AN INTRODUCTION TO BLOCKCHAIN

VICTOR SAWMA

DEC 2018

What is a blockchain?

- » is a **novel** solution that provides **trustless trust**
- » is a **shared, trusted, public, distributed ledger of transactions**
- » allows **public inspection** of the system
- » a **de-centralized** system
- » is a **distributed P2P** database
- » maintains a **continuously growing** list of **transactional records**
- » is **cryptographically secured** from **tampering and revision**

A Few Basics

To understand blockchains, one must first understand:

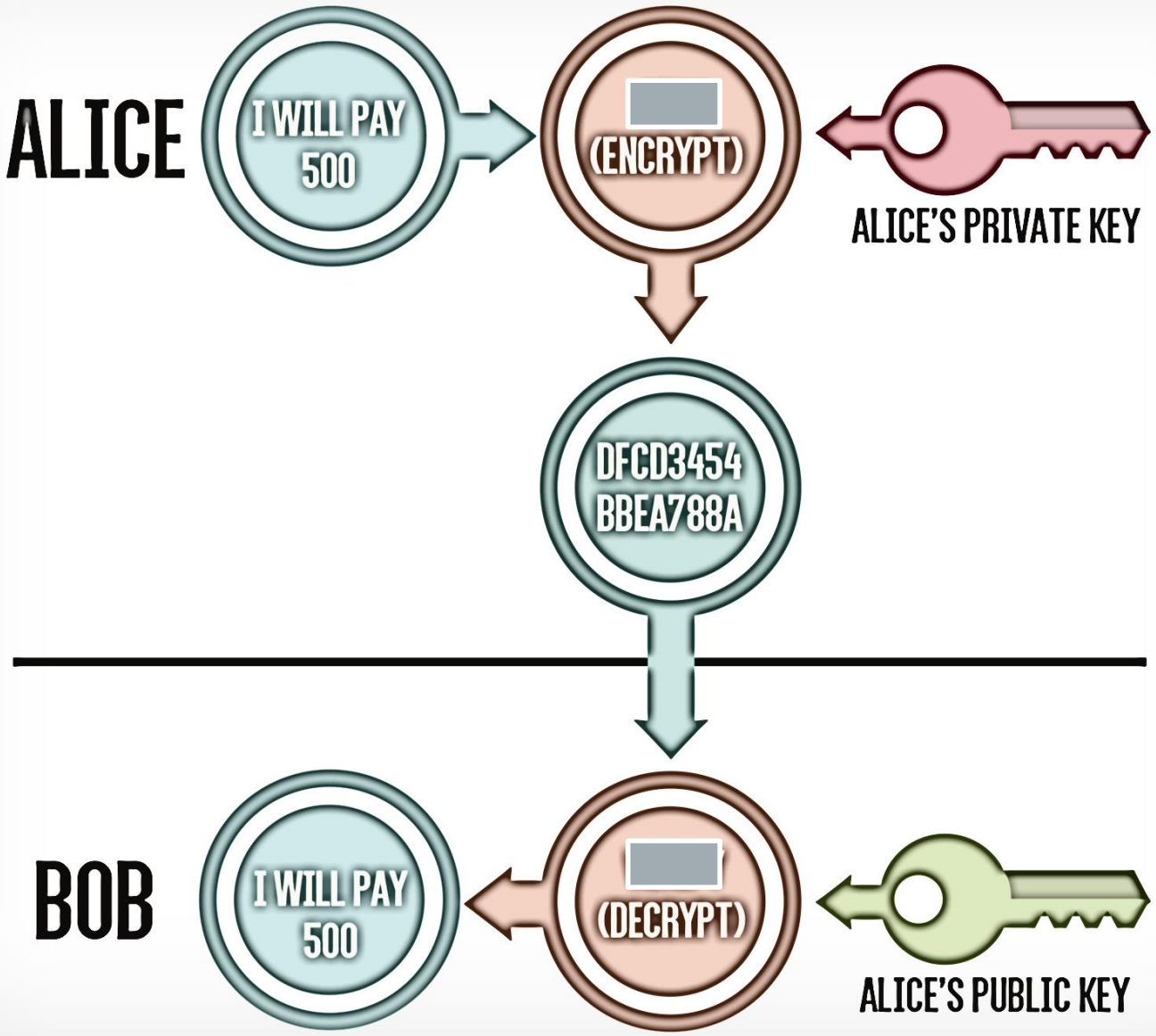
- Public key crypto systems
- Digital signatures
- Cryptographic hashes

Public Key Crypto Systems

» ENCRYPT & DECRYPT

» Keys are the inverse of each other (Public & Private)

» Mathematically proven



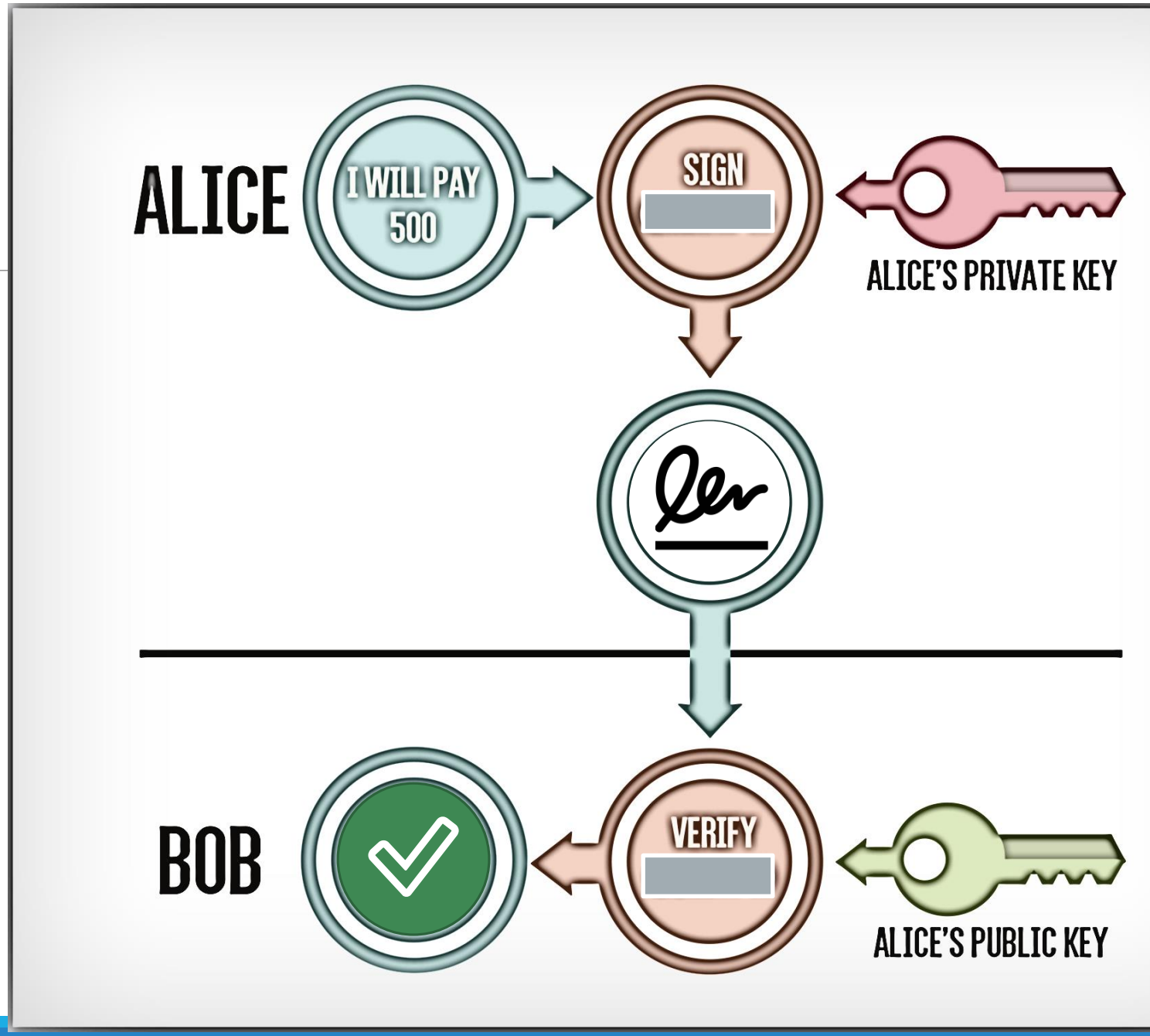
Digital Signatures

» SIGN & VERIFY

» Keys are inverse of each other

» Public and Private Keys

» Provides non-repudiation



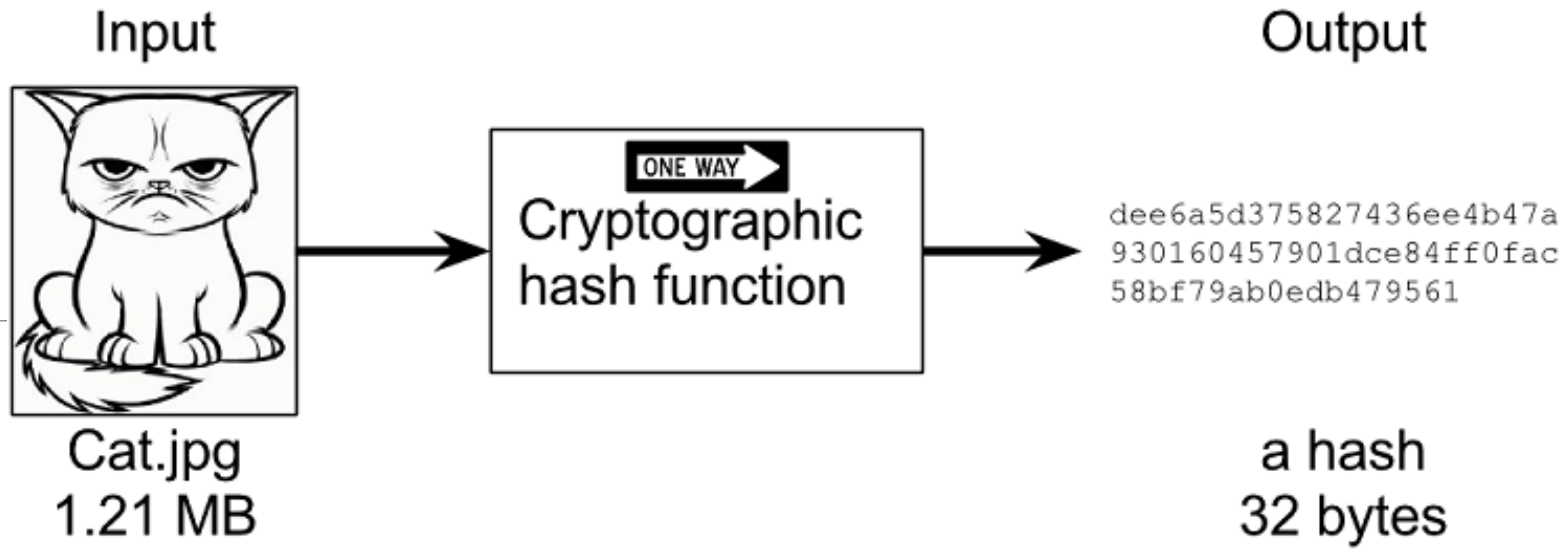
Crypto Hashing Functions

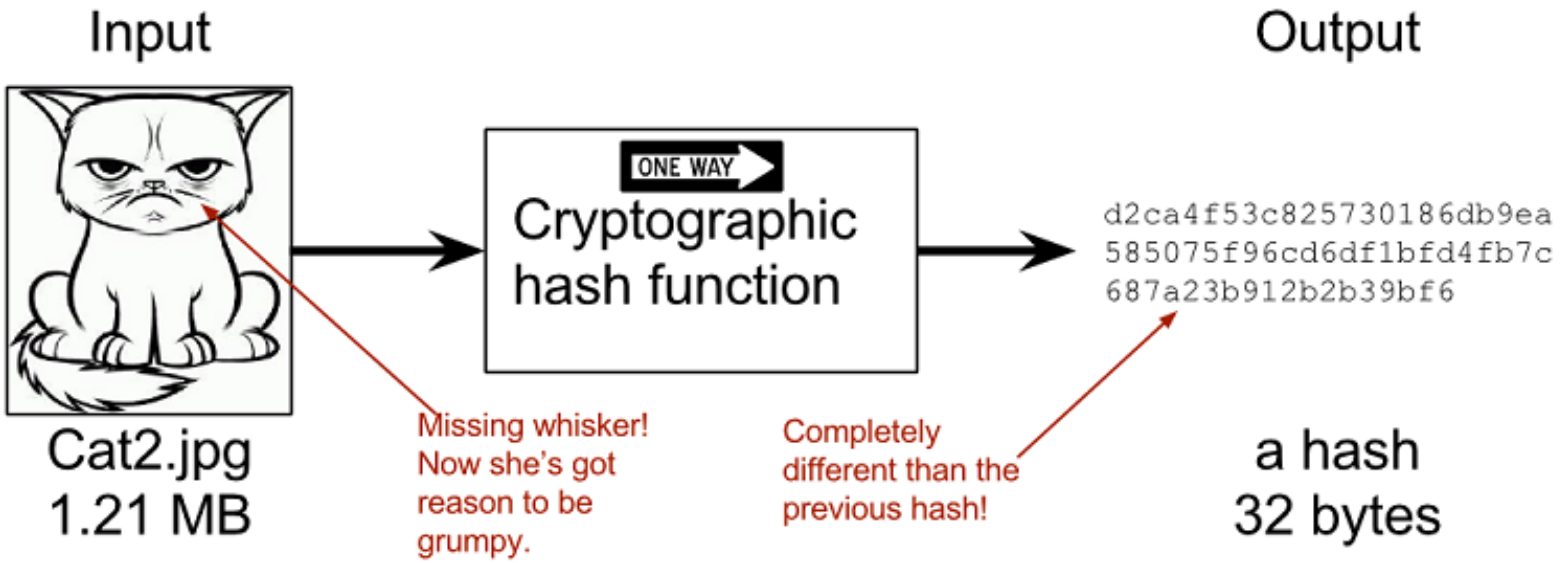
» One-Way compression algorithm / system

» Any input provides a fixed size output

» Changing one bit changes the whole hash

» Mainly used for integrity





The Basics Combined

If Alice wants to send a message **M** to Bob, Alice can:

» **H**ash the message (nobody can tamper with the message anymore)

»**S**ign the generated hash (Alice cannot deny later on sending it)

»**E**ncrypt the message (only Bob can see it)

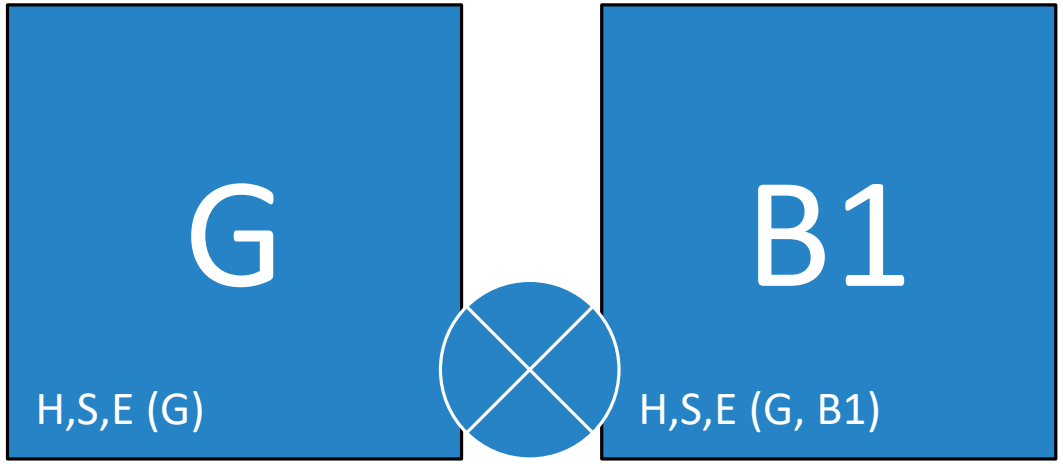
BACK TO THE BLOCKCHAIN

A Block in the Chain

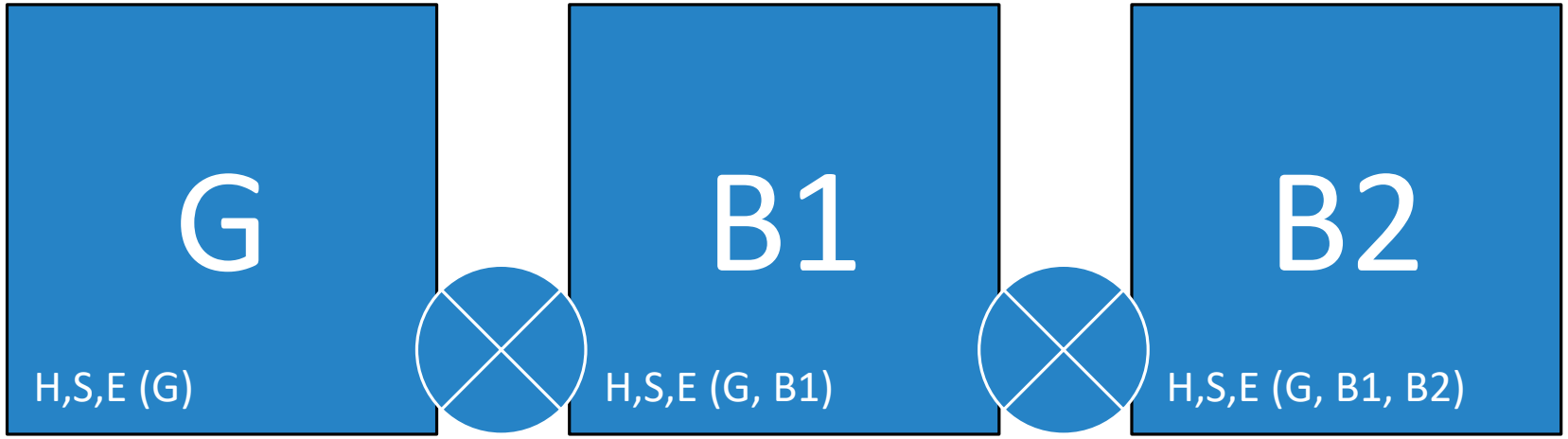
- can store any data
- LIMITED storage size
- First block is known as the **Genesis Block (G)**

A Block in the Chain

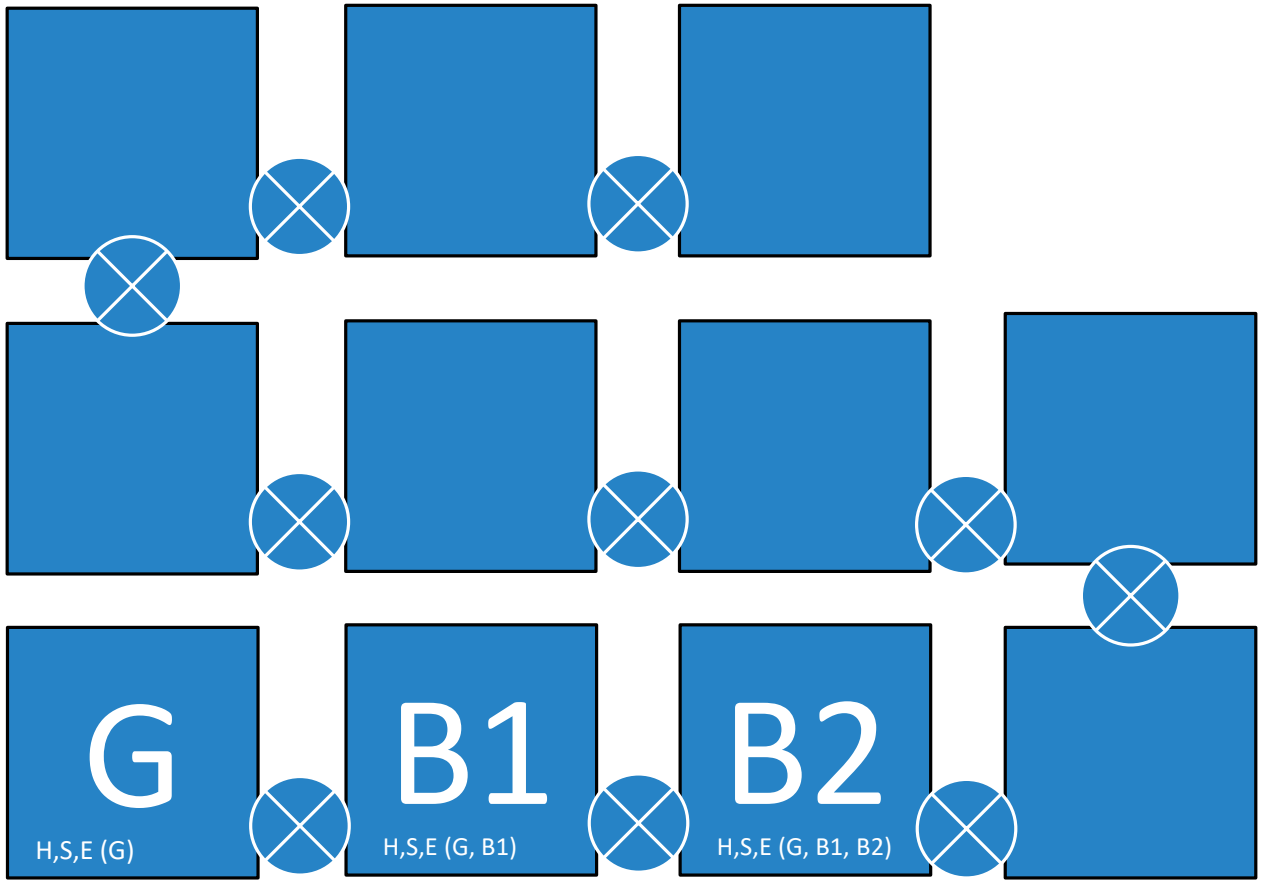
The Ledger in the Chain



The Ledger in the Chain



The **Ledger** in the Chain



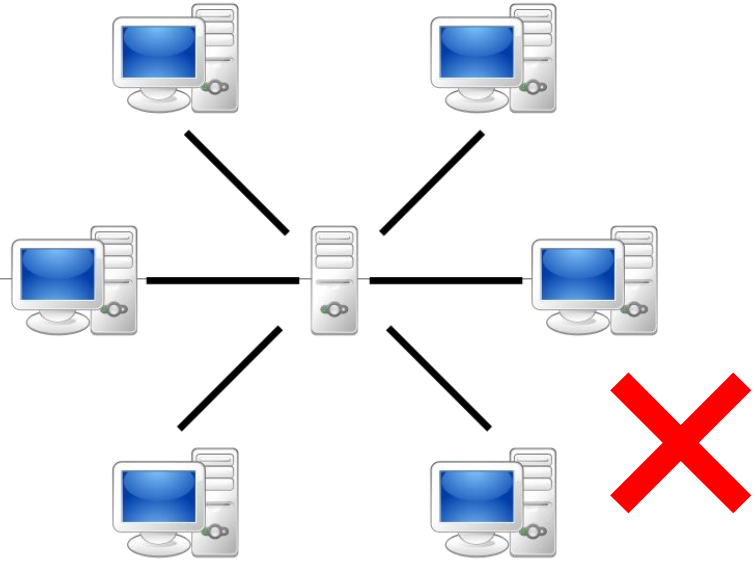
Peer-2-Peer Networks (P2P)

» No center exists. De-centralized by nature

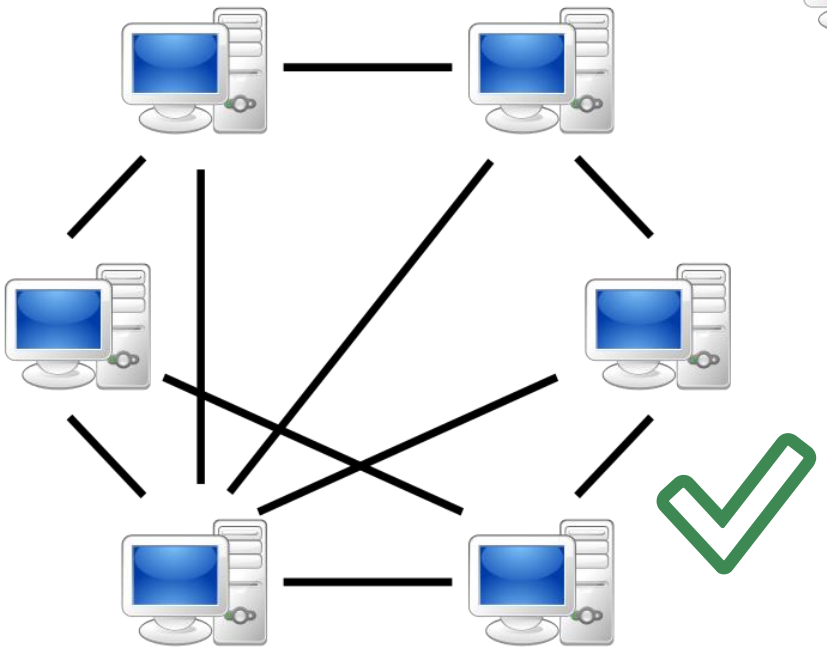
» All nodes are connected to each other

» Only way to get network down is to shut down all servers.

Switched Network



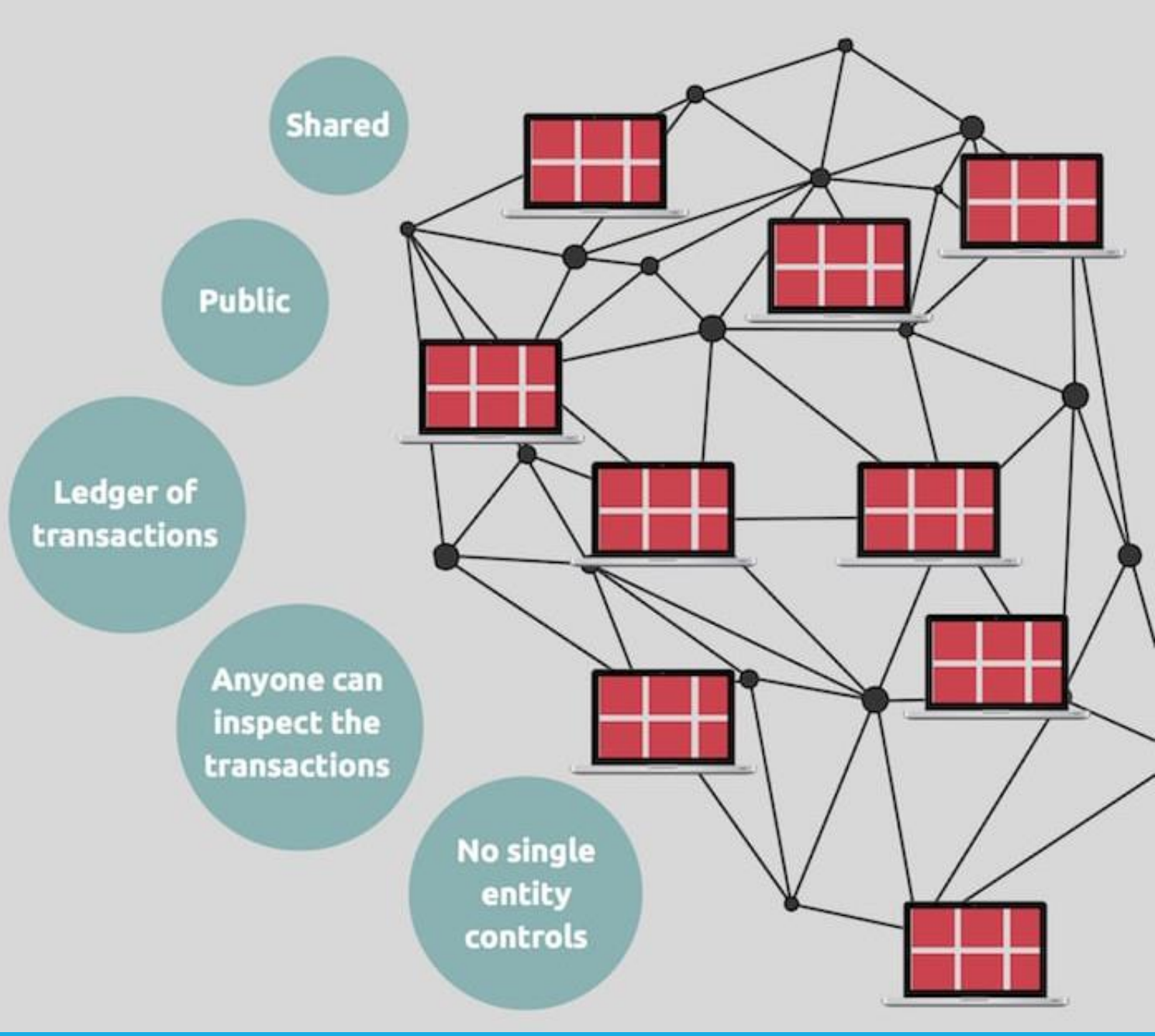
P2P Network



Distributed Ledger

» Ledgers are shared across many network servers (known as miners)

» Network uses a Peer-2-Peer structure



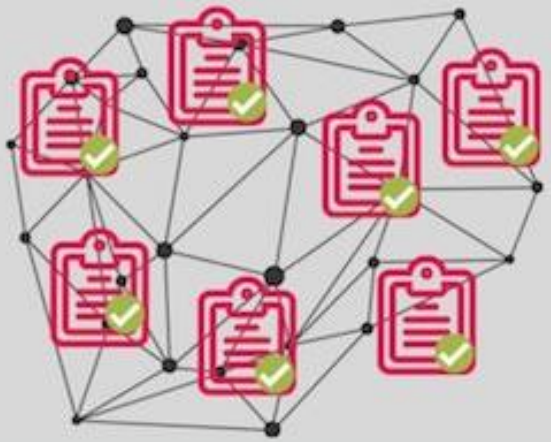
Blockchain Consensus

» Updating the blockchain requires network consensus

» All miners are notified

» Each miner verifies the legitimacy of the transaction

» Majority of network must accept the change to become legitimate



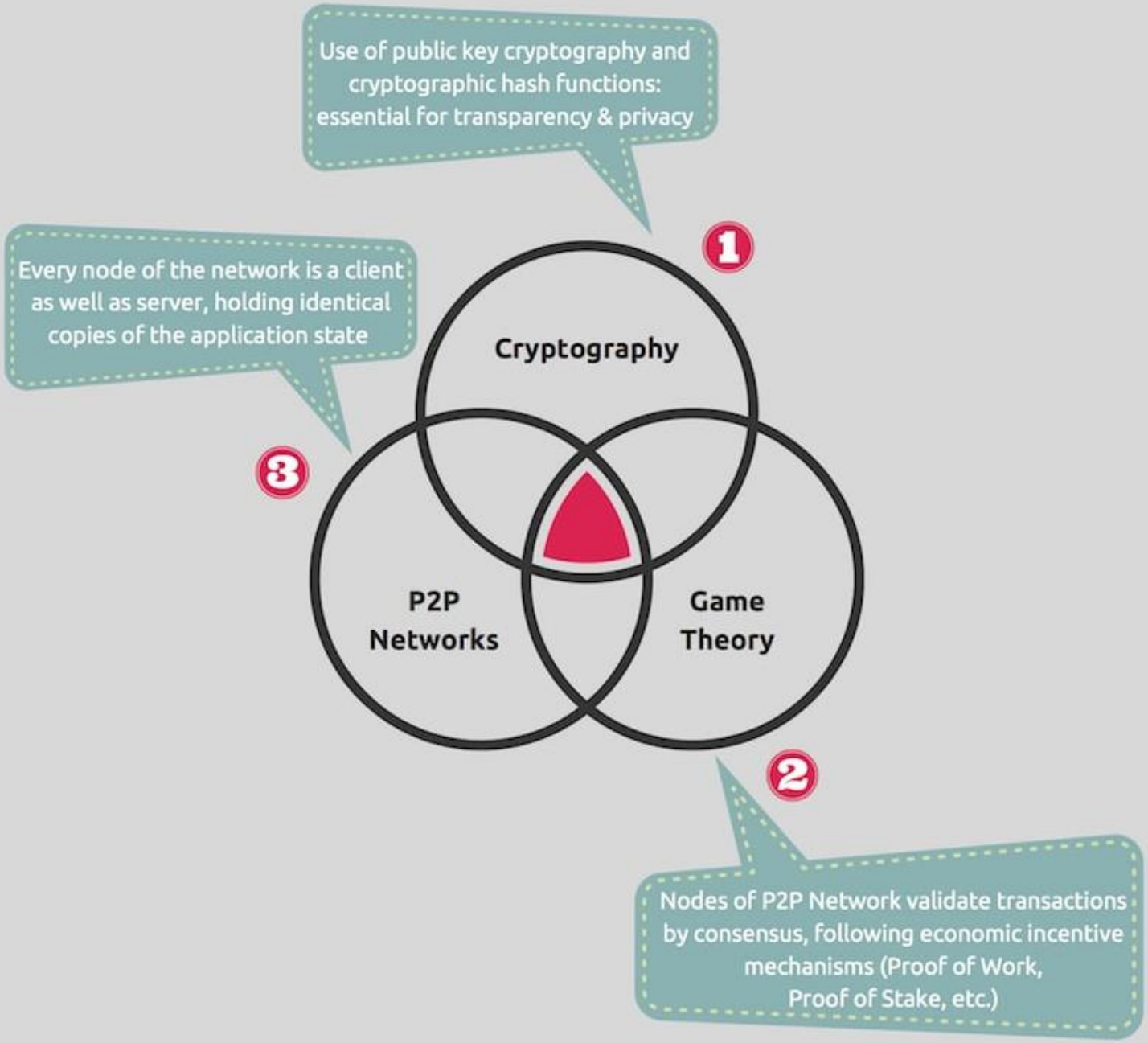
Each network participant keeps a copy of the entire blockchain - the file where all past transactions are recorded. Consensus of network validators verifies new transactions. In the Bitcoin network transactions are validated by network miners who are incentivised to verify transactions through PoW (Proof of Work).

Blockchain Technologies

» Cryptography for data protection and tampering

» P2P for De-centralization

» Game Theory for incentives to miners



Again, What is a blockchain?

- is a **novel** solution that provides **trustless trust**
- is a **shared, trusted, public, distributed ledger of transactions**
- allows **public inspection** of the system
- a **de-centralized** system
- is a **distributed P2P** database
- maintains a **continuously growing** list of **transactional records**
- is **cryptographically secured** from **tampering and revision**

USING THE

BLOCKCHAIN

Where Are Blockchains Used?

- Tokens (Bitcoin, Ethereum, etc)
- Smart Contracts (Ethereum)

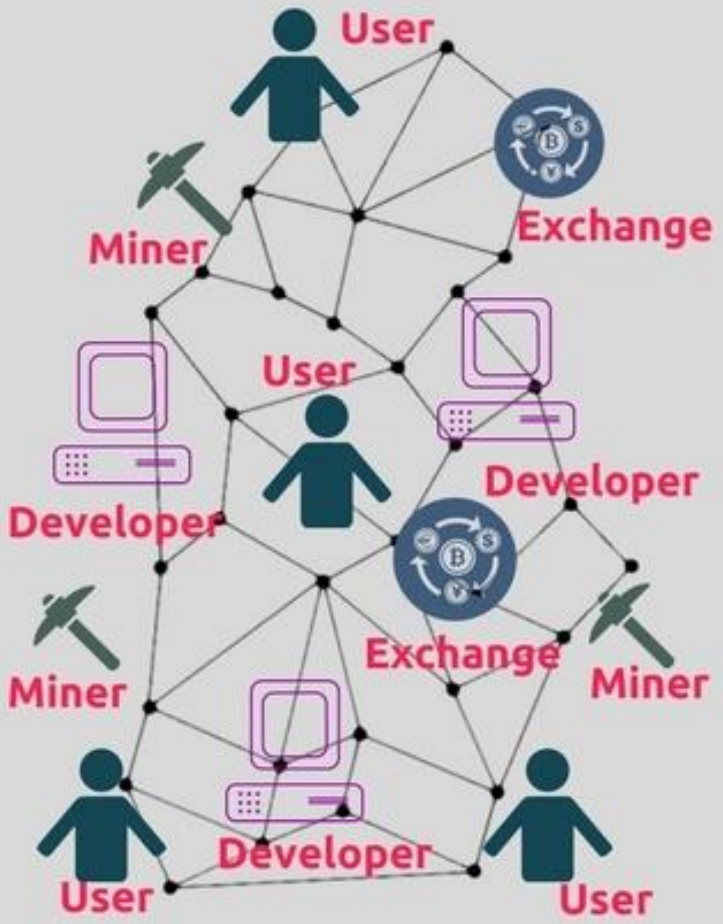
Traditional Organizations

Top Down Management

One legal entity
Employment contracts

Many layers of management for coordination & enforcement of processes. Many information & decision bottleneck as well as sources of corruption.

Decentralized Autonomous Organizations (DAOs)



Distributed Network of Autonomous Stakeholders

No centralized legal entity!
No employment contracts!

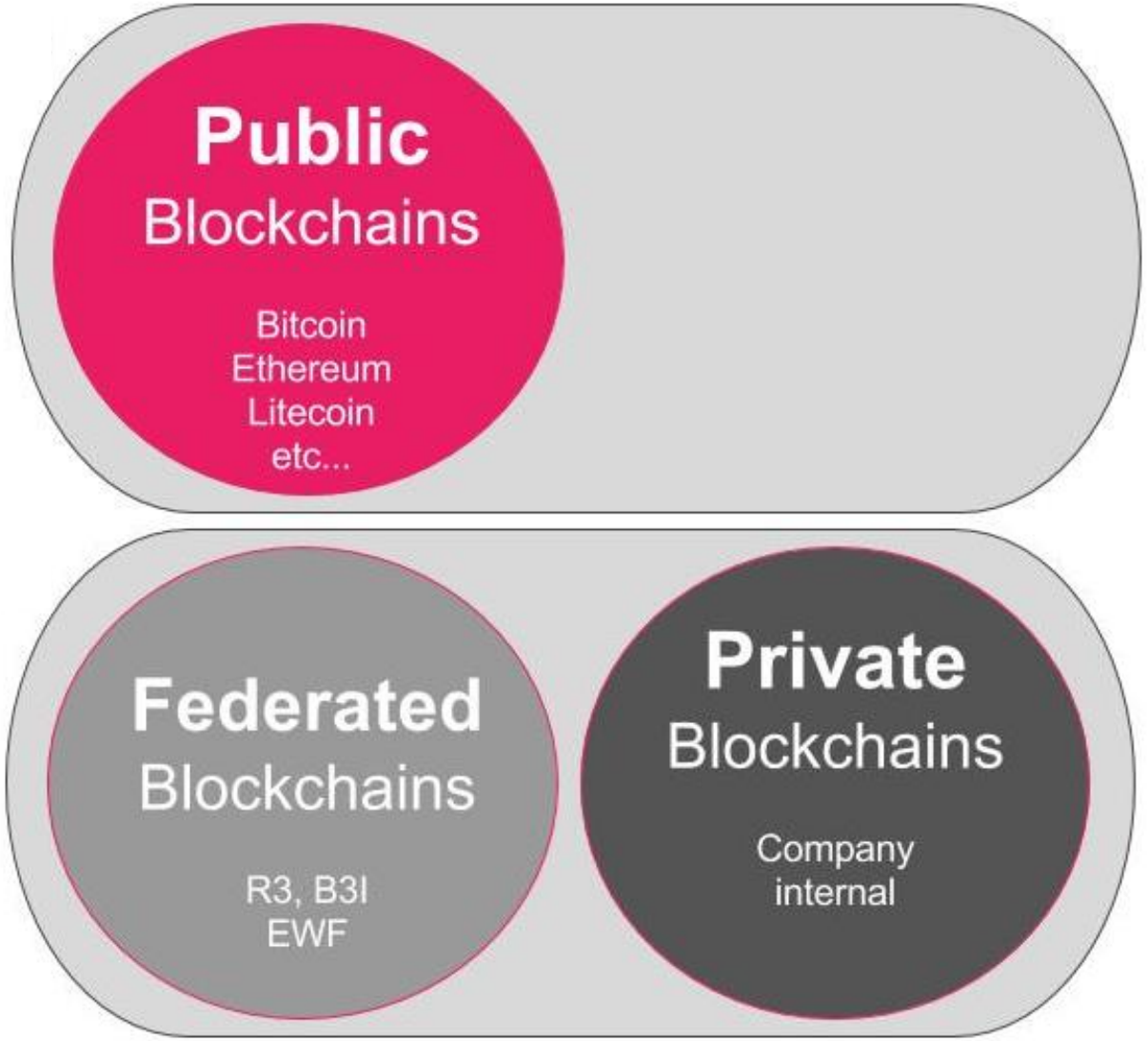
Machine consensus around token governance rulsets and smart contracts instead of legal employment contracts.

Types of Blockchains

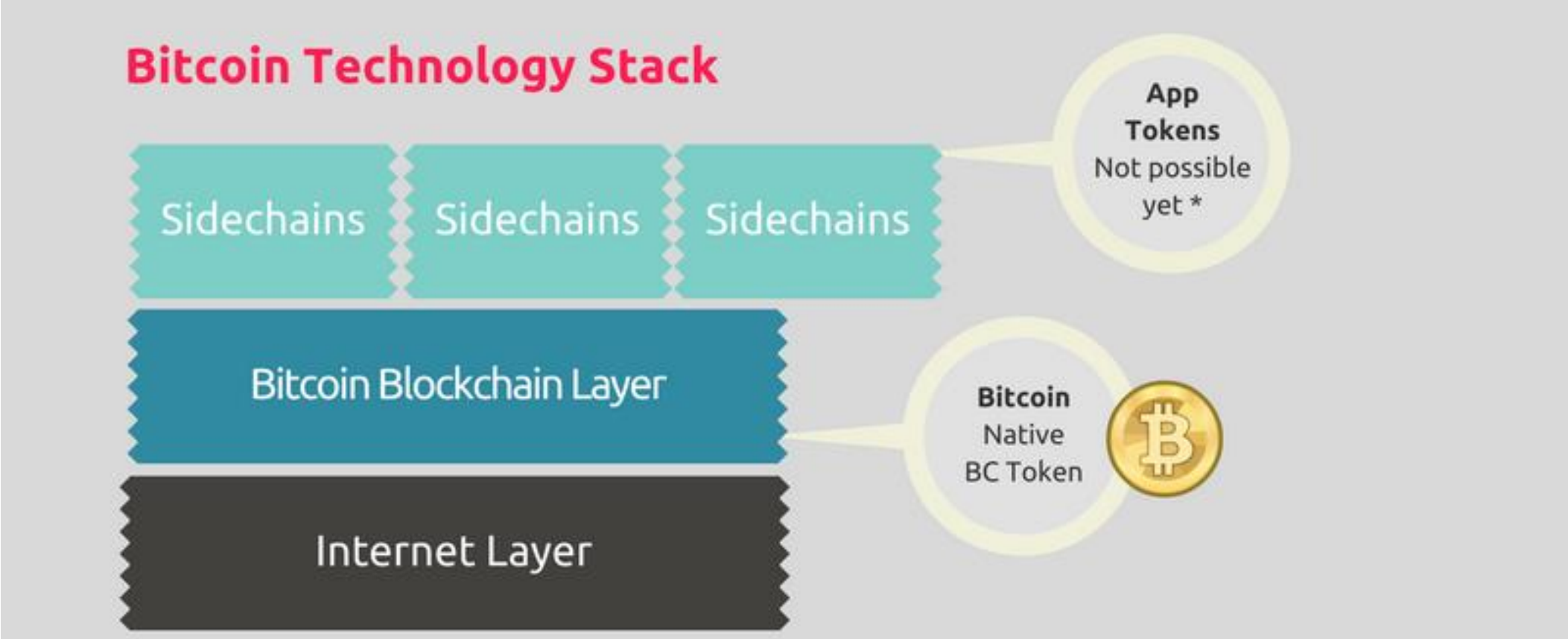
»Public: Bitcoin, Ethereum, Litecoin, Monero, Dash, Dodgecoin, etc.

»Federated: R3 (Banks), B3I (Insurance), EWF (Energy)

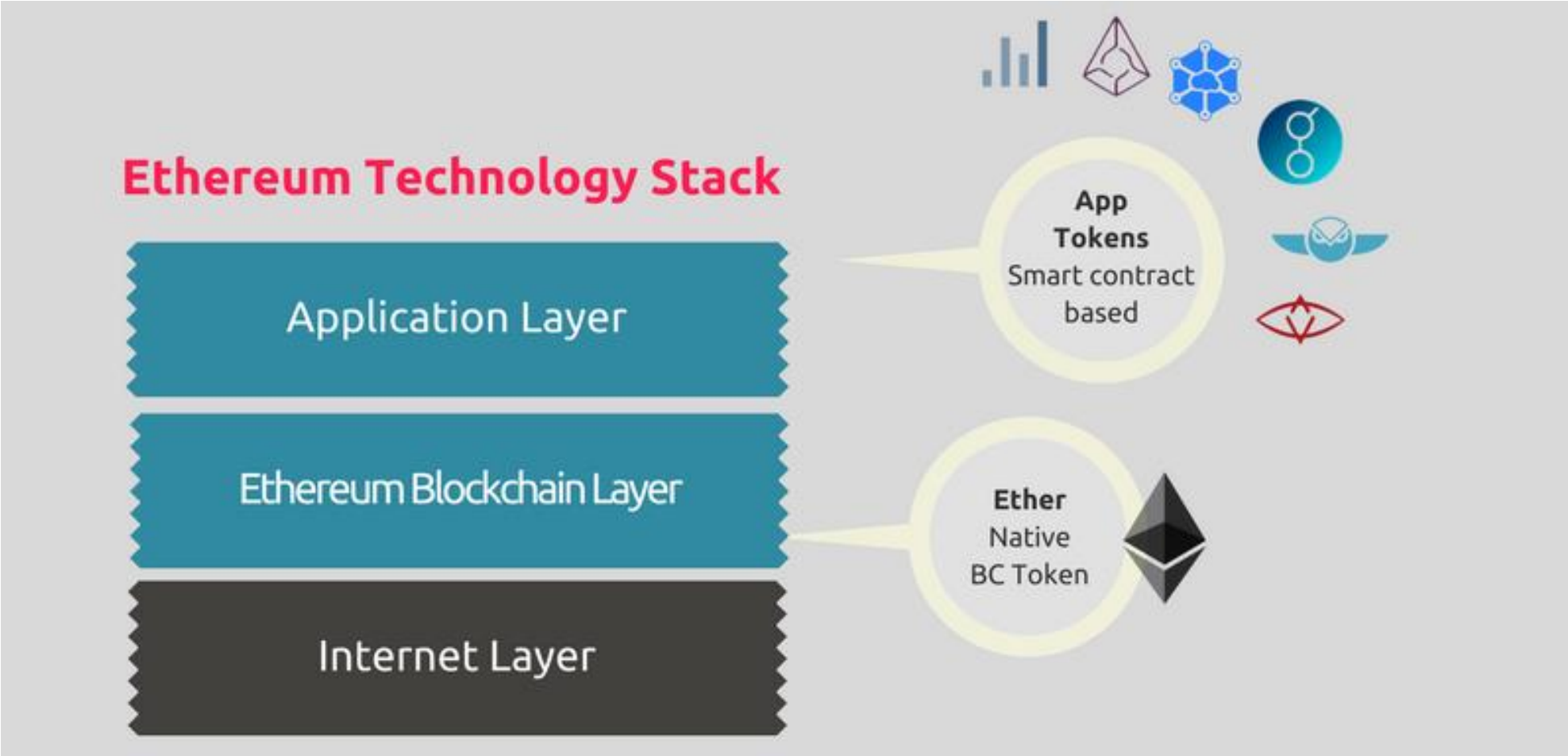
»Private: Monax, Multichain



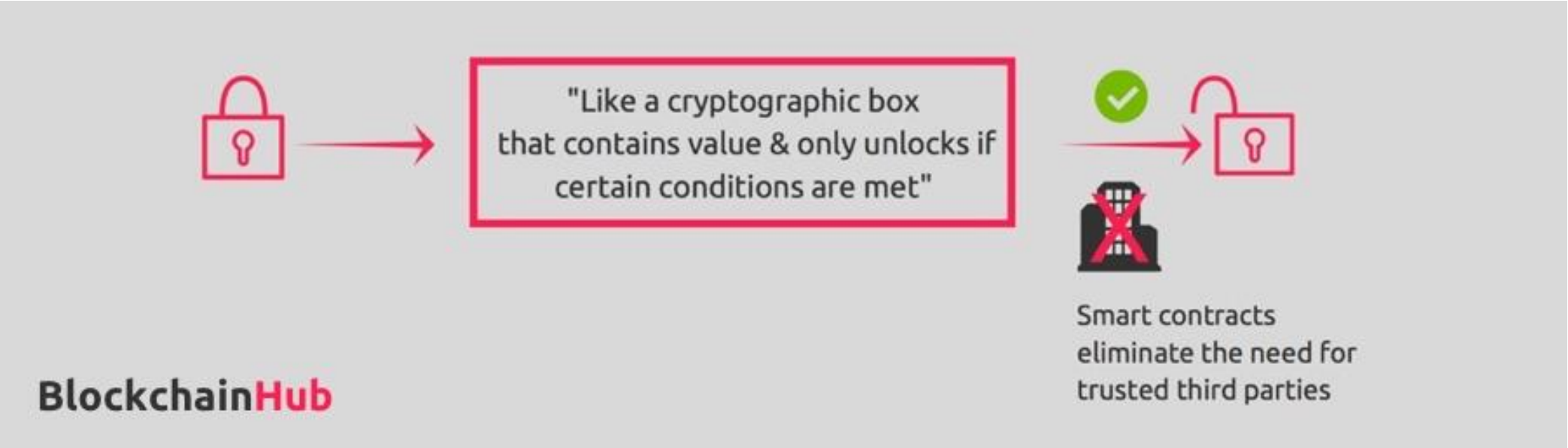
Bitcoin


Bitcoin Technology Stack
Sidechains
Sidechains
Sidechains
App
Tokens
Not possible
yet *
Bitcoin Blockchain Layer
Bitcoin
Native
BC Token
Internet Layer

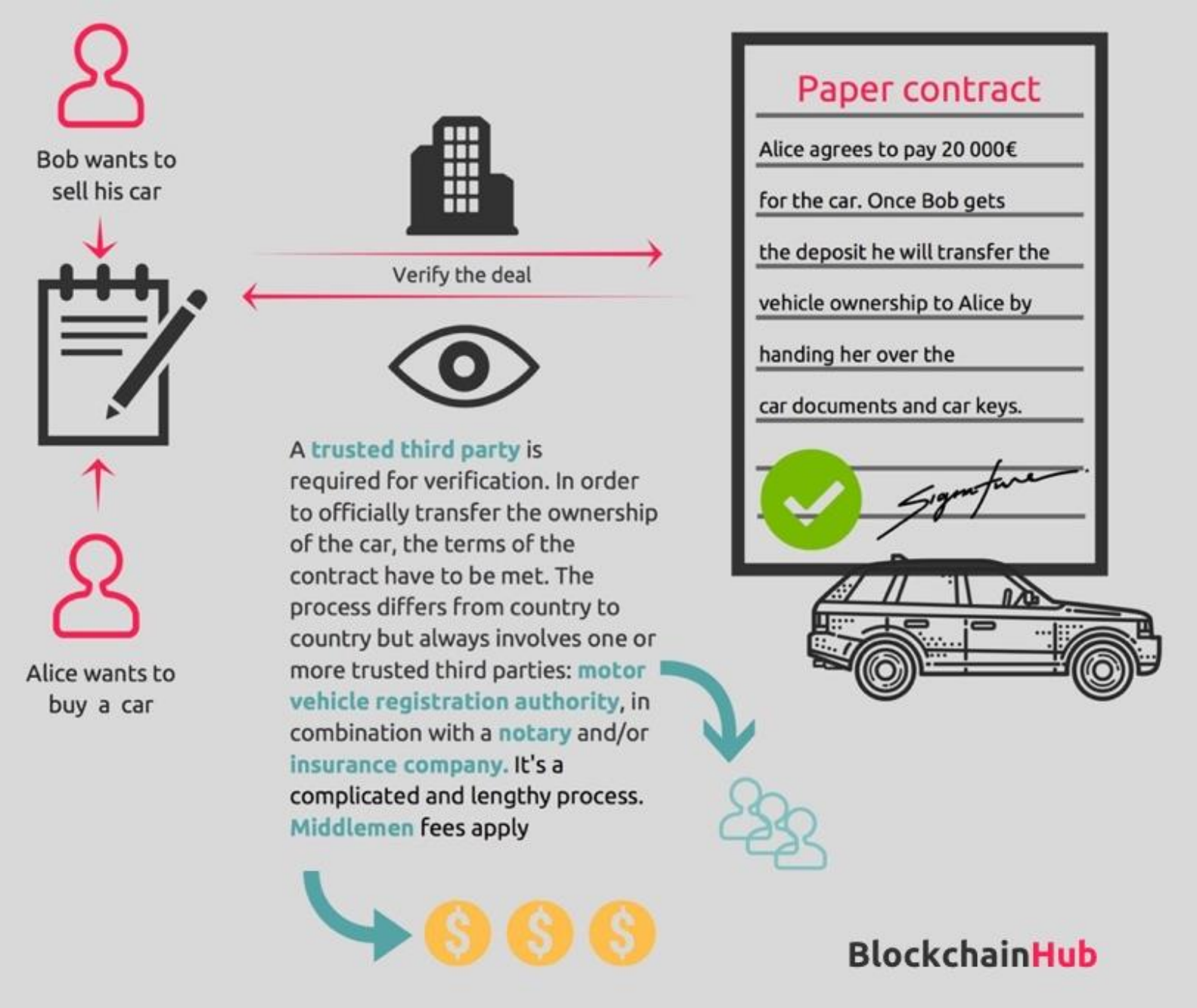
Ethereum


Ethereum Technology Stack
Application Layer
Ethereum Blockchain Layer
Internet Layer
App
Tokens
Smart contract
based
Ether
Native
BC Token

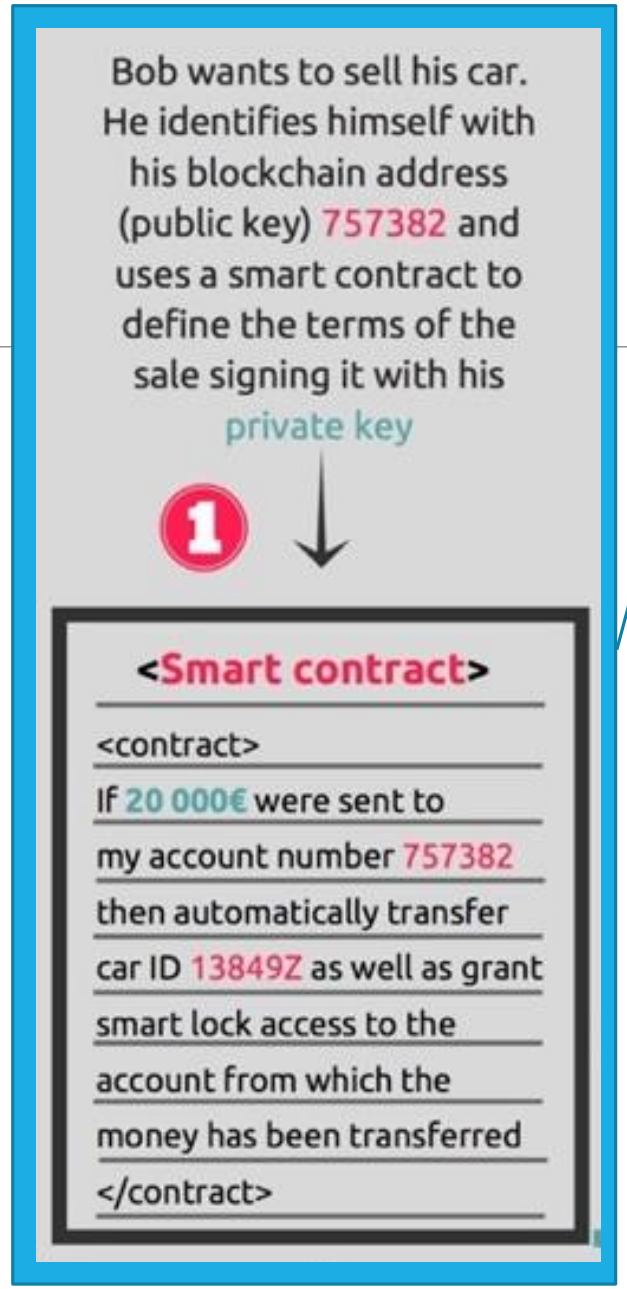
Smart Contracts

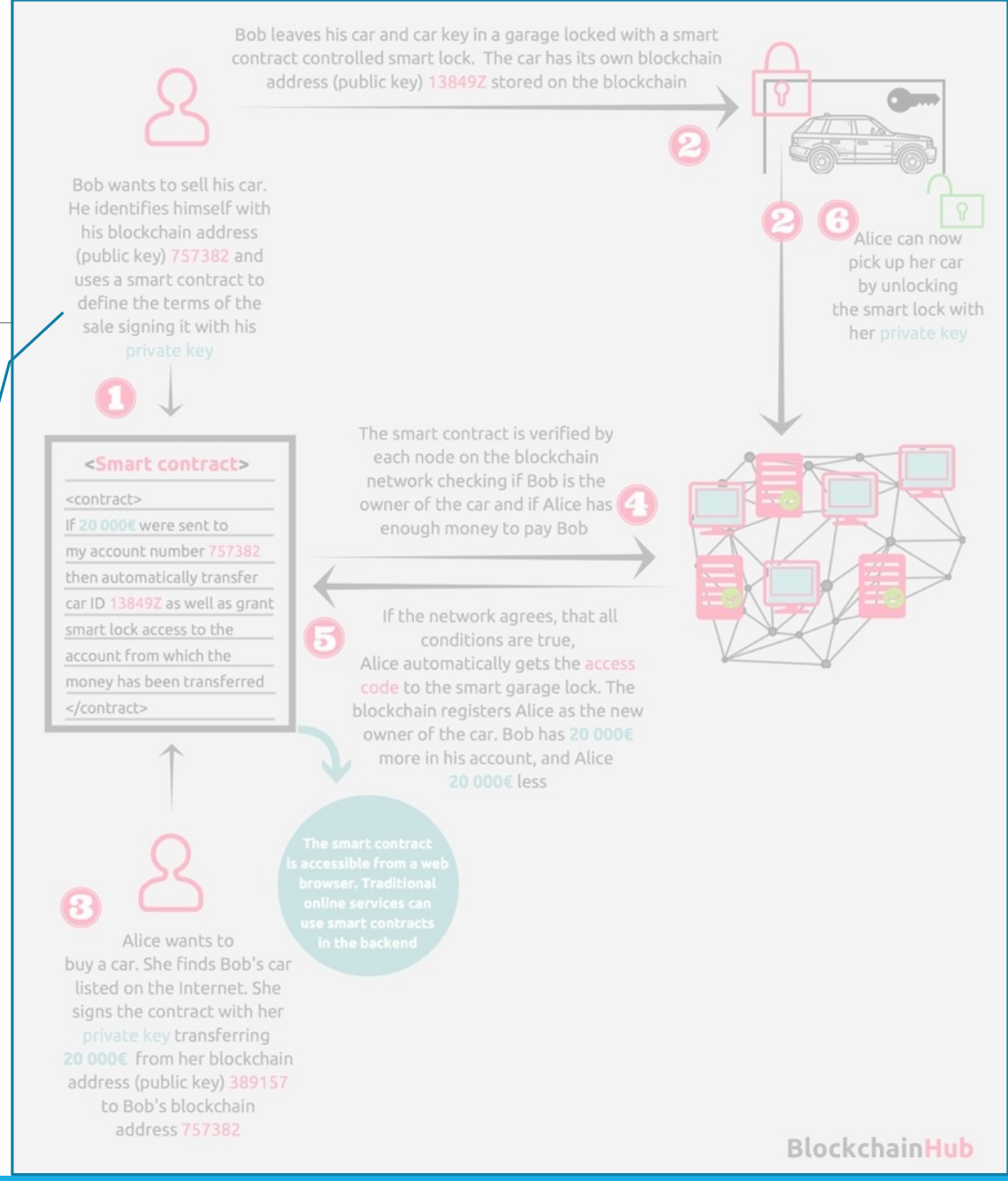


Traditional Car Sale

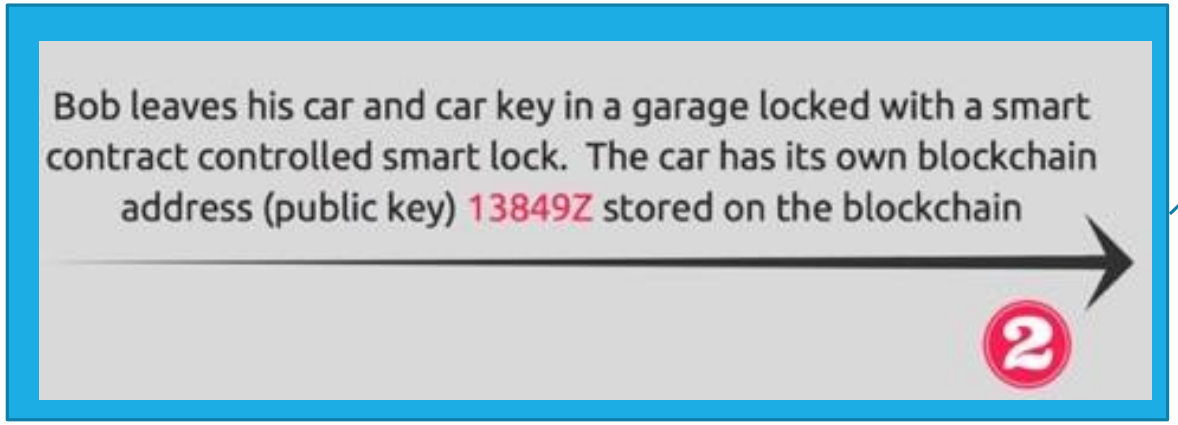


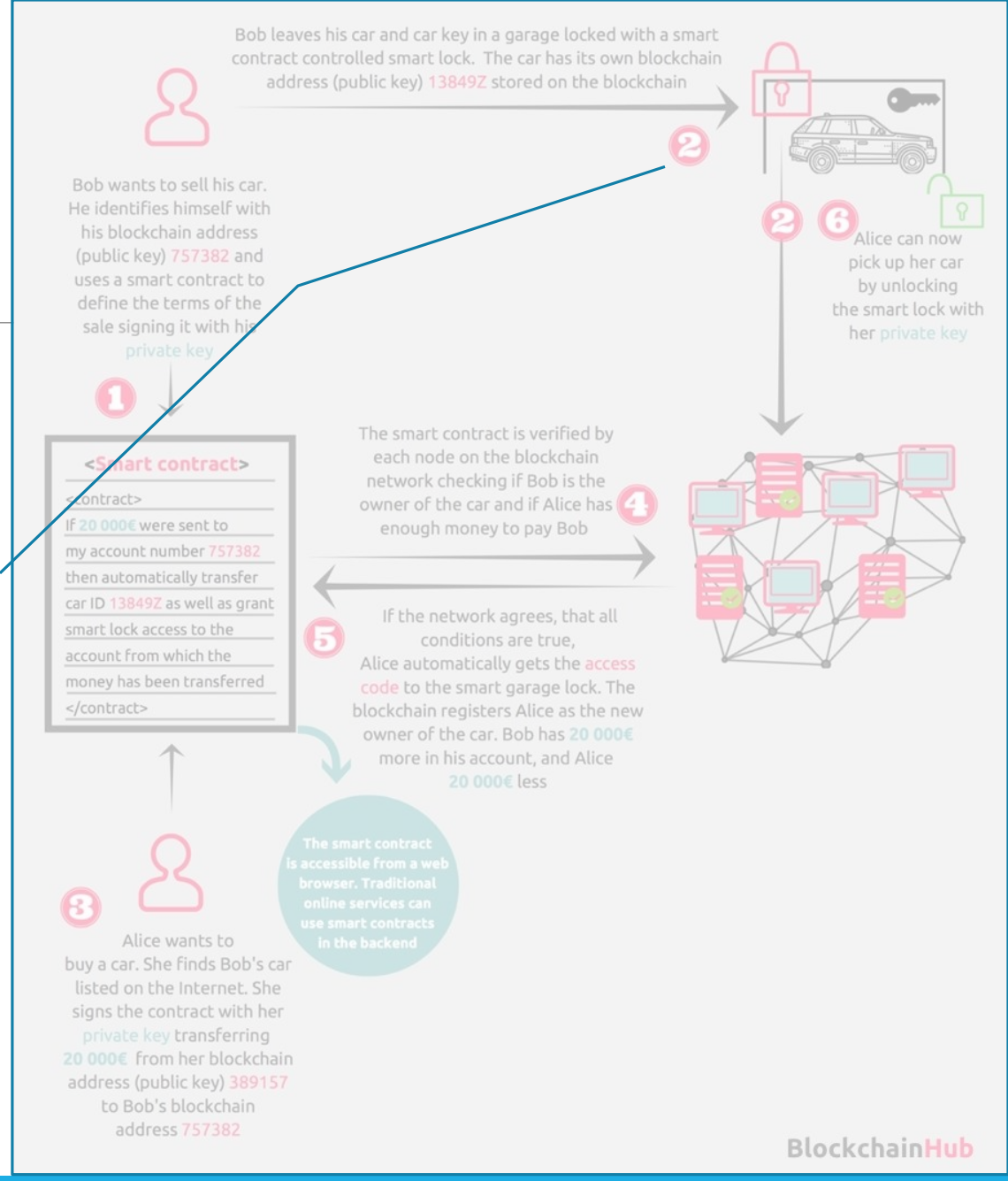
Smart Contract Car Sale



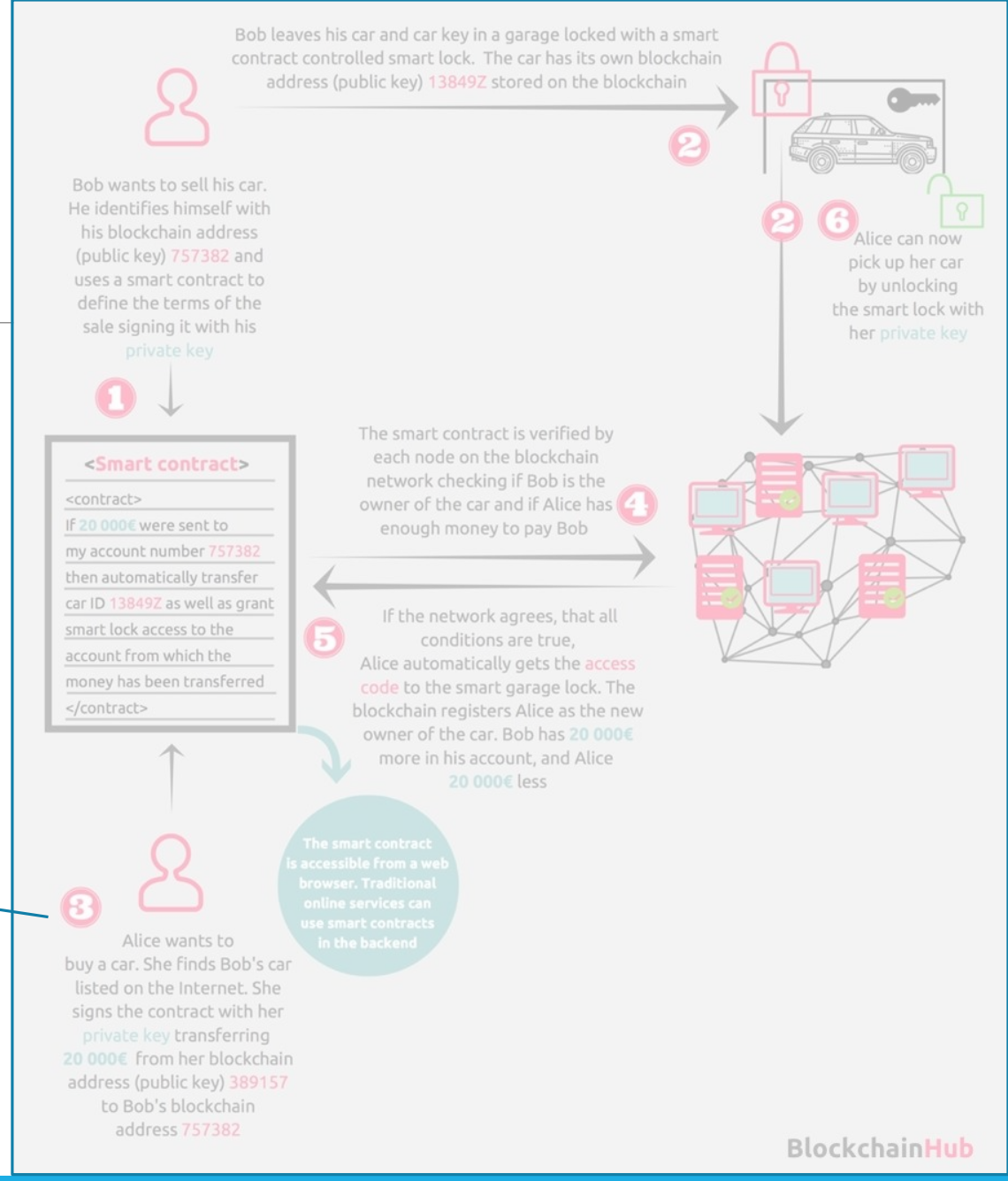


Smart Contract
Car Sale

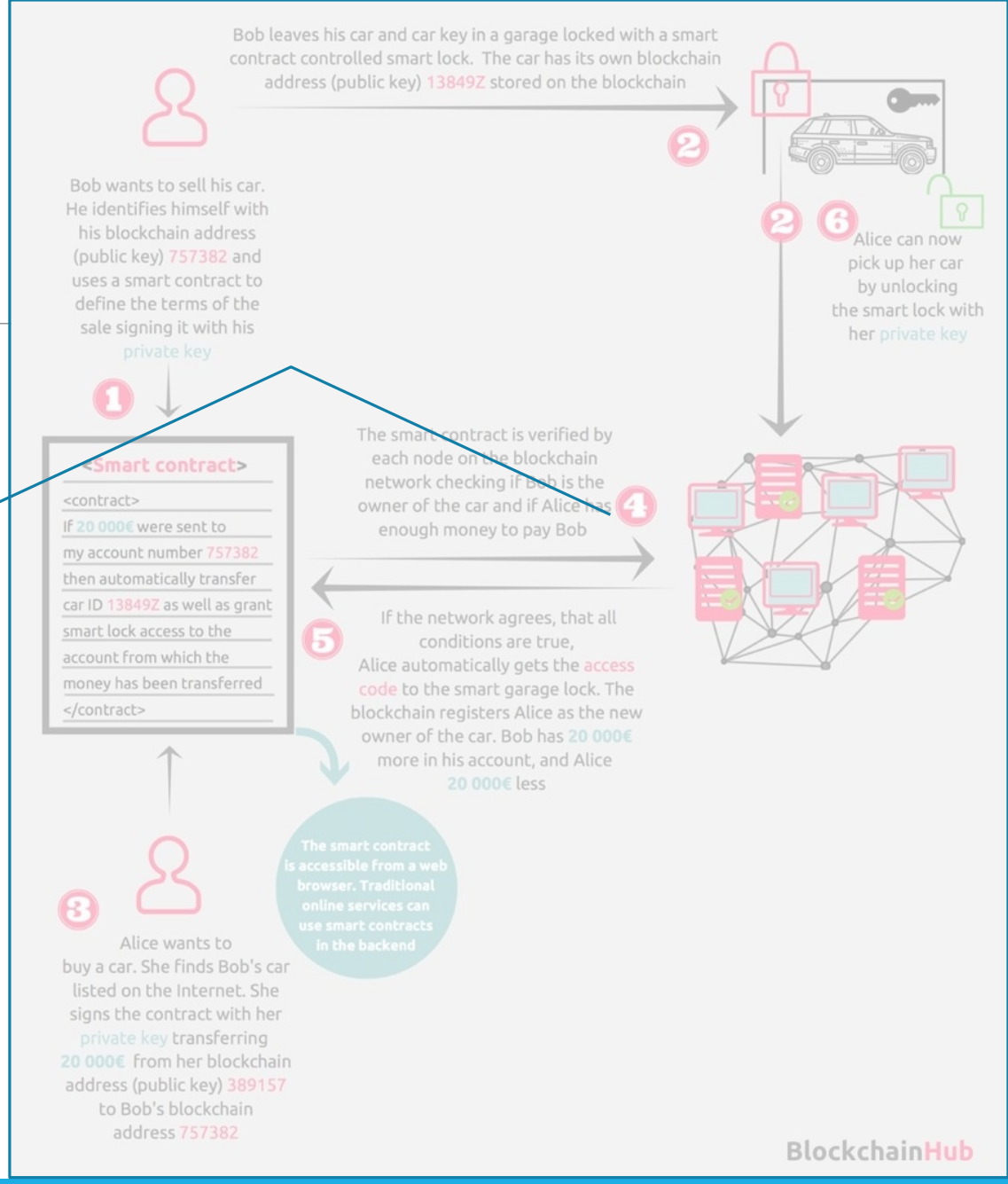




Smart Contract
Car Sale

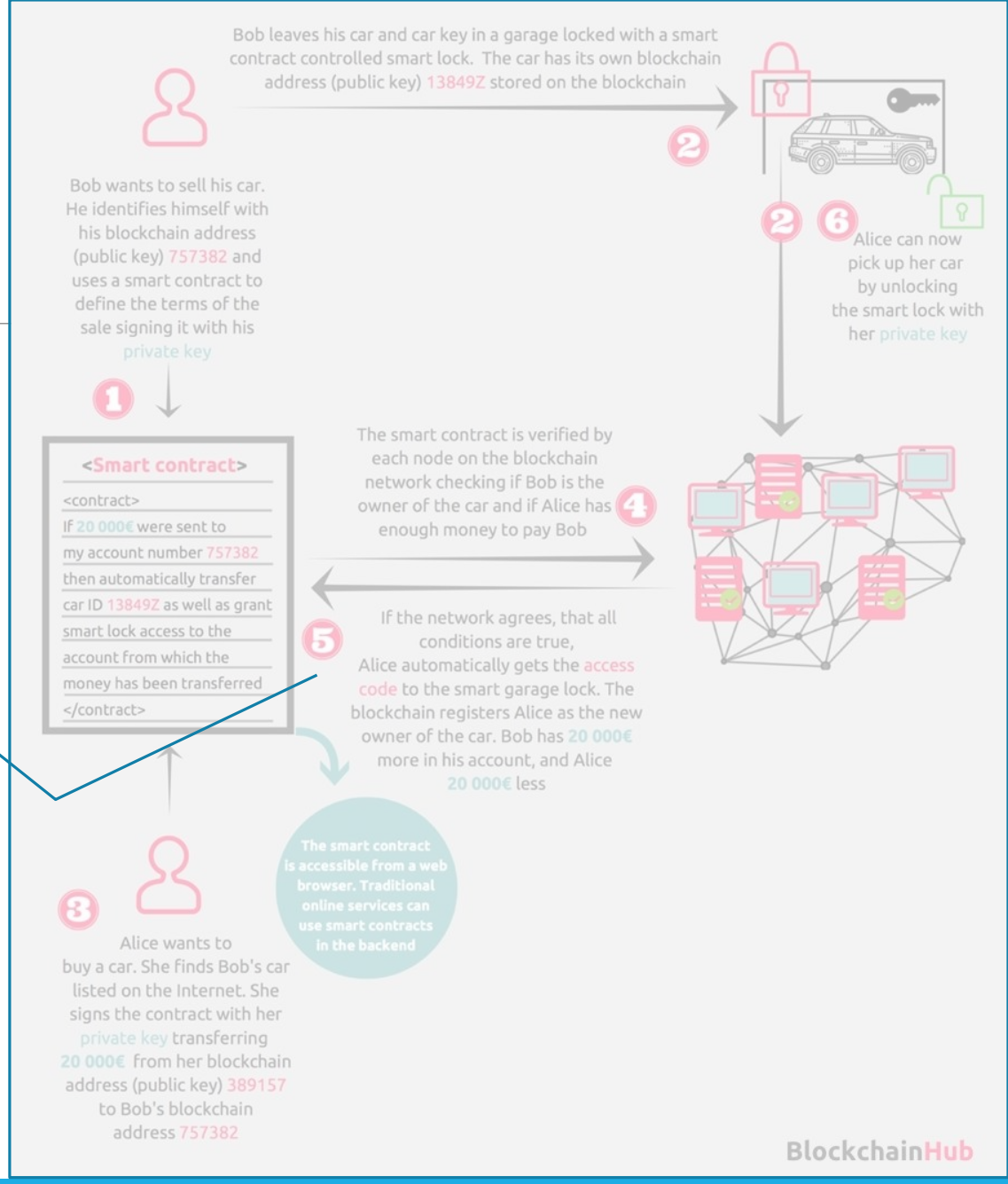


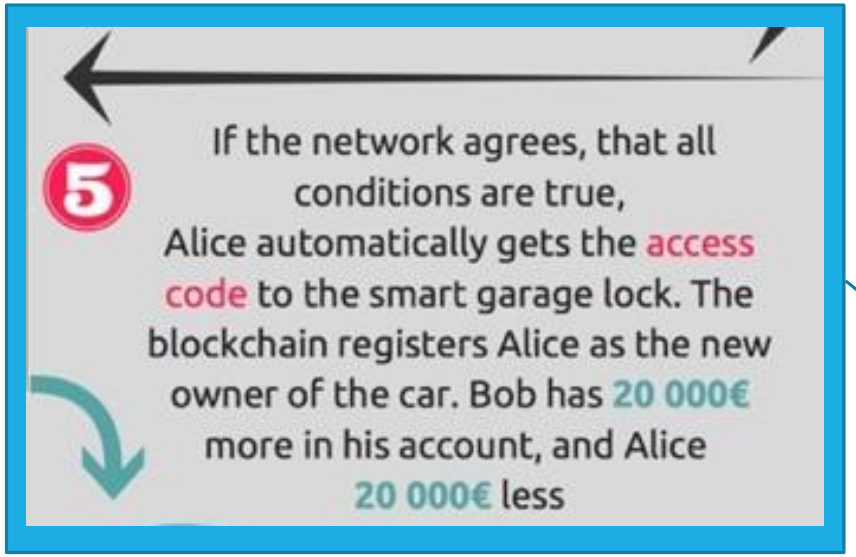
Smart Contract
Car Sale



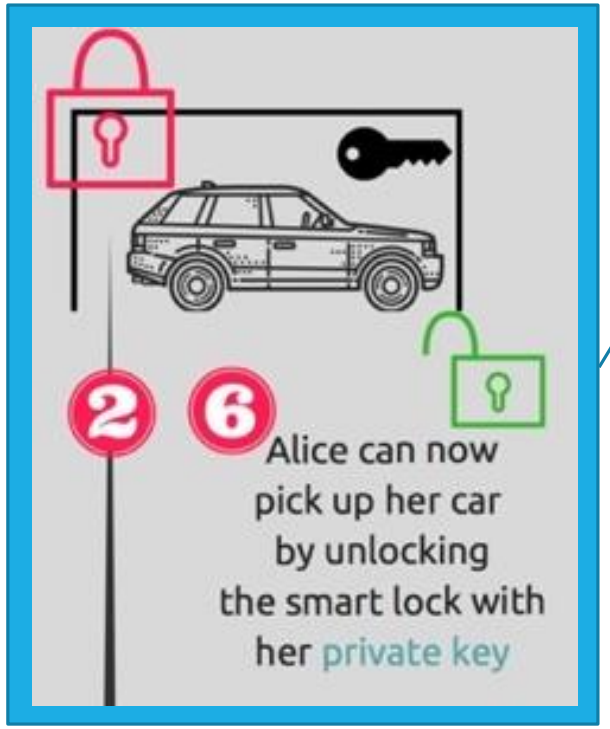
The smart contract is verified by each node on the blockchain network checking if Bob is the owner of the car and if Alice has enough money to pay Bob 4

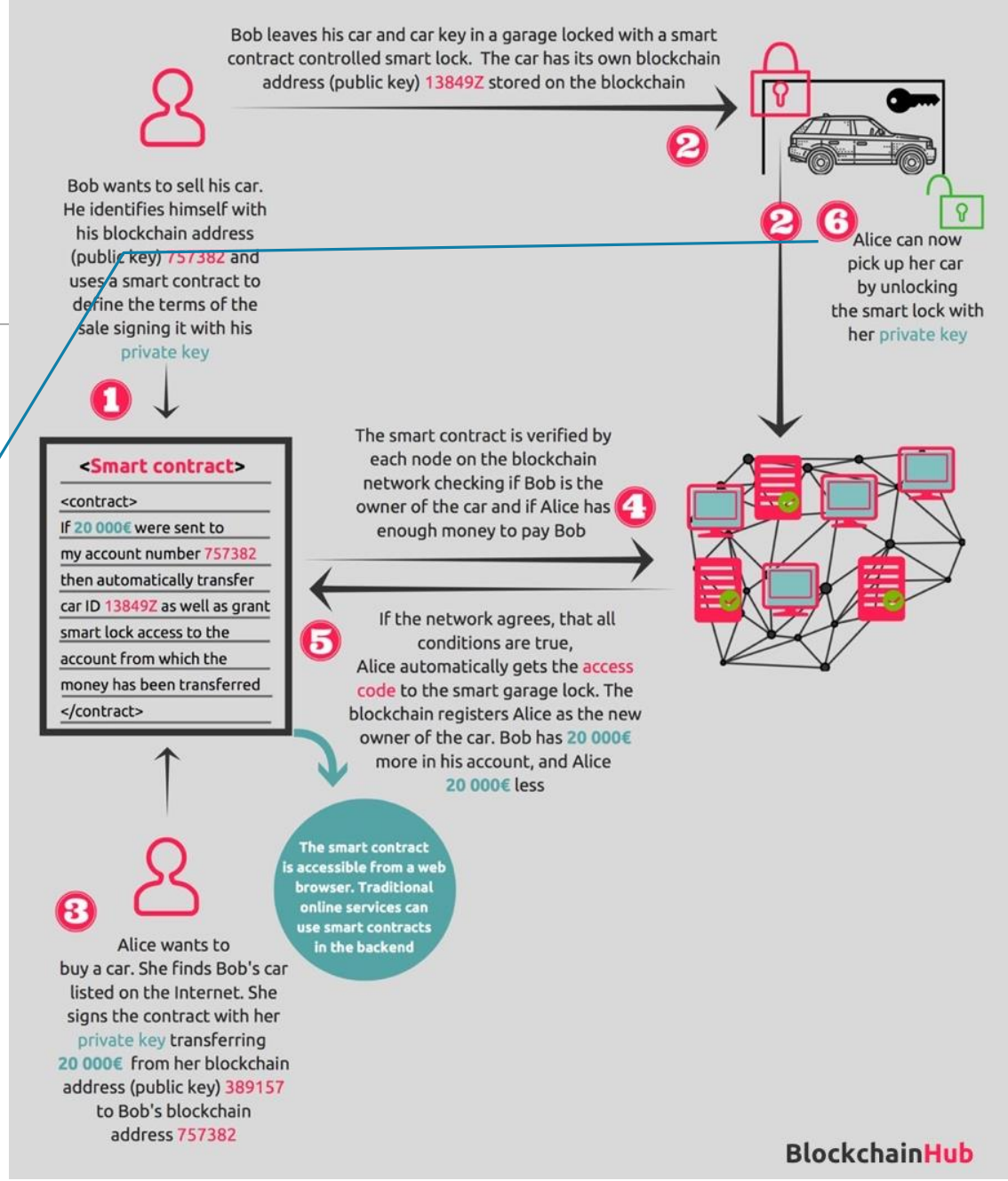
Smart Contract
Car Sale



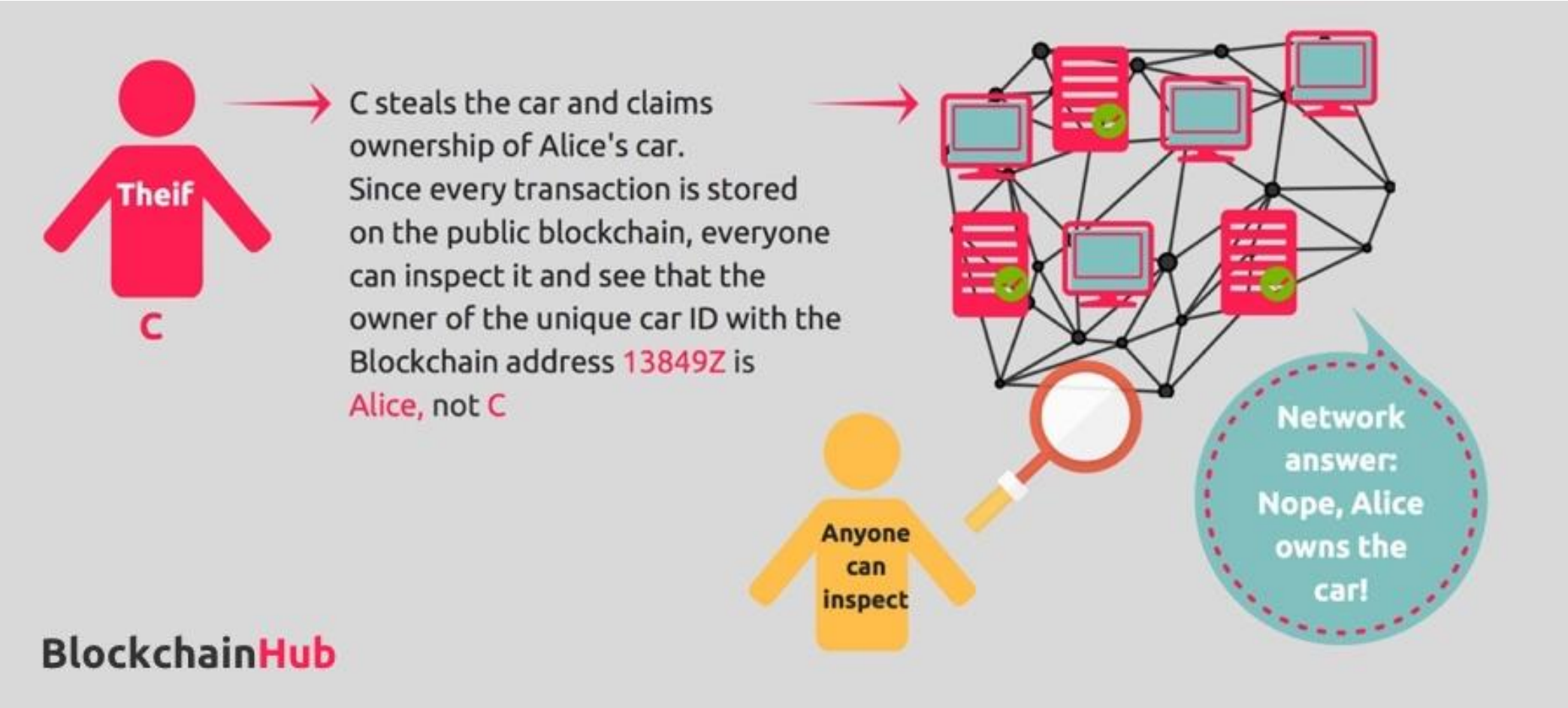


Smart Contract
Car Sale

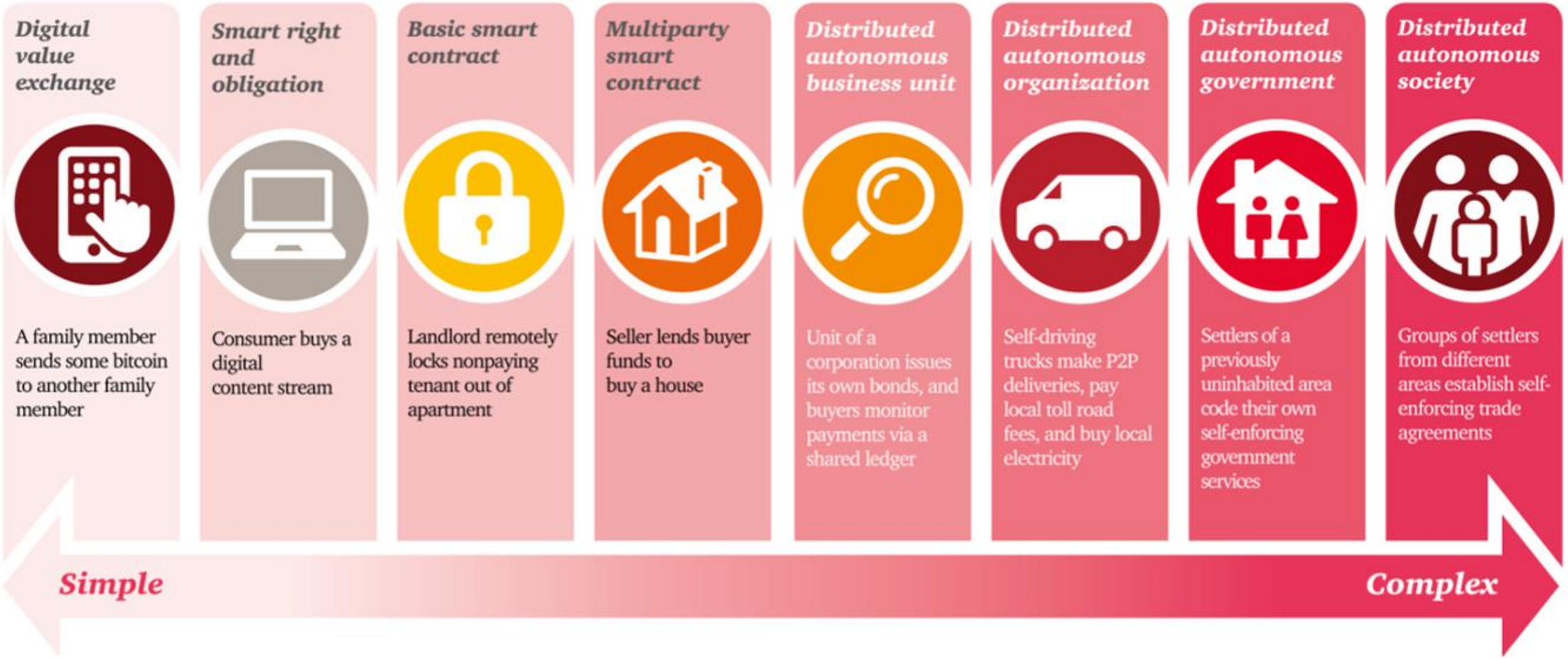




Can We Trust Smart Contracts?



Smart Contracts Types



ANY QUESTIONS ABOUT

BLOCKCHAIN ?

THANK YOU

I CAN BE REACHED AT

VSAWMA@NDU.EDU.LB
VICTOR.SAWMA@INTOUCHMENA.COM