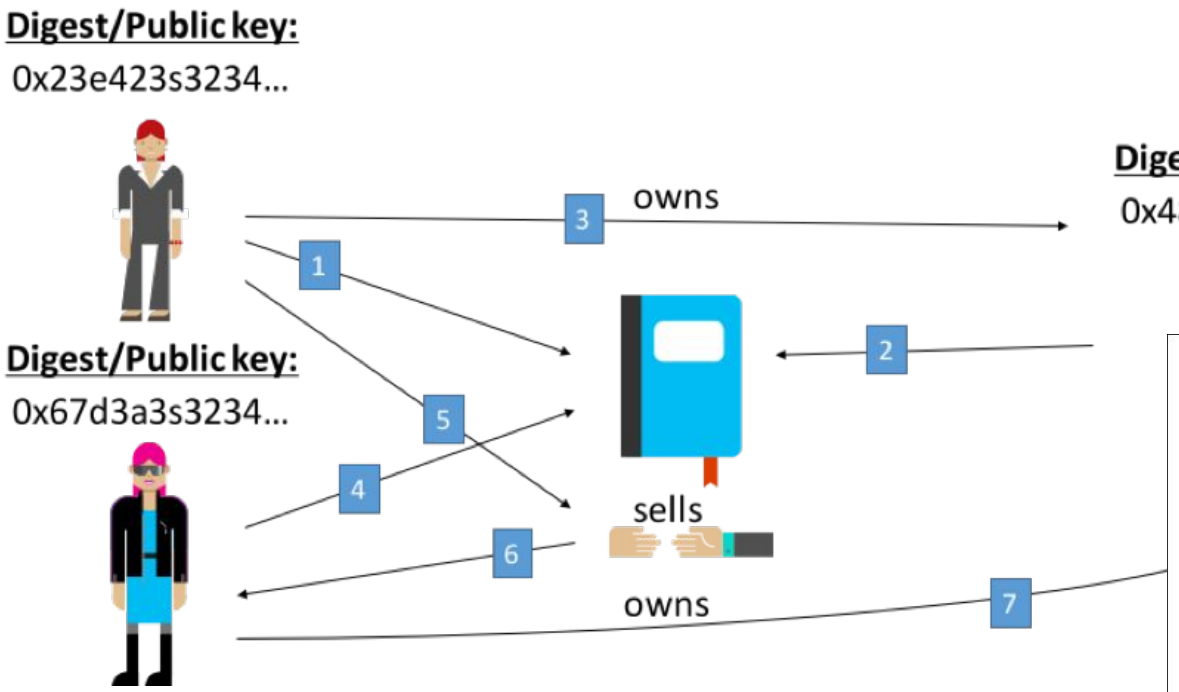


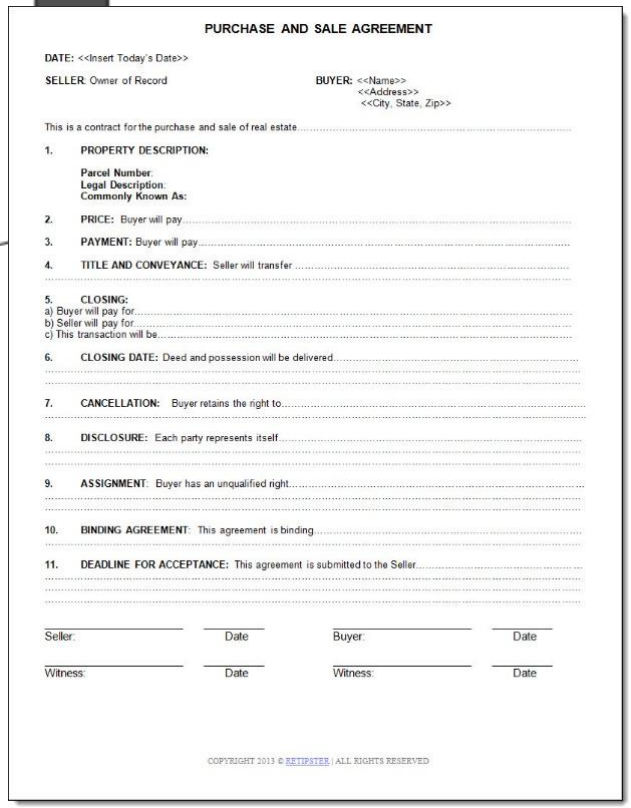
Basics – Tokenization composites



Source: Introducing Project "Bletchley" *Marley Gray, Principle Architect PM - Microsoft - Azure Blockchain Engineering*

Smart contracts over tokenized assets





PURCHASE AND SALE AGREEMENT

DATE: <<Insert Today's Date>>

SELLER: Owner of Record

BUYER: <<Name>>
<<Address>>
<<City, State, Zip>>

This is a contract for the purchase and sale of real estate.

1. **PROPERTY DESCRIPTION:**
   Parcel Number:
   Legal Description:
   Commonly Known As:
2. **PRICE:** Buyer will pay
3. **PAYMENT:** Buyer will pay
4. **TITLE AND CONVEYANCE:** Seller will transfer
5. **CLOSING:**
   a) Buyer will pay for
   b) Seller will pay for
   c) This transaction will be
6. **CLOSING DATE:** Deed and possession will be delivered.
7. **CANCELLATION:** Buyer retains the right to
8. **DISCLOSURE:** Each party represents itself
9. **ASSIGNMENT:** Buyer has an unqualified right
10. **BINDING AGREEMENT:** This agreement is binding.
11. **DEADLINE FOR ACCEPTANCE:** This agreement is submitted to the Seller.

Seller: Date Buyer: Date

Witness: Date Witness: Date

Source: Introducing Project "Bletchley" *Marley Gray, Principle Architect PM - Microsoft - Azure Blockchain Engineering*

But what do you put on the ledger?

- Tracking the ownership of money
  - Cryptocurrency is actually a special case
  - Could be even fiat
- Tracking the ownership/status of assets
  - Physical, logical, financial
  - Cryptographic tokenization
- But you can use it as a database, too
- Changes will be ruled by smart contracts
- We will demonstrate these concepts as we progress

Some digital asset types

- Cryptocurrency
- Central bank currency
- Digital currency
- Commodity-backed tokens
- Equity tokens
- Accounting tokens
- Digital collectible
- Utility tokens

https://www.coindesk.com/periodic-table-blockchain-classify-tokens/

THE FOURTH INDUSTRIAL REVOLUTION?

Industrial revolutions

- 1st: urbanization, steam engine
- 2nd: steel, oil, electricity, internal combustion engine
- 3rd: digitization, ICT, Internet
- 4th: technology embedded within societies
  - DLT is identified as a key component

*We've never had this capability before – **trusted transactions directly** between two or more total strangers, **authenticated by mass collaboration**, and powered by **collective self-interests**, rather than by corporations motivated by profit or governments motivated by power.*

Source: World Economic Forum: Realizing the Potential of Blockchain, June 2017.

2017: “A rapidly emerging sector”

Harvard Business Review

INFORMATION & TECHNOLOGY

The Promise of Blockchain Is a World Without Middlemen

by Vinay Gupta

MARCH 08, 2017

in Will Do

ystem

Giving Unchained: Pl

the Blockchain

So

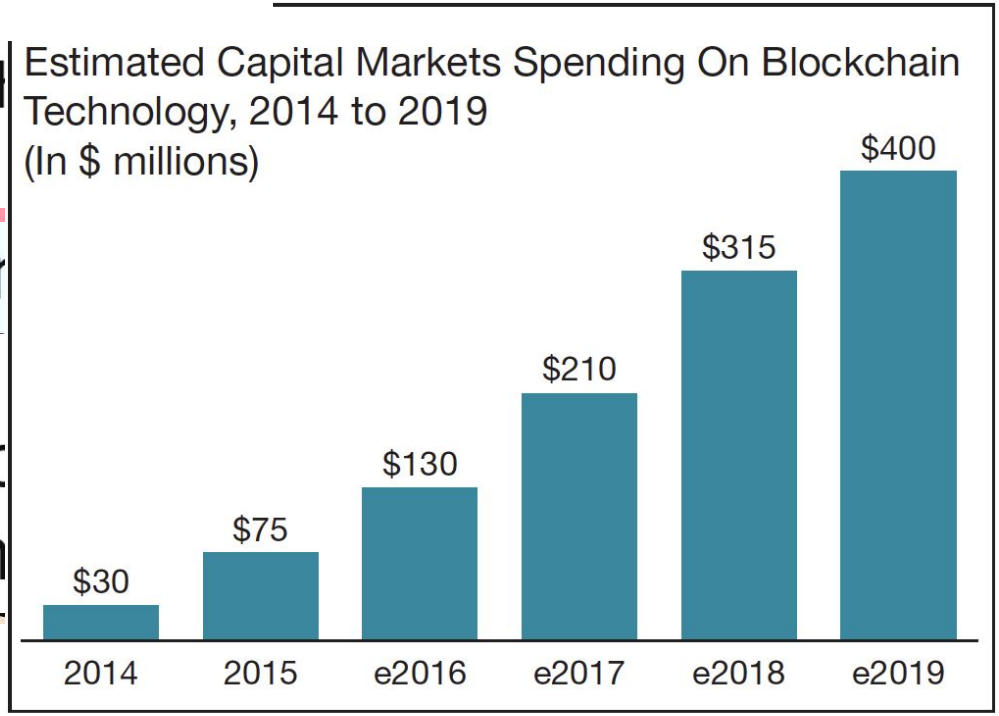
Pa

Blockchain Inter

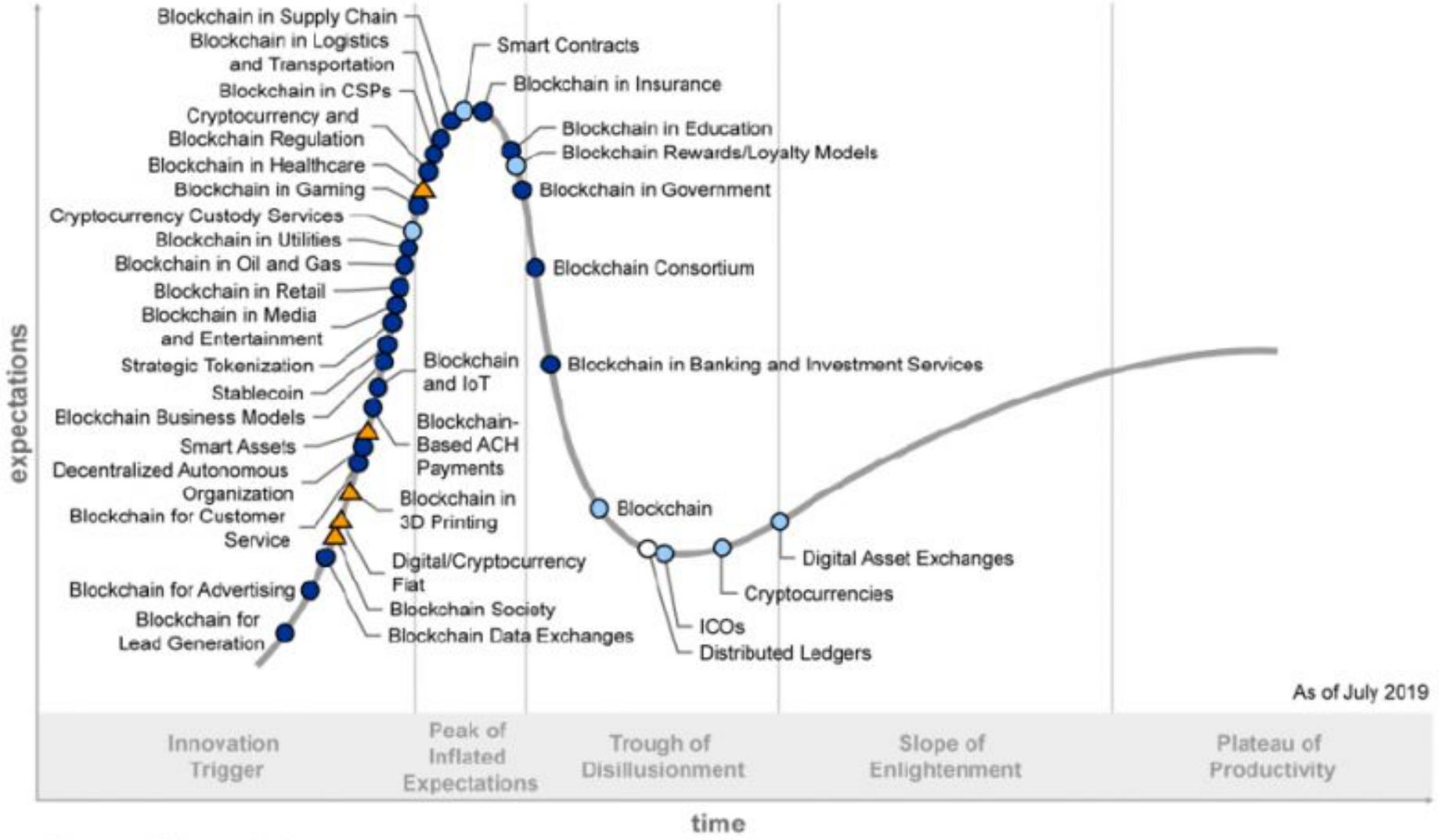
News

Dao.Casino – Dec

Gambling Econon



Hype Cycle for Blockchain Business, 2019

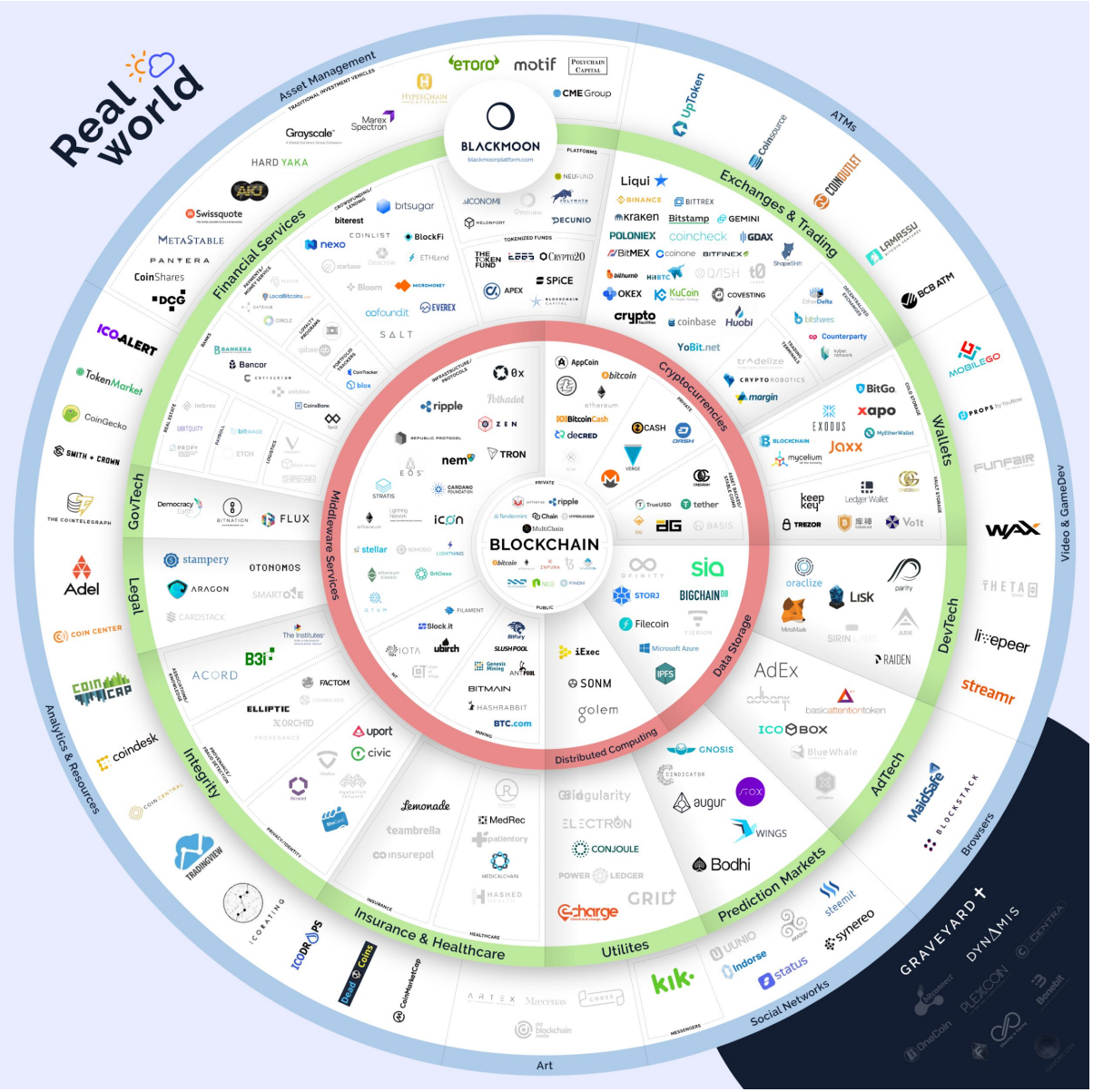


Plateau will be reached:

○ less than 2 years ◯ 2 to 5 years ● 5 to 10 years ▲ more than 10 years ⊗ obsolete before plateau

Source: Gartner
ID: 390391

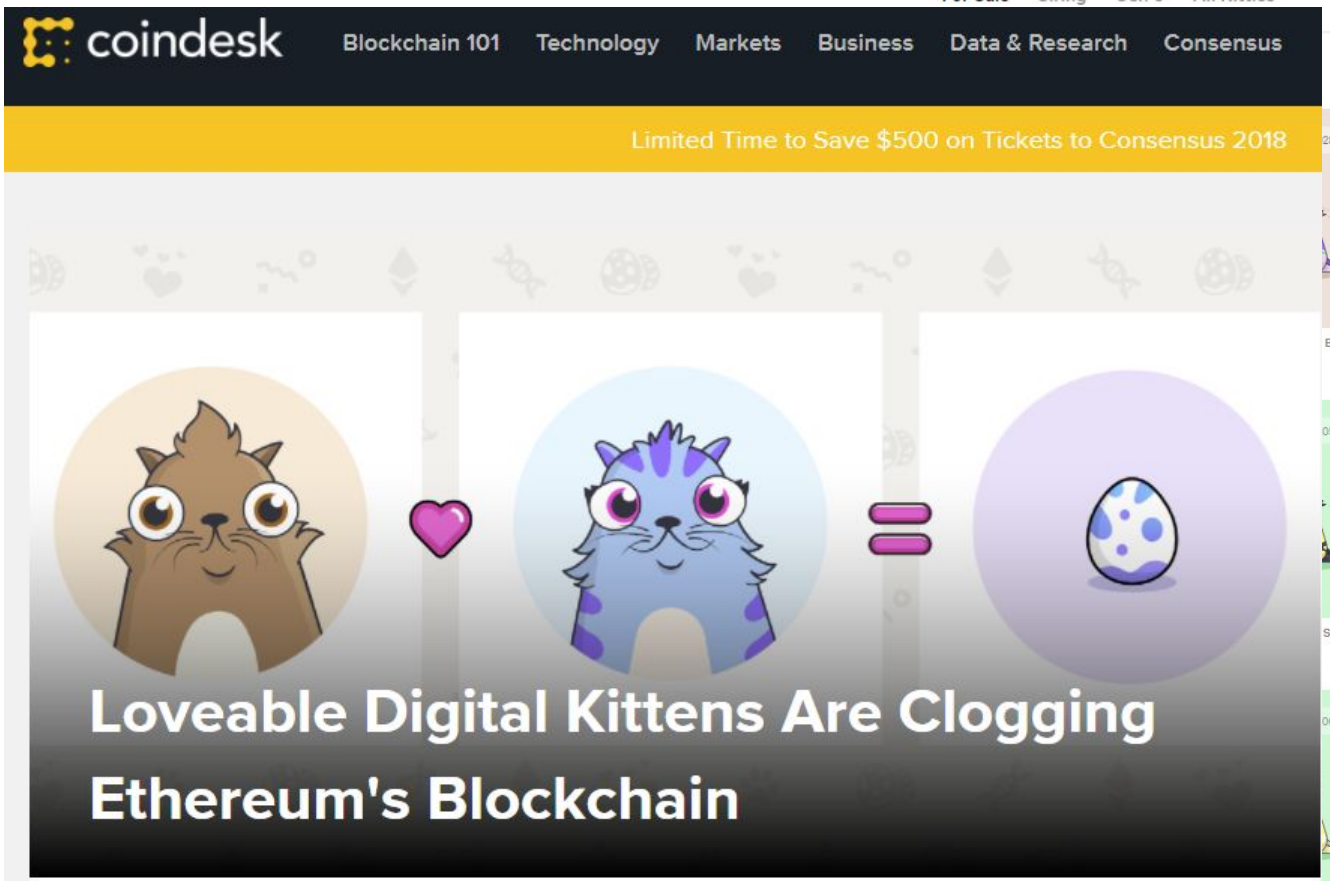
Blockchain project ecosystem

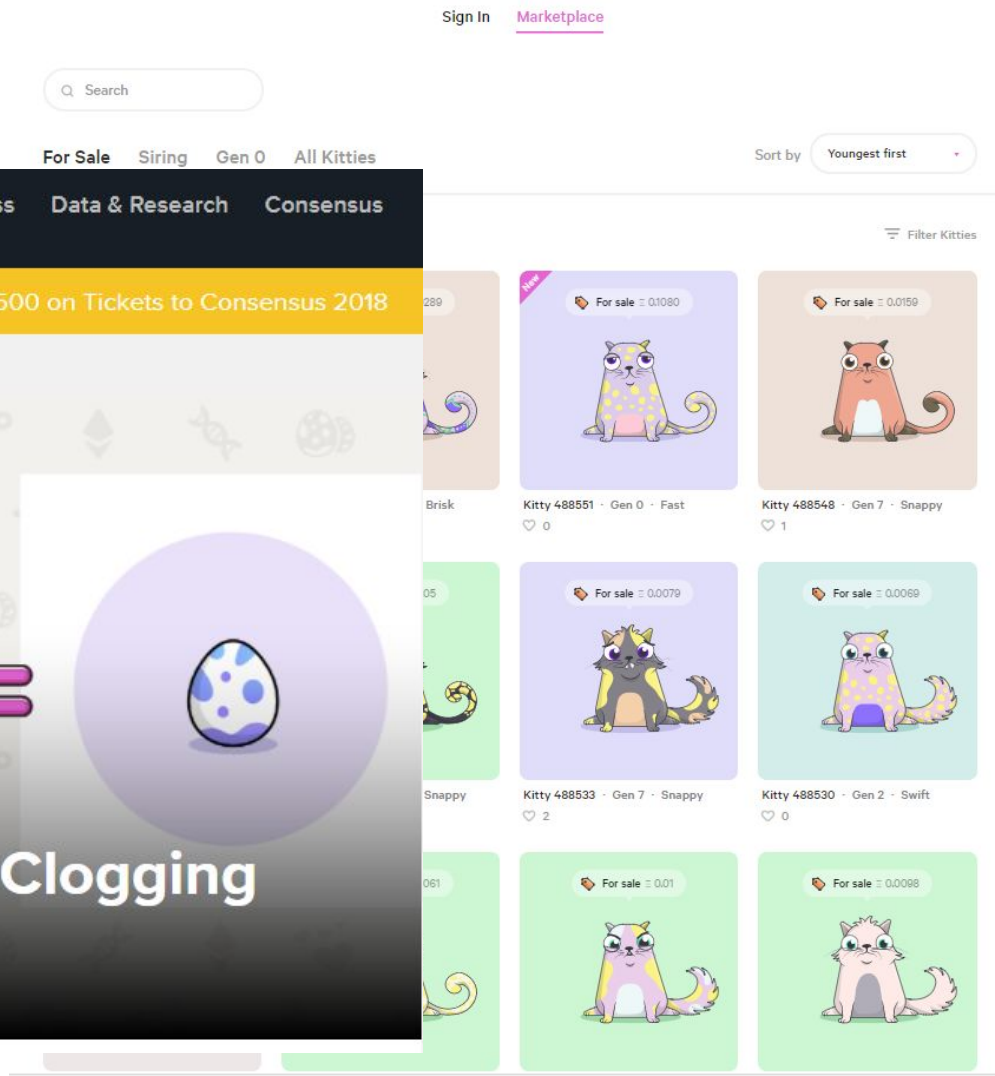


https://news.blackmooncrypto.com/the-blockchain-ecosystem-v3-six-months-after-the-hype-ca14e9879001

A NOTE ON PERFORMANCE

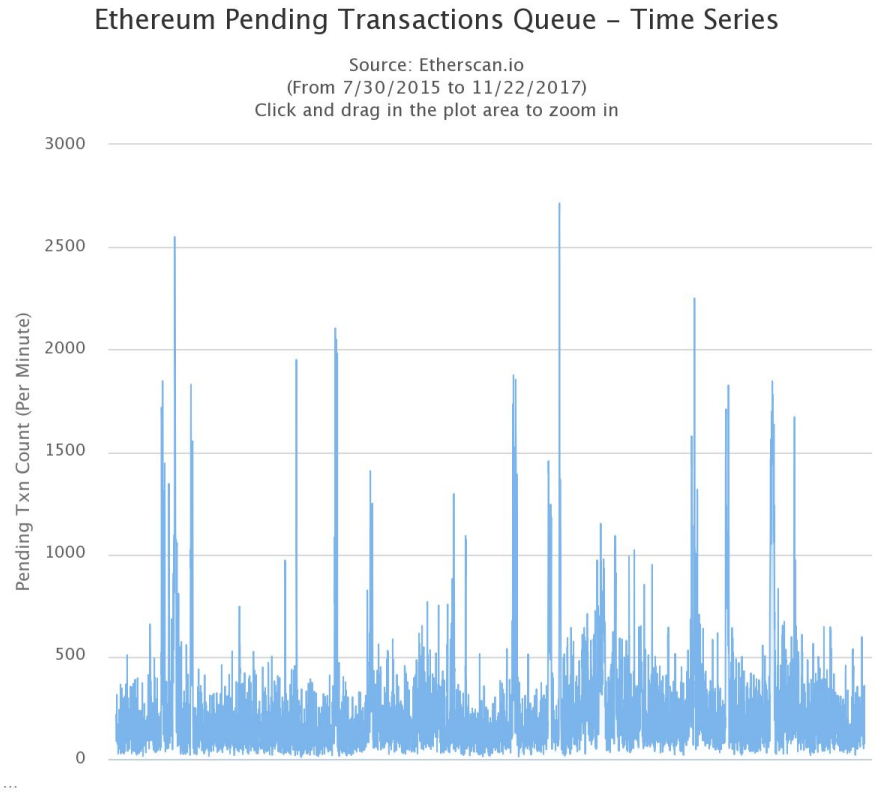
CryptoKitties! ☺️☹️





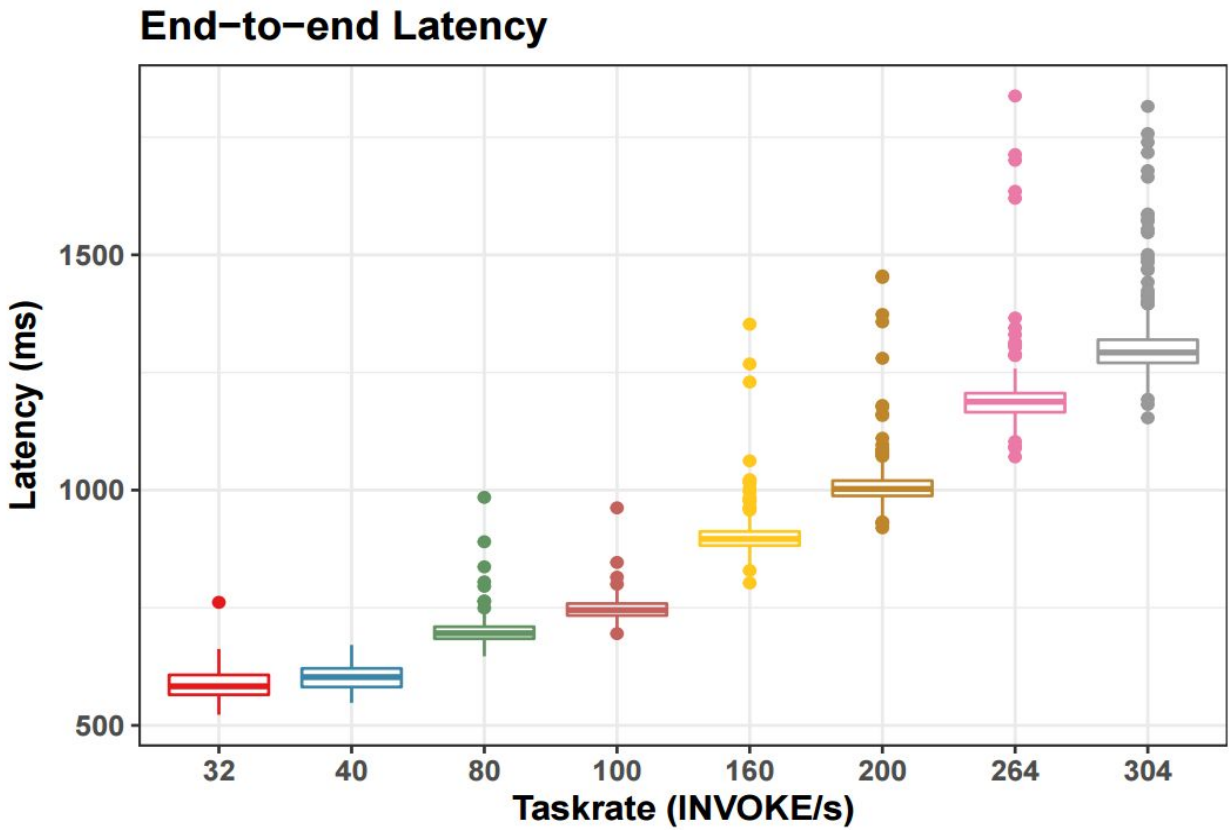
Public Blockchain: performance

- Throughput
- Latency: **variance**
- Price: **variance**



Private Blockchain performance

- HL fabric v0.6
- Due to blocks: still latency and size limits, but
- **Tunable**
- **Plannable**
- **Protectable**
- v1.x: 3000 Tps and beyond



Topics we plan to cover during the course