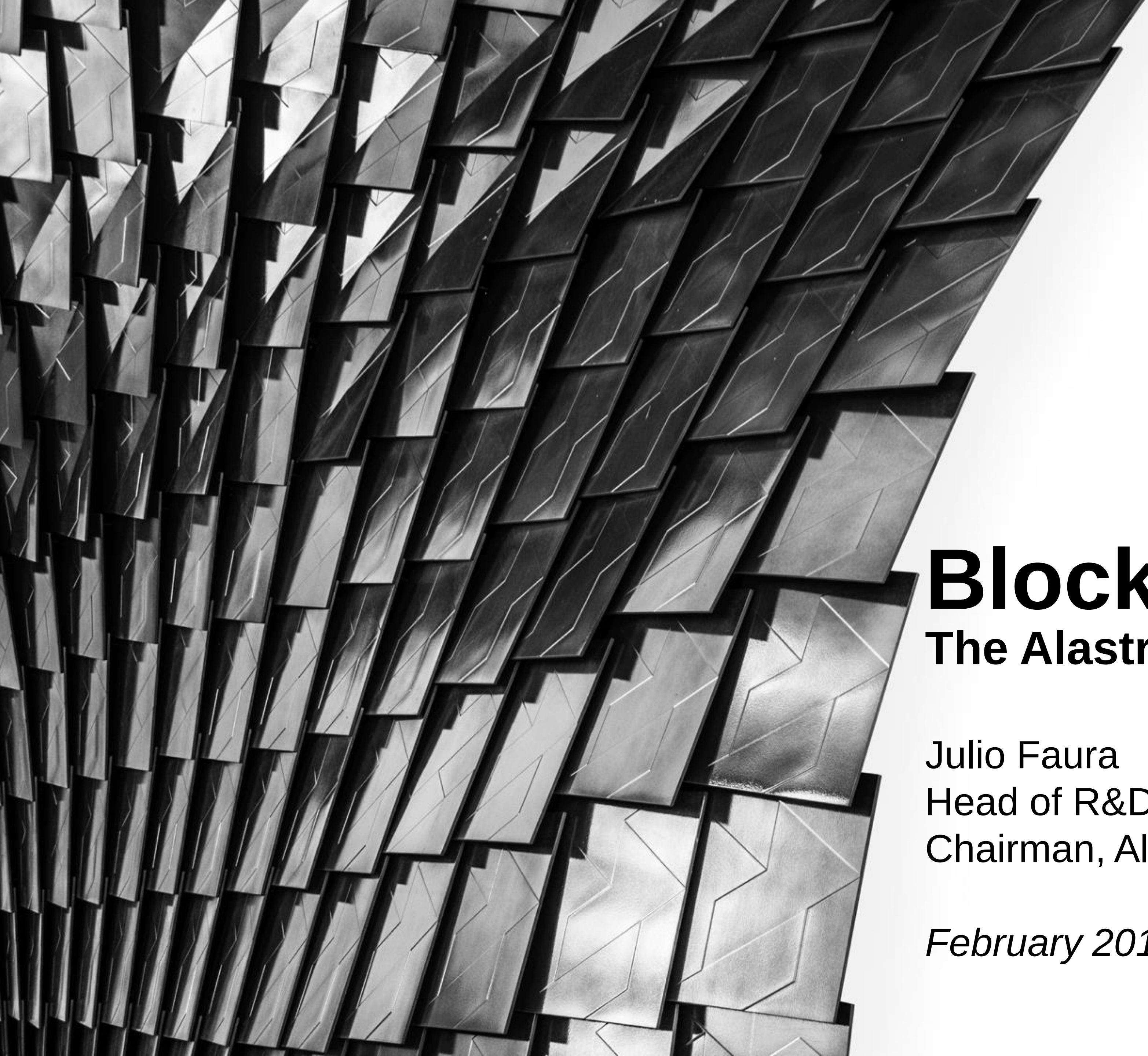


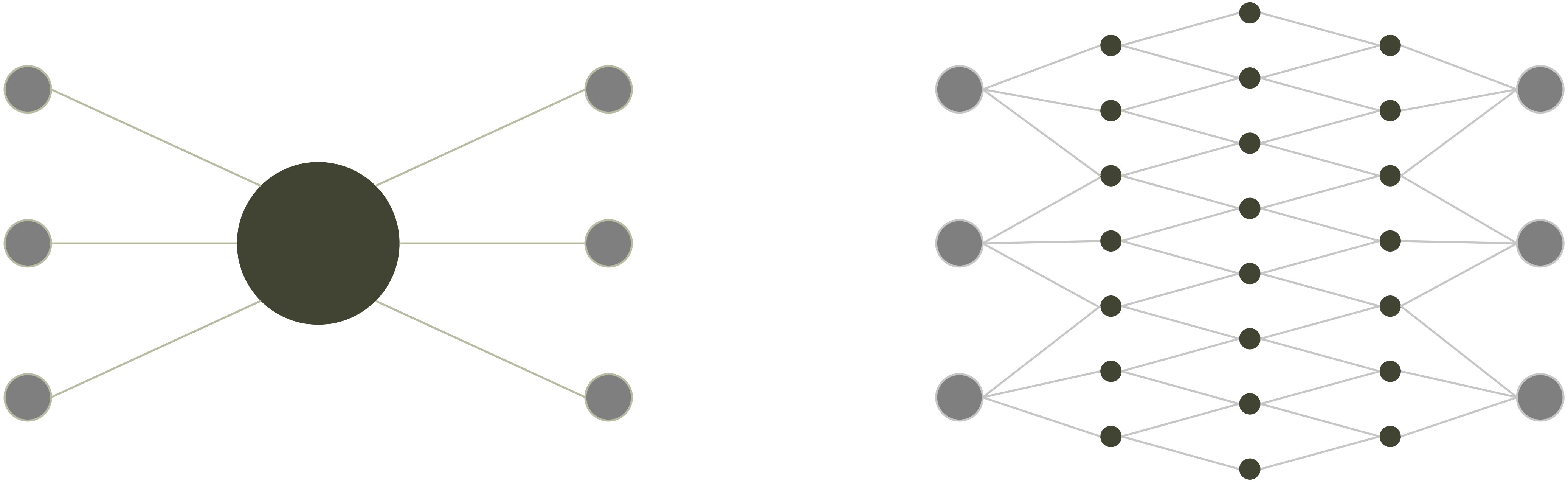
Blockchain platforms

The Alastria case

Julio Faura
Head of R&D, Santander
Chairman, Alastria

February 2018

Blockchain: the “internet of value”



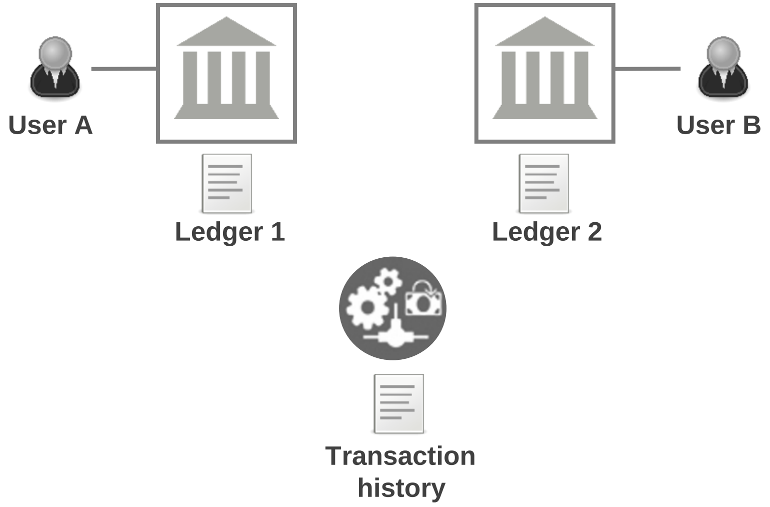
Blockchain does to **value**

what

internet made to **communications**

Blockchain is a *shared* ledger

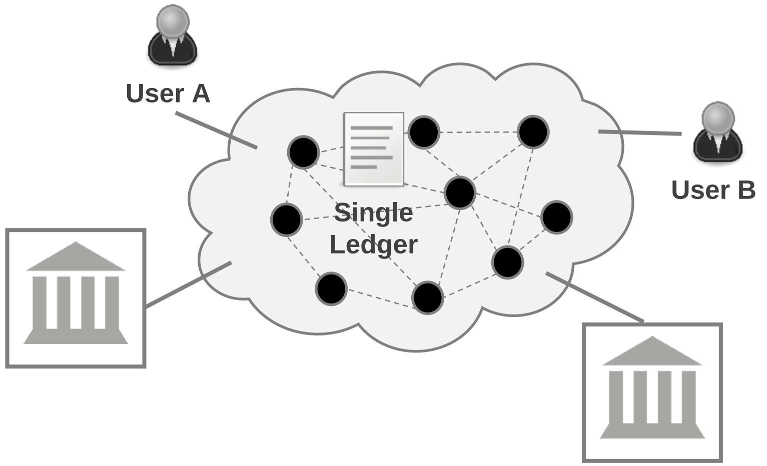
Today's world



- Separate ledgers => dependent on individual entities / sources of trust
- Intermediaries and reconciliations
- Off-ledger messages
- Batches

Vs

Blockchain



✓ Single, shared ledger => single version of truth

✓ Trustless

✓ Hyper-replicated => resilient and immutable, yet cheap

✓ In real time

=> Fast, cheap, secure and interoperable

Blockchain is *trustless*

Ledger (initial)

Public key	Amount
Public key	Amount
Public key 1	**Amount1**
Public key 2	Amount2
…	…

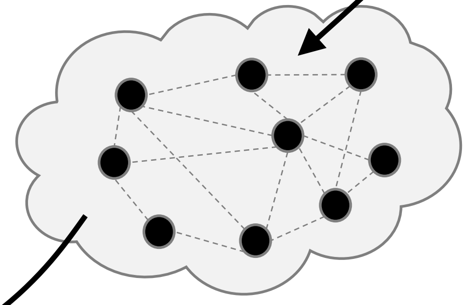
Ledger (final)

Public key	Amount
Public key	Amount
Public key 1	Amount1-Q
Public key 2	**Amount2+Q**
Public key	Amount
…	

New transaction

Q	**Public key 2**	**Signature**

Private key 1



- ✓ Anybody can generate public / private key pairs
- ✓ Anybody can check signatures
- ✓ The community *collectively* audits transactions and accepts them into the ledger

=> No *individual* trusted entity needed
… which makes it cheap and secure

Beyond cryptocurrencies: smart contracts are *programs* (and *data*) on the shared ledger

Cryptocurrencies (e.g. Bitcoin)

Public key	Amount
Public key	Amount
Public key	Amount
Public key	Amount
…	…

- The ledger stores amounts of cryptocurrency
- (Very simple) rules can be attached to ledger entries

Smart contracts (e.g. Ethereum)

```
contract cryptobank {
    mapping(address => uint) public balance;
    function transfer(uint amount, address receiver)
        if(balance[msg.sender] >= amount) {
            balance[msg.sender] -= amount;
            balance[receiver] += amount;
        } else {
            throw;
        }
    }
    ...
```

- The ledger stores programs and data
- Programs are Turing-complete (i.e. general purpose)
- Data in smart contracts can represent anything
- Smart contracts can interact with other smart contracts
- Cryptocurrencies can also be supported – and used to pay for shared computing power / notarization

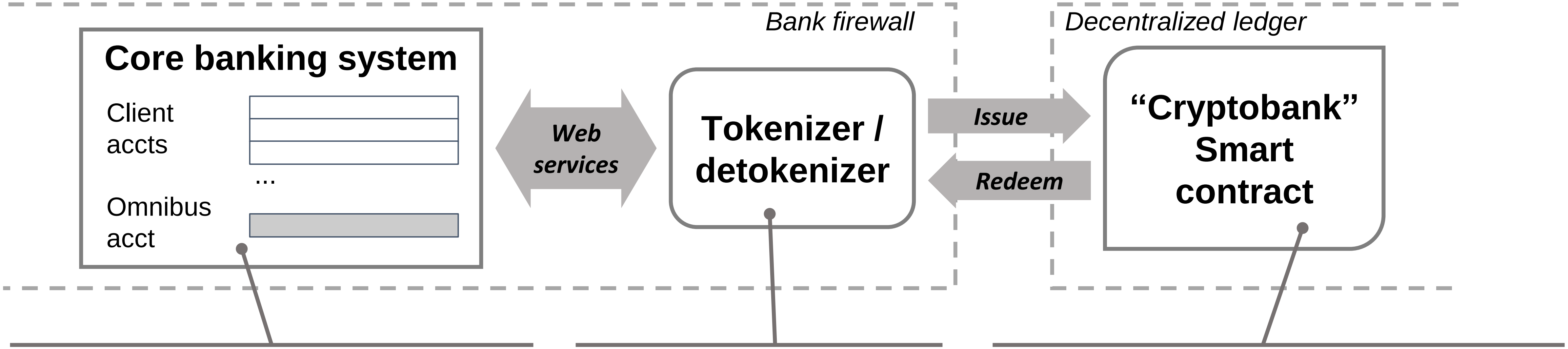
A smart contract-enabled blockchain (e.g. Ethereum) is a shared computing platform where transactions are:

✓ **Notarized**

✓ **Immutable**

✓ **Real time**

Tokenization makes blockchain useful in the *real* world



- ”Real” (fiat) money stays in an omnibus account in the bank
- Easy integration through web services

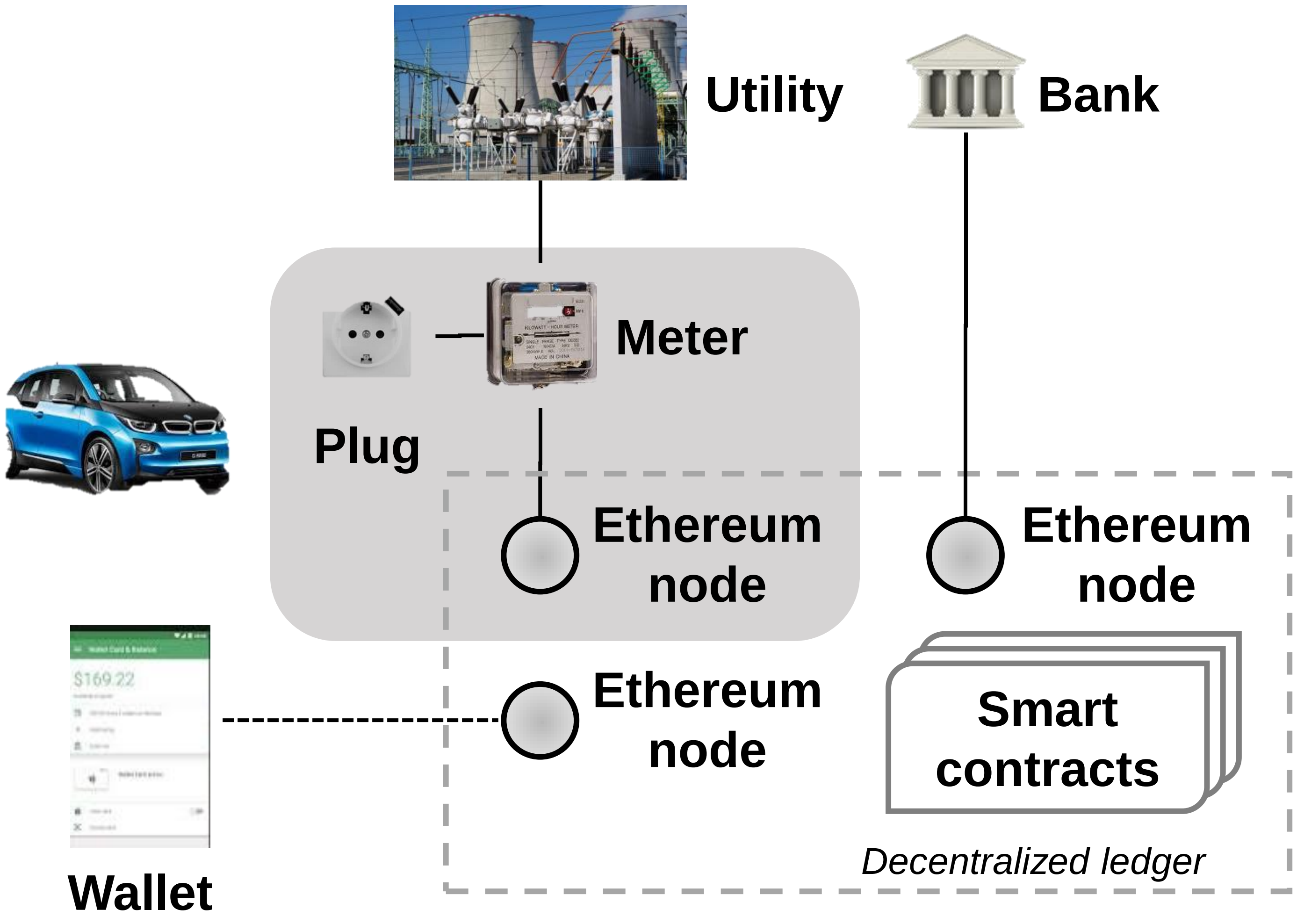
- Tokenizer deployed within bank’s data center (no external API calls needed)

- Client digital balances issued on a smart contract, backed 1:1 with funds in the omnibus account

… and now money is digital and globally interoperable (through other smart contracts!)

Anything (besides money) **can be tokenized!!**

An example: recharging an electrical car

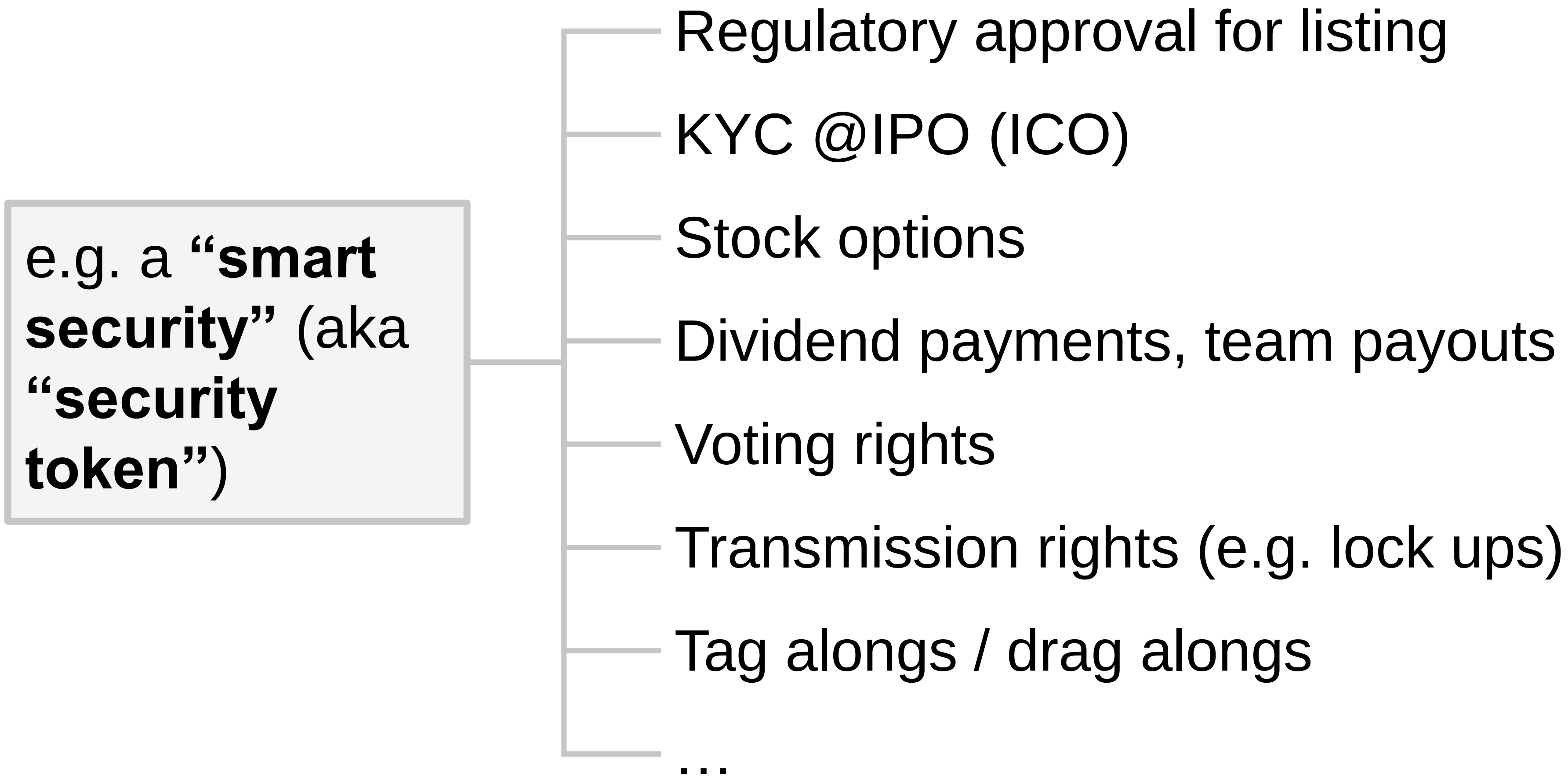


- ✓ User prefunds wallet with tokenized cash
- ✓ User pays tokenized money to smart plug
- ✓ Meter delivers energy to car
- ✓ Home owner redeems cash from bank

… concept allows for *uberization* of electric car recharges

Beyond tokenization: native digital assets

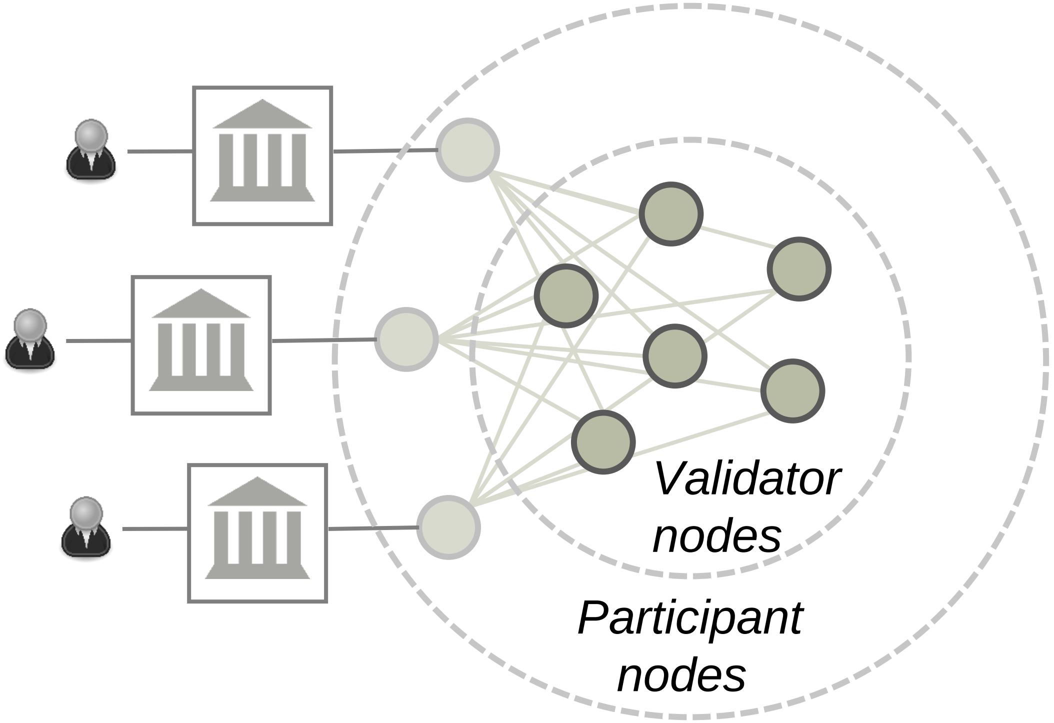
“An asset that is natively registered in the shared ledger, with contractual obligations implemented with smart contracts”



e.g. a **“smart security”** (aka **“security token”**)

- Regulatory approval for listing
- KYC @IPO (ICO)
- Stock options
- Dividend payments, team payouts
- Voting rights
- Transmission rights (e.g. lock ups)
- Tag alongs / drag alongs
- …

Permissioned blockchains: a *pragmatic* first step for enterprises



✓ **Not dependent on *individual* sources of trust, but on a trusted set of validators => Not 100% trustless, but good enough**

✓ **Private – only nodes *permissioned* by the validators can participate**

✓ **Simple consensus algorithms can be used (instead of proof of work)**

✓ **Much more scalable and performant**

✓ **Needs to implement governance mechanism**

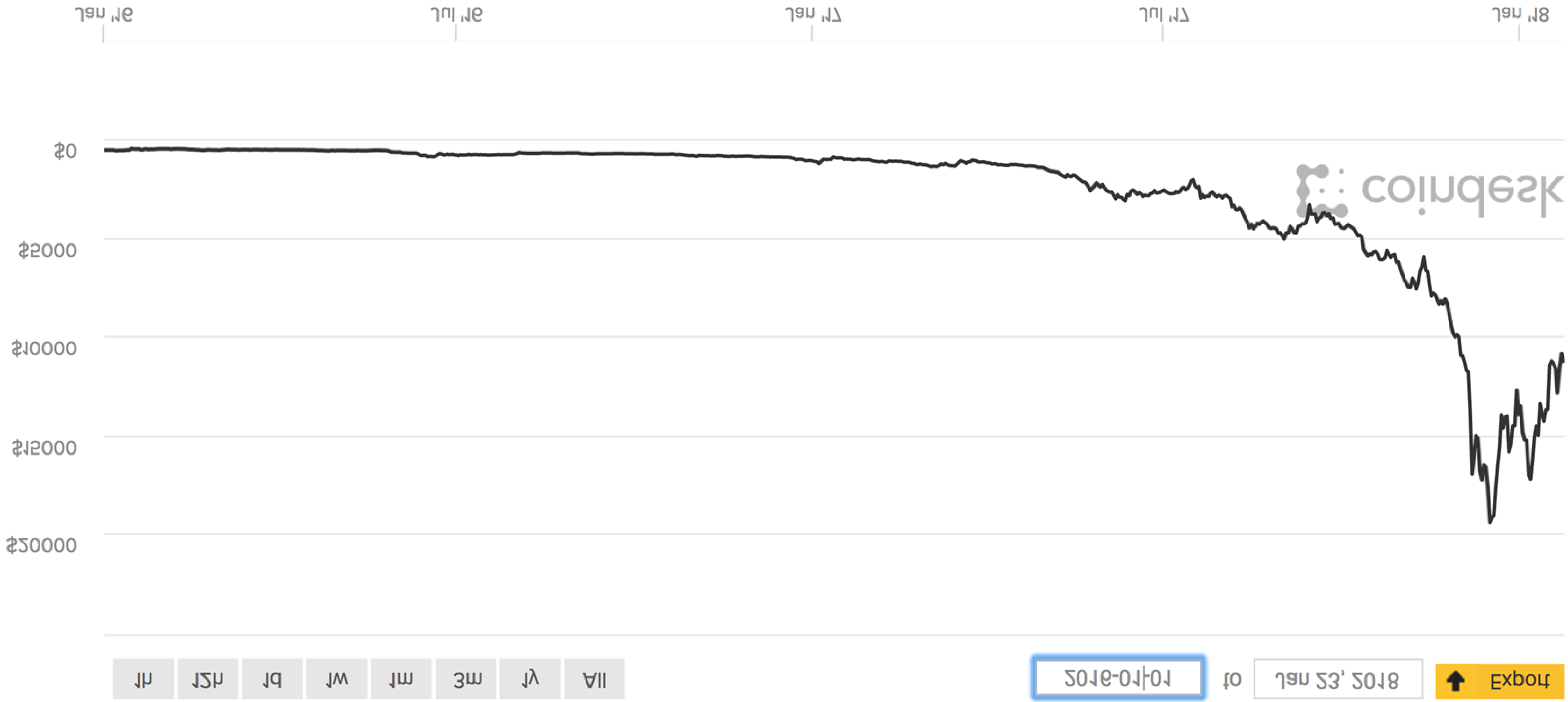
… but needs to implement governance mechanisms

Hola Alastria!

World’s first nation-wide, multi-sectorial, enterprise grade, permissioned Blockchain network

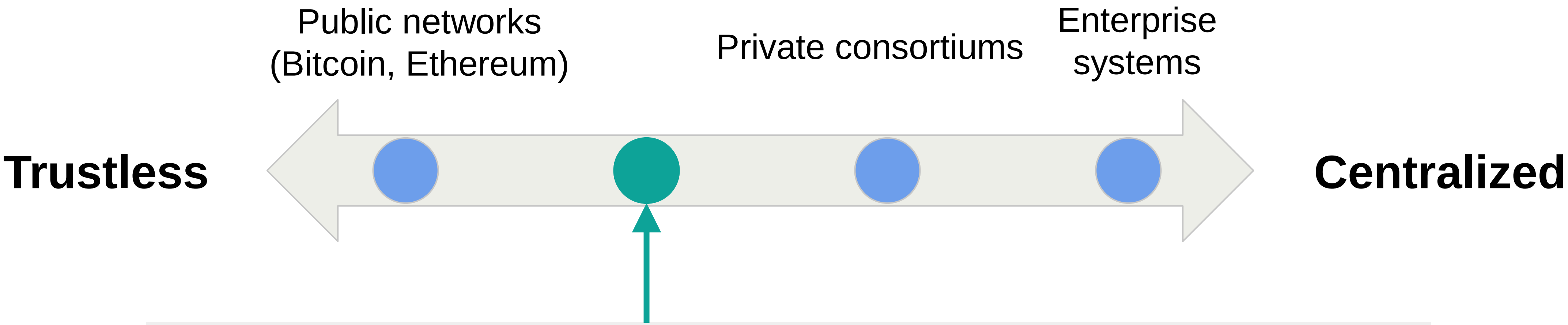
… made in Spain ;-)

Bitcoin evolution



2016-01-01 to Jan 23, 2018

Why Alastria?



Public-Permissioned network, compatible with regulation

- No cryptocurrency embedded => low and predictable transactional cost
- Higher performance and scalability (>1.000 tx/sec)
- Transaction finality in one block, with legal validity (legal identities)
- Depends on a trusted validator set => “Good enough”

… but requires implementing a Decentralized Governance Model

Over 170 members – and counting!

Finance and insurance

Abanca
AndBank
Banca March
Banc Sabadell
Banco Santander
BCC
Bankia
BBVA
BME
CaixaBank
Caja Rural
Cajamar
Ebroker
Inversis
Kutxabank
Mapfre
Multiasistencia
Norbolsa
RedSys
…

Energy, oil and gas

Aduriz Dist.
Cepsa
Endesa
Entelgy
Gas Natural F.
Iberdrola
Repsol
Tecnalia
Viesgo
…

Telecoms & industry

Correos
Ferrovial
Fujitsu
Informa
Mas Movil
Pangea
Telefonica
Worldline
…

Legal & consultancy

Accenture
Addalia
Atmira
AT Sistemas
Blue TC
CIC Consulting
Councilbox Tech
Cuatrecasas
Deloitte
Ejaso
Everis
EY
Garrigues
Grant Thornton
Indra
Management Sol
Roca Junyent
SAP
Sopra Steria
UST Global
…

Universities & institutions

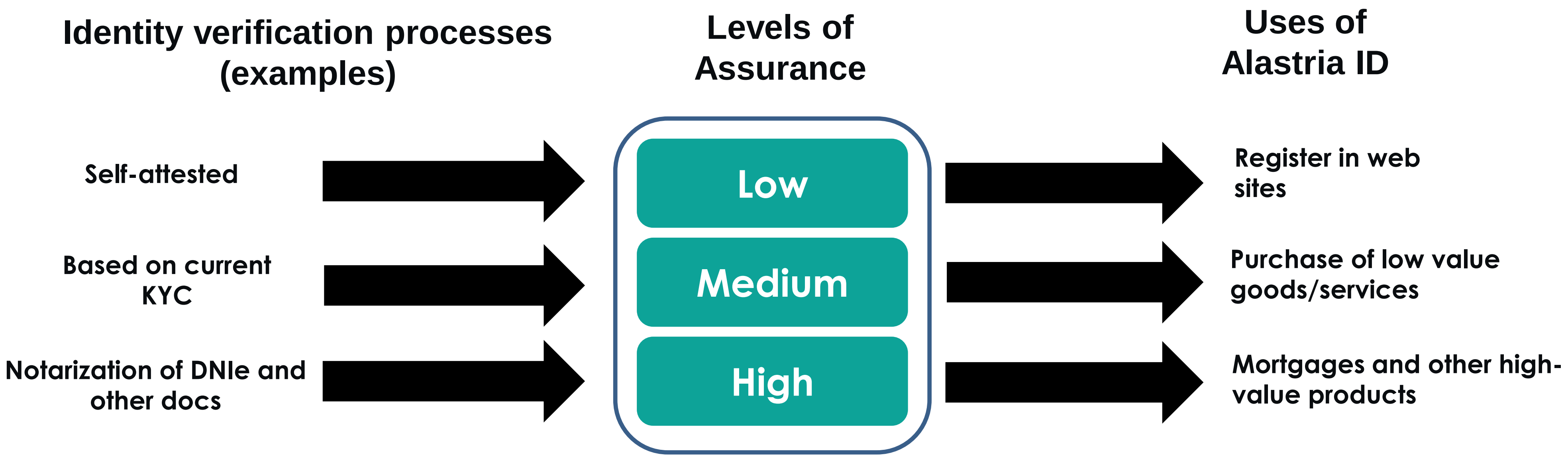
ACEC
ADISPO
AEFI
Andalucía Smart City
APTE
Foment Treball
ICADE
IEB
Notarnet
Univ Girona
Univ Málaga
Univ Valencia
Univ S Pablo CEU
…

Startups & specialists

Biid
Blockchain España
Blockchain Logic
Bloo Media
Coinbase AM
Contextual
Deka SW Labs
Go Madrid
Iberian Crypto
Farmers
Ivnosys
Logalty
Makrin
Microapps
Nextchance Invest
Nodalblock
Nettit
Pitagorines Group
Plexus
Secutix
Ubiquat
…

Alastria ID: legal identity on blockchain

- Allows implementing products and services complying with Spanish (and European) regulation.
- Self Sovereign Identity (SSI), for protection and empowerment of the user.



Identity verification processes (examples)

Levels of Assurance

Uses of Alastria ID

Self-attested

Based on current KYC

Notarization of DNIe and other docs

Low

Medium

High

Register in web sites

Purchase of low value goods/services

Mortgages and other high-value products

Key ideas

1. Coopetition

2. Tokenization => digitization

3. Digital identity => legally binding

4. Collaboration between large and small

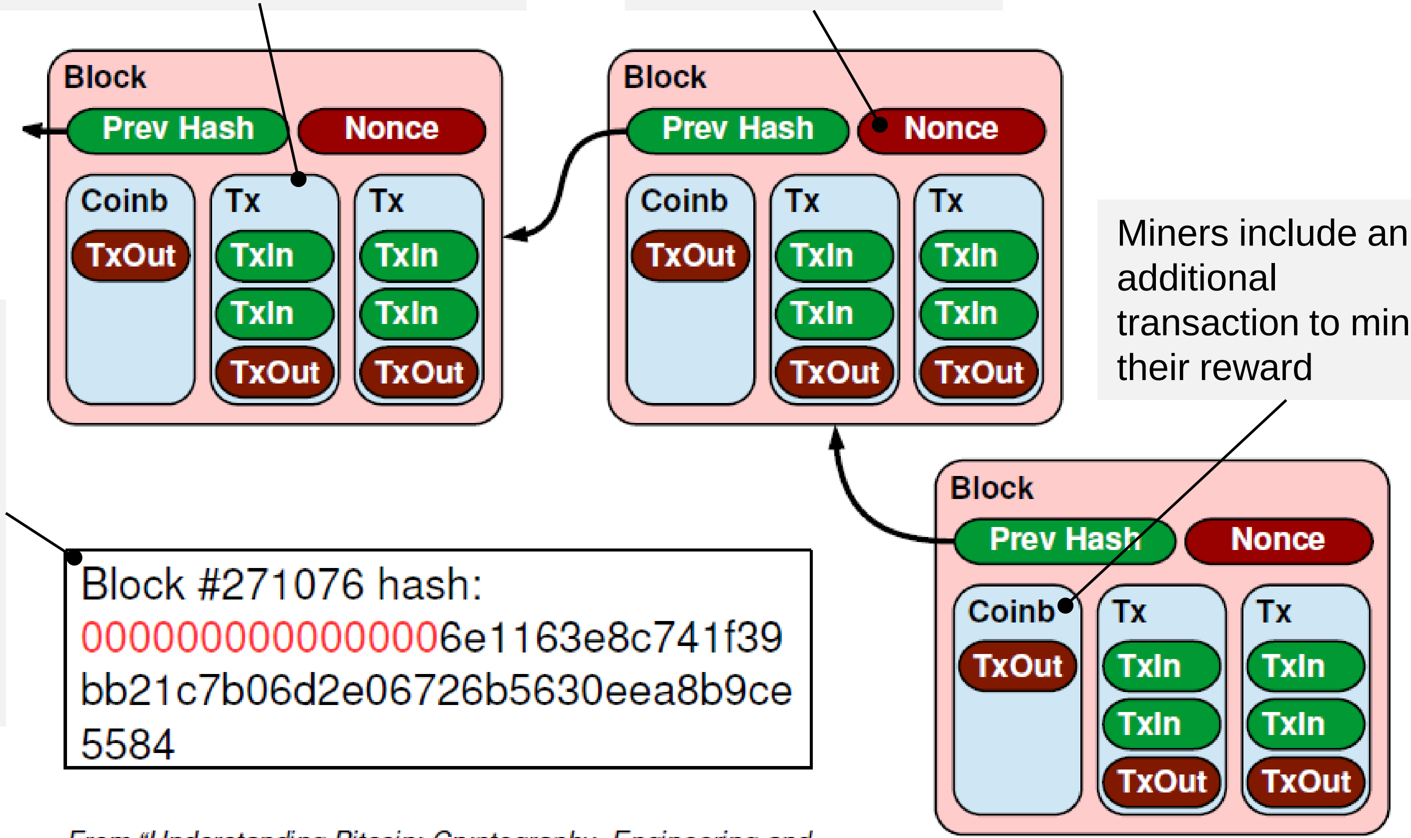
=> innovation

Thank you

A community *certifying* transactions

Miners include as many transactions as possible as they may earn fees in addition to newly minted bitcoins

Random seed to change in order to find the right hash



Miners include an additional transaction to mint their reward

The “crypto-puzzle” used as a “proof of work” consists in changing a random seed (“nonce”) until the hash of the whole block starts with a given number of zeros

Block #271076 hash:
0000000000000006e1163e8c741f39
bb21c7b06d2e06726b5630eea8b9ce
5584

From “Understanding Bitcoin: Cryptography, Engineering and Economics”, Pedro Franco, © Wiley 2014, used with permission

Cryptocurrencies are digital cash

Public key	Amount
Public key	Amount
Public key	Amount
Public key	Amount
…	…

✓ Just an entry in a database

✓ Not backed by any authority

✓ Totally anonymous – no KYC, no AML, no control

✓ More or less like “digital gold”

✓ Yet infinitely traceable (on a pseudonymous basis)

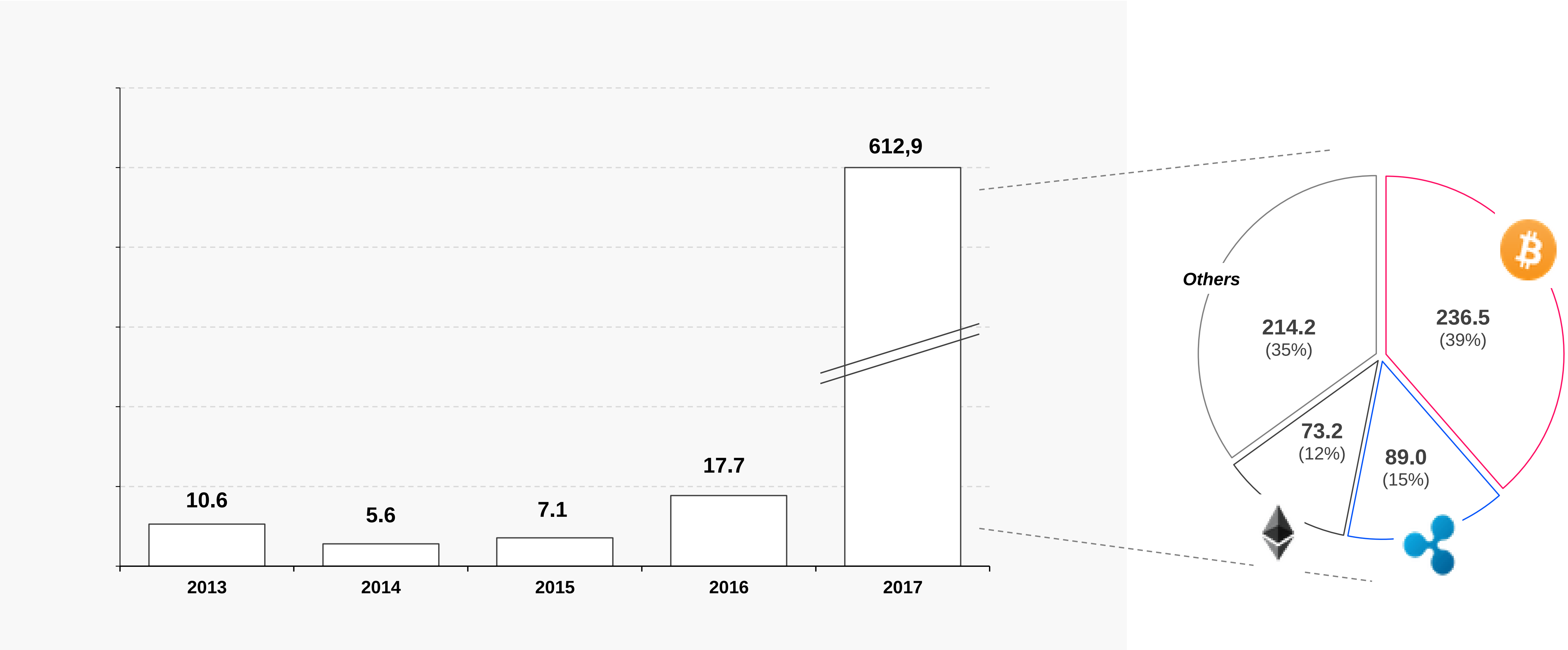
… interchangeable by (traditional) cash at exchanges (regulators permitting)

… exchange rate only determined by the market

… subject to brutal speculation

… useful for illegal uses (trafficking, money laundering, ransomware …)

… and the market is *hot*



Applications of tokenization

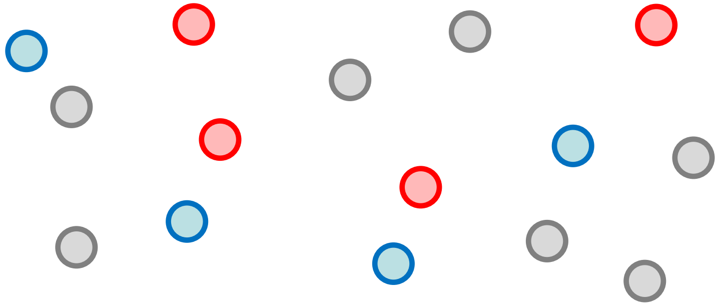
Anything involving different, disconnected parties needing to transact on a legally binding basis:

- Digital cash, digital central bank money
- International payments, micropayments, payments for digital services
- Capital markets trading, settlement, collateral management, syndicates, asset management
- Digital identity, asset registries
- Voting, public administration, government benefits
- Supply chain, trade finance
- Digitalization of equipment use (e.g. car sharing, car recharging, shared computing resources)
- Workflows (e.g. Internal audit, regulatory approvals, insurance claims)

… and the combination of the above!

Consensus algorithms increase performance in permissioned blockchains (e.g. Quorum)

QuorumChain

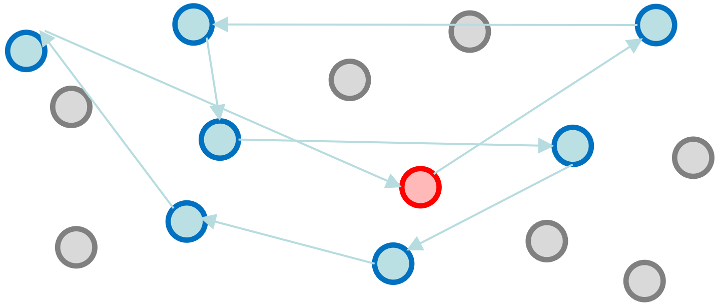


🔴 = **Voter**: casts votes regarding validity of proposed blocks with pending transactions

🔵 = **Blockmaker**: appends blocks to the Blockchain when quorum is achieved

⚪ = **Observer**: gets full copy of the Blockchain and can interact with it (e.g. submitting transactions

RAFT



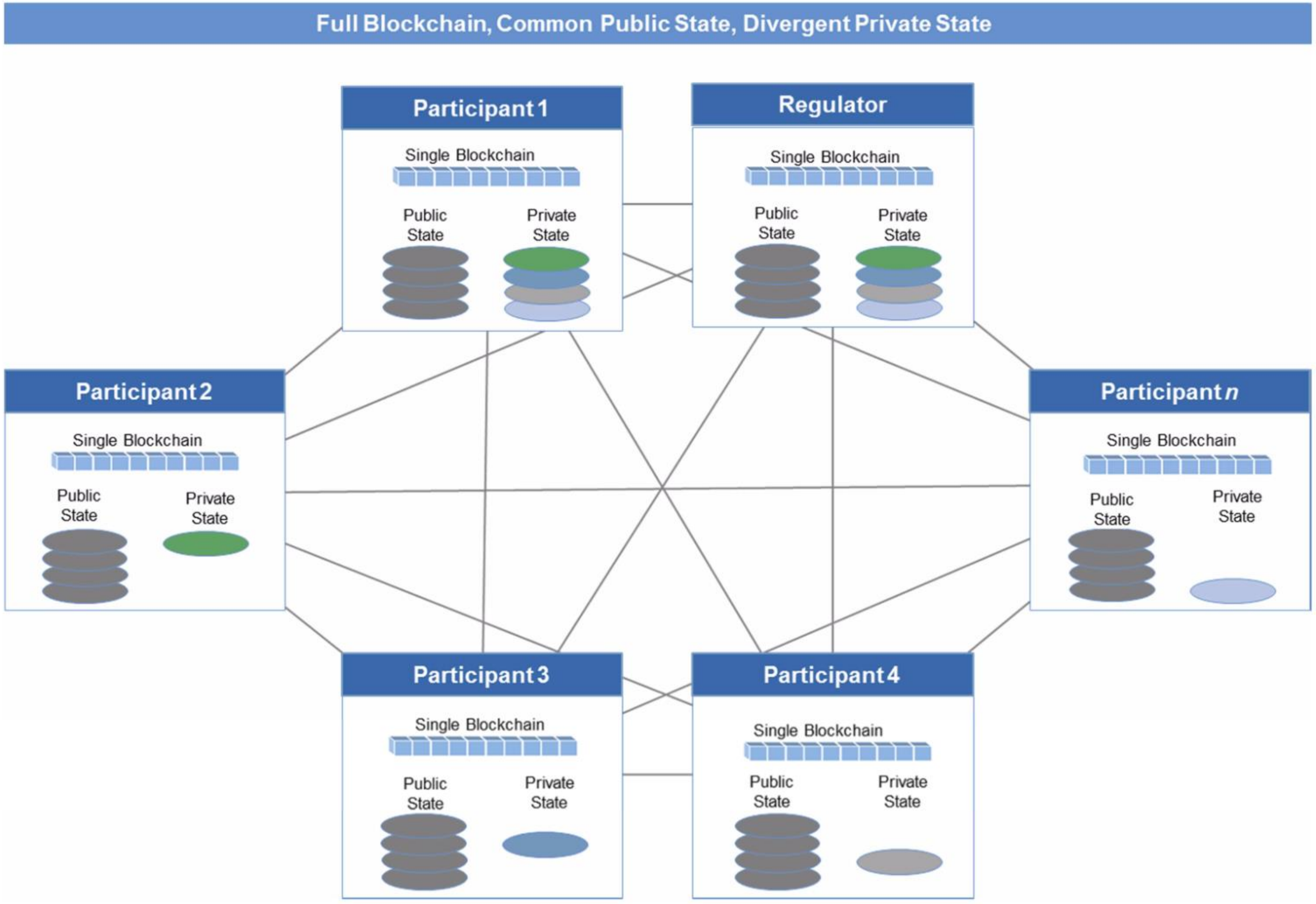
🔴 = **Leader**: creates new blocks and proposes it to followers, then instructs them to apply it to chain head

🔵 = **Follower**: accepts blocks created by leader, then becomes leader in turns, on a round robin fashion

⚪ = **Observer**: (same as QuorumChain)

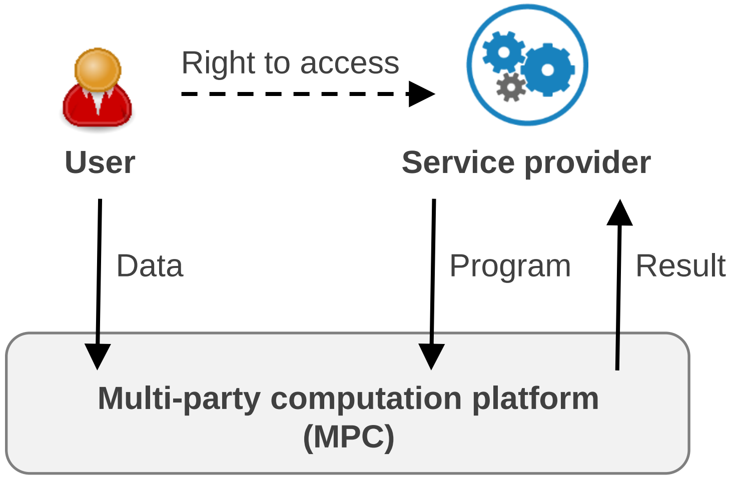
Next in roadmap: PBFT (e.g. Istanbul, already available)

Privacy is paramount



- ✓ **Private smart contracts are implemented as “sub-blockchains”**
- ✓ **Payloads only stored in participating nodes**
- ✓ **Private transactions notarized anyway by the (common) underlying blockchain**

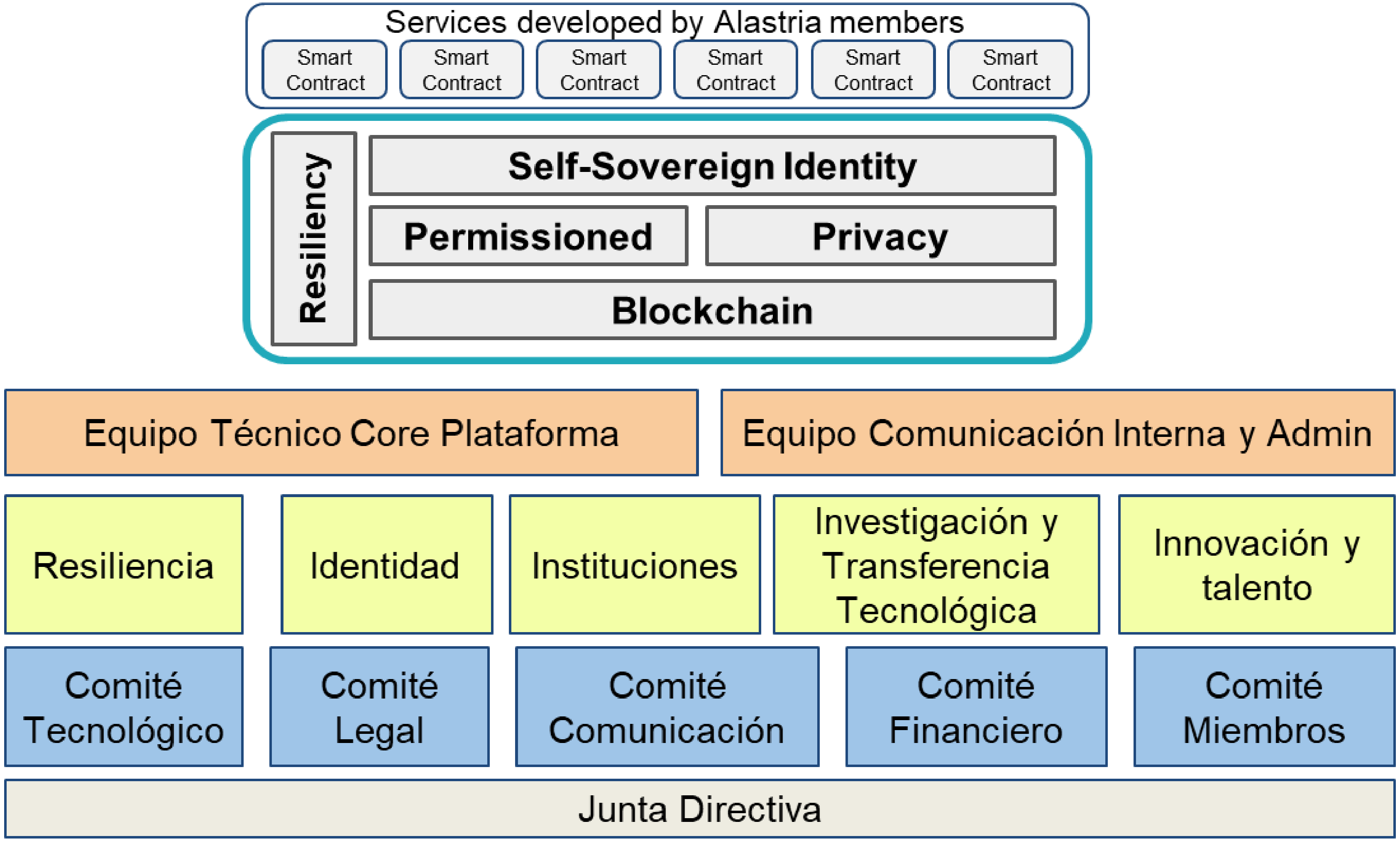
Going forward: zero knowledge proofs and multi-party computational platforms



- ✓ Users store data securely in the MPC platform
- ✓ Users (temporarily) grant service providers access to particular pieces of data for particular uses
- ✓ Service providers can then reference users' data in their programs, but they cannot *retrieve* the data verbatim
- ✓ Service providers can retrieve the (transformed) results of their computation

- **Users can grant access to their personal data without sharing it verbatim**
- **Therefore, providers cannot see, make copies or redistribute the raw data. Nor use it for any other purposes but the ones they have been given access for**
- **Users can revoke data access at any time, without any trail**
- **Secrets can be shared and access can be managed by groups of users**

Governance & coopetition



Services developed by Alastria members

Smart Contract | Smart Contract | Smart Contract | Smart Contract | Smart Contract | Smart Contract

Resiliency

Self-Sovereign Identity

Permissioned

Privacy

Blockchain

Equipo Técnico Core Plataforma

Equipo Comunicación Interna y Admin

Resiliencia

Identidad

Instituciones

Investigación y Transferencia Tecnológica

Innovación y talento

Comité Tecnológico

Comité Legal

Comité Comunicación

Comité Financiero

Comité Miembros

Junta Directiva