Høgskolen på Vestlandet

DAT159
Module3 – Blockchain technology

L19 - Smart contracts | Scalability solutions

Lars-Petter Helland, 23.10.2018

Today

- Smart contracts
- Scalability solutions

Reading / viewing material

[BG] BitFury Group, Smart Contracts on Bitcoin Blockchain *(cursory)*

- https://bitfury.com/content/downloads/contracts-1.1.1.pdf

[KH1] [KH2] Kevin Healy, Ethereum in Depth: Smart Contracts - Part 1 and 2

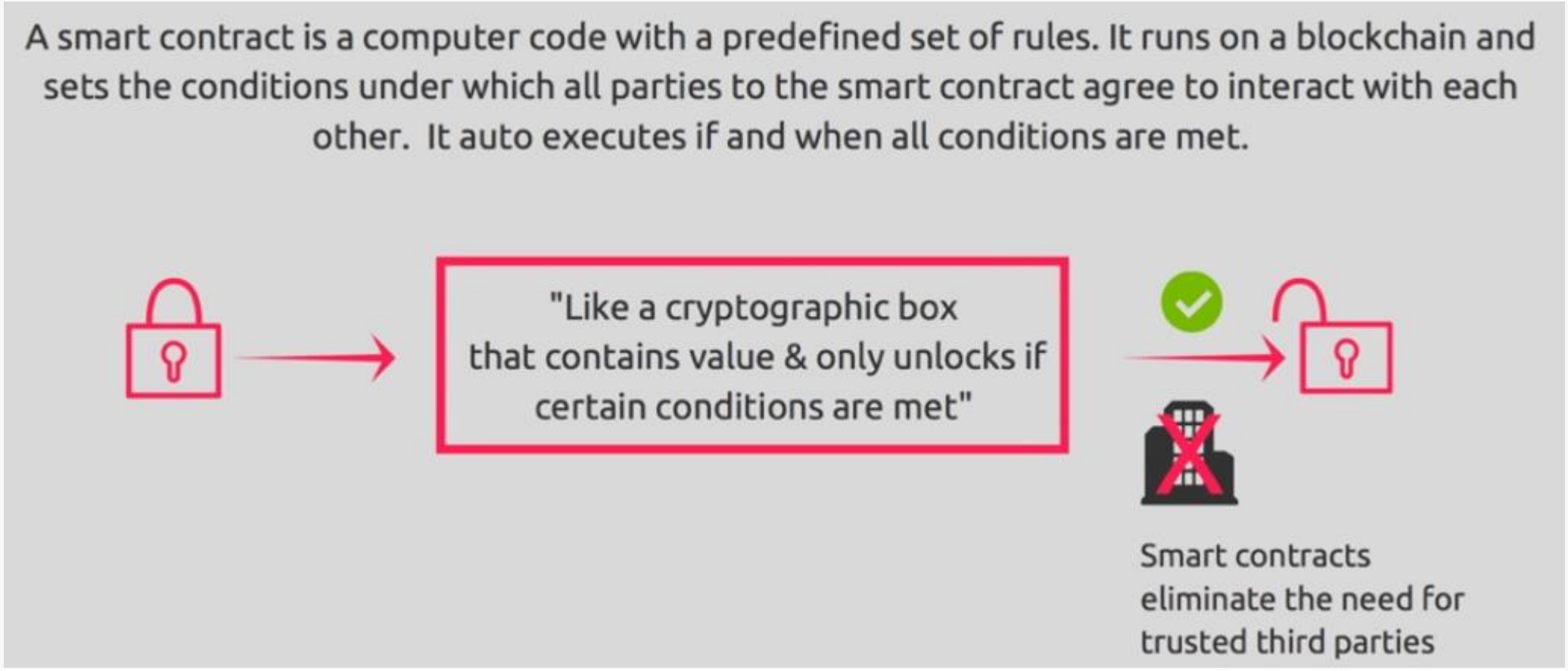
- https://www.youtube.com/watch?v=w9WLo33KfCY
- https://www.youtube.com/watch?v=TC-bDQZbXd0

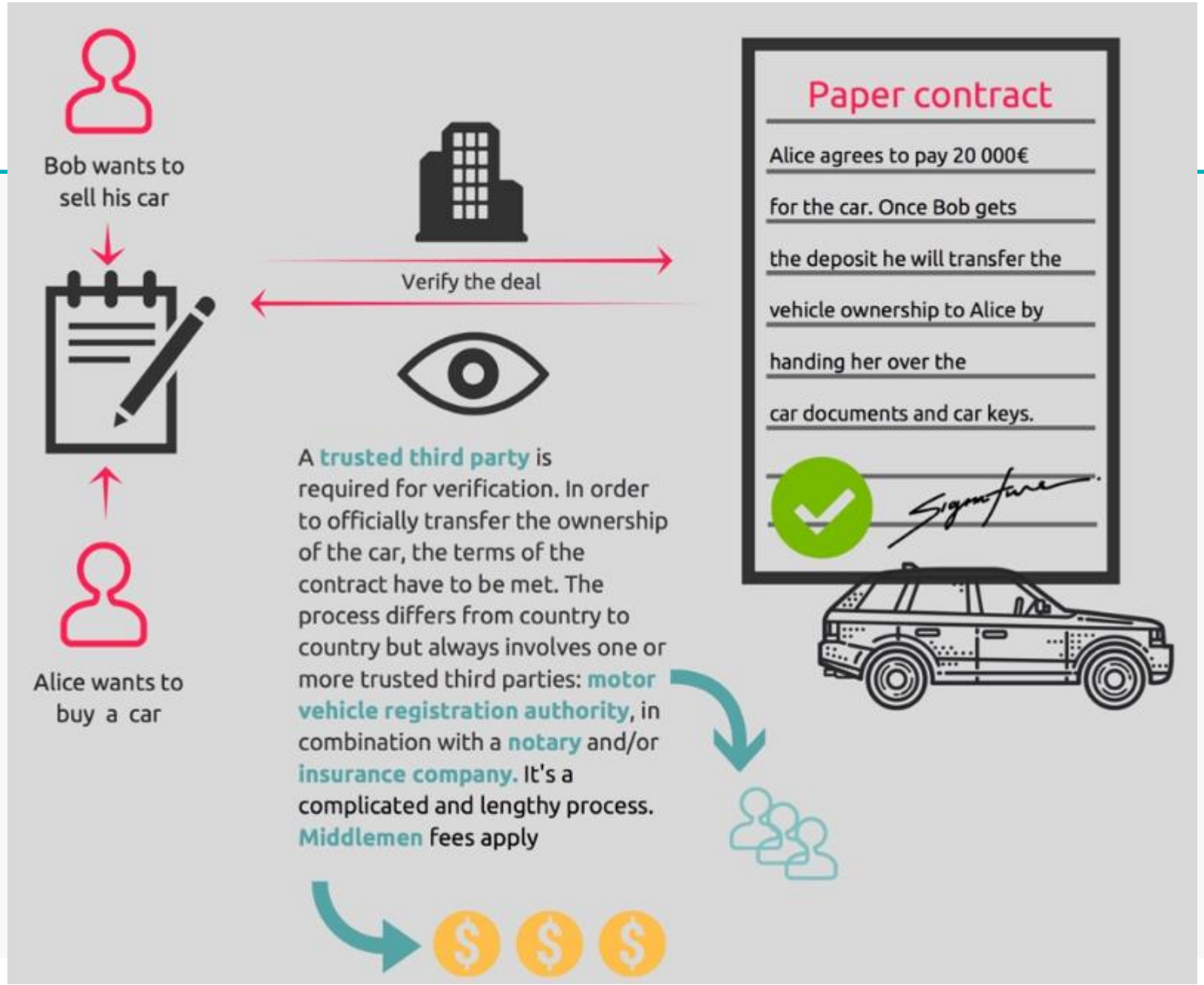
[xx] xx, on scalability *(cursory)*

- https://www.investinblockchain.com/solving-blockchain-scalability-problem/
- https://cryptopotato.com/blockchains-and-the-scalability-problem/

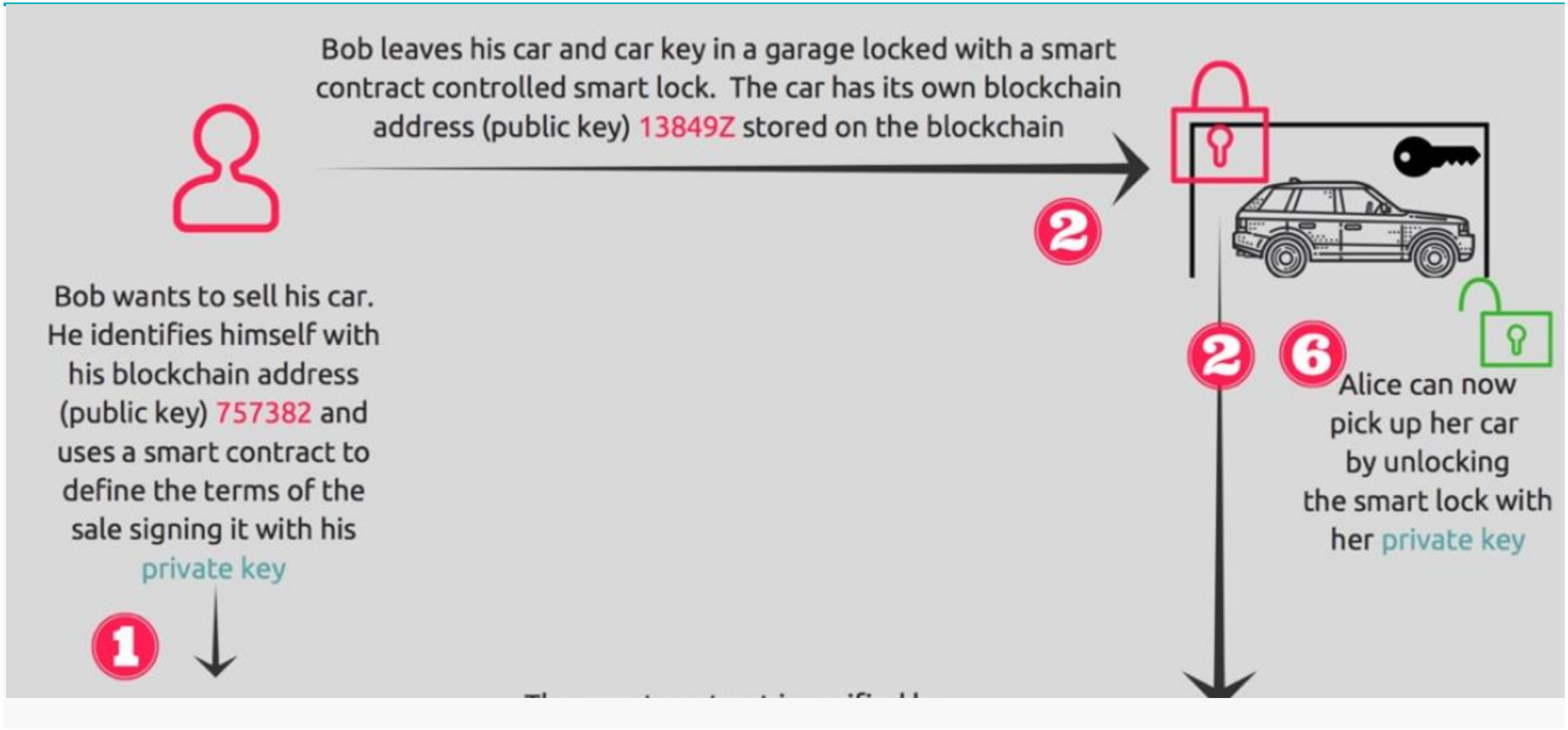
https://blockchainhub.net/blog/infographics/smart-contracts-explained/

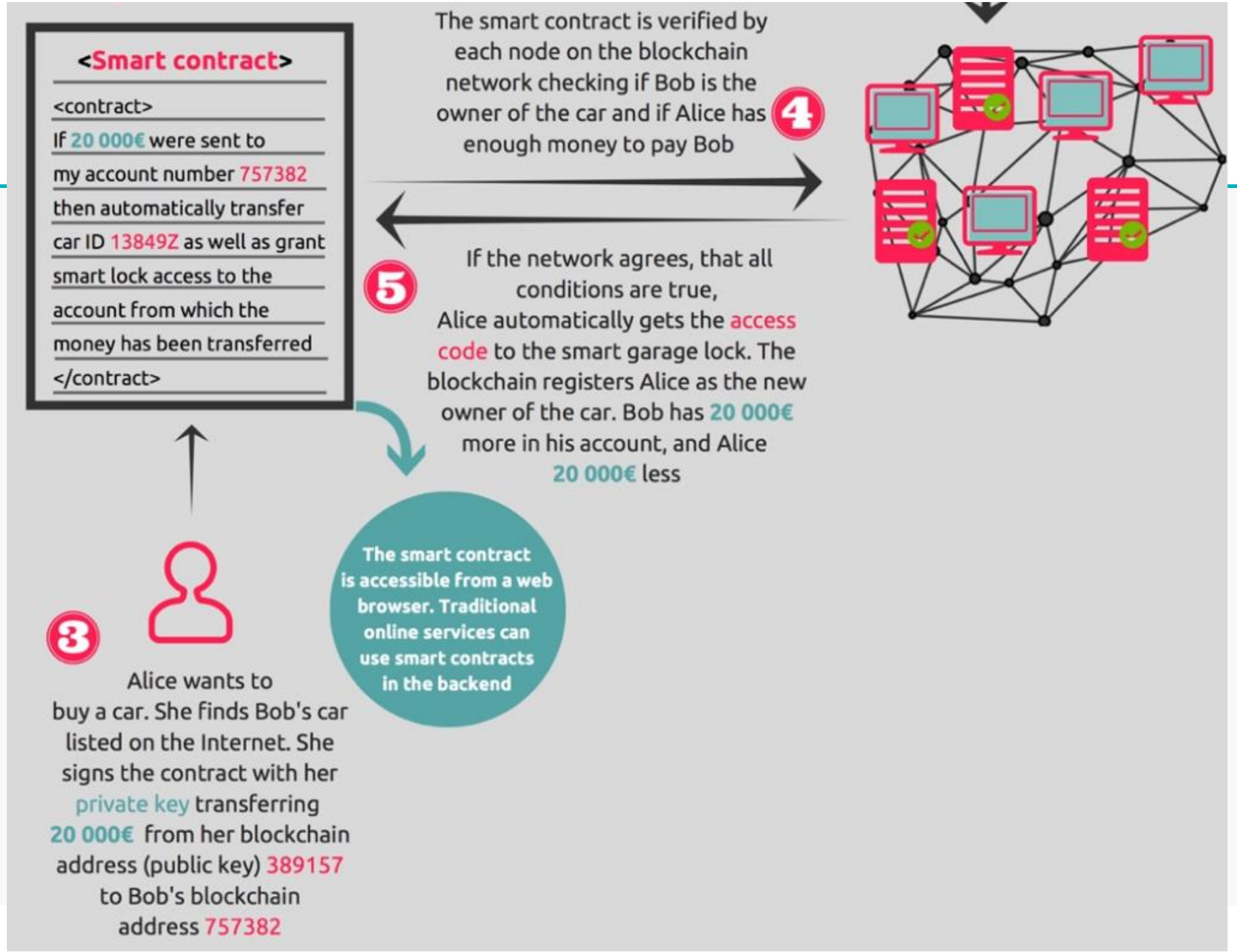
Smart contracts




Bob wants to sell his car
Verify the deal
Paper contract
Alice agrees to pay 20 000€
for the car. Once Bob gets
the deposit he will transfer the
vehicle ownership to Alice by
handing her over the
car documents and car keys.
Signature
Alice wants to buy a car
A trusted third party is required for verification. In order to officially transfer the ownership of the car, the terms of the contract have to be met. The process differs from country to country but always involves one or more trusted third parties: motor vehicle registration authority, in combination with a notary and/or insurance company. It's a complicated and lengthy process. Middlemen fees apply

Using a smart contract




<Smart contract>
<contract>
If 20 000€ were sent to
my account number 757382
then automatically transfer
car ID 13849Z as well as grant
smart lock access to the
account from which the
money has been transferred
</contract>
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
If the network agrees, that all conditions are true, Alice automatically gets the access code to the smart garage lock. The blockchain registers Alice as the new owner of the car. Bob has 20 000€ more in his account, and Alice 20 000€ less
5
The smart contract is accessible from a web browser. Traditional online services can use smart contracts in the backend
3
Alice wants to buy a car. She finds Bob's car listed on the Internet. She signs the contract with her private key transferring 20 000€ from her blockchain address (public key) 389157 to Bob's blockchain address 757382

Does Bitcoin have smart contracts capabilities?

- As you know, Bitcoin uses the **scripting language Script** to transfer (unlock and lock) value on the Bitcoin blockchain.
- There are some functions (opcodes) in the Script language that offers some smart contract functionality.
- There is a possibility to require multiple signatures to unlock coins.
- There is a possibility to lock coins for a certain time.
- People have done payment channels, escrows, atomic cross-chain trading, ... (see https://bitfury.com/content/downloads/contracts-1.1.1.pdf)

- But really, there are better blockchains for smart contracts.

Ethereum, https://www.ethereum.org/

- Maybe the most known / successful platform for smart contracts is the Ethereum blockchain.
- Ethereum was proposed in 2013 by Vitalik Buterin, and the network was up and running in 2015.
- The cryptocurrency for the Ethereum network is called **Ether** (symbol Ξ), and is divided into 10^{18} Wei, evt. 10^{9} GWei.
- Buterin had argued that Bitcoin needed a scripting language for application development. Failing to gain agreement, he proposed development of a new platform with a more general scripting language.

Ethereum smart contract capabilities

- Ethereum uses a Turing-complete language called **Solidity** to program smart contracts. *(also Serpent, LLL, Mutan, Viper, ...)*
- In Ethereuem, smart contracts are **independent actors** with their own addresses.
- Each smart contract has associated scripts that allow it to process incoming transactions. Thus, transactions in Ethereum have no predefined semantics compared with Bitcoin where all transactions transfer value; **the semantics of a transaction is defined by its destination**.
- The Ethereum blockchain stores not only transactions, but also **system states**. The Ethereum scripting language has special instructions to read and write data from / to the blockchain.

Ethereum accounts

- In Bitcoin, there is only one type of "account", the one represented by a key-pair, and controlled by a private key.

- In Ethereum, there are two types of accounts
  - **Externally owned account** (EOAs): an account controlled by a private key (like in Bitcoin).
  - **Contract**: an account that has its own code, and is controlled by code.

Let us look at a few videos that explains how it works

Ethereum in Depth: Smart Contracts - Part 1: What is a Smart Contract?

- https://www.youtube.com/watch?v=w9WLo33KfCY
- Let's look at the first 12 minutes (later he shows more examples)

Ethereum in Depth: Smart Contracts - Part 2: How to Create and Publish a Smart Contract

- https://www.youtube.com/watch?v=TC-bDQZbXd0
- Let's look at the first 12 minutes, then jump to near the end (in between he shows code)


Pause

Now

There is a lot of development going on in the blockchain sphere to create (better) solutions to known problems and limitations in current blockchains, in areas like scalability, privacy, interoperability, consensus, decentralization, security, etc...

Scalability is a big problem that must solved, and we will look closer at that.

Bitcoin and Ethereum suffered badly from congestion in the popular days of December 2017.

If the network is not able to handle the incoming transactions fast and cheap, it will fail!

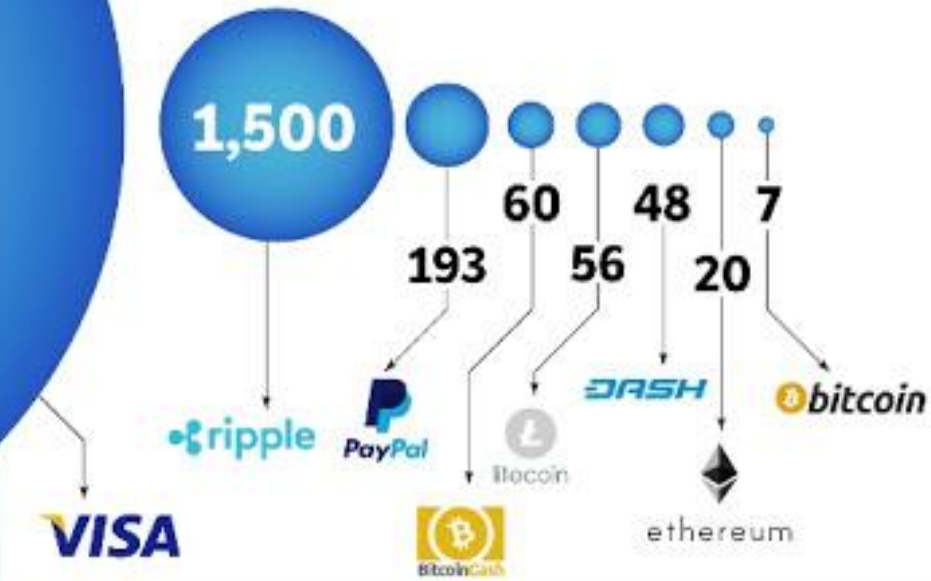
Also, if blockchain-networks should be used in micro-payments and in IoT-solutions, we need much faster and scalable networks.

https://www.abitgreedy.com/transaction-speed/

BY THE NUMBERS

Cryptocurrencies transaction speeds per second compared with Visa and Paypal

Dash, bitcoin and ethereum bring up the rear. Consistent transaction delays when traders transfer their currency are common, as their popularity outpaces their network's processing capabilities



24,000

transactions per second are processed by Visa (a 60-year-old company), making it the fastest payment network measured

Cryptocurrencies, particularly ripple, have extremely fast transaction speeds for such new technology, suggesting they may have the capability to become viable payment solutions on a larger scale

Source: Howmuch.net

What are the alternatives scaling solutions?

- Increased block size
- Increased block frequency
- Data compression (SegWit / Schnorr / MAST)
- Sharding
- More centralized consensus (delegated consensus)
- Off-chain solutions - Payment channels
- Off-chain solutions - Chains of chains
- Different topologies (DAG, Tangle, Lattice, Hashgraph)

Increased block size

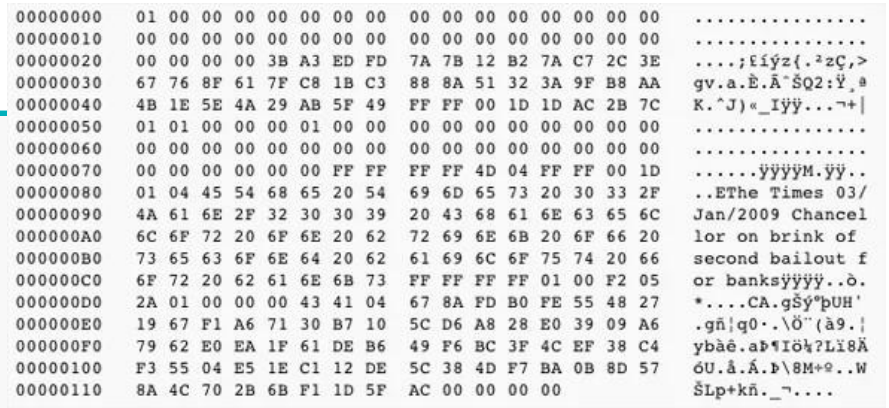
- **Bitcoin** has a max block size of **1MB**, and creates a new block every **10 minutes** on average. With a max of ~ 4000 transactions per block, this gives us a max of ~ **7 transactions / second**.
- By increasing the block size, we can fit more transactions into one block, and thus improve the transaction rate.

- **Bitcoin Cash** (a fork of Bitcoin) is a proponent of this solution, and has increased the block size to **32MB**. This gives ~ **200 transactions / second**.
- The problem with increased block size is more network traffic, as well as higher requirements for the nodes => can lead to centralization?

Increased block frequency

- What about increased block frequency? Do we really need to wait 10 minutes for the next block to finish?
- **Litecoin** (a Bitcoin clone), **Ethereum**, and many others have a block frequency of much less than 10 minutes.
- Litecoin creates a new block every 2,5 minutes (and also have larger blocks) => ~ **50 transactions / second**.
- Ethereum creates a new block every 15 seconds, but has room for less transactions per block => ~ **20 transactions / second**.
- The problem with increased block frequency can be security. It is more easy to attack a network with less work done in the proof-of-work.

Data compression



- Bitcoin is quite compressed as it is (all the data is stored in a compact serialized format).
- Could it be even more compressed?
- **Segregated Witness** = unlocking script removed from block
- **Schnorr Signatures** = combining multiple signatures into one
- **Merklized Abstract Syntax Tree (**MAST) = compressing the locking scripts

Sharding

- In a blockchain, **all** the nodes in the network normally validate and store **all** the blocks. What if that is not necessary?
- In Ethereum, something called sharding is proposed as a solution to the scaling problem. (Plan to rollout in 2020/20121)
- Sharding is, generally speaking, that a database is broken in to little pieces called "shards".
- In a blockchain, we can group subsets of nodes into shards, which in turn process transactions specific to that shard. => Parallell processing.
- (The technical solution of synchronizing state across shards is quite advanced)

More centralized consensus (delegated consensus)

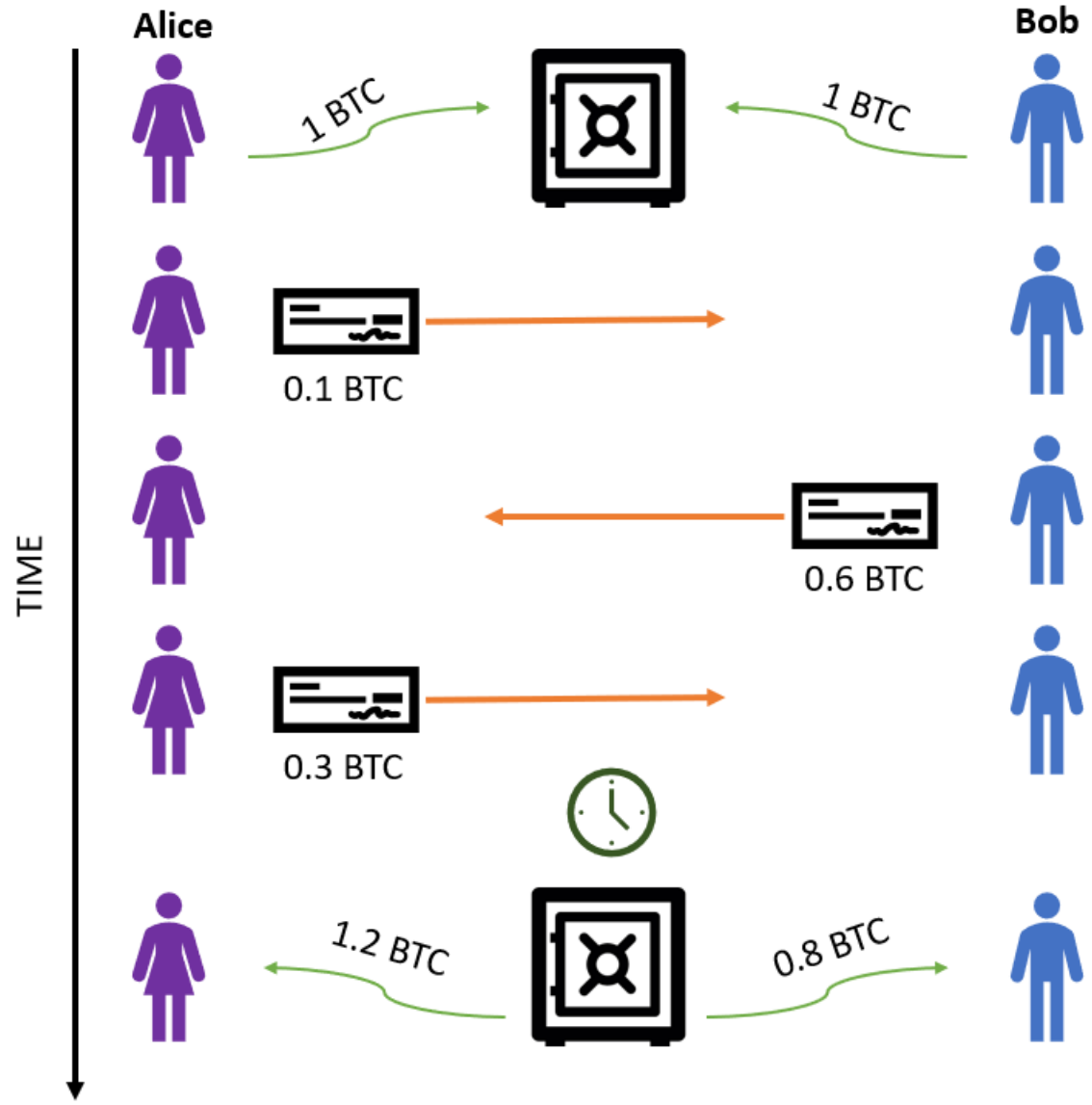
- One argument for a more centralized consensus protocol is that it is faster
- There is less need for networking (/synchronization), and the nodes can be equipped with better hardware.
- Some blockchains use what is called Delegated Consensus (DPoS).
- **EOS** is probably the most discussed example. Claims **1000+ tx/sec**.

- Vitalik Buterin: "EOS's scalability is NOT because of DPOS or anything similar; its claimed scalability comes entirely from the fact that it requires each node to have a much higher computational capacity, making it impossible for anyone but large businesses to run full nodes. We could do that too, but won't because it's contrary to the goals of decentralization."

Off-chain solutions - Payment channels

- It may seem unnecessary to record every little purchase (of a cup of coffee) on the blockchain.
- Why not set up an payment channel (a smart contract) with your local coffee shop, and once in a while send a summary of the transactions to the blockchain.
- In **Bitcoin**, the awaited solution is called the **Lightning Network**.
- In **Ethereum**, the solution is called **Raiden**.
-
- While the previous scaling suggestions only scale "a little" (x2, x5, x10), off-chain solutions can scale "a lot" (x10000+).

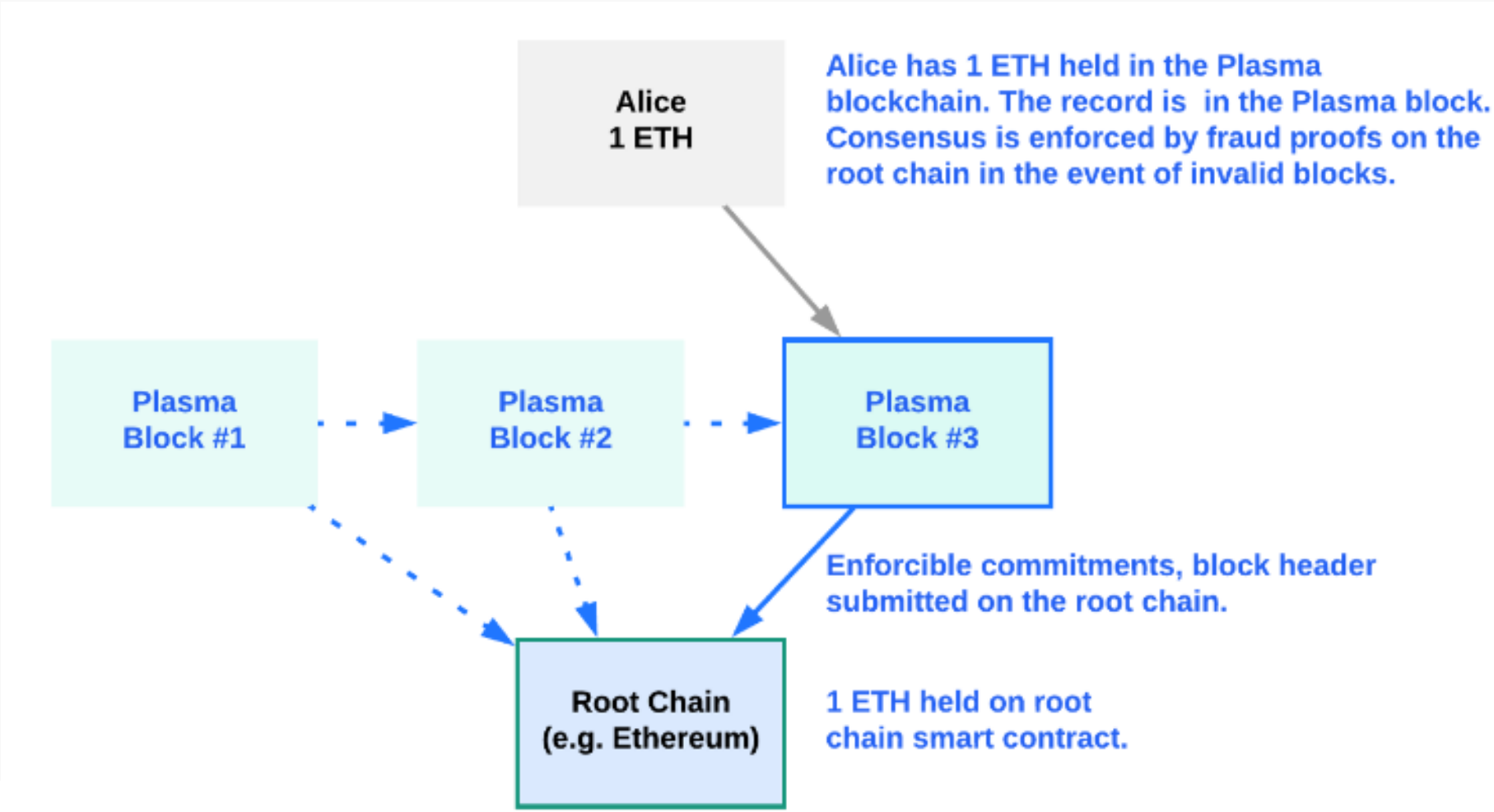
Payment channels (Lightning network)



› See also https://cointelegraph.com/explained/lightning-network-explained for an explanation

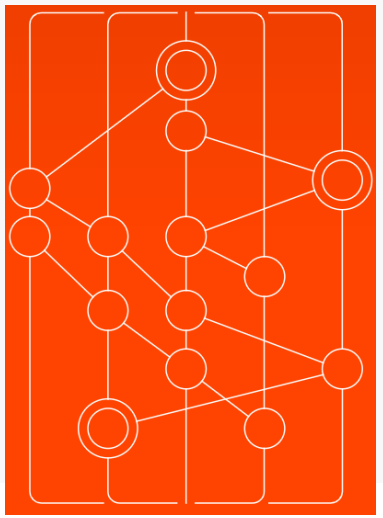
Off-chain solutions - Chains of chains - Ethereum Plasma

https://blog.goodaudience.com/how-omisego-will-bring-plasma-in-everyones-daily-life-45c9d81a3258



Different topologies (DAG, Tangle, Lattice, Hashgraph, ...)

- All the blockchains we have mentioned so far are **chains of blocks**. Can we organize the blocks using other topologies?
- Some have looked at the benefits of using **Directed Asyclic Graphs** (DAGs) as an alternative.
- DAGs have most often no blocks, and are friendly to small, fast payments.
- One benefit can be better scalabilty. A few examples:
  - IOTA **- ~ 500 tx/sec ?**
  - Nano - **~ 7 000 tx/sec ?**
  - IoT Chain - **~ 10 000 tx/sec ?**
  - Hedera Hashgraph **- ~ 100 000 tx/sec ?**



TRANSACTIONS PER SECOND

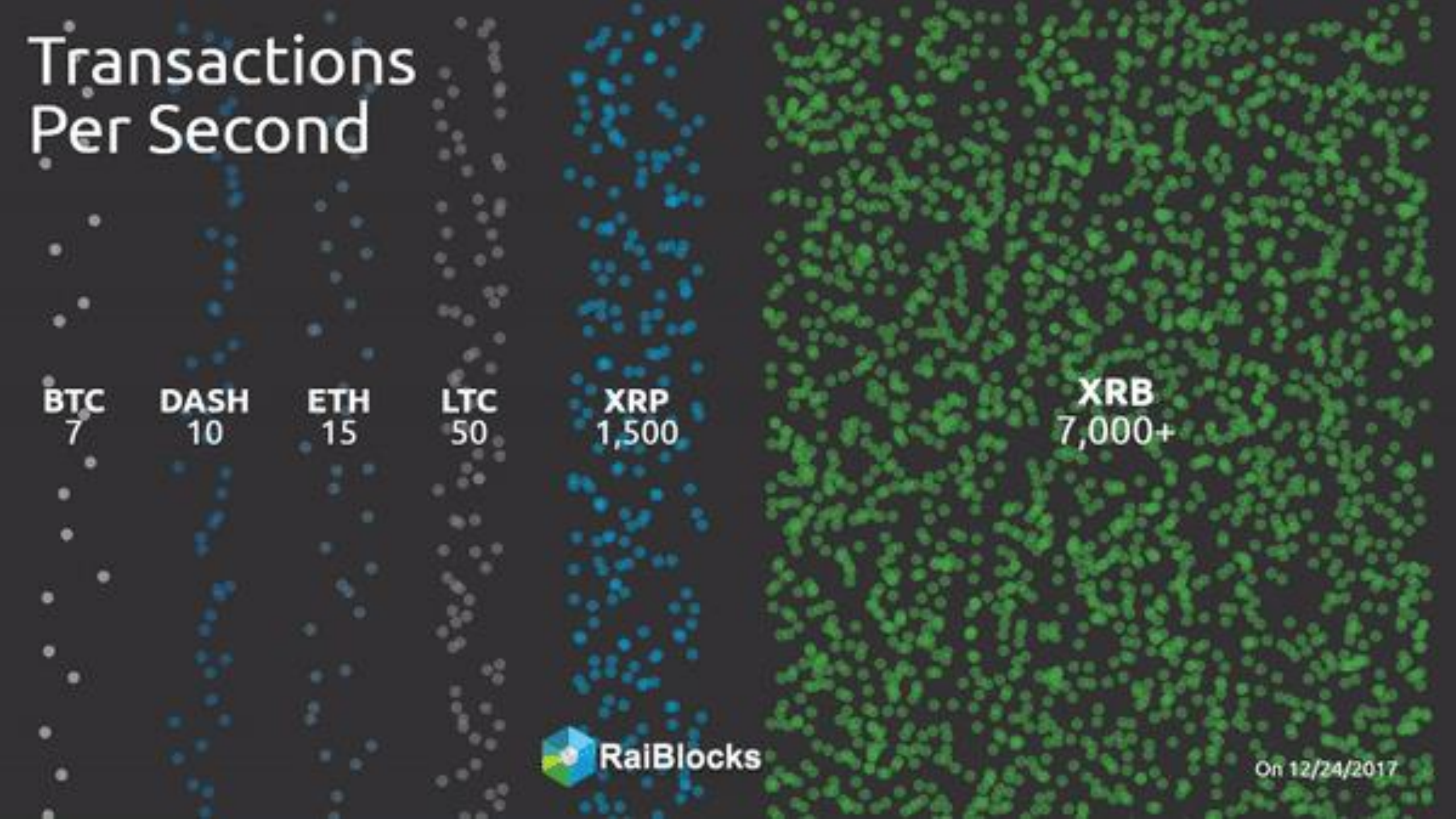
BTC - 7

PayPal - 193

XRP - 1,500

VISA - 56,000

omise (after plasma) (OMG) - 1 MILLION+


Transactions
Per Second
BTC
7
DASH
10
ETH
15
LTC
50
XRP
1,500
XRB
7,000+
RaiBlocks
On 12/24/2017


PHEW!

Module summary - we have looked at

- How a distributed network processes and secures a transaction
- Construction and structure of blockchains
- Distributed trust and consensus, Proof of Work
- Basic building blocks, outputs, inputs, keys, addresses, hashpointers
- Block content and transactions
- Examples of blockchains (e.g. Bitcoin and Ethereum)
- Application areas
- Ecosystems and infrastructure
- Smart contracts
- Possible Scalability solutions

Next

- That's it
- Oblig3 ... (I hope to see some of you Friday @8:15)