IBM Client Innovation Center **Netherlands**

UCL CBT

The Institution of Engineering and Technology

Exploring the Blockchain Revolution

An Overview of Distributed Ledger Technology (DLT) Networks

19 September 2023 | Vasileios Theodosiadis & Konstantina Koutsogiannopoulou

Host: Dr Denis Prager

Disclaimer: This material is created only for educational purposes, and by no means it includes an exhaustive list of standards or use cases. It does not also represent any views of current or previous affiliations.

Agenda

1. **Who Are We?**
2. Blockchain Fundamentals
3. Blockchain Architecture
4. Tokens
5. Digital Identity
6. Complex Use Cases

Who Are We?

About us

Vasileios Theodosiadis

- Blockchain Project Manager & Consultant
- 11 commercial engagements (5 blockchain projects)
- Research on governance structure in enterprise blockchain networks
- Industry Associate at UCL CBT

- MSc in Information Systems Management (in collaboration with Jaguar Land Rover)
- BSc in Computer Science (in collaboration with FORTH)

Konstantina Koutsogiannopoulou

- Blockchain Application Developer (6 projects)
- People Manager at IBM CIC NL
- Member of CTO IBM NCEE Office

- MSc in Management of Innovation
- BSc in Management Science & Technology

wbs WARWICK BUSINESS SCHOOL

JAGUAR LAND ROVER

UCL CBT

UNIVERSITY OF CRETE

FORTH FOUNDATION FOR RESEARCH AND TECHNOLOGY - HELLAS

IBM

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

RSM Erasmus | Rotterdam School of Management Erasmus University

Who Are We?

What does IBM do?

Who Are We?

CIC Netherlands

- **Founded in 2013** in Groningen
- **3 locations:** Groningen, Amsterdam, Eindhoven
- Around **200 employees** & growing
- 30+ **different nationalities**
- **Average age is 29**

Agenda

1. Who Are We?
2. **Blockchain Fundamentals**
3. Blockchain Architecture
4. Tokens
5. Digital Identity
6. Complex Use Cases

So, what do you know about blockchain?

Distributed Ledger Technologies (DLT)

- **Distributed Ledger Technologies (DLT)**

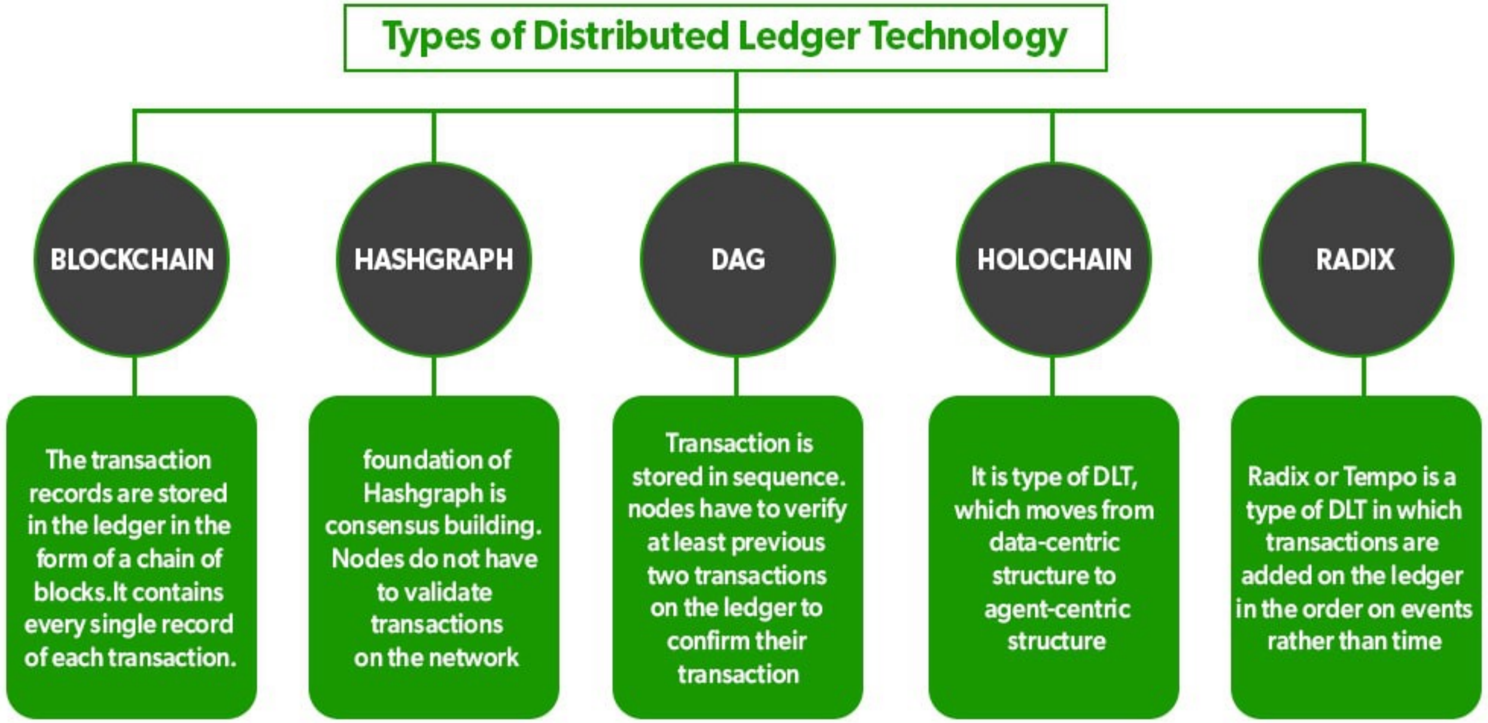
Decentralised digital systems that record, store, and share information across multiple locations, ensuring transparency, security, and immutability.

Decentralisation

Transparency

Security

Immutability



Types of Distributed Ledger Technology

BLOCKCHAIN

The transaction records are stored in the ledger in the form of a chain of blocks.It contains every single record of each transaction.

HASHGRAPH

foundation of Hashgraph is consensus building. Nodes do not have to validate transactions on the network

DAG

Transaction is stored in sequence. nodes have to verify at least previous two transactions on the ledger to confirm their transaction

HOLOCHAIN

It is type of DLT, which moves from data-centric structure to agent-centric structure

RADIX

Radix or Tempo is a type of DLT in which transactions are added on the ledger in the order on events rather than time

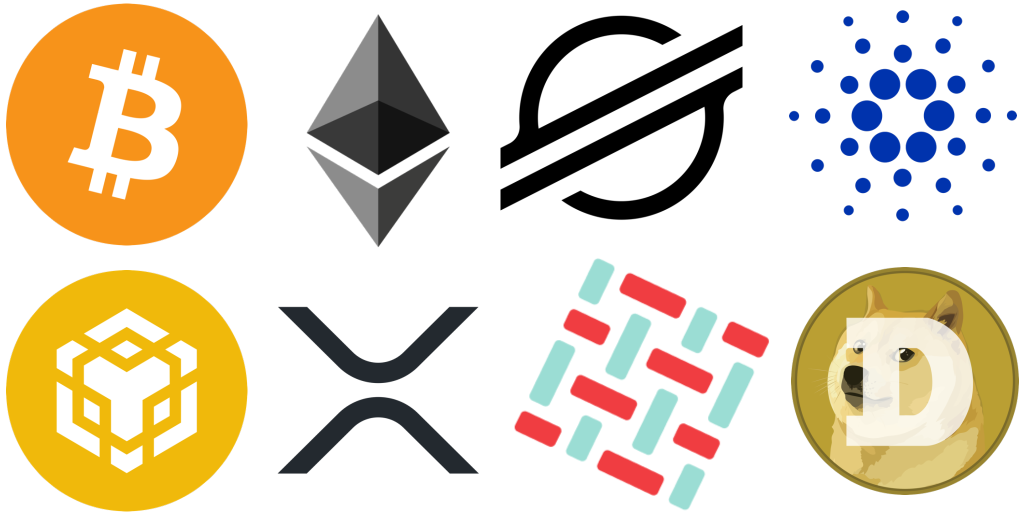
Sources:

https://www.geeksforgeeks.org/blockchain-and-distributed-ledger-technology-dlt/

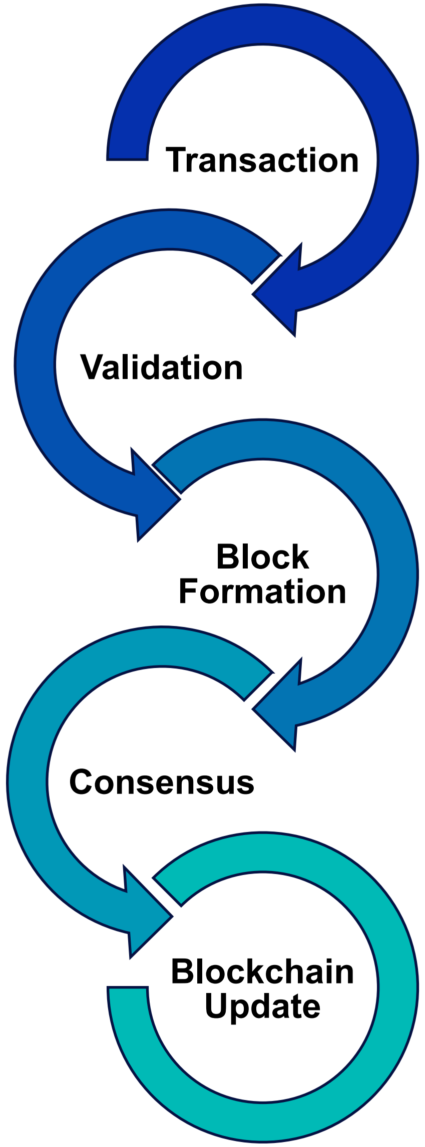
https://www.analyticssteps.com/blogs/5-types-distributed-ledger-technologies-dlt

Blockchain

- **Blockchain**, a type of DLT, is a chronological chain of blocks containing transactional data.
- Each block is linked to the previous one, forming a secure and tamper-resistant ledger.
- Examples:



Transaction Lifecycle



Public vs Private Blockchain

Public

- For example, Bitcoin, Ethereum
- Transactions are viewable by anyone
- Participant identity is more difficult to control

Private

- For example, Hyperledger Fabric
- Network members are known but transactions are private
- No need for mining

Source:
https://www.techtarget.com/searchcio/tip/Permissioned-vs-permissionless-blockchains-Key-differences

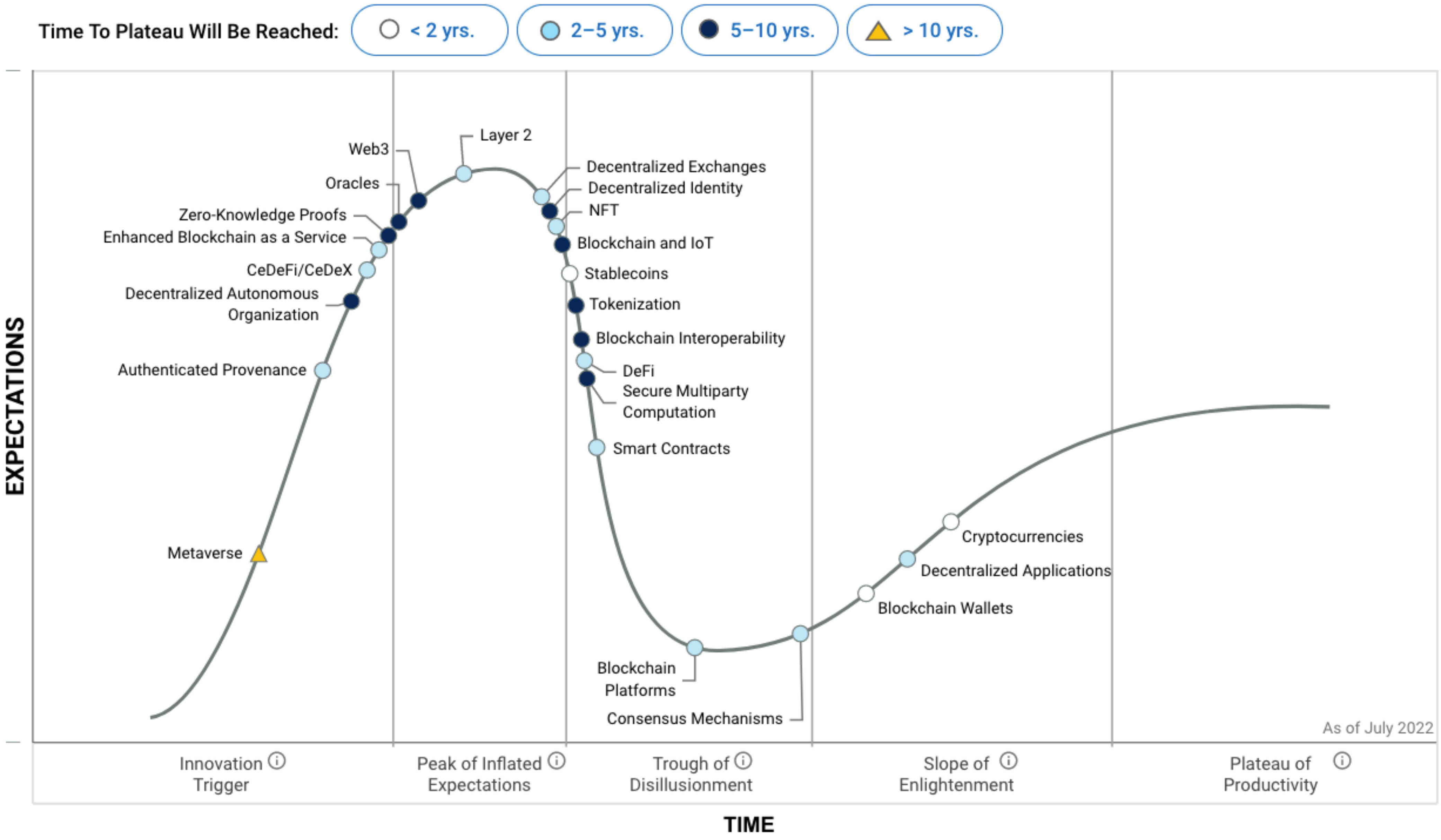
Bitcoin

- First and best-known cryptocurrency
- Introduction to blockchain technology
- Funds transfer between wallets
- No intermediaries
- Decentralised consensus mechanism

Source:

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized business review.

Hype Cycle for Blockchain (2022)



Source:

https://blogs.gartner.com/avivah-litan/2022/07/22/gartner-hype-cycle-for-blockchain-and-web3-2022/

Problems that blockchain is trying to solve

Trust

Data Security

Traceability

Cost

Digital Identity

Fraud

A good blockchain use case...

Is a business network involved?

Is consensus used to validate transactions?

Must the record of transactions be immutable, or tamper proof?

Is an audit trail, or provenance, required?

Should dispute resolution be final?

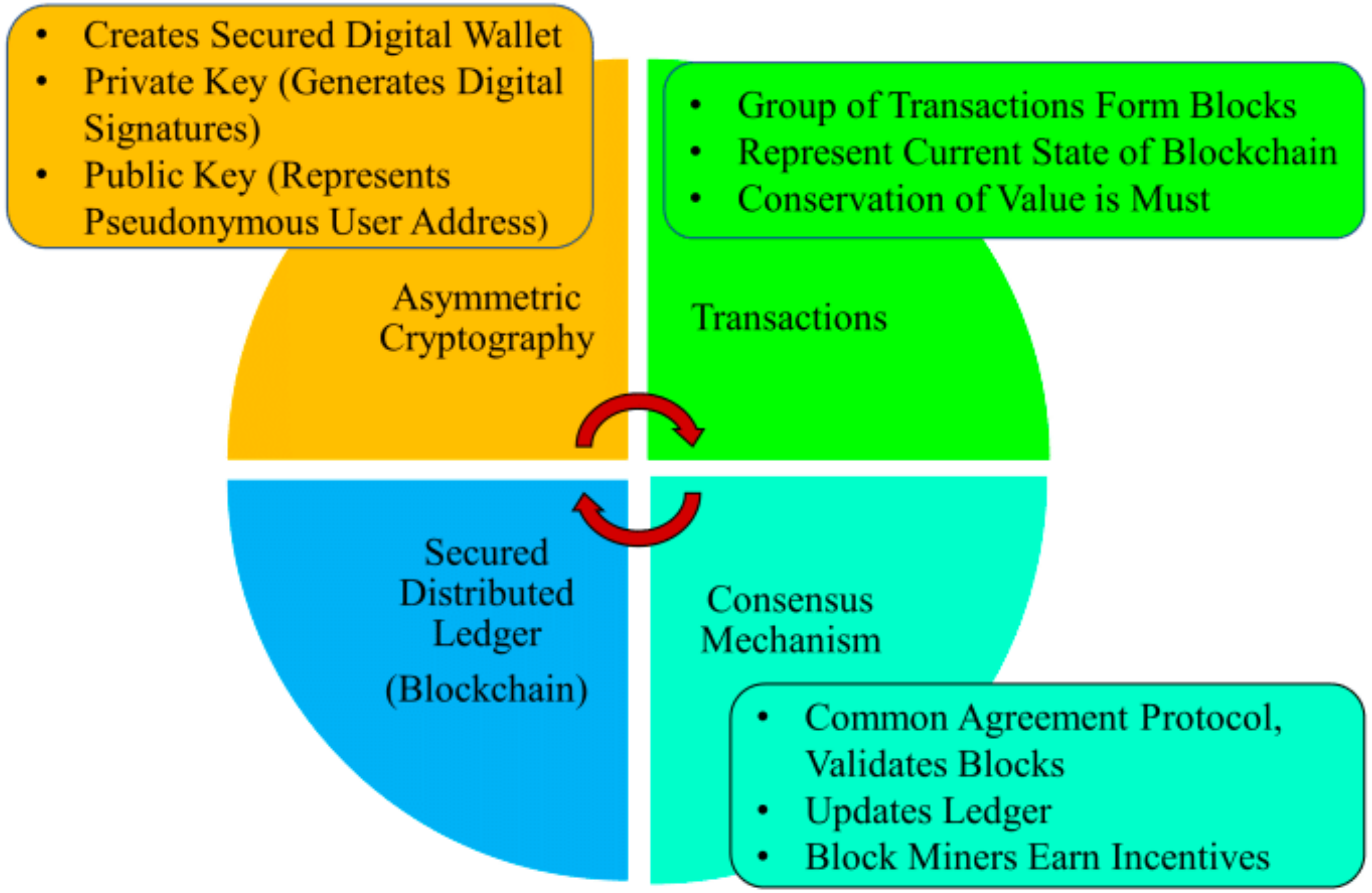
If you answered yes to the first question and to at least one other, then your use case would benefit from blockchain technology.

Agenda

1. Who Are We?
2. Blockchain Fundamentals
3. **Blockchain Architecture**
4. Tokens
5. Digital Identity
6. Complex Use Cases

Basic Components of a Blockchain

- Peer-to-Peer Network
- Node
- Ledger
- Wallet
- Nonce
- Hash
- Consensus mechanism
- Smart Contracts
- Cryptography



- Creates Secured Digital Wallet
- Private Key (Generates Digital Signatures)
- Public Key (Represents Pseudonymous User Address)

Asymmetric Cryptography

- Group of Transactions Form Blocks
- Represent Current State of Blockchain
- Conservation of Value is Must

Transactions

Secured Distributed Ledger

(Blockchain)

Consensus Mechanism

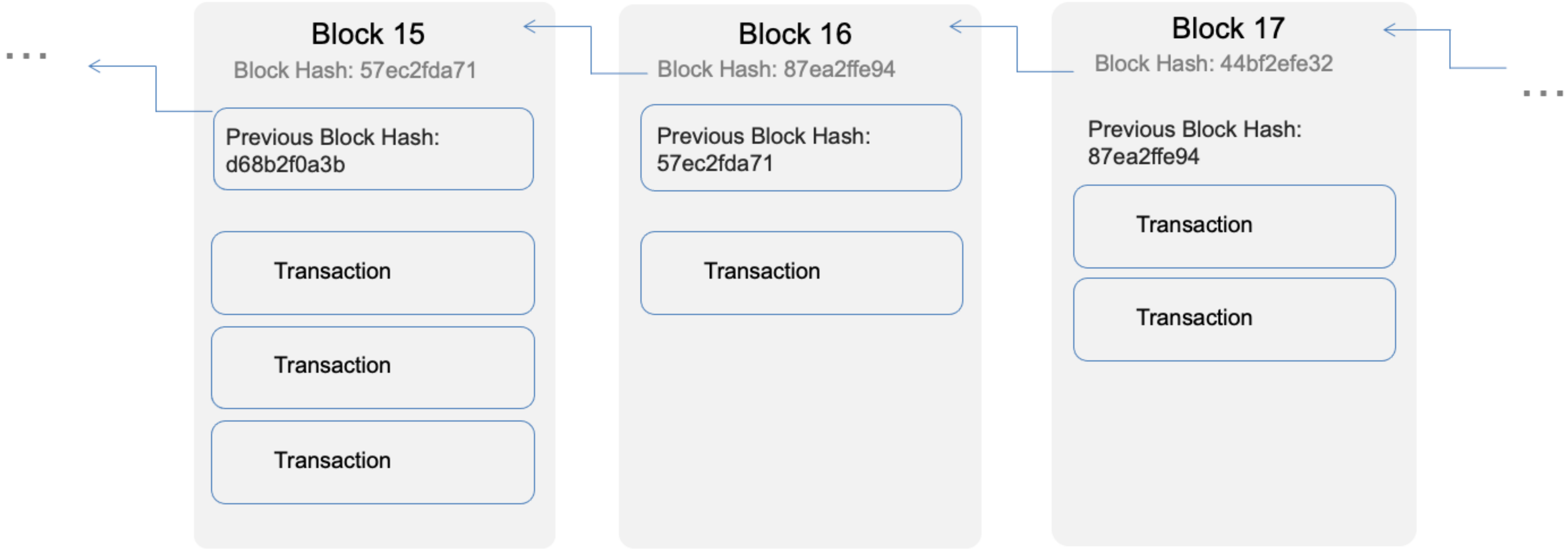
- Common Agreement Protocol, Validates Blocks
- Updates Ledger
- Block Miners Earn Incentives

Sources:

https://www.identity.com/key-components-of-a-blockchain-network/

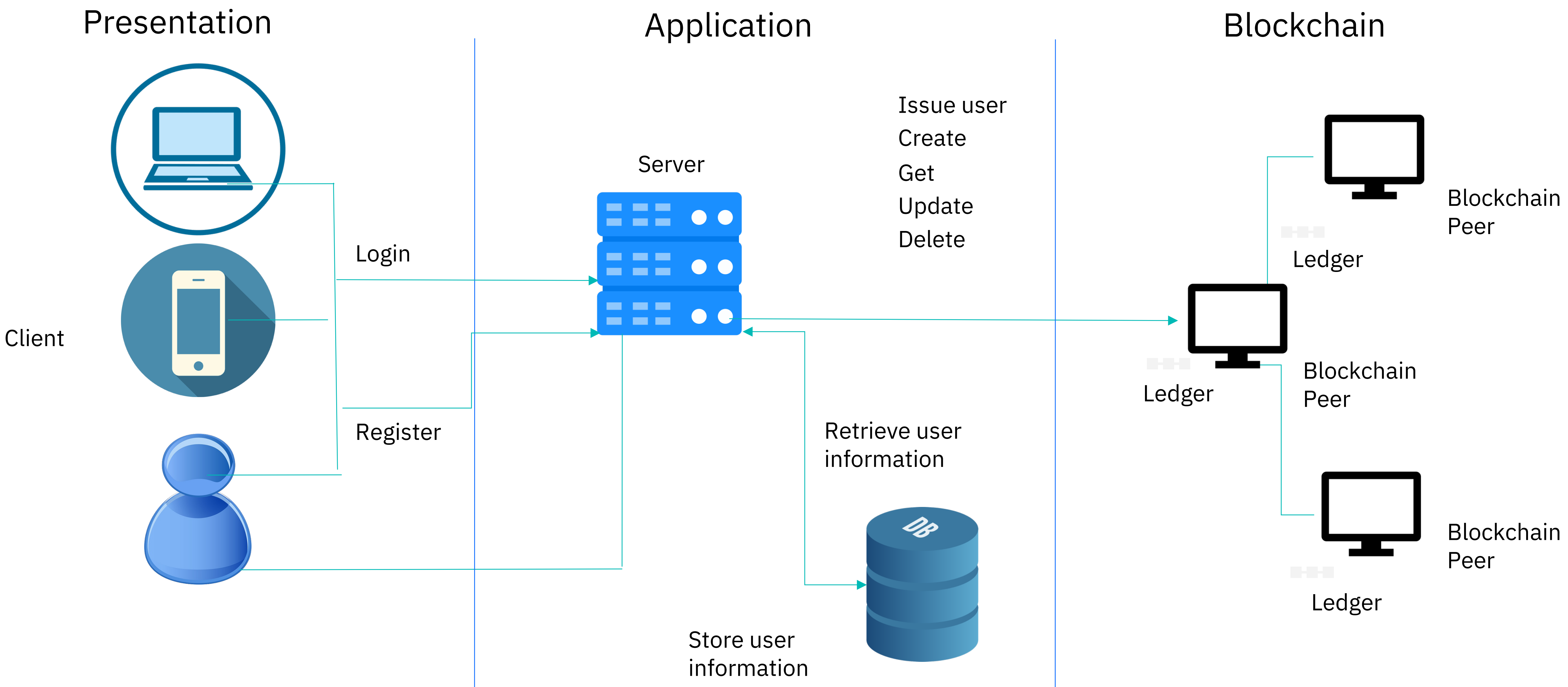
https://www.researchgate.net/figure/Core-components-of-blockchain_fig1_326102908

Block Detail



- A blockchain is made up of a series of blocks with new blocks always added to the end
- Each block contains zero or more transactions and some additional metadata
- Blocks achieve immutability by including the result of a hash function of the previous block
- The first block is known as the “genesis” block

Blockchain Architecture



Transactional Operations - Optimisation

Layer 1: Building block

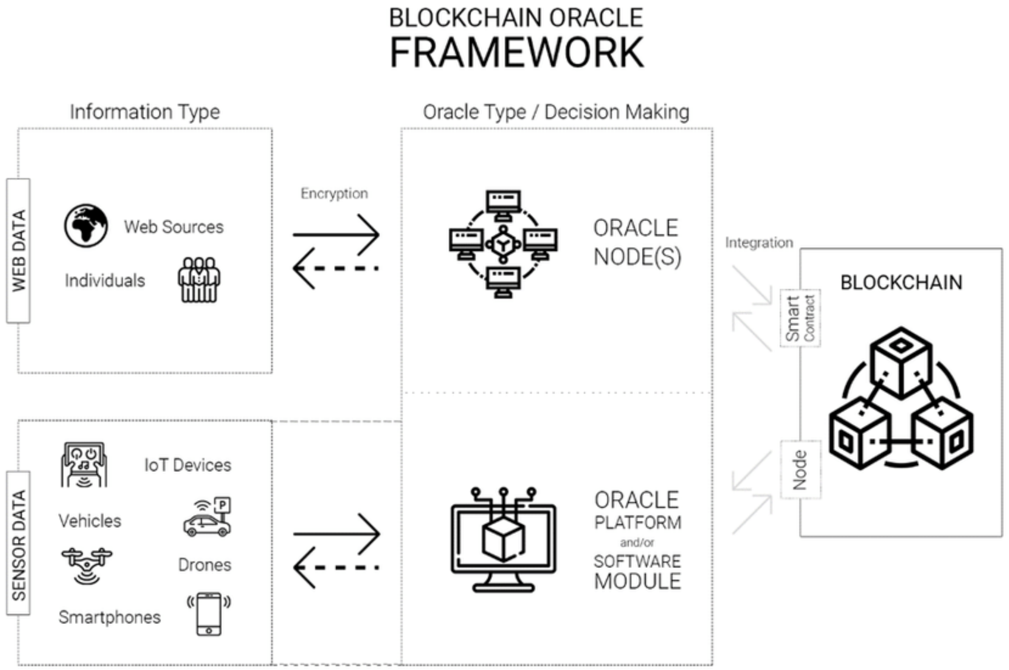
Layer 2: Scaling Solution

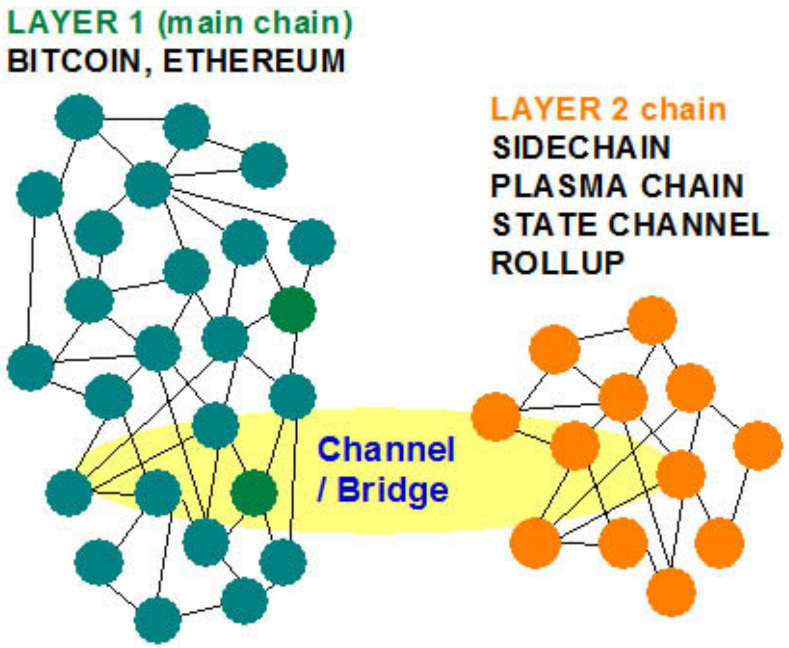
Sidechain vs Parachain

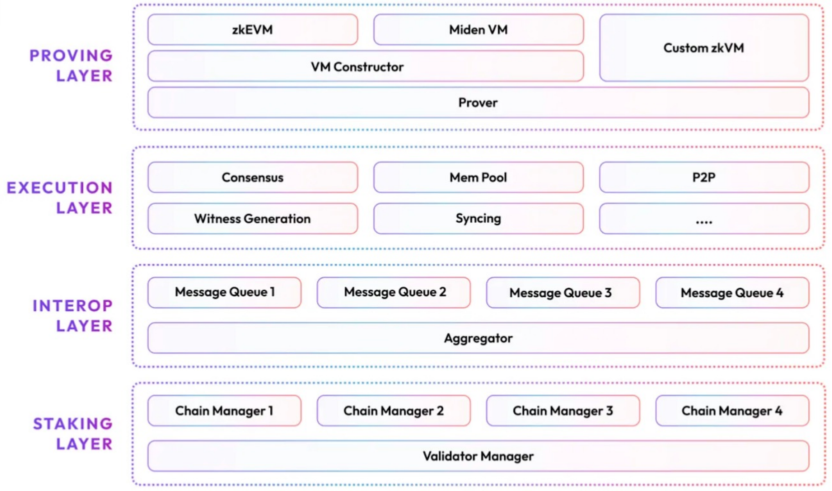
Oracles

Zero Knowledge Proof

Layers of Interoperability







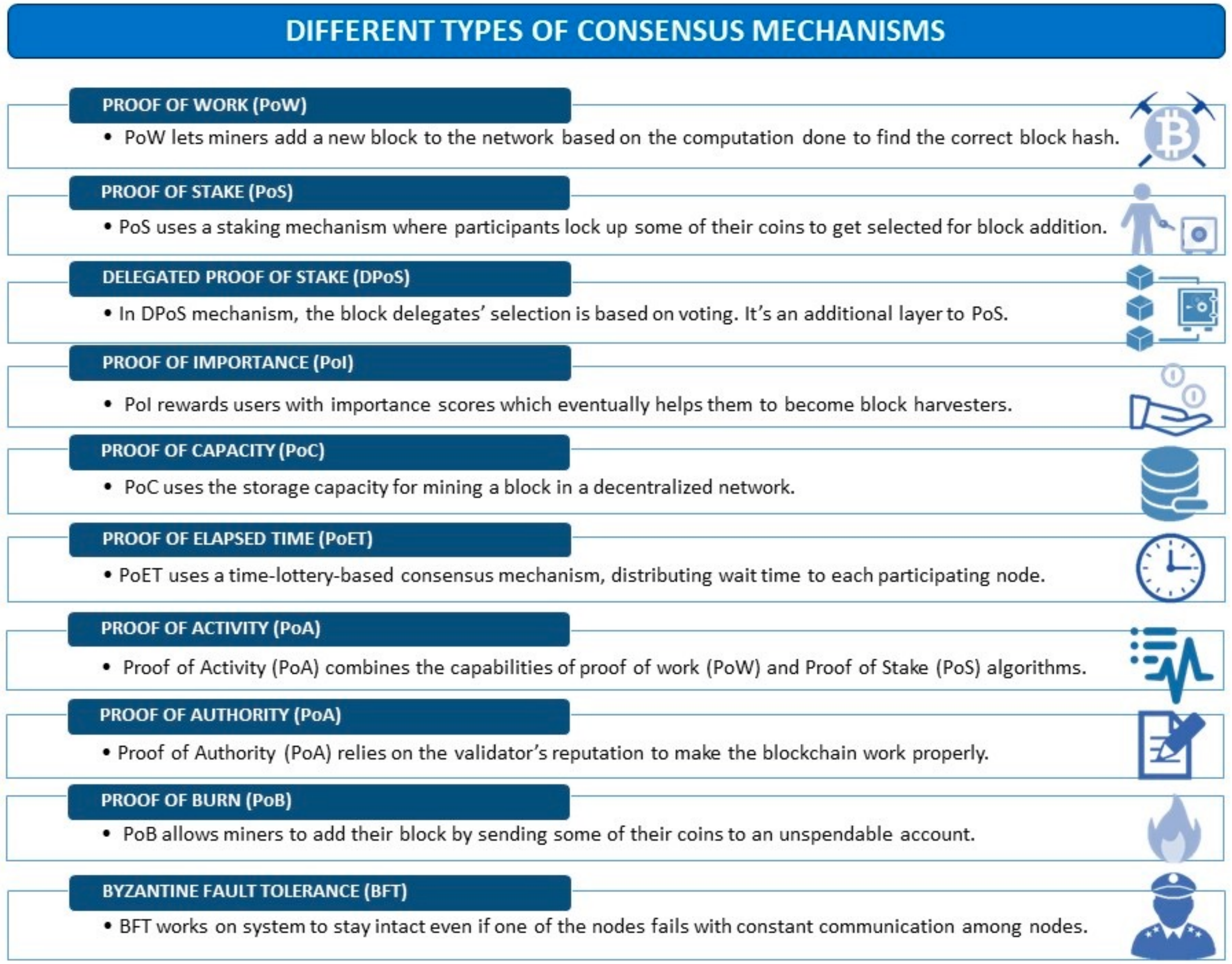
Polygon 2.0

Sources:

https://www.researchgate.net/figure/Blockchain-oracle-framework-a-graphical-representation_fig2_344079826

https://www.analyticssteps.com/blogs/introduction-layer-2-scaling-solutions

Consensus Mechanisms



DIFFERENT TYPES OF CONSENSUS MECHANISMS

PROOF OF WORK (PoW)
- PoW lets miners add a new block to the network based on the computation done to find the correct block hash.

PROOF OF STAKE (PoS)
- PoS uses a staking mechanism where participants lock up some of their coins to get selected for block addition.

DELEGATED PROOF OF STAKE (DPoS)
- In DPoS mechanism, the block delegates' selection is based on voting. It's an additional layer to PoS.

PROOF OF IMPORTANCE (PoI)
- PoI rewards users with importance scores which eventually helps them to become block harvesters.

PROOF OF CAPACITY (PoC)
- PoC uses the storage capacity for mining a block in a decentralized network.

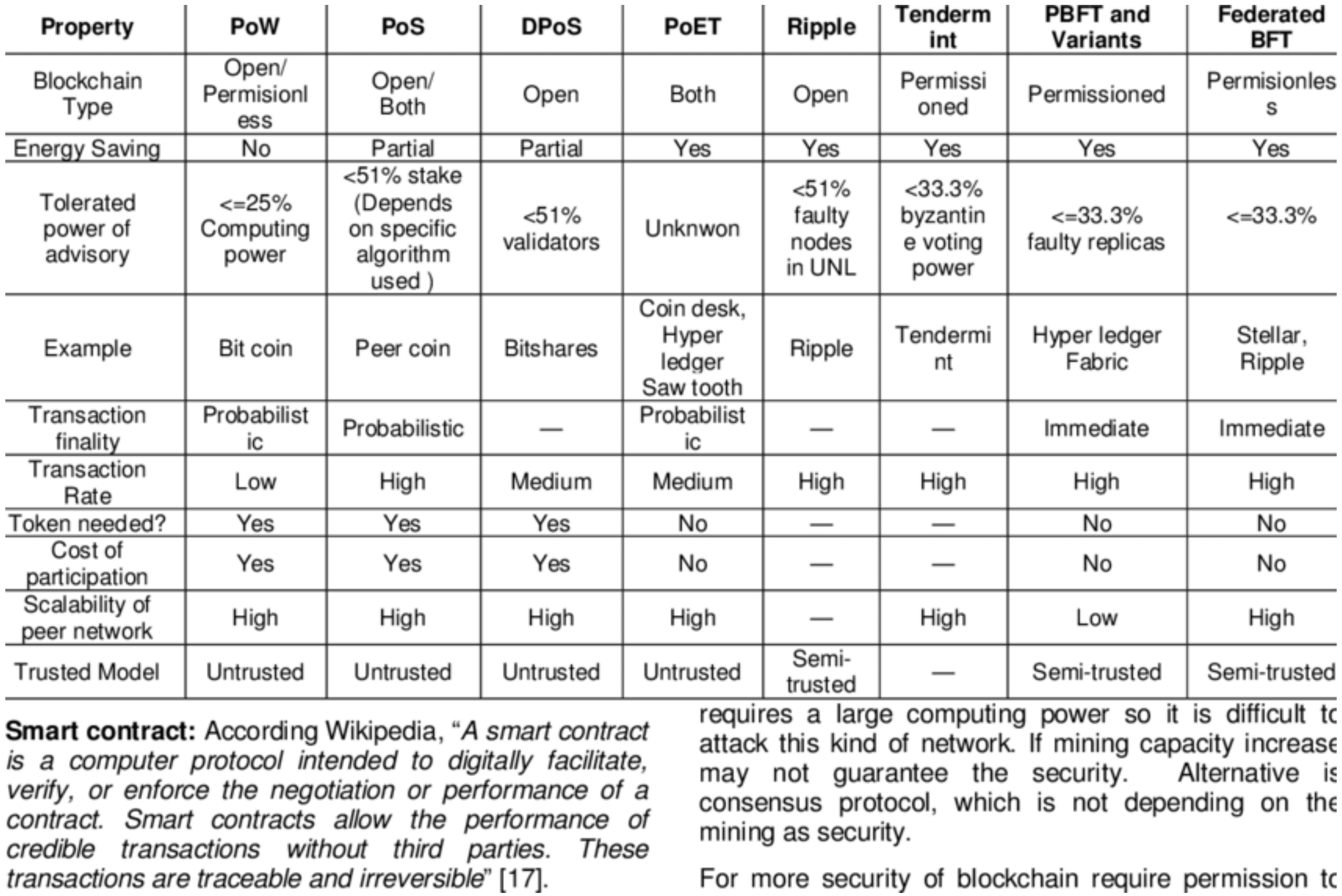
PROOF OF ELAPSED TIME (PoET)
- PoET uses a time-lottery-based consensus mechanism, distributing wait time to each participating node.

PROOF OF ACTIVITY (PoA)
- Proof of Activity (PoA) combines the capabilities of proof of work (PoW) and Proof of Stake (PoS) algorithms.

PROOF OF AUTHORITY (PoA)
- Proof of Authority (PoA) relies on the validator's reputation to make the blockchain work properly.

PROOF OF BURN (PoB)
- PoB allows miners to add their block by sending some of their coins to an unspendable account.

BYZANTINE FAULT TOLERANCE (BFT)
- BFT works on system to stay intact even if one of the nodes fails with constant communication among nodes.



Property	PoW	PoS	DPoS	PoET	Ripple	Tendermint	PBFT and Variants	Federated BFT
Blockchain Type	Open/ Permisionless	Open/ Both	Open	Both	Open	Permissioned	Permissioned	Permisionless
Energy Saving	No	Partial	Partial	Yes	Yes	Yes	Yes	Yes
Tolerated power of advisory	<=25% Computing power	<51% stake (Depends on specific algorithm used)	<51% validators	Unknwon	<51% faulty nodes in UNL	<33.3% byzantine voting power	<=33.3% faulty replicas	<=33.3%
Example	Bit coin	Peer coin	Bitshares	Coin desk, Hyper ledger Saw tooth	Ripple	Tendermint	Hyper ledger Fabric	Stellar, Ripple
Transaction finality	Probabilistic	Probabilistic	—	Probabilistic	—	—	Immediate	Immediate
Transaction Rate	Low	High	Medium	Medium	High	High	High	High
Token needed?	Yes	Yes	Yes	No	—	—	No	No
Cost of participation	Yes	Yes	Yes	No	—	—	No	No
Scalability of peer network	High	High	High	High	—	High	Low	High
Trusted Model	Untrusted	Untrusted	Untrusted	Untrusted	Semi-trusted	—	Semi-trusted	Semi-trusted

Smart contract: According Wikipedia, "*A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are traceable and irreversible*" [17].

requires a large computing power so it is difficult to attack this kind of network. If mining capacity increase may not guarantee the security. Alternative is consensus protocol, which is not depending on the mining as security.

For more security of blockchain require permission to

Sources:

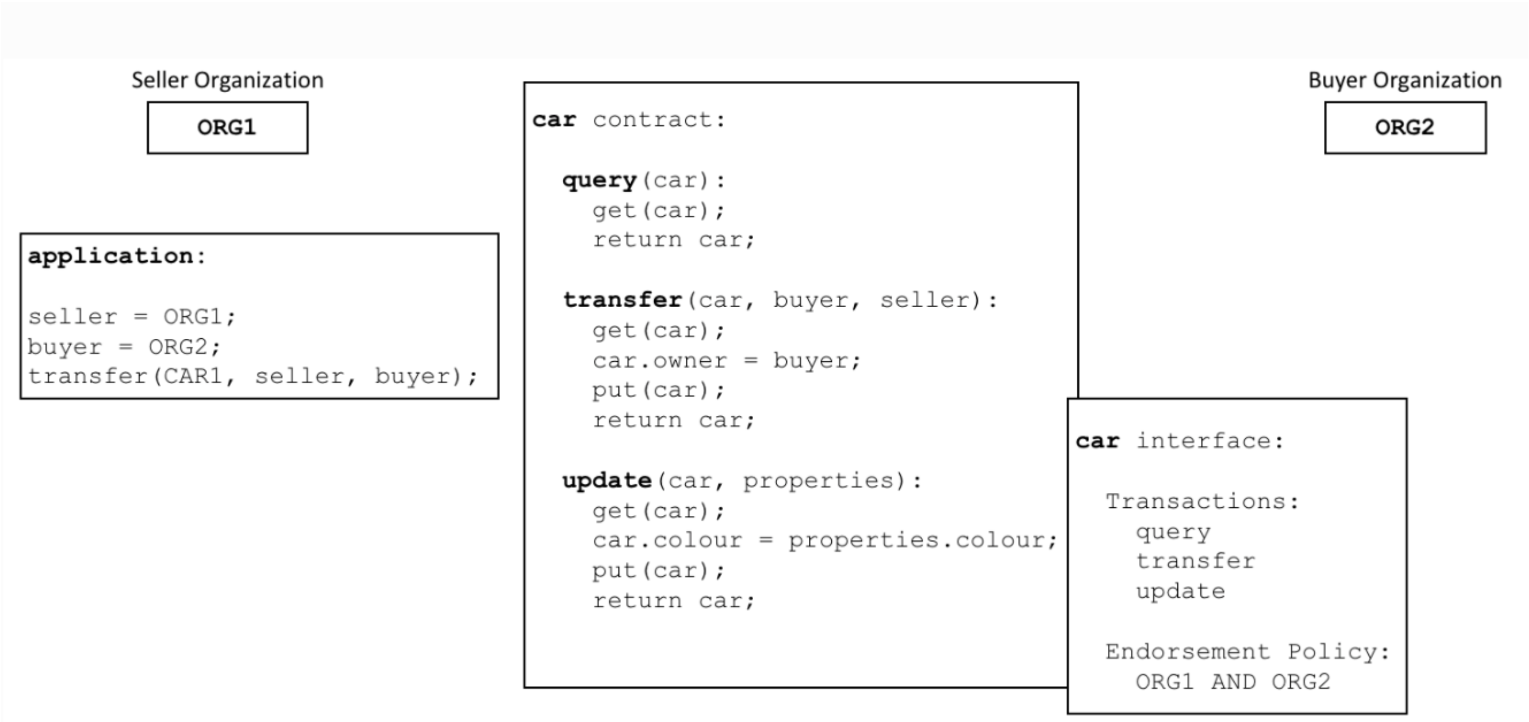
https://www.shiksha.com/online-courses/articles/consensus-mechanisms-in-blockchain/

https://www.researchgate.net/publication/341788606_Comparisons_of_Blockchain_based_Consensus_Algorithms_for_Security_Aspects

Smart Contracts

Smart contracts are self-executing, digital agreements with the terms of the contract directly written into code.

Automation **Transparency** **Trustless** **Security**



Seller Organization

ORG1

```
application:

seller = ORG1;
buyer = ORG2;
transfer(CAR1, seller, buyer);
```

```
car contract:

  query(car):
    get(car);
    return car;

  transfer(car, buyer, seller):
    get(car);
    car.owner = buyer;
    put(car);
    return car;

  update(car, properties):
    get(car);
    car.colour = properties.colour;
    put(car);
    return car;
```

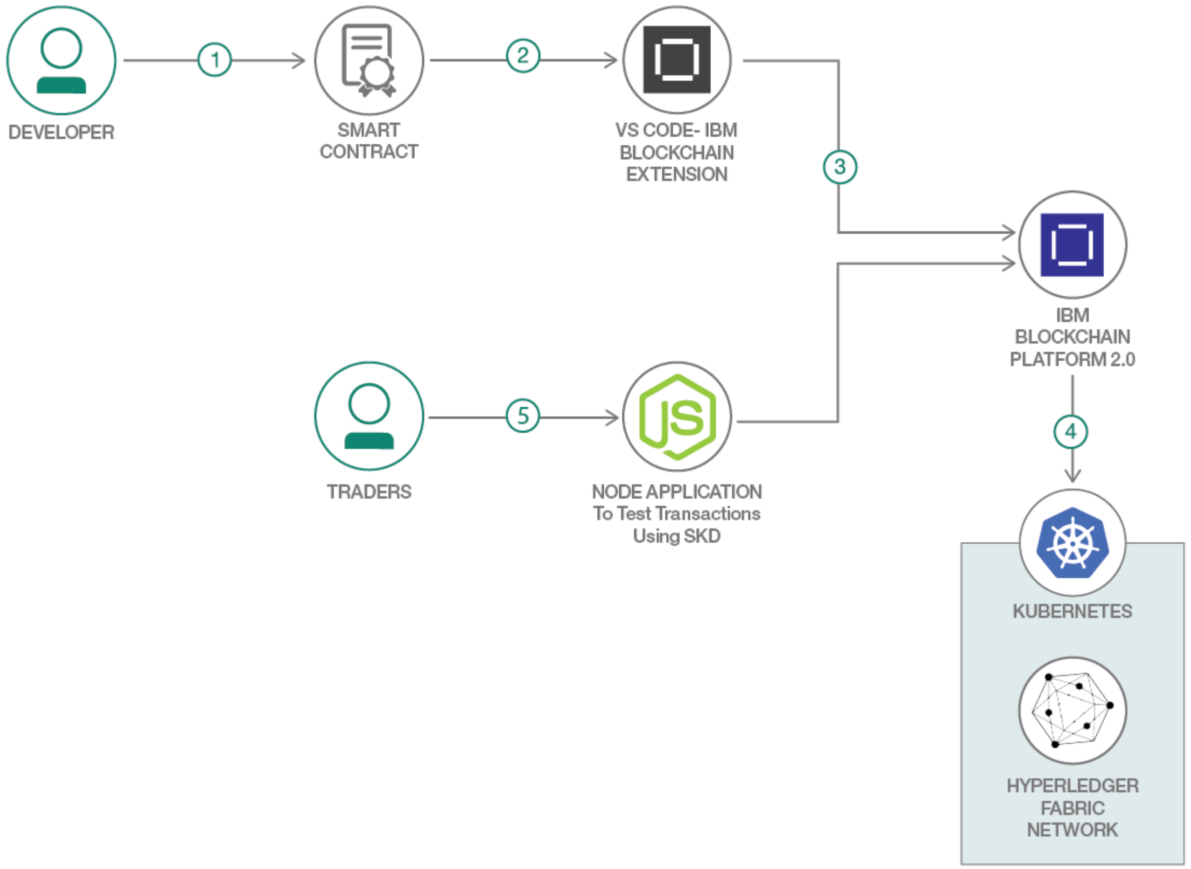
Buyer Organization

ORG2

```
car interface:

  Transactions:
    query
    transfer
    update

  Endorsement Policy:
    ORG1 AND ORG2
```


DEVELOPER
1
SMART CONTRACT
2
VS CODE- IBM BLOCKCHAIN EXTENSION
3
IBM BLOCKCHAIN PLATFORM 2.0
4
KUBERNETES
HYPERLEDGER FABRIC NETWORK
TRADERS
5
NODE APPLICATION To Test Transactions Using SKD

Sources:

https://hyperledger-fabric.readthedocs.io/en/latest/smartcontract/smartcontract.htm

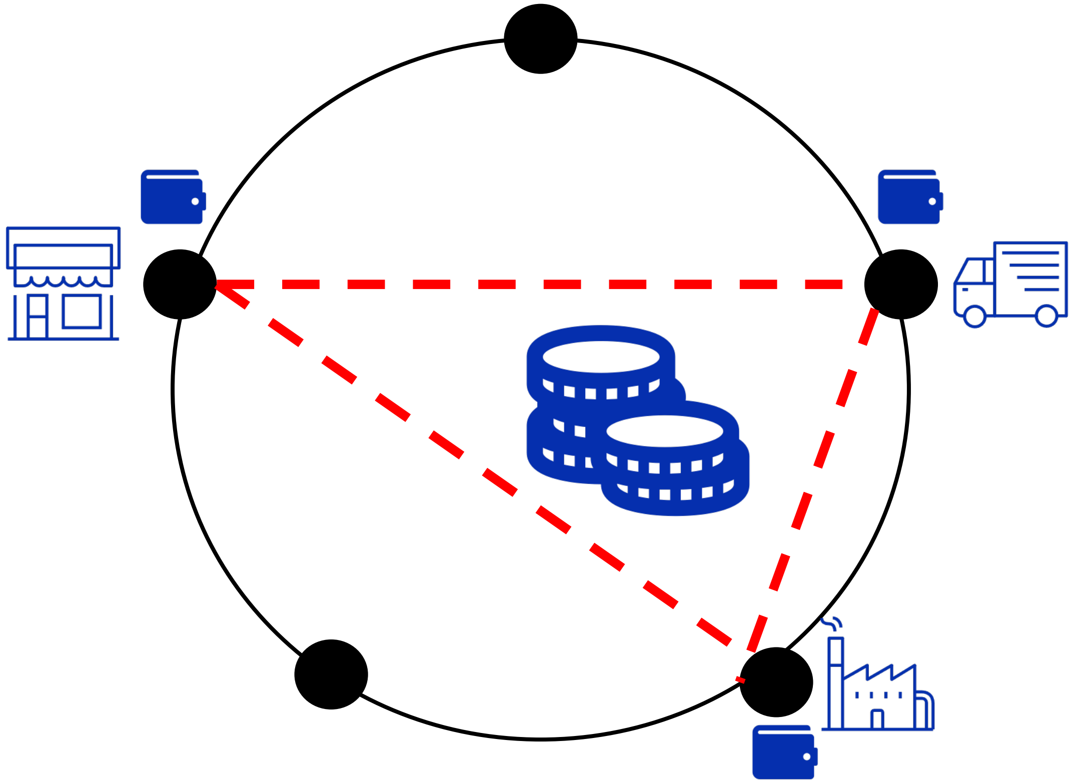
https://developer.ibm.com/patterns/build-a-blockchain-network/l

Agenda

1. Who Are We?
2. Blockchain Fundamentals
3. Blockchain Architecture
4. **Tokens**
5. Digital Identity
6. Complex Use Cases

Overview

- Digital representation of assets
- Value storage, exchange
- Wide range of types & applications
- $24TN market by 2027 (WEF)



Lifecycle

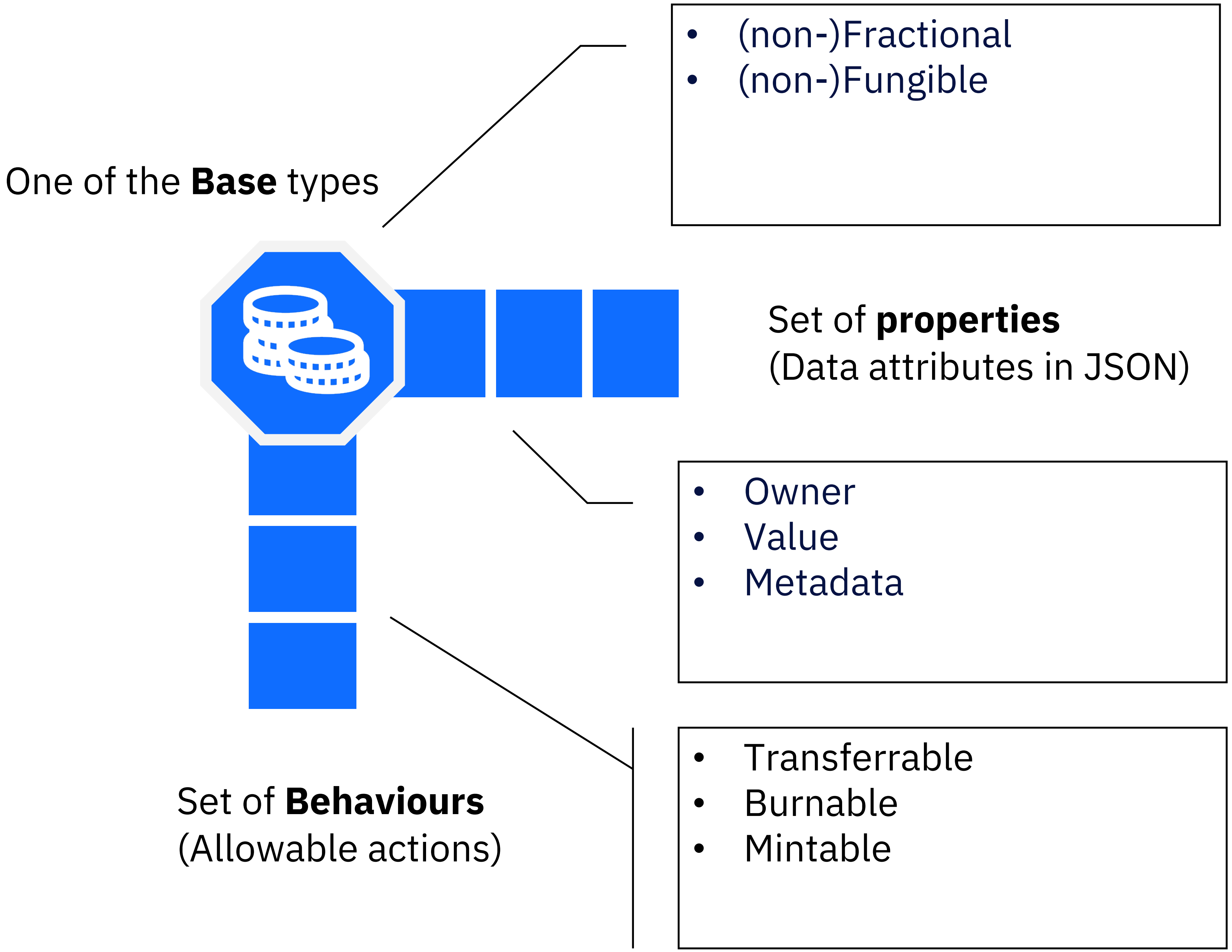
- Issuance
- Assignment
- Activation
- Transfer
- Revocation
- Expiration / Redemption

Benefits

- Greater market liquidity
- Higher fractionalisation
- Faster clearing & settlement
- Inclusivity
- Reduced cost

Source;
https://www.gbm.hsbc.com/-/media/gbm/insights/attachments/potential-of-tokenisation.pdf

Taxonomy Structure



One of the **Base** types

- (non-)Fractional
- (non-)Fungible

Set of **properties**
(Data attributes in JSON)

- Owner
- Value
- Metadata

Set of **Behaviours**
(Allowable actions)

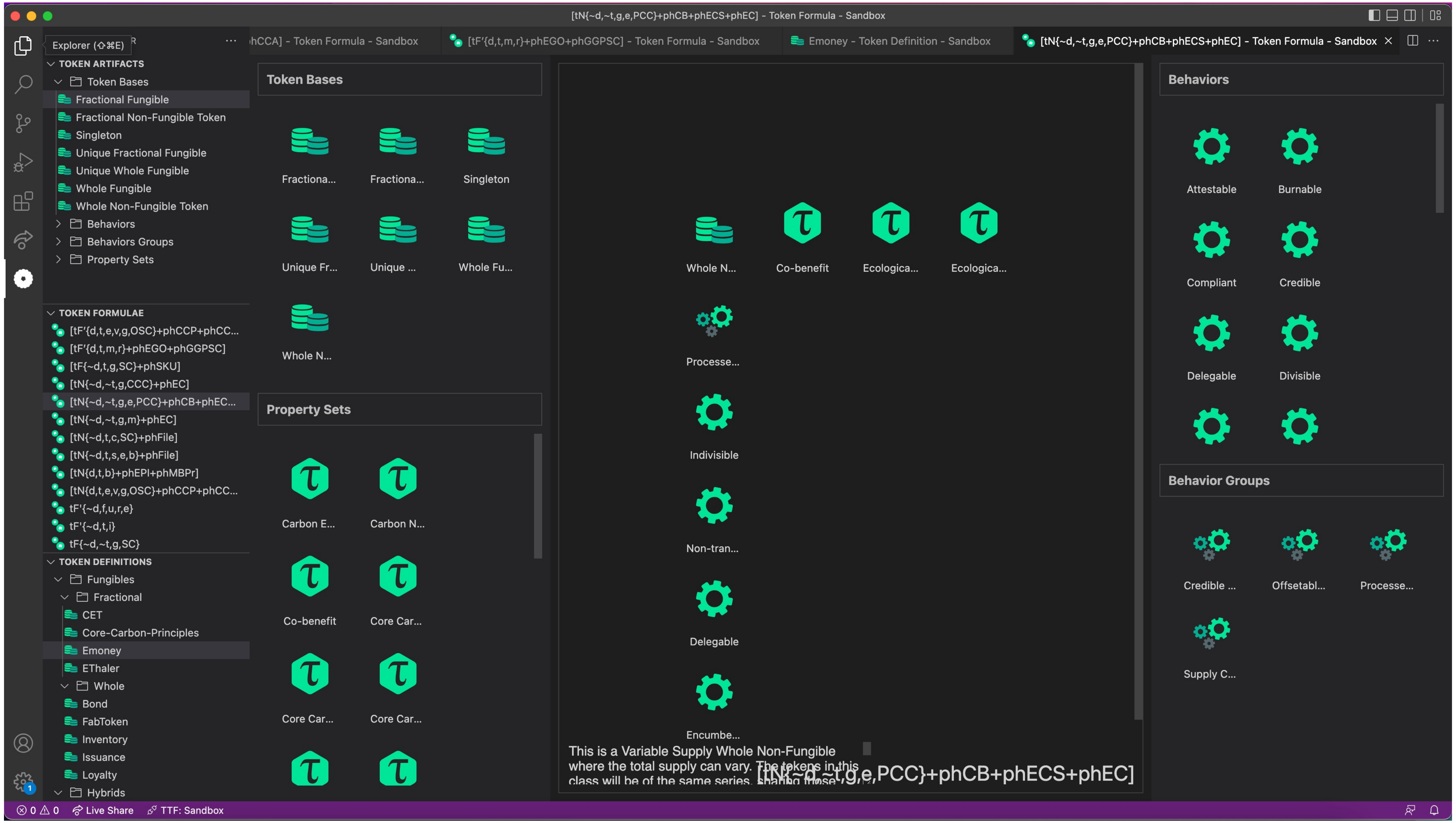
- Transferrable
- Burnable
- Mintable

Sources:

https://github.com/InterWorkAlliance/TokenTaxonomyFramework/blob/master/TTF-Book.pdf

https://github.com/InterWorkAlliance/TokenTaxonomyFramework/blob/main/token-taxonomy.md

Taxonomy Framework: Token Designer



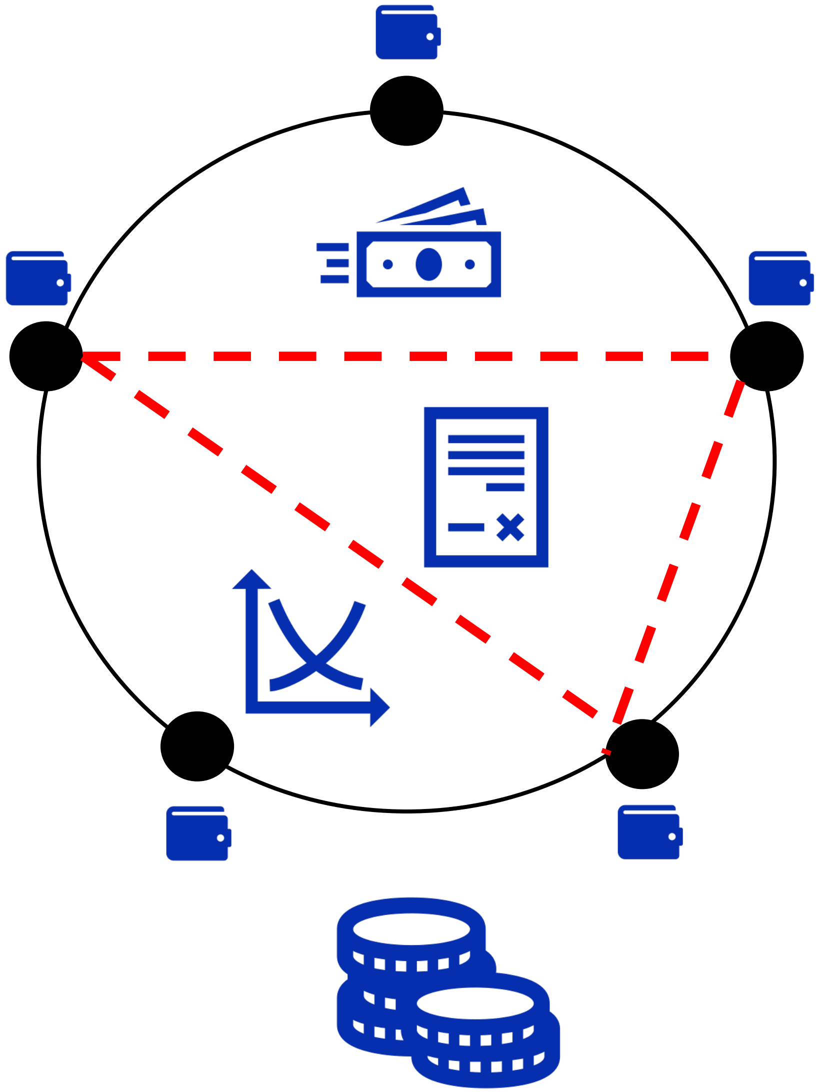
This is a Variable Supply Whole Non-Fungible where the total supply can vary. The tokens in this class will be of the same series, sharing those

[tN{~d,~t,g,e,PCC}+phCB+phECS+phEC]

Source to download VS plugin:
https://marketplace.visualstudio.com/items?itemName=InterWorkAlliance.token-designer

Taxonomy

Tokens	Main purposes	Examples
Governance	Decision-making	Vote to improve network / ecosystem
Utility	Access	Rewards, payments
Security	Ownership	Equity, bonds
Non-fungible (NFT)	Unique Representation, Digital Twins	Membership right, right to artefacts
Liquidity provider (LP)	Enhanced liquidity	Reward for supporting exchanges

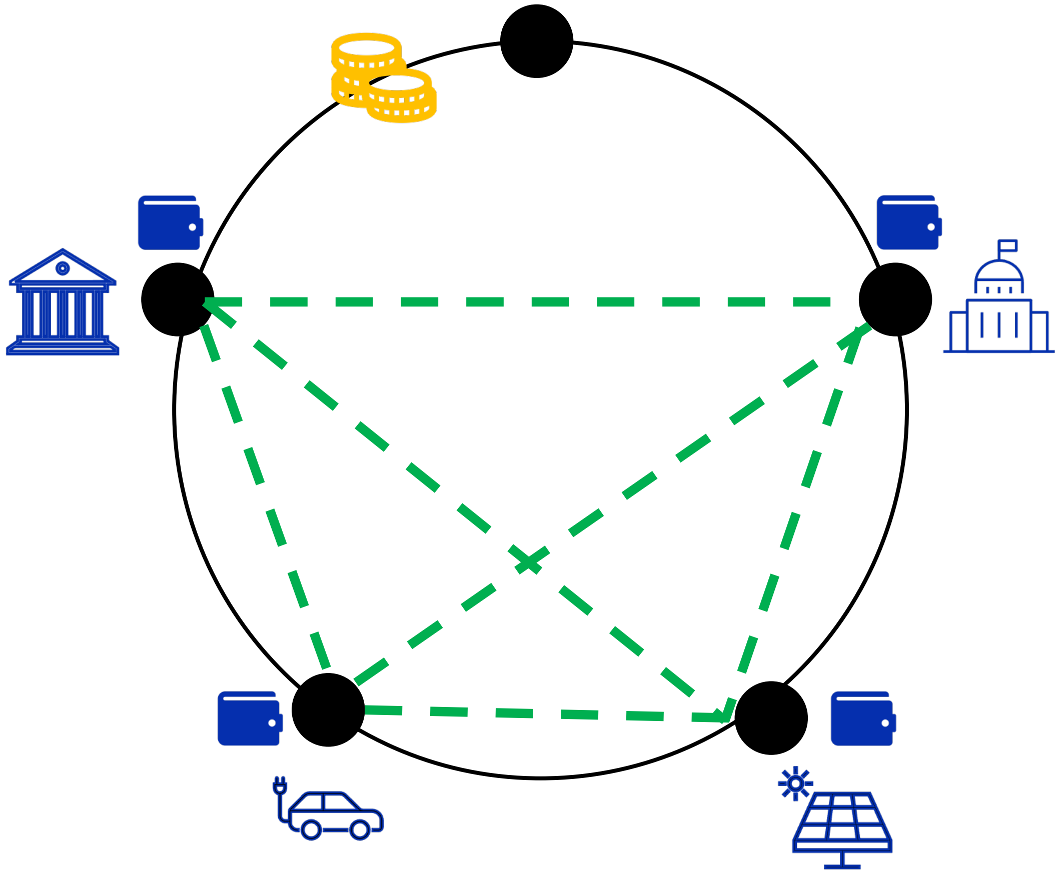


Source:

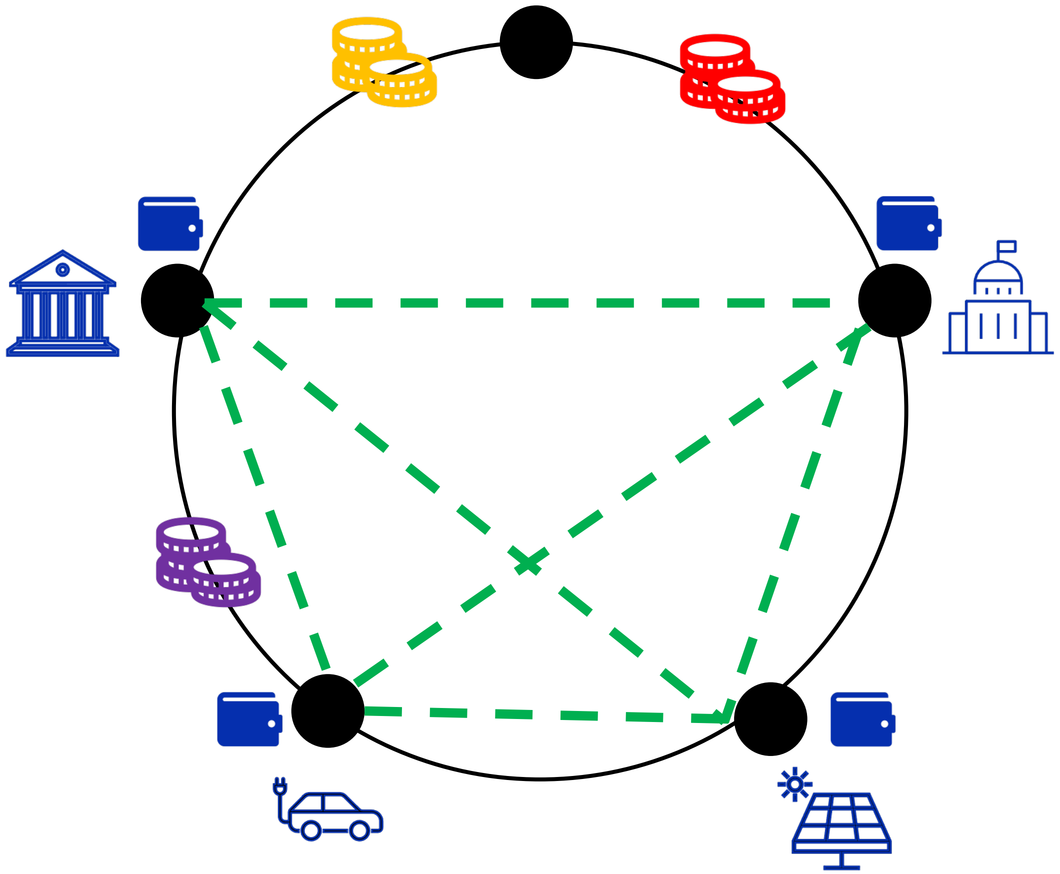
https://global-uploads.webflow.com/602fa386a0b6705bf095dbce/635a7a8704fcf67b9eb9700b_Upside_Taxonomy-of-Tokens.pdf

Private vs Public Asset Exchange

- Private network for tokenised energy certificates



- Public network for tokenised energy certificates



Source:

https://www.ibm.com/blog/revolutionizing-renewable-energy-certificate-markets-with-tokenization/

Standards to ensure compliance and interoperability

ERC Token Standards

ERC standard	Applications
ERC-20	Fungible token standard
ERC-721	Non-fungible token standard
ERC-1155	Multi-token standard
ERC-725	Identity standard
ERC-223	Superset of ERC-20 with increased economic security
ERC-621	Superset of ERC-20 to increase / decrease the total #tokens in circulation
ERC-1400	Security token standard
ERC-827	Superset of ERC-20 to support third party apps development on Ethereum
ERC-884	Superset of ERC-20 to represent equity issued by any Delaware corporation
…	

Industry Standards (e..g RE100 for Energy Industry)

Standardised certificate information (RE100)
Resource / Fuel type
Serial ID
Generator ID
Generator name
Generator location
Date of generation
Issuance date
…

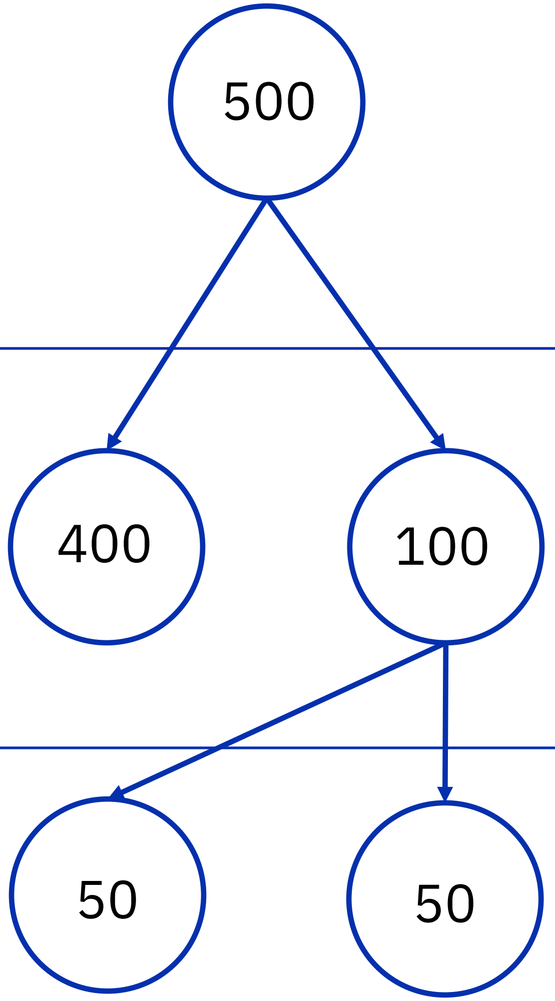
Sources:

https://www.blockchain-council.org/ethereum/erc-token-standards/

https://www.there100.org/sites/re100/files/2020-09/RE100%20Making%20Credible%20Claims.pdf

Recording the Network’s State

UTXO model



Account model

Alice: £500

Bob: £50

Charlie: £0

State n

Alice: £400

Bob: £50

Charlie: £100

After Alice sent £100 to Charlie

State n+1

Alice: £400

Bob: £100

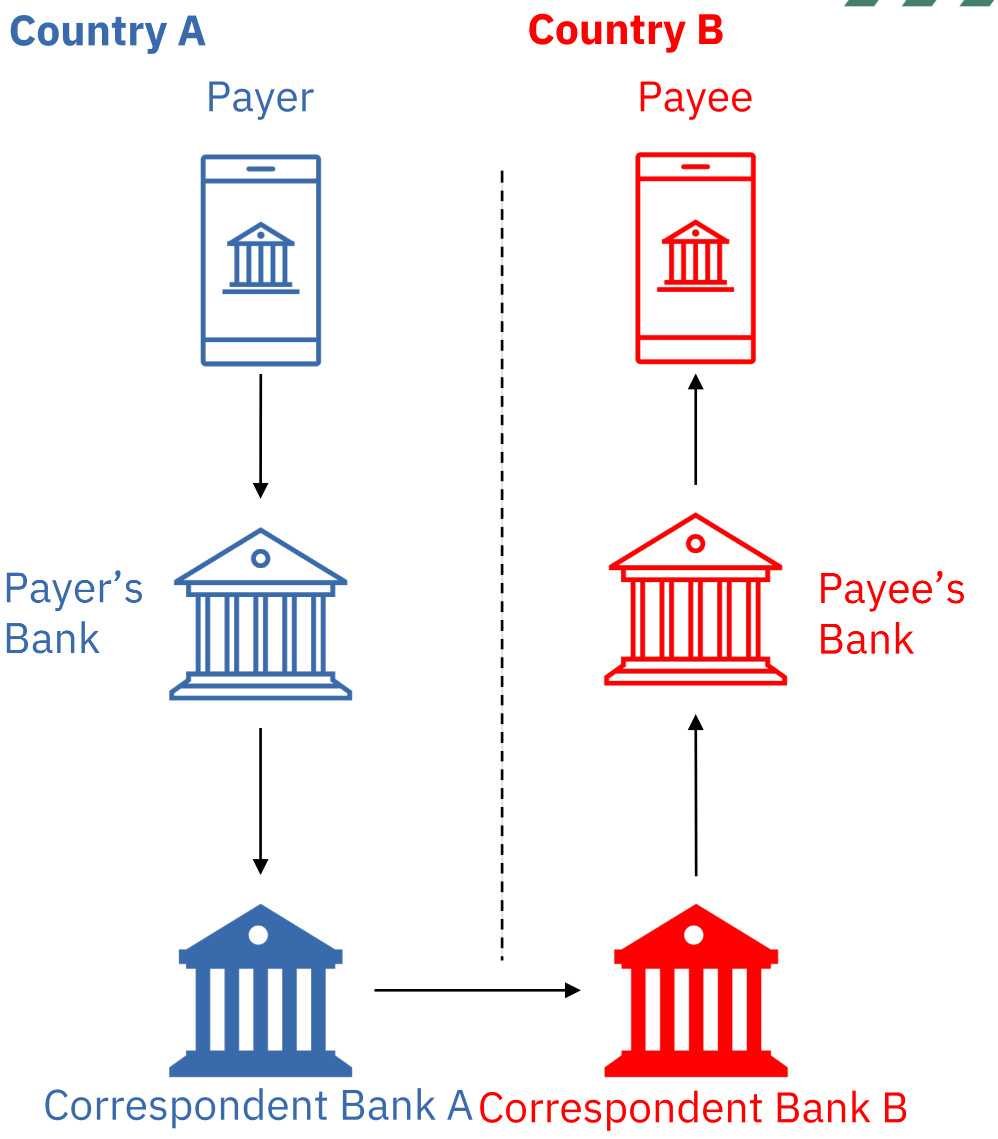
Charlie: £50

After Charlie sent £50 to Bob

State n+2

How CBDC can modernise cross-border payments

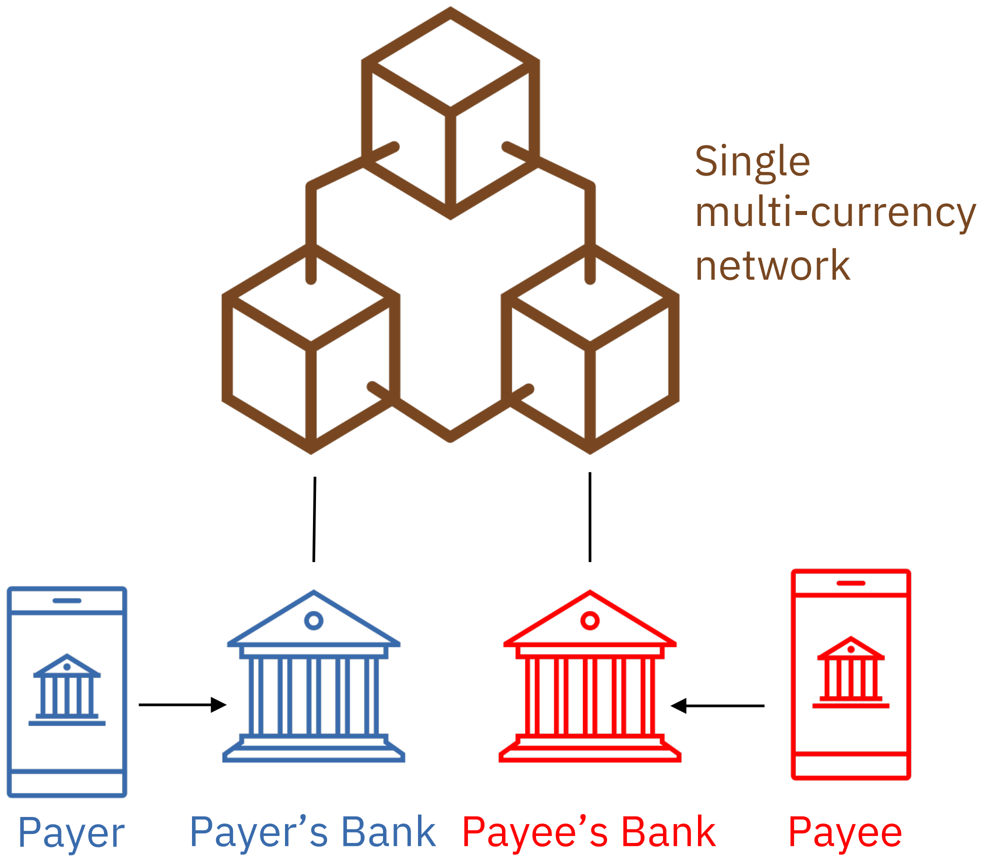
Current cross-border payment setting (simplified)



Pain points in current cross-border transactions

- High transacting fees
- Low-speed transactions
- High operational complexities
- Increased challenges for correspondent banks
- Diversity in terms of jurisdictions, liquidity availability

Desired cross-border payment setting (simplified)



Retail CBDC

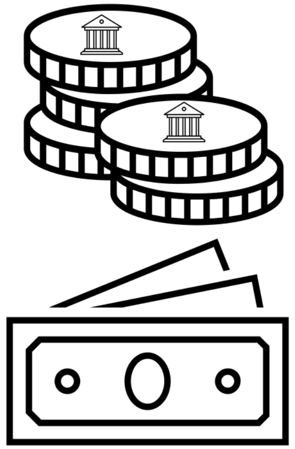
Advantages

- Immediate clearing & settlement for retailers and tax authorities (?)
- Low processing fees (?)
- Government subsidies (without fraud)
- Inclusivity

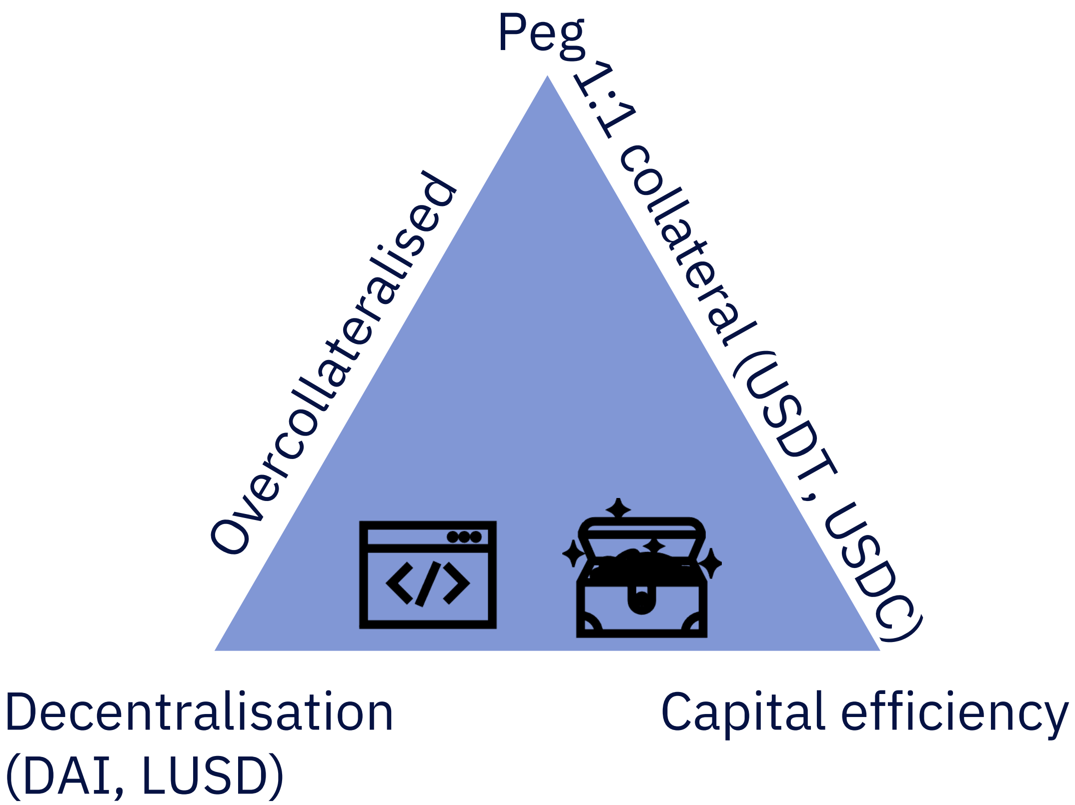
Societal concerns

- Privacy
- Capital control
- Uncertainty in added value

Role of commercial banks?



Stablecoins



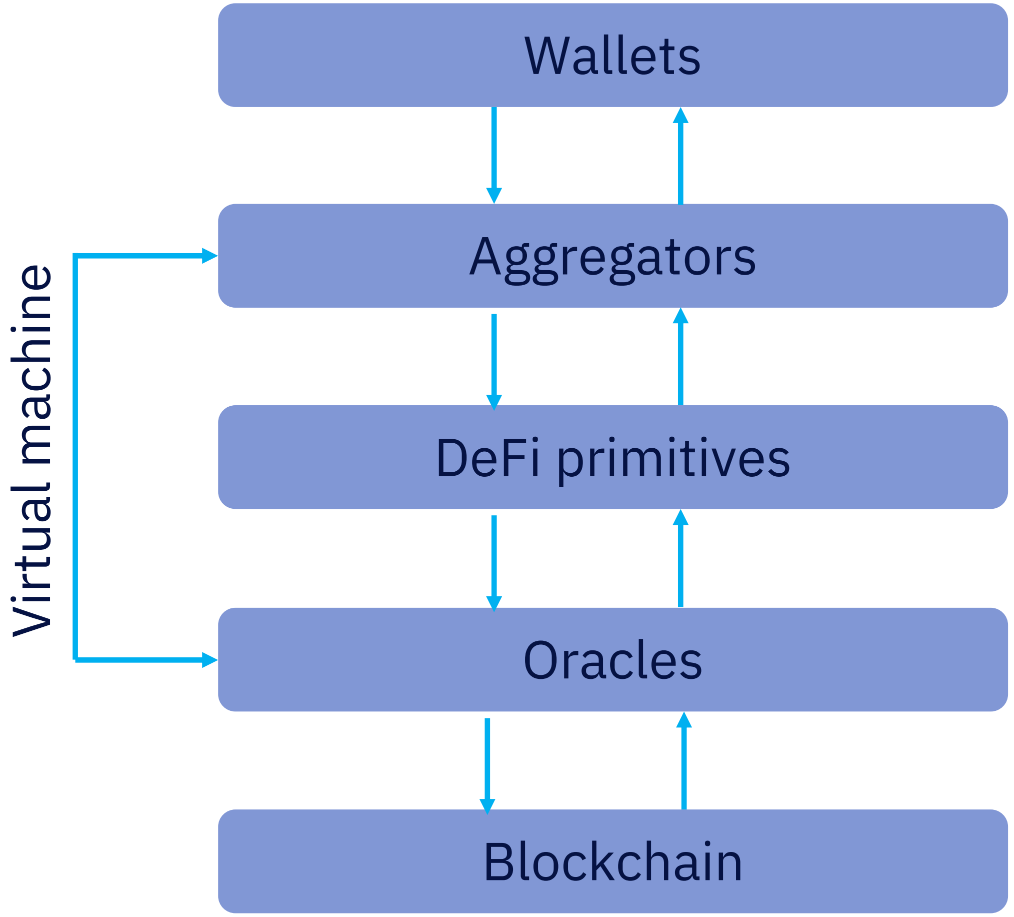
Types

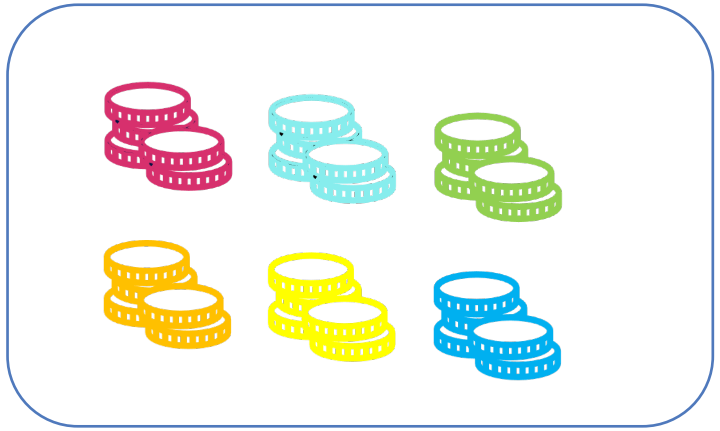
- Algorithmic
- Collateralised
- Mixed

Exchanges

- Increased demand, new coins issuance to keep peg to $1
- Often, dual tokenisation layer in place
    - Token A maintains peg
    - Token B absorbs market volatility

Decentralised Finance (DeFi)





Agents

- Users
- Liquidity Providers
- Arbitrageurs
- Application Designers

Risks

- High volatility
- Immature governance
- Complex financial incentives
- Dependency on off-chain oracles
- Attacks (e.g., front-running)

Source:

Jensen, J. R., von Wachter, V., & Ross, O. (2021). An introduction to decentralized finance (defi). Complex Systems Informatics and Modeling Quarterly, (26), 46-54.

Agenda

1. Who Are We?
2. Blockchain Fundamentals
3. Blockchain Architecture
4. Tokens
5. **Digital Identity**
6. Complex Use Cases

Why do we need digital identities?

- ≈ 1 billion people globally lack a legally recognized form of identification.*
- ≈ 30% of calls to banks’ call centers were related to access requests due to misplaced or forgotten passwords*

Significant Operational Costs

- Massively paper-based & error-prone processes
- Digitisation often with insufficient digitalisation
- Limited integration with other systems
- Duplicated processes
- In-person identity verification

Limited Customer Experience

- Lack of ownership and control
  - Possible credentials revocation by third parties
- Siloed environments
  - Limited portability and interoperability for credentails
- In-person identity verification

Increased Compliance Risks

- Heavily regulated industry
  - Fraud prevention (KYC/AML)
- GDPR compliance
  - Only essential information allowed to be processed
  - Additional responsibility for data controllers
- Privacy protection
- Strict security mechanisms

*Source: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks

Self-Sovereign Identity (SSI) as a Solution

Key SSI features that address all limitations of traditional identities

Empowers Users to Own and Control Identities

- Selective disclosure of attributes
- Required consent

Enables Interoperability across Platforms

- Portable and application-agnostic digital identity
- Multitenancy and multiplicity
- Community standards for identities

Ensures Fast and Secure Verification with Blockchain as Bedrock

- Immutable and decentralised ledger for transactions
- Higher service availability

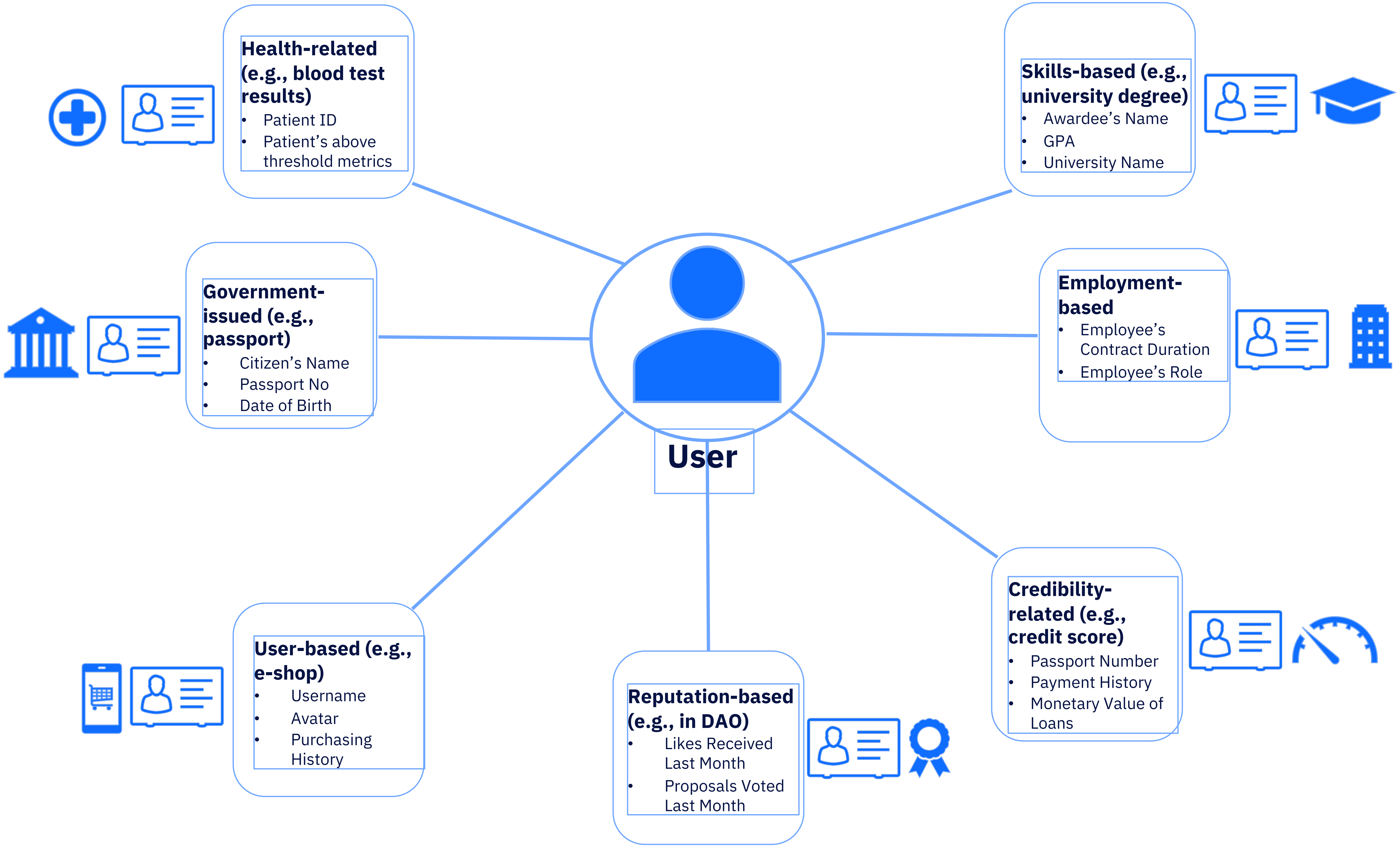
Accelerates Back-office Operations

- Streamlined KYC/AML
  - Aadhar contributed to reduced KYC verification cost for financial institutions from ≈ $5 to ≈ $0.70 per customer*

*Source:

A. Gelb and A. Diofasi Metz, “Identification revolution: Can digital ID be harnessed for development?” Center for Global Development, October 2017.

Different Forms of Web3 Identities



Health-related (e.g., blood test results)
- Patient ID
- Patient’s above threshold metrics

Skills-based (e.g., university degree)
- Awardee’s Name
- GPA
- University Name

Government-issued (e.g., passport)
- Citizen’s Name
- Passport No
- Date of Birth

User

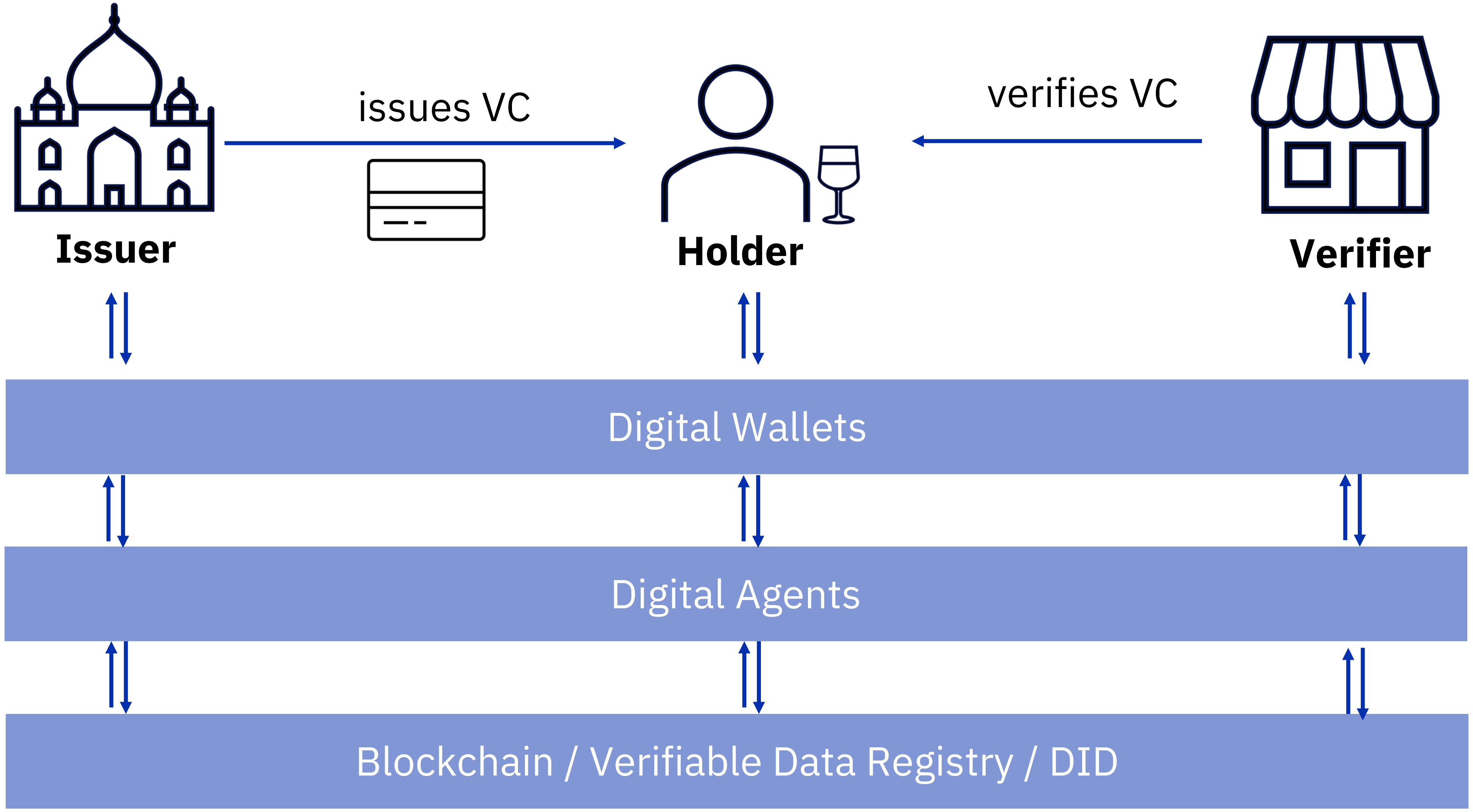
Employment-based
- Employee’s Contract Duration
- Employee’s Role

User-based (e.g., e-shop)
- Username
- Avatar
- Purchasing History

Reputation-based (e.g., in DAO)
- Likes Received Last Month
- Proposals Voted Last Month

Credibility-related (e.g., credit score)
- Passport Number
- Payment History
- Monetary Value of Loans

Self-Sovereign Identities: Architecture



Agenda

1. Who Are We?
2. Blockchain Fundamentals
3. Blockchain Architecture
4. Tokens
5. Digital Identity
6. **Complex Use Cases**

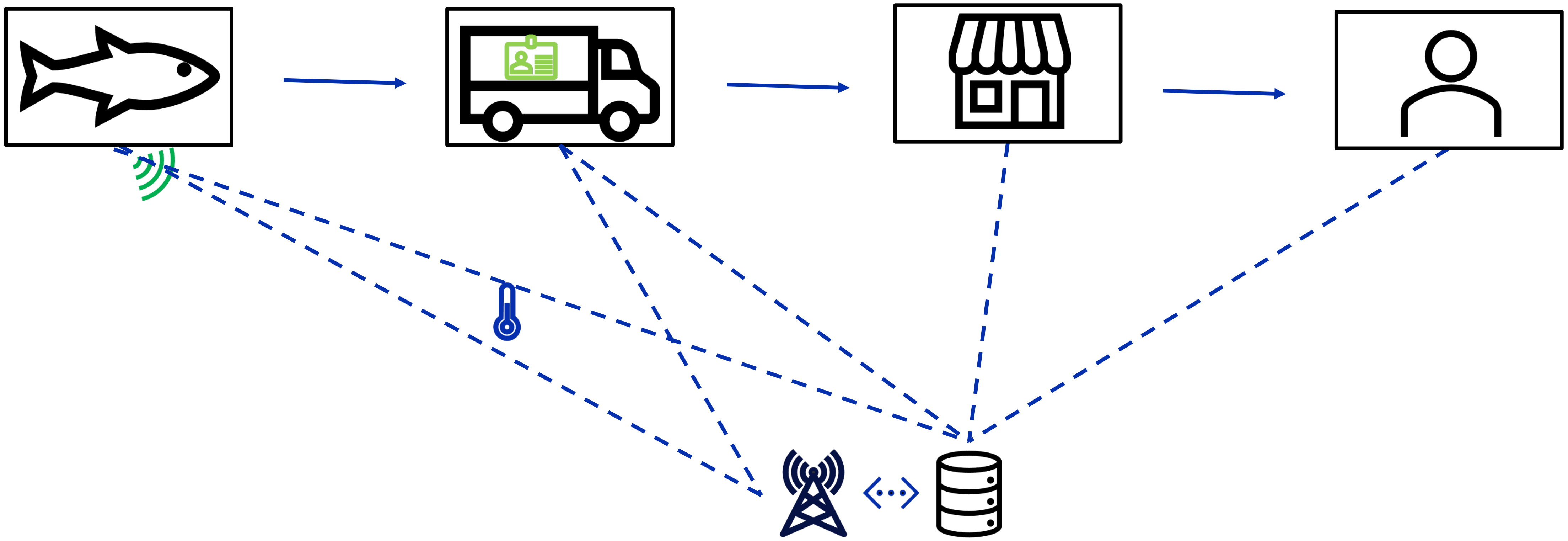
Enterprise use cases

- Supply chain
  - Automotive
  - FMCG
  - Banking & finance
  - Industrial products
  - Oil & petroleum

- CBDCs
- Other financial products (e.g. bonds, securities)
- Energy certificates
- Tokenised vouchers
- Real estate

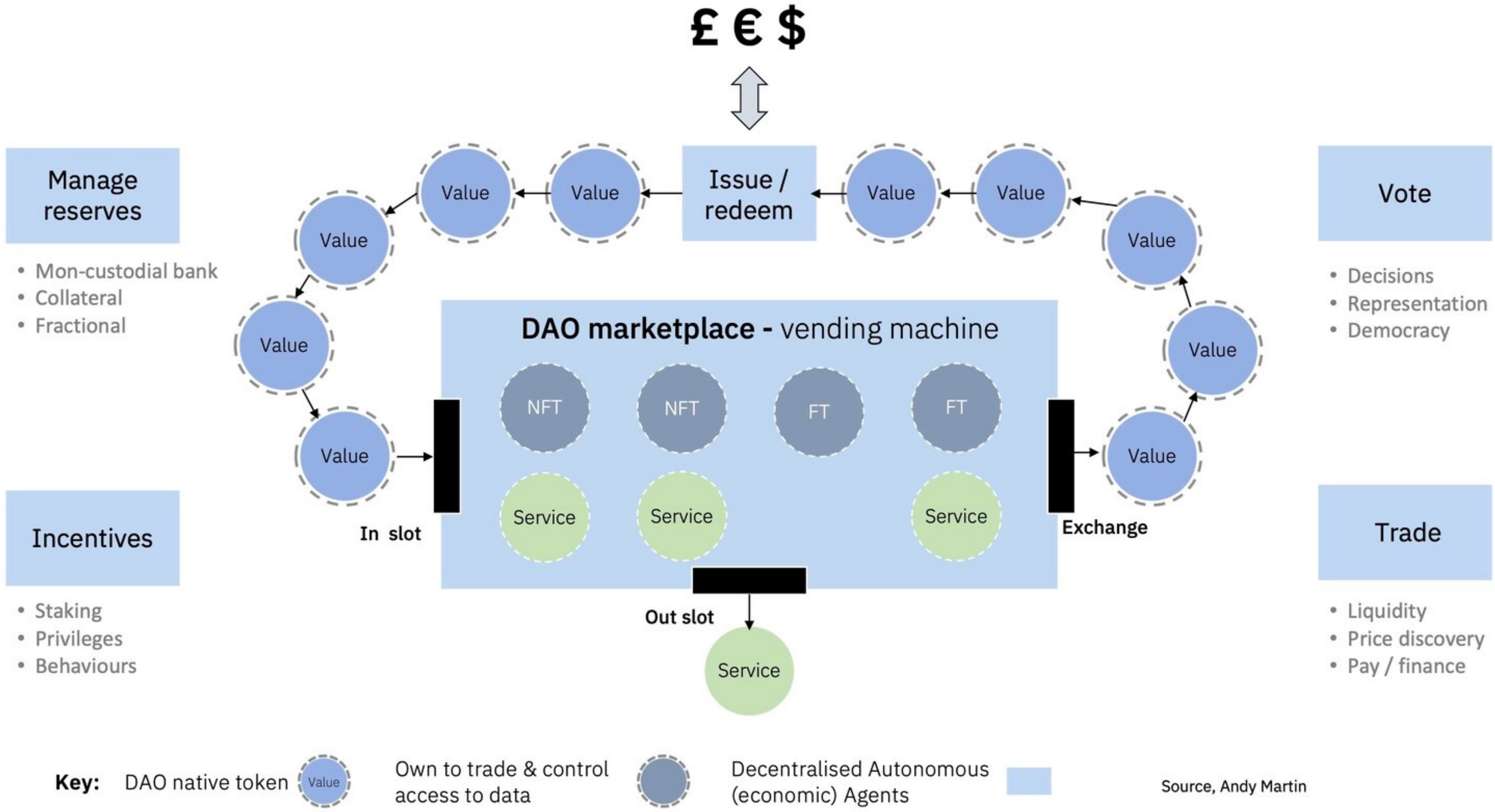
- Voting (eligibility)
- Artwork certificate
- Reputation
- Digital passport
  - Vaccination certificate
  - Proof of age

Supply Chain (Provenance)



Complex Use Cases

DAO Marketplace



Source, Andy Martin

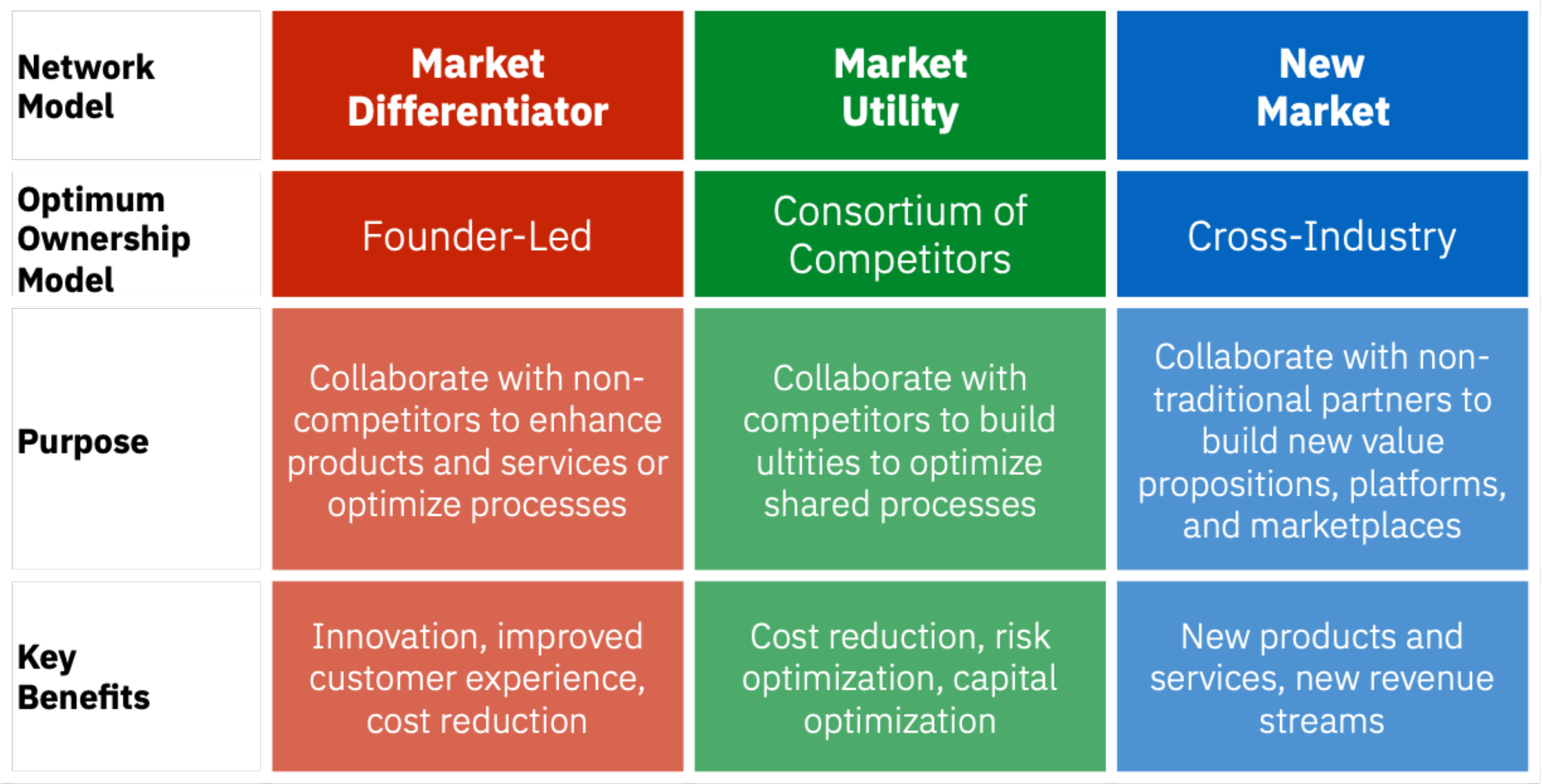
Source:

https://www.linkedin.com/pulse/web3-operating-system-part-2-andy-martin/

Blockchain networks are not only about technology

- Theory of nations
- Voting mechanisms
- Behavioural economics
- Graph theory
- Multi-agent system theory

Private Market Models



Network Model	Market Differentiator	Market Utility	New Market
Optimum Ownership Model	Founder-Led	Consortium of Competitors	Cross-Industry
Purpose	Collaborate with non-competitors to enhance products and services or optimize processes	Collaborate with competitors to build ultities to optimize shared processes	Collaborate with non-traditional partners to build new value propositions, platforms, and marketplaces
Key Benefits	Innovation, improved customer experience, cost reduction	Cost reduction, risk optimization, capital optimization	New products and services, new revenue streams

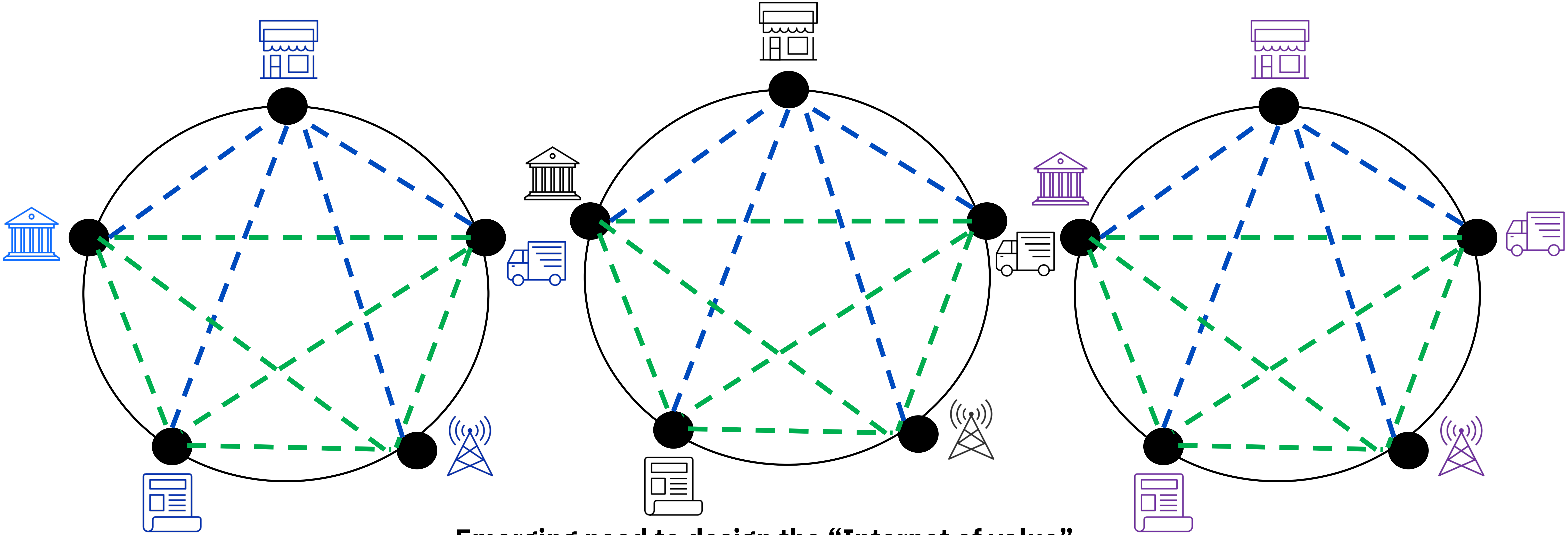
Sources:

https://www.linkedin.com/pulse/new-market-models-blockchain-andy-martin/

https://www.linkedin.com/pulse/building-business-cases-blockchain-blog-number-1-andy-martin-1

Additionally: Goldsby, C., & Hanisch, M. (2022). The Boon and Bane of Blockchain: Getting the Governance Right. *California Management Review*, *64*(3), 141-168.

Isolated new market networks have limited value

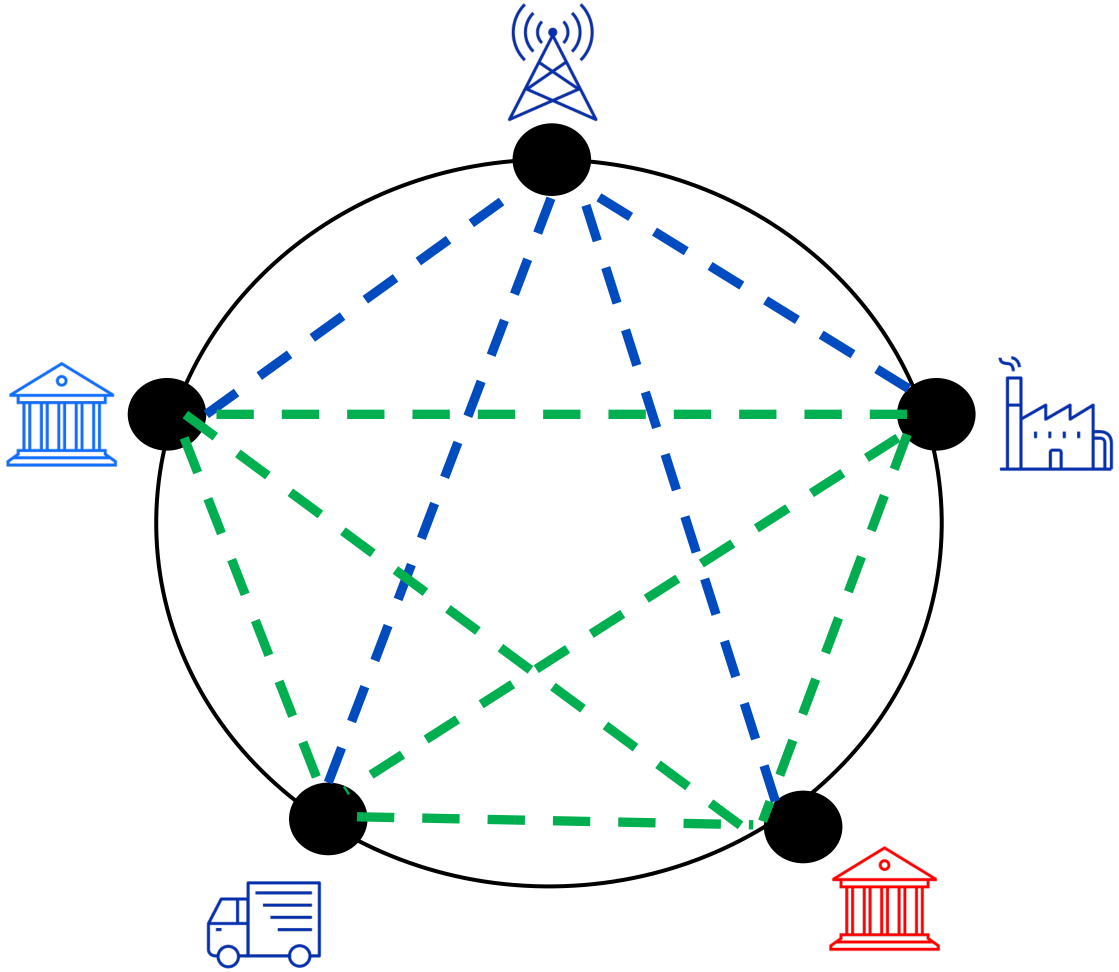


Emerging need to design the “Internet of value” on a public network*

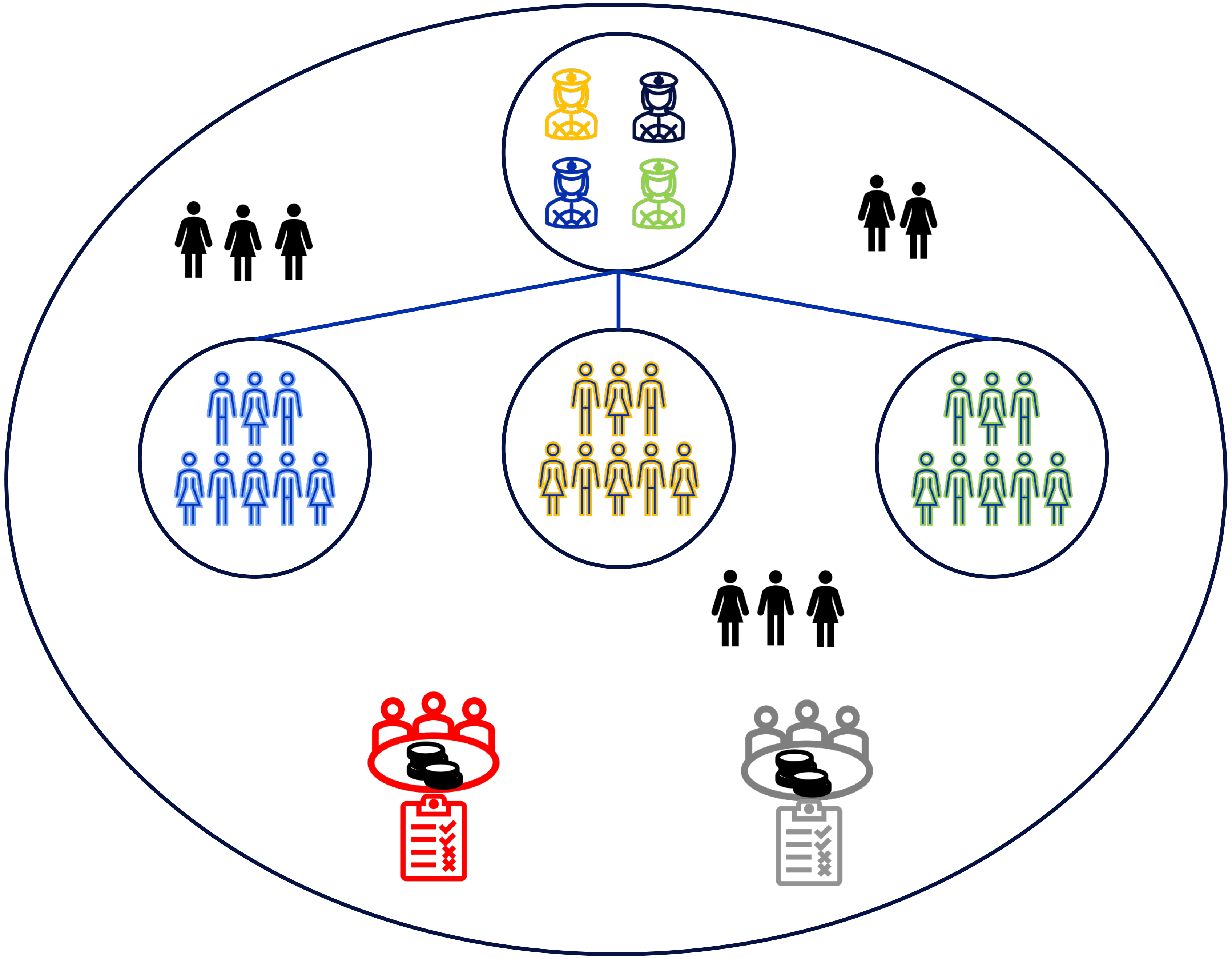
● General member

Disclaimer: interconnection between private networks could be an option, among other alternatives

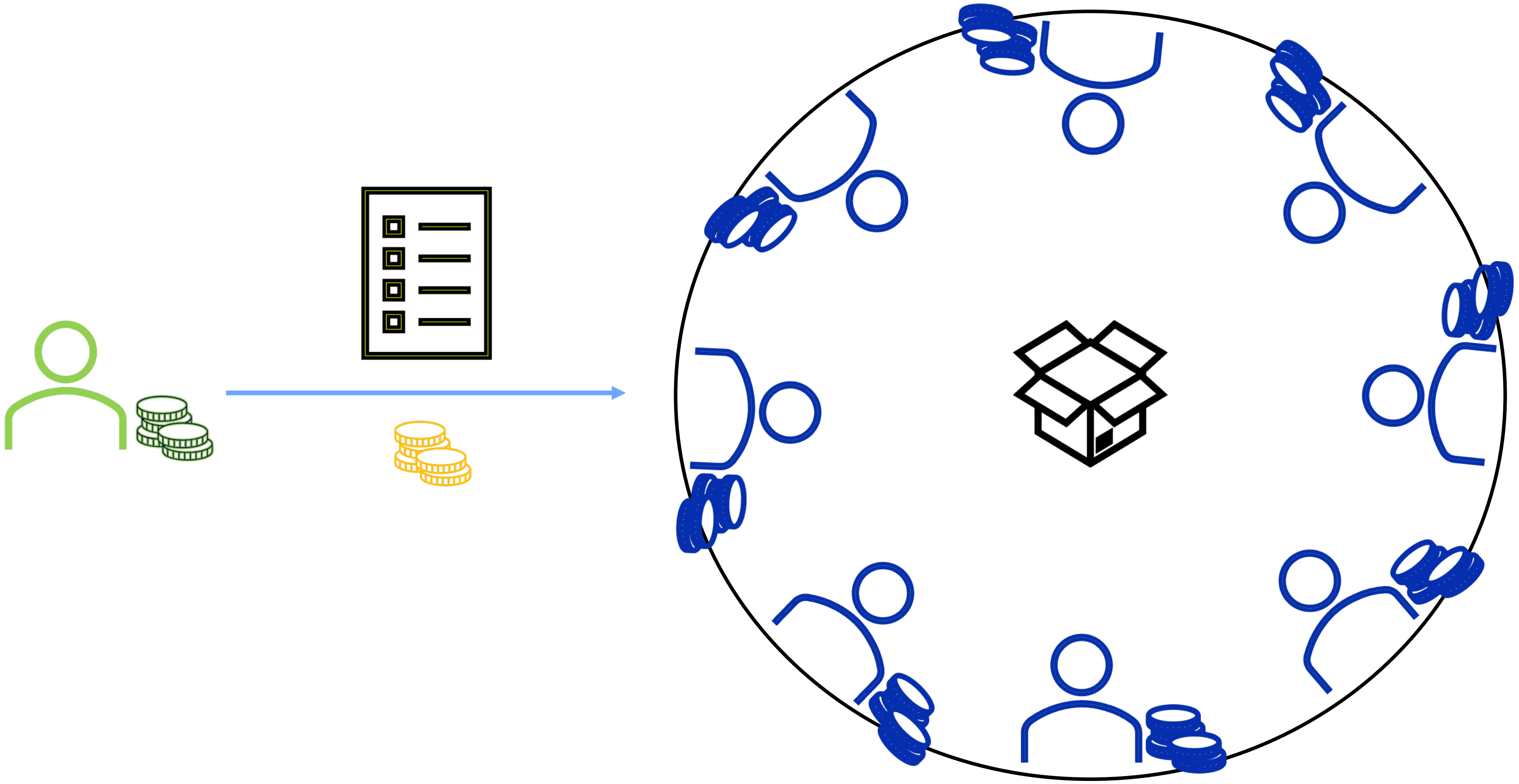
Towards the “Internet of value”



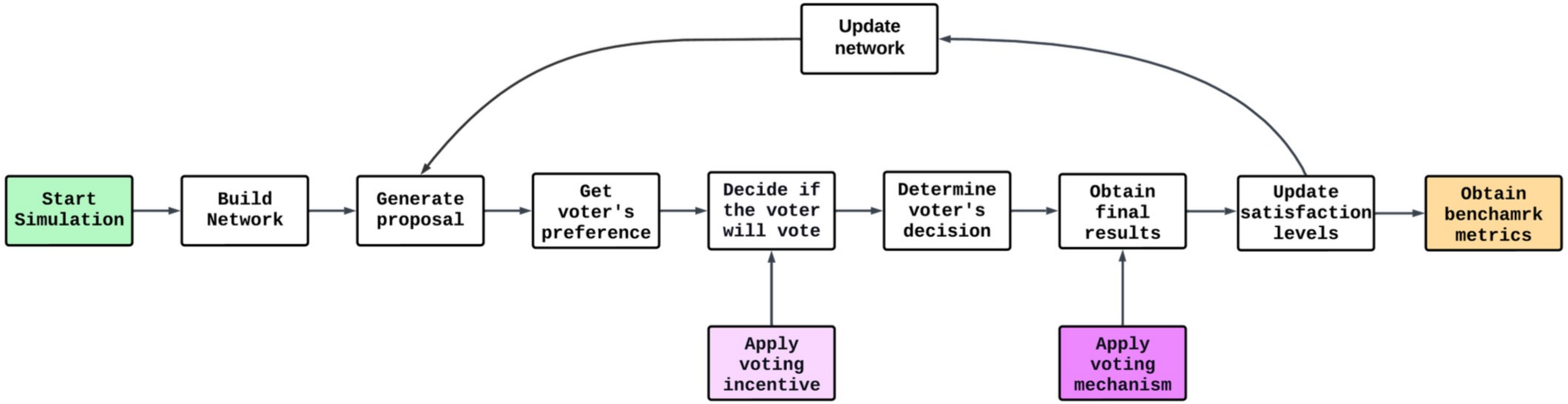
Decentralised Autonomous Organisations (DAOs)



Governance in DAOs



Designing public networks for enterprises



Fitness evolution model & Block model

- Fitness function
  - Business relations, connections, power

Voting simulation

- Voting incentives
  - Token-based, reputation, penalty
- Voting mechanisms
  - Token-based, reputation, penalty

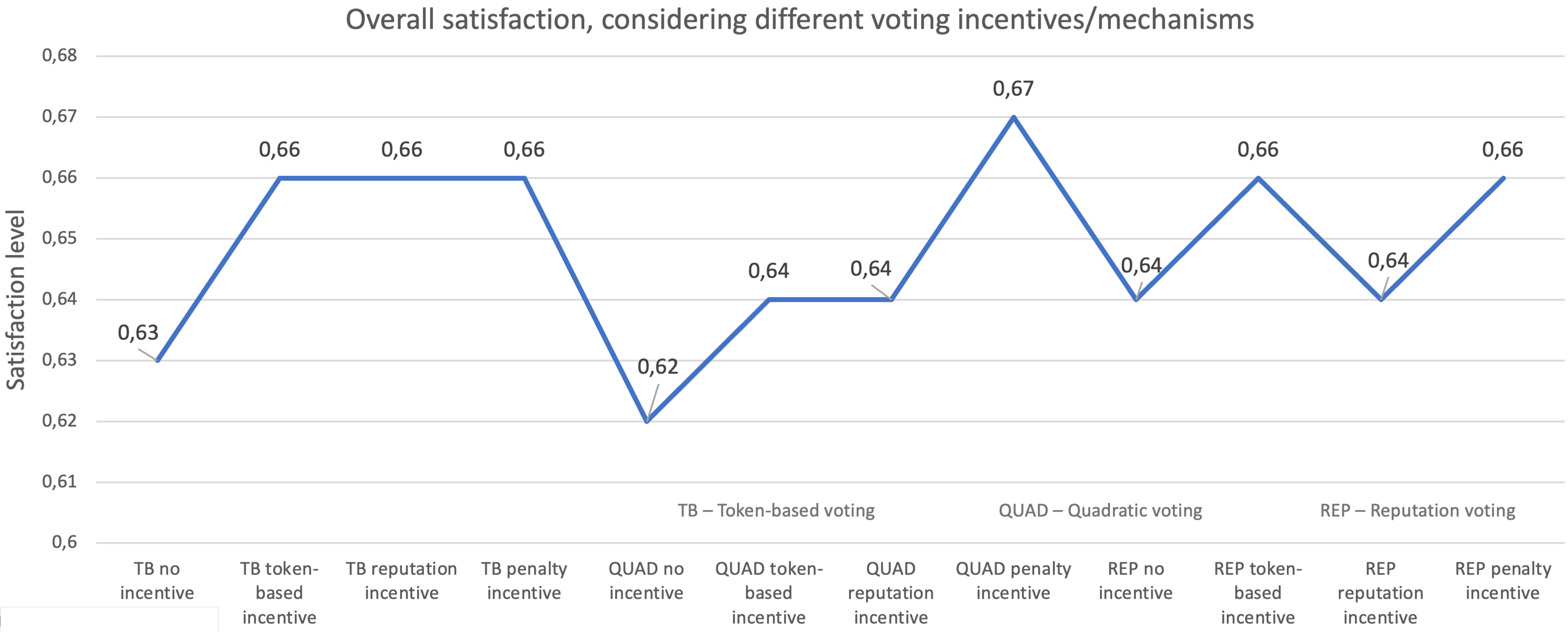
Evaluation framework

- Network wellness
- Impact on decentralisation
- Voting fairness

Source:

Dimitrov, S. Exploring decentralised governance settings for not-for-profit public blockchain networks. MSc dissertation at University College London, 2023

Designing public networks for enterprises: Simulation Results



Source:

Dimitrov, S. Exploring decentralised governance settings for not-for-profit public blockchain networks. MSc dissertation at University College London, 2023

Challenges

Traditional Enterprises

- Scepticism towards blockchain and fear of change
- Data sharing concerns
- Limited buy-in from executive stakeholders
- Outdated legsislative and regulatory framework
- Funding

Web3

- Complex setting for new joiners
- Significant room for stakeholders’ education
- Uncertainty in community goals and commitments
- Outdated legsislative and regulatory framework

Thank you!

Vasileios Theodosiadis

Blockchain Project Manager, IBM CIC NL

Industry Associate, UCL CBT

Konstantina Koutsogiannopoulou

Blockchain Developer, Manager, CTO Office, IBM CIC NL

IBM Client Innovation Center

Netherlands