ALASTRIA

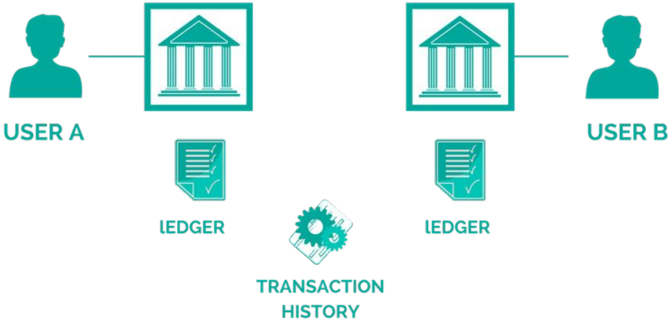
BLOCKCHAIN INTRO

OCTUBRE 2017

BLOCKCHAIN IS A *SHARED* LEDGER

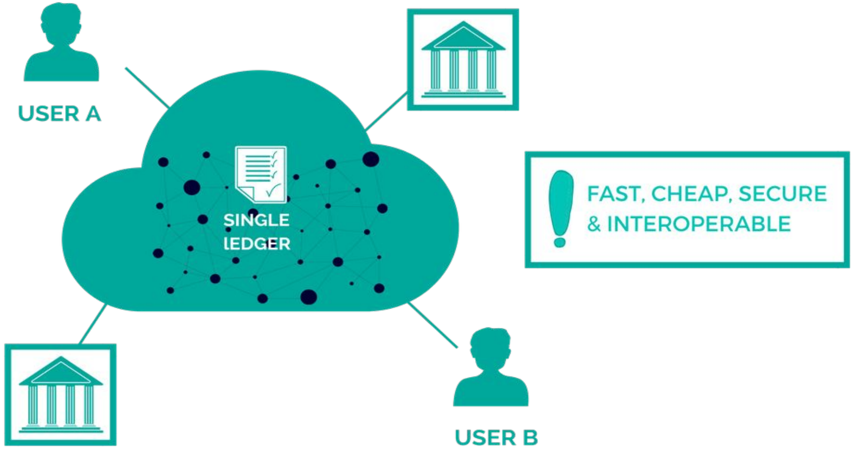
TODAY'S WORLD

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



BLOCKCHAIN

- ➔ Single, shared ledger => single version of truth
- ➔ Trustless
- ➔ Hyper-replicated => resilient and immutable, yet cheap
- ➔ In real time



BLOCKCHAIN IS *TRUSTLESS*

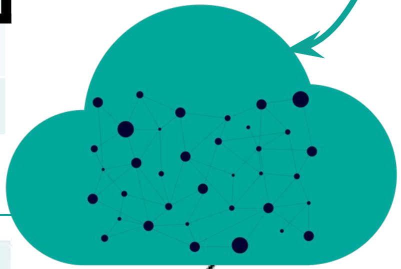
LEDGER INITIAL

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

NEW TRANSACTION

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

private key 1



LEDGER FINAL

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

- 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

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)

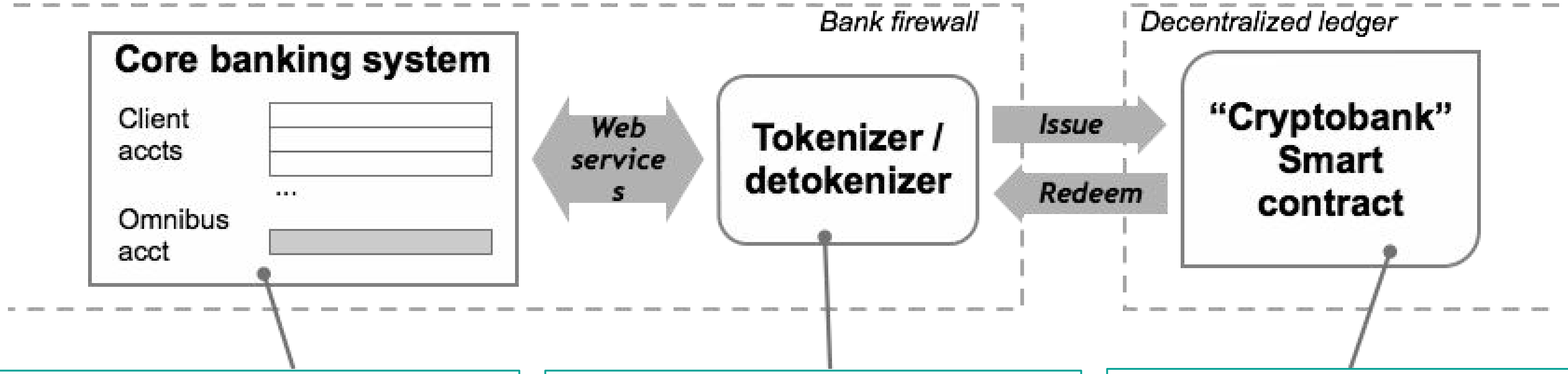
```
contract cryptobank {
    mapping(address => uint) public balance;
    function transfer(uint amount, address
receiver)
        if(balance[msg.sender] >= amount) {
            balance[msg.sender] -= amount;
            balance[receiver] += amount;
        } else {
            throw;
        }
  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

- ➔ 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

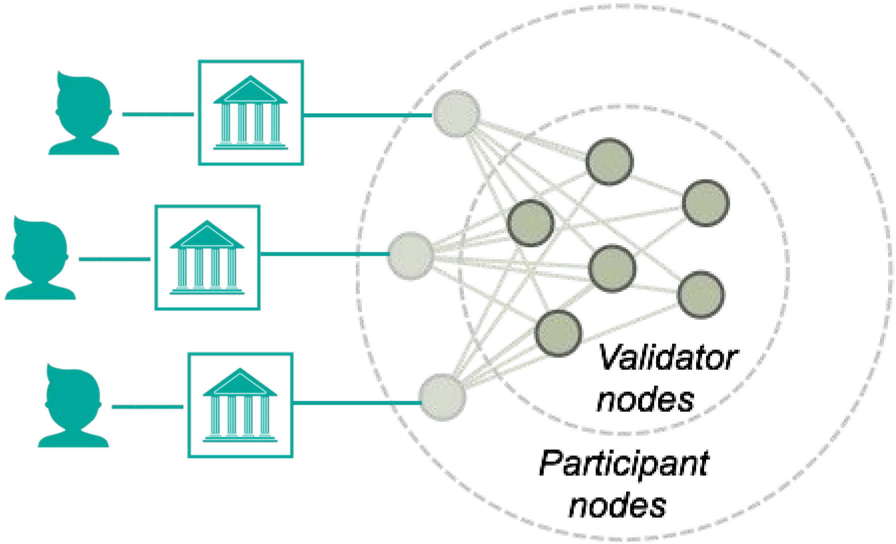
- ➔ Tokenizer deployed within bank's data center (no external API calls needed)

- ➔ 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!)

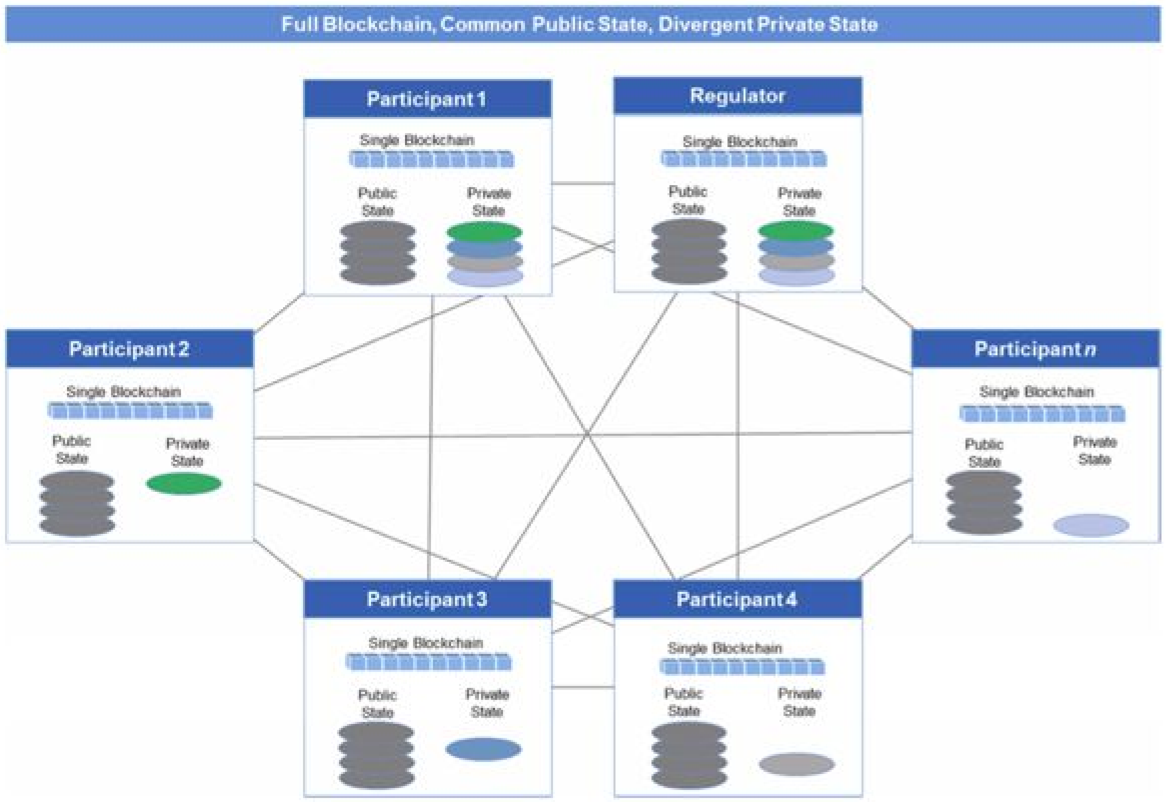
➔ **Anything (besides money) can be tokenized!!**

PERMISSIONED BLOCKCHAINS: A PRAGMATIC STEP FOR ENTERPRISES

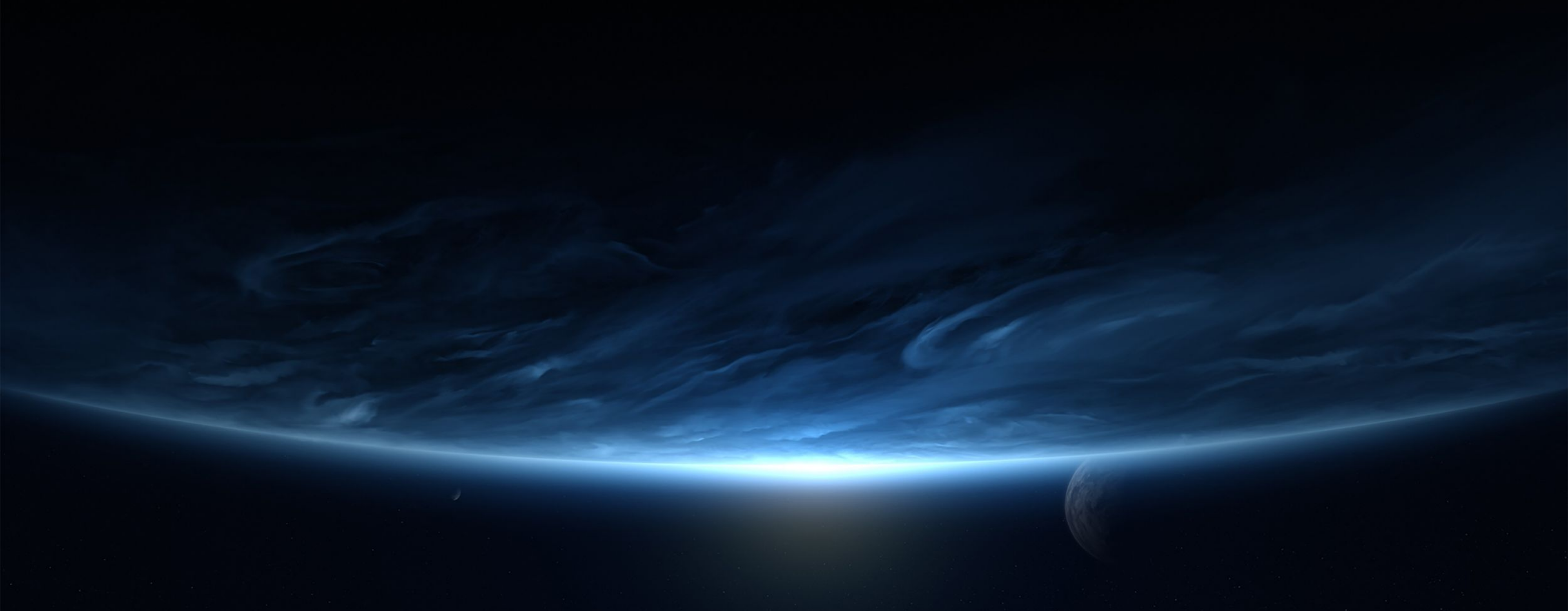


- Not dependent on individual sources of trust, but on a trusted set of validators => Not 100% trustless, but good enough
- Private – only nodes permissioned by the validators can participate
- Simple consensus algorithms can be used (instead of proof of work)
- Much more scalable and performant
- Needs to implement governance mechanism
- … but needs to implement governance mechanisms

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



ALASTRIA

BARCELONA, OCTUBRE 2017