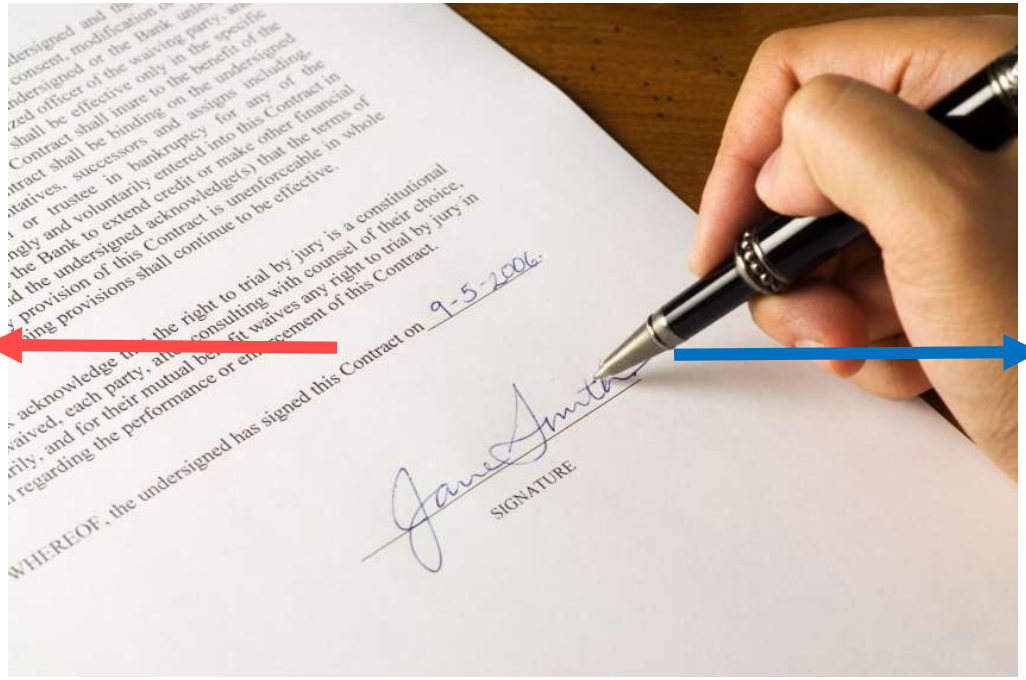
A Glimpse into the Future Decentralized Data Ecosystems

Timo Hotti – OP Financial Group
timo.hotti@op.fi

OP

The key problem: How to digitalize and decentralize contracts, the key building block of the economy?

Digital Paper
- Pre-requisites?
- Execution Flow?
- T&Cs?
- Outcomes?

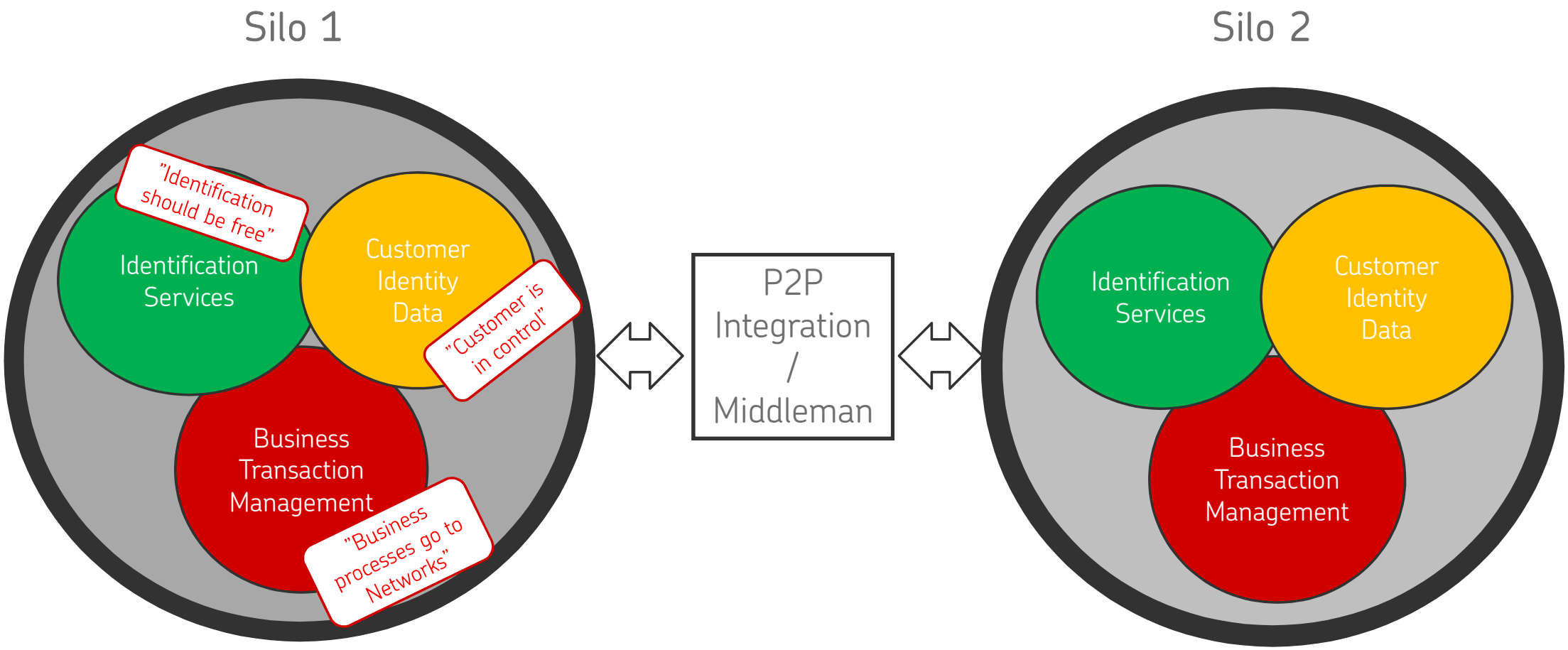


Digital Signers
- Identification?
- Authorization?
- Signing?
- Verification?

”Blockchain” can help on both sides!

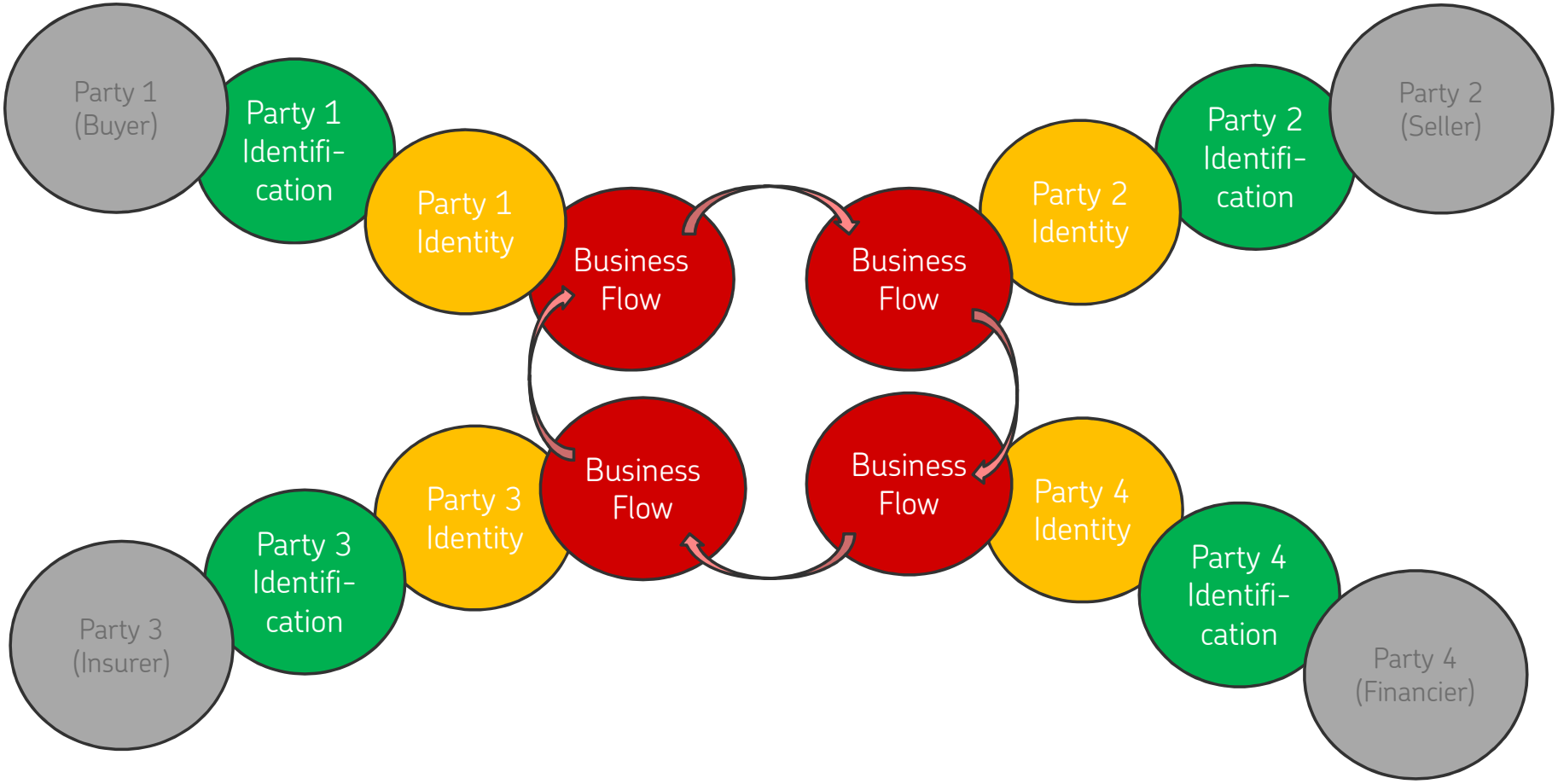
OP

Our current way of building systems



OP

Future – bilateral business transactions convert into multilateral network-based business flows



OP

What is ”blockchain” (DLT) good for?

It is good for **Digitalization** and **Decentralization** of **Transactions** and **Data Assets**

1. Cryptographically secured **decentralized** way to execute a **digital business process** between parties in a network without intermediaries

   E.g. execute a trade

2. **Decentralized** and secure way to create and manage **digital data assets** in a network in a manner where no single party, except for their owner, can control the assets alone

   E.g. create and manage a **digital identity** and **data related to the identity**

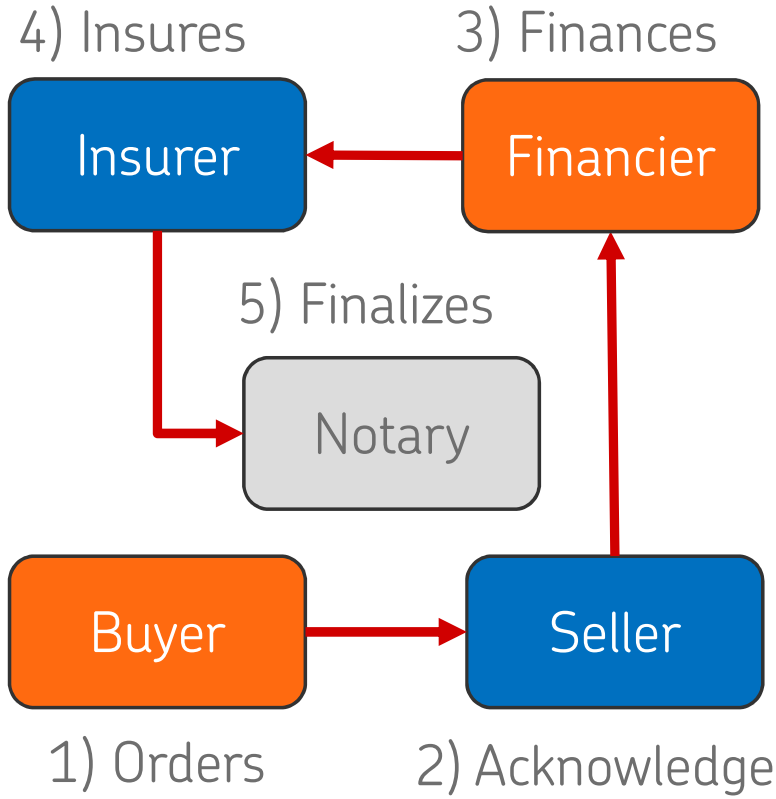
These two uses of ”blockchain” can and should be combined together!

Theory Part 1 – ”The Digital Paper”

Business Transaction Management

Digitalizing the Paper of the Contract – Part 1: Contract Execution Flows

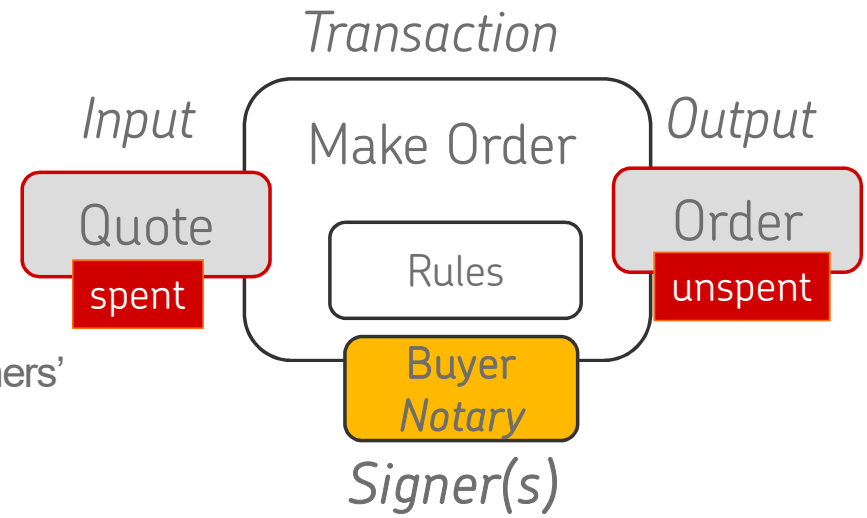
- DLT = Decentralized data management method for efficient management of **contract data**
  - The contract has more than one party
  - Every party has its own copy of the contract, delivered and maintained by the flows related to the contract
  - When the contract is executed, it is validated and digitally signed by its parties
- DLT-protocol executing the flow ensures, that the state of the contract is the same in all copies of the contract
- The Notary ensures, that the contract has been approved by all parties of the contract



Business Transaction Management

Digitalizing the Paper of the Contract – Part 2: Approval of a Transaction

- A Transaction consumes **input states**, from which the logic of the transaction creates **output states**
  - Each party of the transaction validates the transaction using its validating rules
- Participants' approvals = **digital signatures**
  - Buyer signs a purchase order
  - Seller signs an invoice, etc.
- All participants of a transaction need to be able to validate each others' signatures and authorizations
  - Hence, a shared digital ID infrastructure is needed
- The notary node of the network confirms the transaction using its signature after the parties have approved the content of the transaction
  - Notary ensures that the transaction inputs are used in one and only one transaction



Project DIAS – Digital Apartment Trading Network

Theory Part 2 – ”The Digital Signer”

Digitalizing the Signers of the Contract – The Infrastructure

Self-sovereign principle

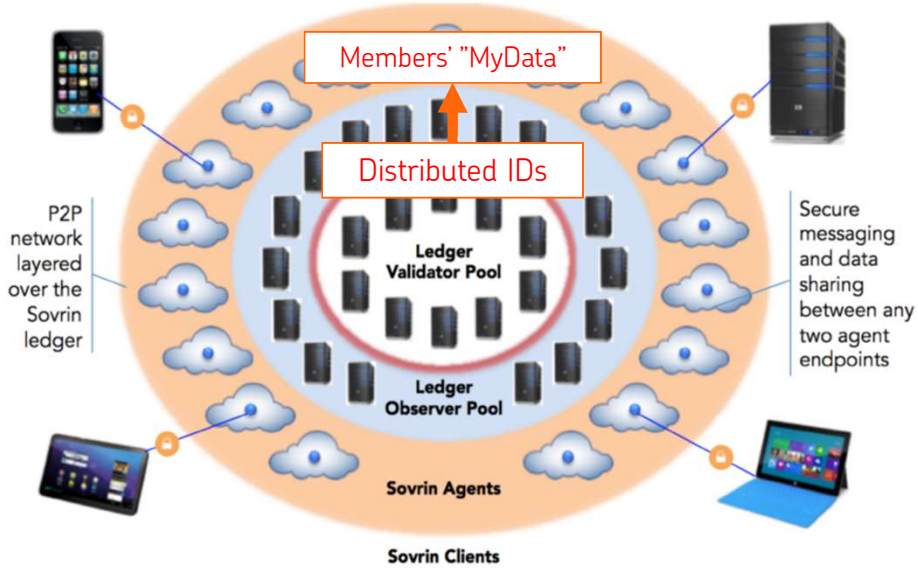
- Entities manage their own data assets in the network
- Trust is provided by the ”blockchain community”

Ledger Network for public identity data

- Identifiers
- Public keys
- Pointer to private data

Agent network for private identity data

- Verifiable identity claims
- Consents



Identity Data Management

HYPERLEDGER INDY

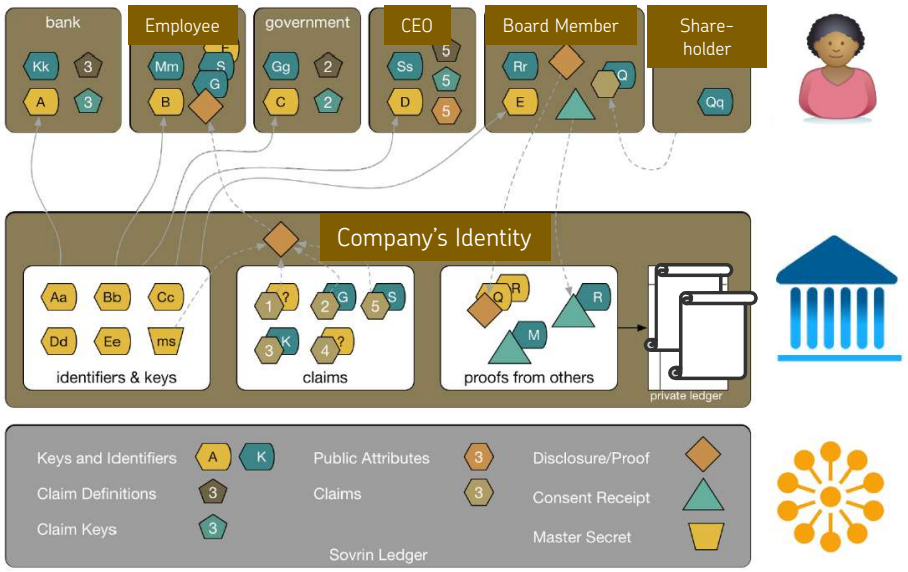
Digitalizing the Signers of the Contract - The Self-Sovereign ID for individuals and businesses

For Individuals

1. Establish the identity (DID – Distributed ID) in the public ledger
2. Create the identity claims in the Agent and have them verified by 3rd parties

For Businesses

1. Design the **structure and content** of the Digital ID for a legal entity as entity's DIDs and verifiable claims
   - Identifiers
   - Ownership structures (shareholder claims)
   - Representation mechanisms (Powers-of-attorney)
2. Design the **legally compliant processes** for creating and maintaining the Digital ID using decentralized transactions
   - Setting up the company
   - Specifying the governance rules
   - Authorize persons as a representatives of the company



OP

Practice – Building a fully decentralized digital trade network

The key innovation– Bringing two crypto & decentralization technologies together

Decentralized Transaction Management

- **Transactions** are executed in the network directly between the parties of the transaction using business logic shared by the parties
- **Crypto** technologies allow creating business processes, where every step is signed by the relevant participants
- **Decentralization**/DLT allows transaction's data to be shared between the participants of the transaction only
- **Technology** used: **R3 Corda**

Decentralized Identity Data Management

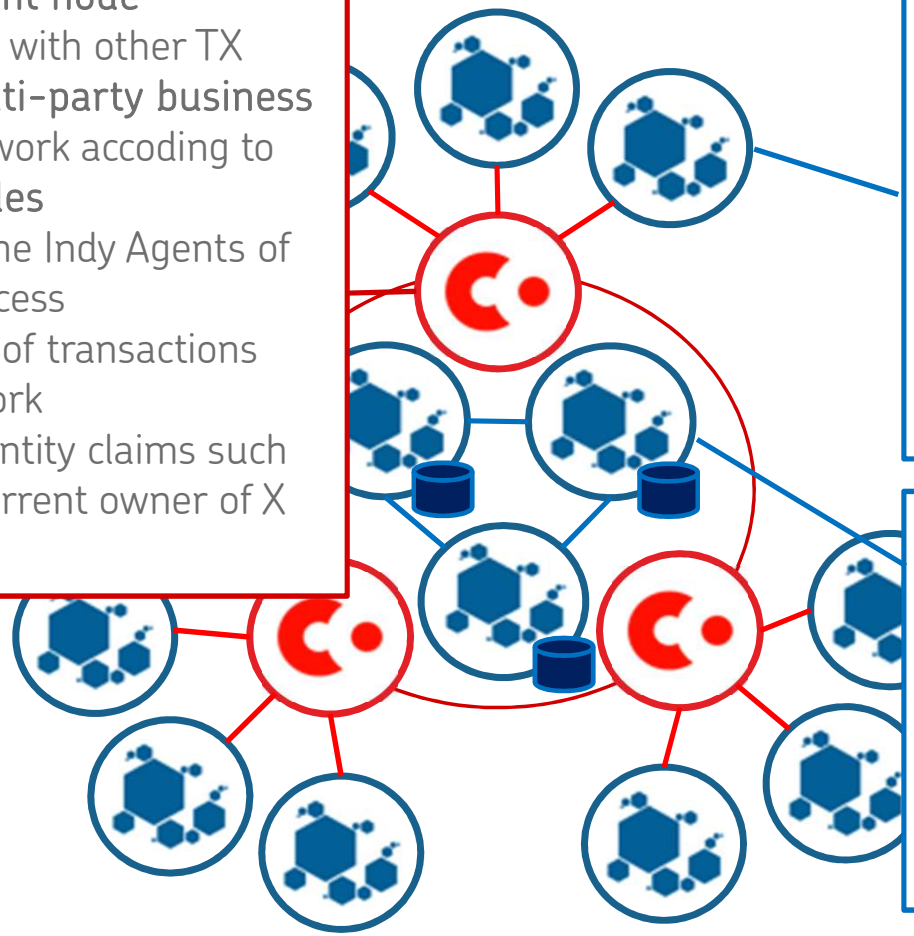
- **Data**, including the identity data, of the parties is managed by the parties themselves
- **Crypto** technologies allow parties to present reliable facts (verifiable claims) about themselves and sign transactions
- **Decentralization**/DLT allows identities to be managed in a network, that is jointly owned by a number of independent entities
- **Technology** used: **Hyperledger Indy**

We combined decentralized transaction management with decentralized identity data management to solve a big business problem previously considered unsolvable

How does the combined crypto data and transaction management network work?

Transaction management node

- Implements, together with other TX mgmt nodes, the **multi-party business processes** of the network accoding to the **jointly agreed rules**
- Communicates with the Indy Agents of the parties of the process
- Maintains the history of transactions executed in the network
- Is able to attest to identity claims such as ”Person A is the current owner of X shares of company Y”



Indy Agent

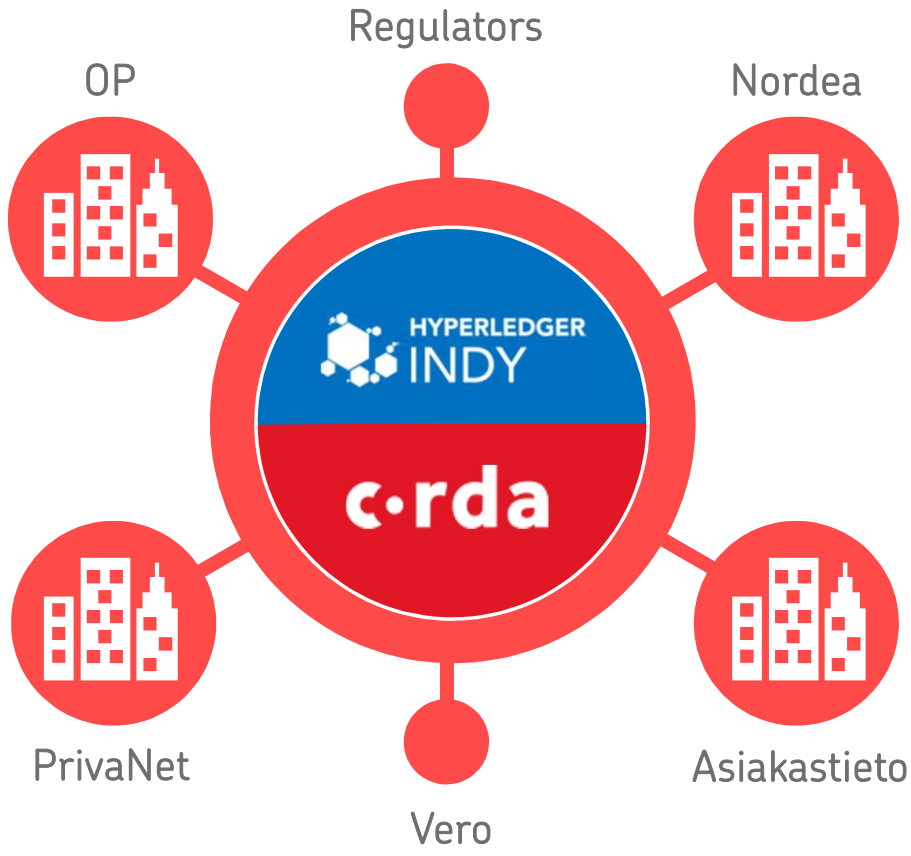
- Manages **private data** of the digital identity
  - It can be anything related to the identity
- Discloses verifiable claims about the identity
  - ”Owner of X shares of company Y”
  - ”Banks with OP”
- May initiate or participate in a process executed in the transaction network

Indy Ledger network

- Manages, in consensus, the **public data** of the digital identities
  - Identifiers
  - Public Keys
  - Address of the Indy Agent of the identity
- Acts as the identity directory of the network

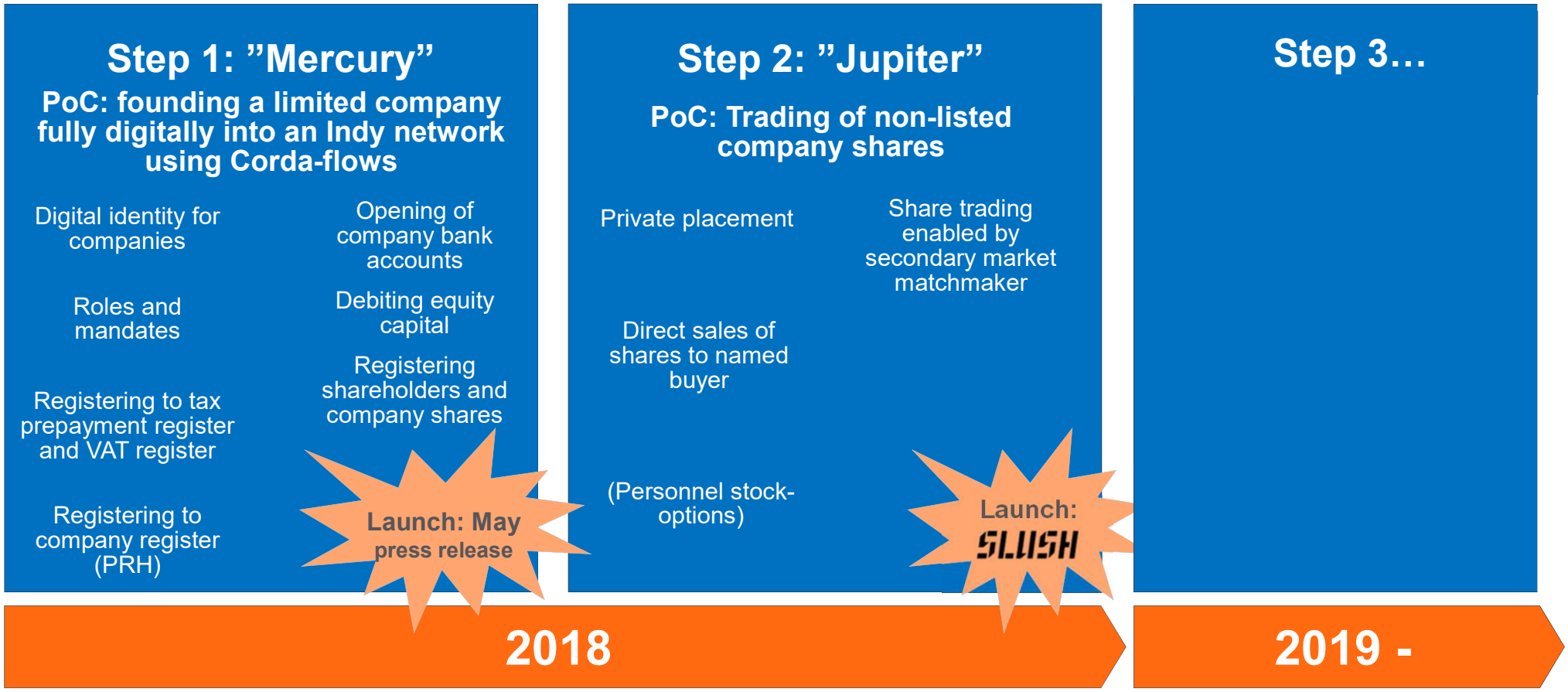
Project Jupiter - Aim and goals

- Demonstrate, how **issuance and trading on non-listed company shares** can be fully digitalised
- Provide all parties **deep technology insight** into how distributed ledger technologies can be harnessed to **decentralize financial data management** and **automate collaborative processes**
- Provide guidance about the **governance, business model and legal implications** of using these technologies.



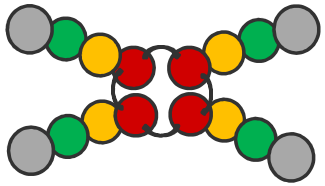
OP

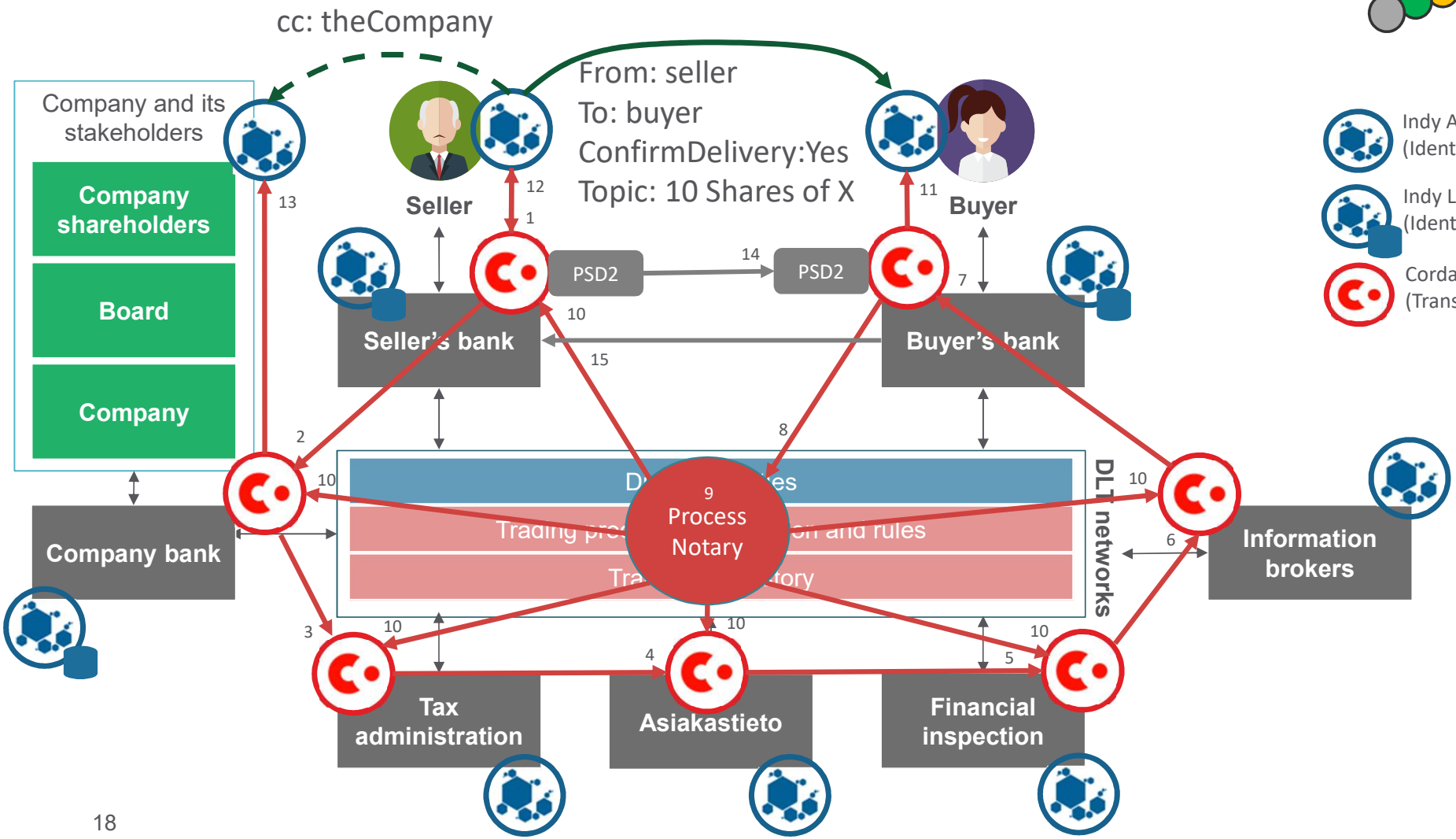
Mercury + Jupiter = PoC of a new digital company ecosystem



OP

Jupiter – How it works





What we have proven

We have proven, that using crypto-based decentralized data and transaction management, we can build a true commerce network, that is...

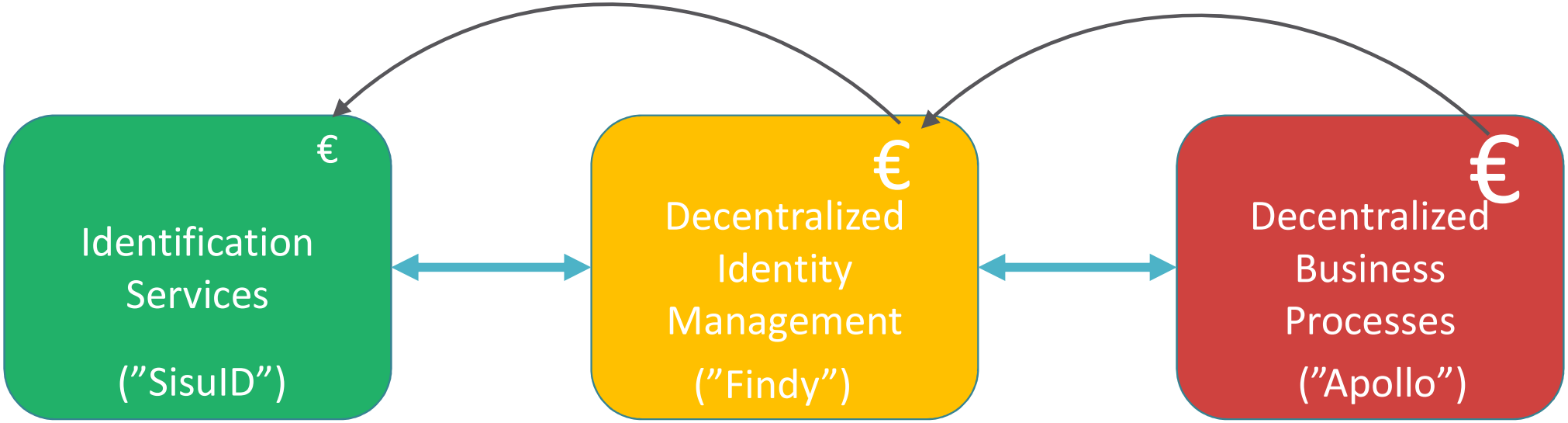
1. Able to quickly implement functionality, that has been generally perceived as Very Difficult
2. Fully decentralized, including the book entry account system
3. Relatively simple from the business logic point of view
4. ”Near-compatible” with the current legislation
5. Utilizes efficiently the European initiatives, such as PSD2 and GDPR
6. Easy to regulate

We have achieved this using ”mainstream” blockchain ideas as an inspiration, but implemented the ideas using technologies, that are suitable for regulated institutions and that meet the privacy and other requirements of the participants.

Future implications

- Decentralized digital identity data management combined with decentralized transaction management enables **direct transfer of value between trusted parties using mutually agreed business logic while keeping parties' data private to the parties**
  - "E-mail for value" / "vMail" / "Internet of value"
- Technology allows building in a fully decentralized manner trade networks, that contain advanced financial processes
  - Identities and their private data, including financial data, will be managed by the parties themselves
  - Transactions will be managed jointly by the parties of the transaction
  - The networks will access the legacy banking systems using Open Banking APIs, such as PSD2
- Banks need to re-define their role to fit these new ecosystems
  - Instead of a Customer coming to the Bank to request for a financing service, the Bank needs to go to the Customer's network to provide the service

The Future Ecosystem

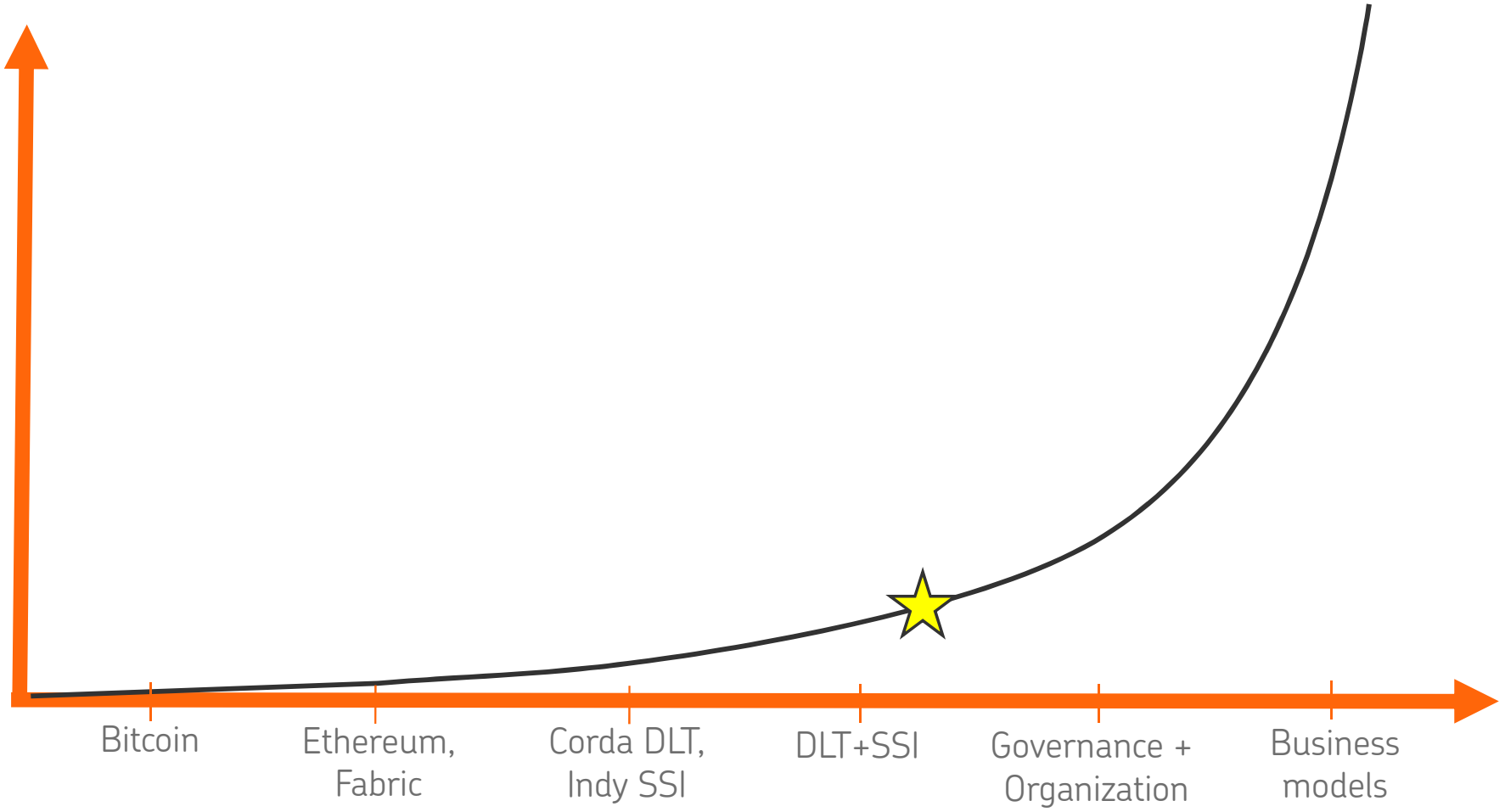


- Identification methods
- Identification data
- Signing keys
- Link to identity wallet

- Self-sovereign principle
- Distributed Ids + Verifiable Claims
- Credentials for biz processes
- PoAs
- Management of identity's data created by biz processes
- For Individuals AND Businesses

- Digital corp ID creation
- Non-listed share trading
- KYC
- Other trade networks
- Other processes, e.g. healthcare

Where are we on the ”Disruption Curve?”



OP