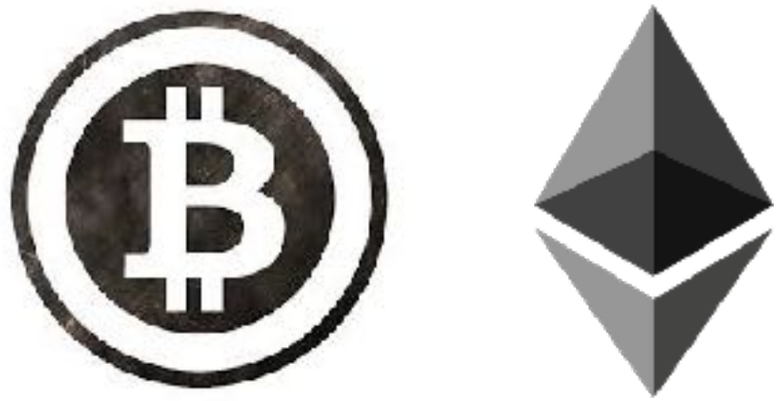
BLOCKCHAIN

intro in layer 8

chris vugrinec Feb - 2018

AGENDA

- *Motivation & Intro*
- *Bitcoin*
- *Ethereum (next gen)*
- *Blockchain, use cases*
- *Enterprise Smart Contracts*
  (Azure Blockchain as a Service)



MOTIVATION – NEW WORLD

Blockchain is revolutionary and will change the world as we know it

Society

Economy

Technology

Society

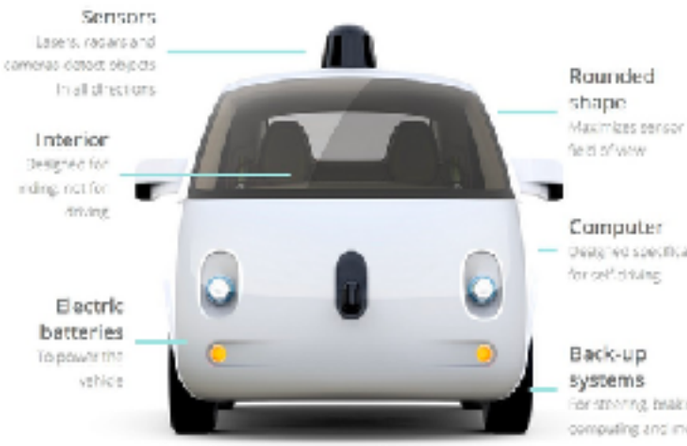
DAO

Decentralized

Autonomous

Organization

DAO

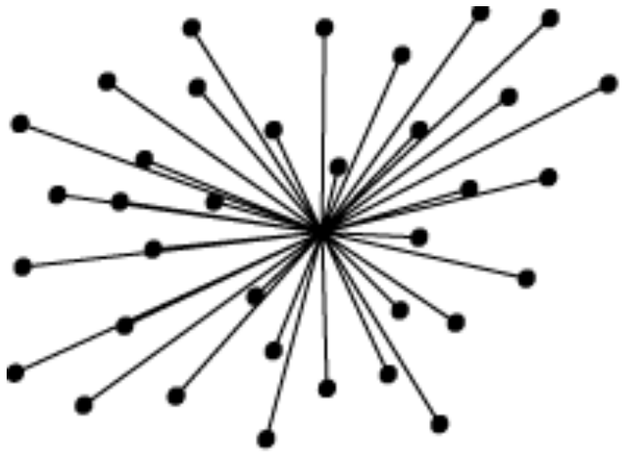


Economy

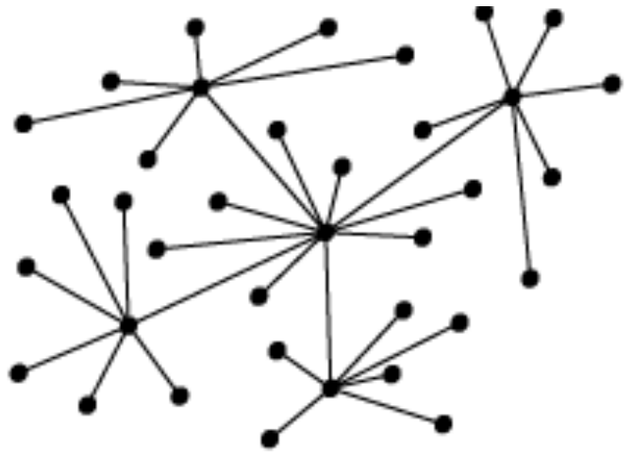
Technology

dApps

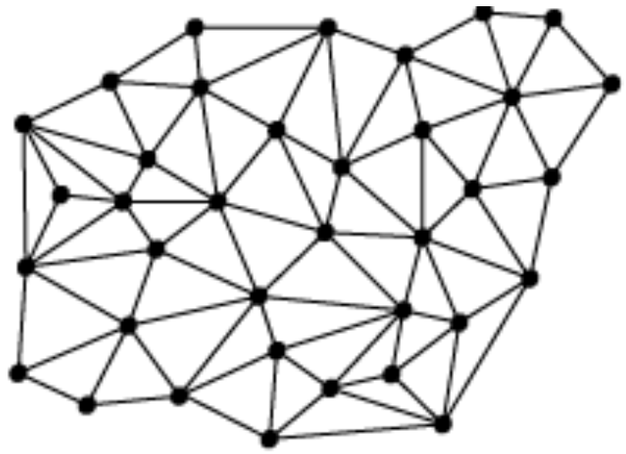
MOTIVATION – ETHICS – INTRO



Centralised



Distributed



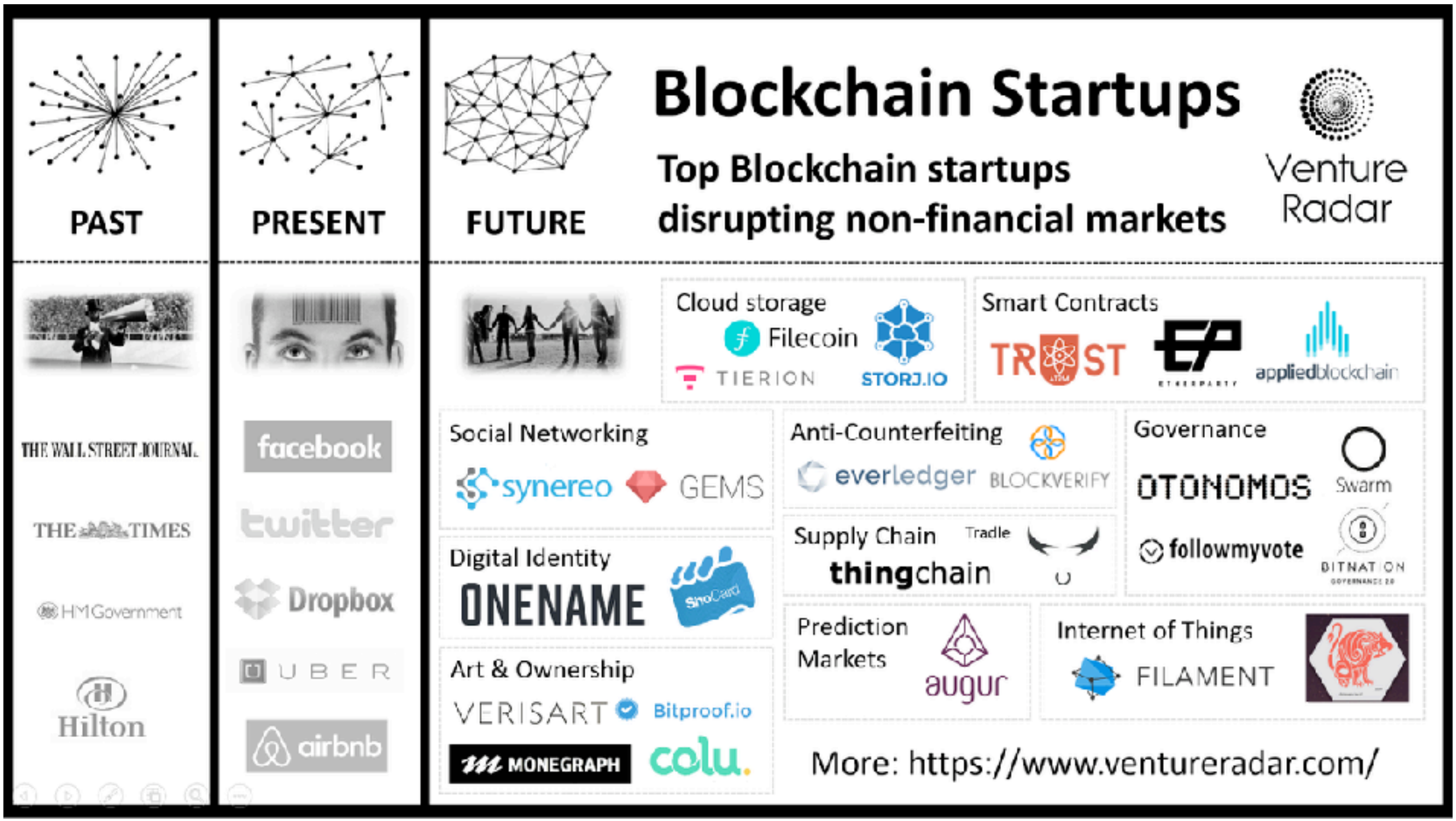
DeCentralised

No more dependencies on traditional centralised institutes

no exclusion, all is equal

knowledge open sourced

PAST – PRESENT – FUTURE



BITCOIN – THE 1ST (BATTLE TESTED)

2008: Whitepaper Satoshi Nakamoto, after banking crisis

2009: 1e tx (blockchain.info)

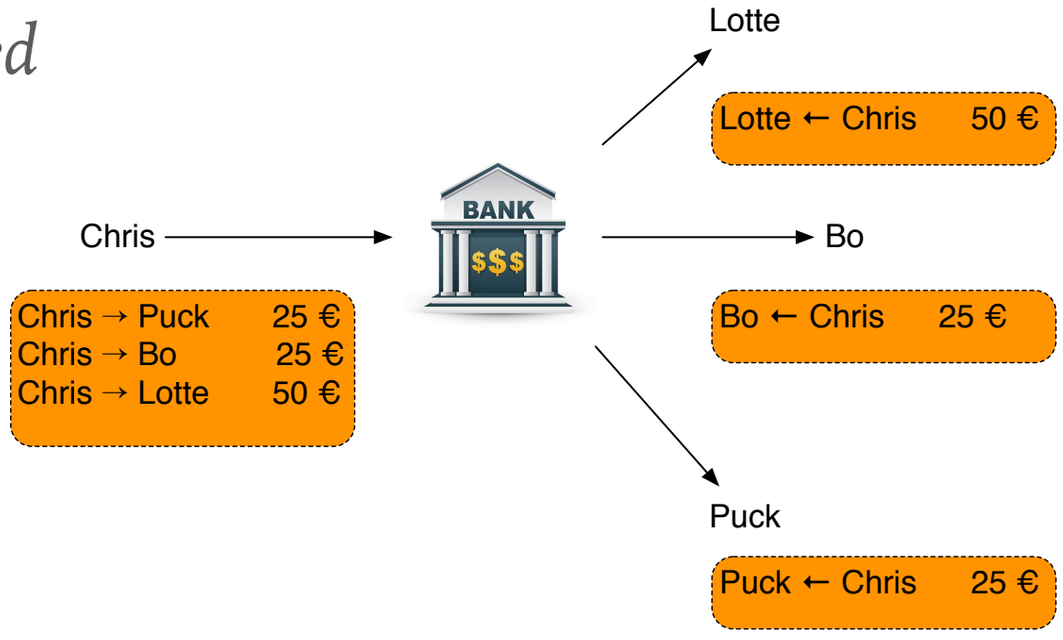
What is it: currency, network, protocol, language

Goal: Internet of Money, Decentralised money available for everyone

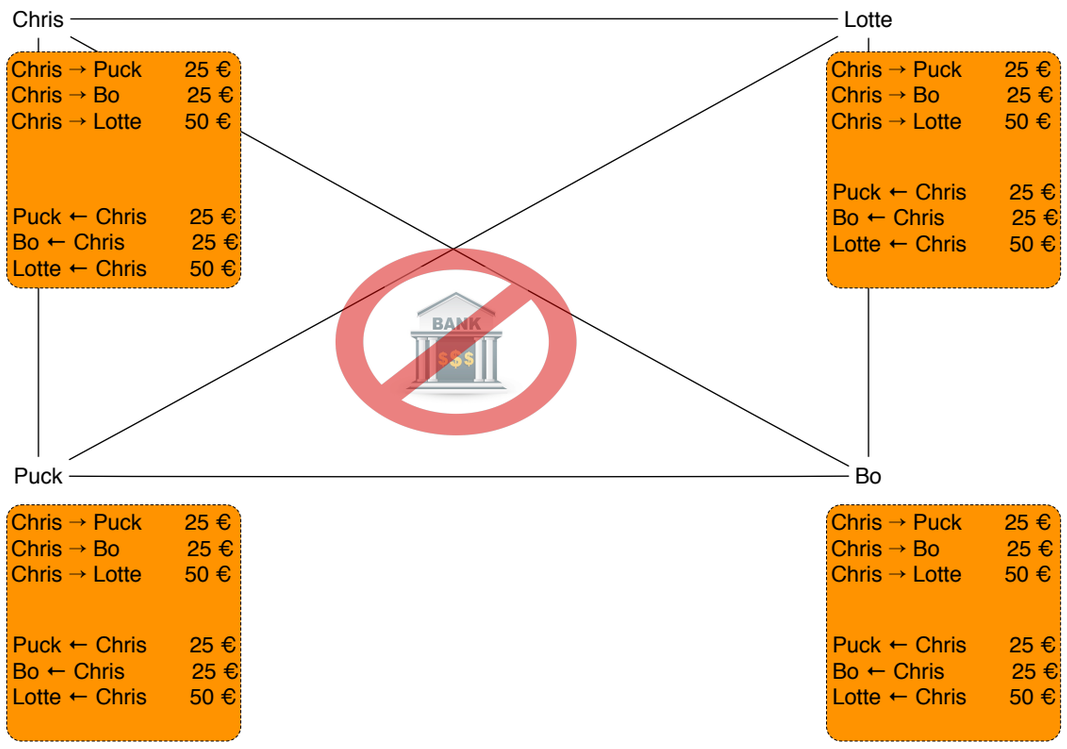
How: Intro in Blockchain (1st to mention blockchain in whitepaper)

DISTRUBUTED LEDGER

Centralised



Decentralised



Problem

How do you make sure that everyone has the same copy of the ledger and that all TX's are registered in the proper order

Byzantyne Fault Tolerance

Double spending

CONSENSUS – BASICS

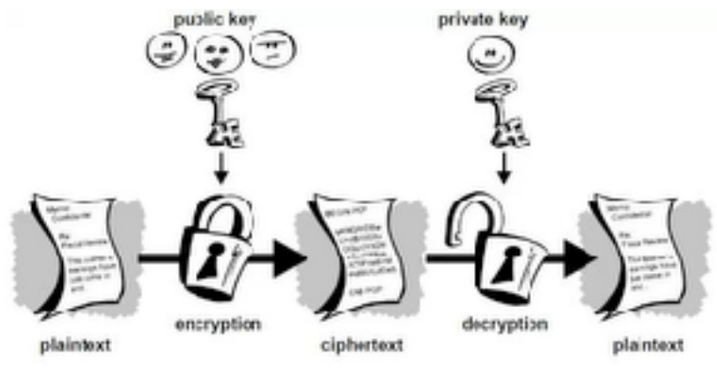
Longest (block)chain = most computational work = Correct ledger

Why not cheat: Incentive: compute power → Block reward + TX Fee = Mining!

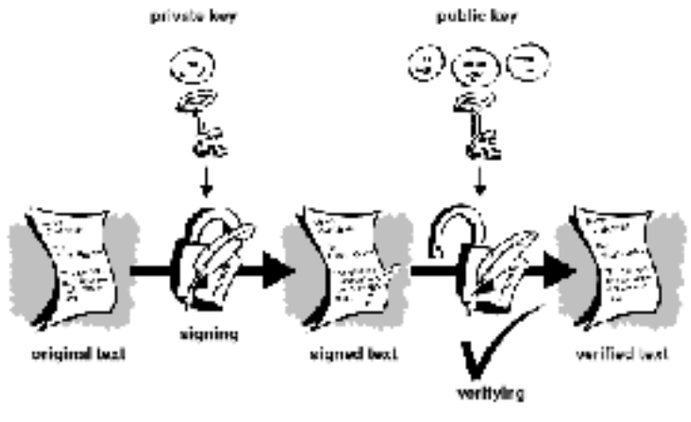
Crypto: Hash/ fingerprint/ Asymmetric Keys

***sign**(message,priv key); **verify**(message, signature, pub key)*

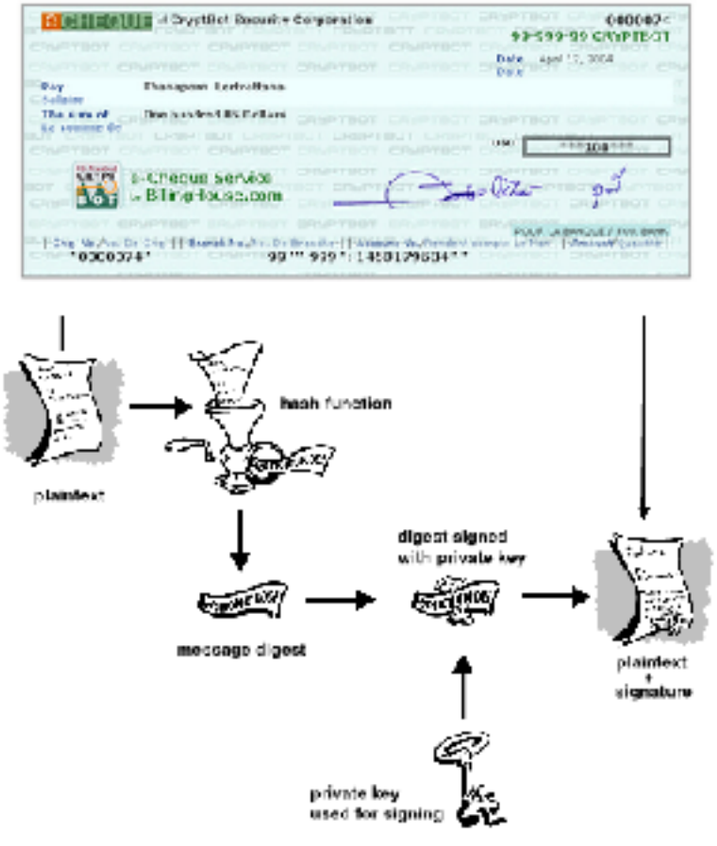
Hashing



Encryption

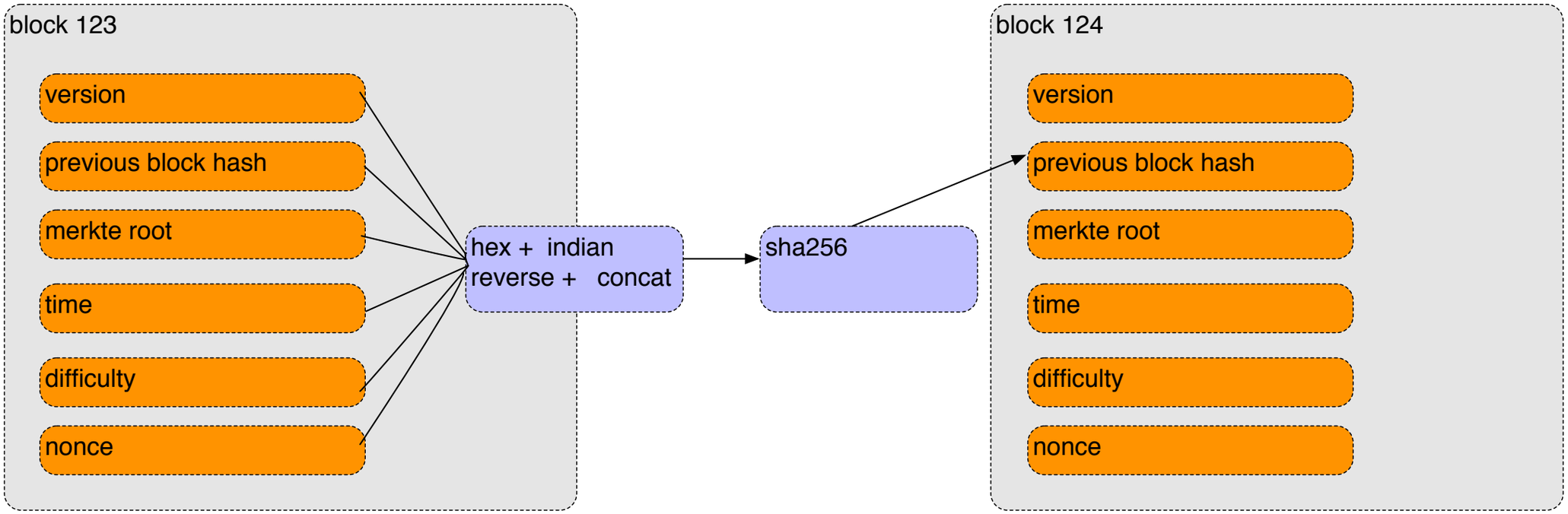


Signing



Signing of TX

BLOCKS - CHAINS



https://blockchain.info/

Block: # 123

Nonce: 11934

Data:
chris --> lotte = 50
lotte <-- chris = 50

chris --> puck = 25
puck <-- chris = 25

chris --> bo = 25
bo <-- chris = 25

Prev: 00000000000000000000000000000000000000000000000000000000000000000

Hash: 00000a72b6343f3aed9bdc9331acb8a84f8af899875b13123f7550914bfd74a

Mine

https://anders.com/blockchain/blockchain.html

Block: # 124

Nonce: 67365

Data:
chris --> lotte = 150
lotte <-- chris = 150

Prev: 00000a72b63343f3aed9bdc9331acb8a84f8af899875b13123f7550914bfd74a

Hash: 00007bcffcc5cc5598b5eb7734c8ef88f53cad0c9da987aaadacc53be8af6269

Mine

MINING - PROOF OF WORK

securing network

censensus - who (which miner) is allowed to add Block with TX

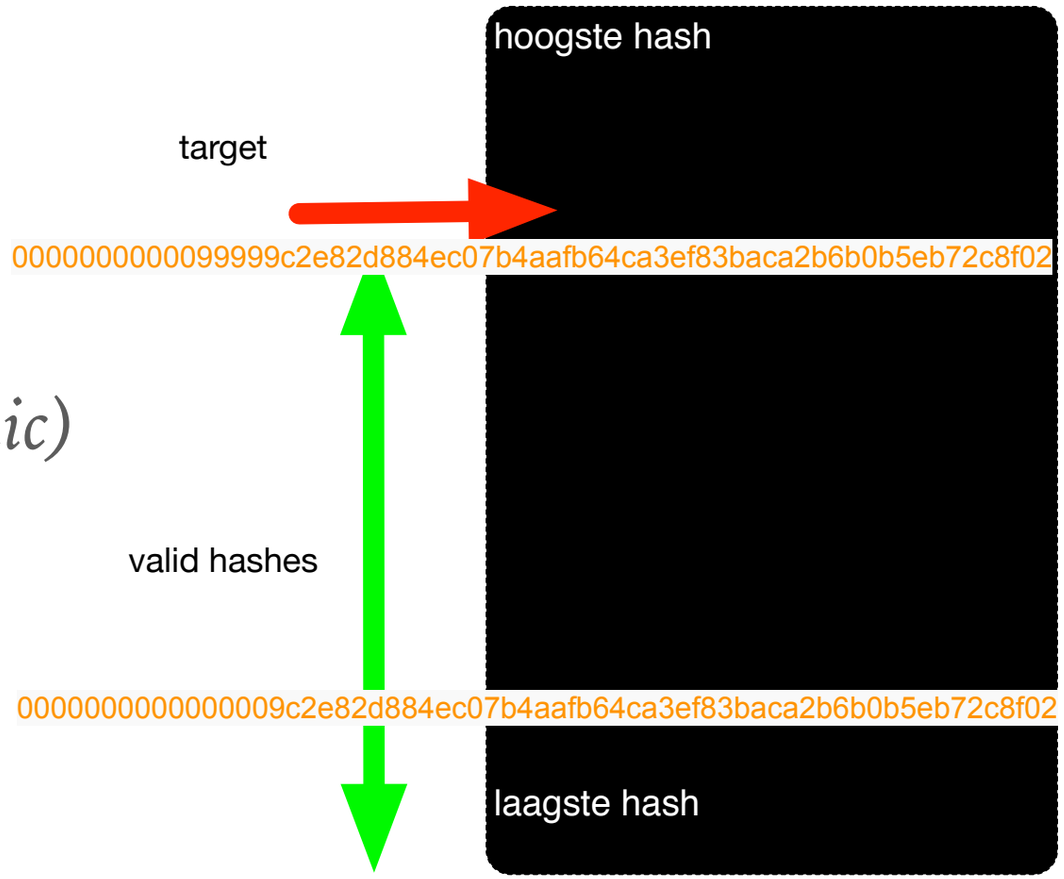
Winner of crypto puzzle gets: TX fee and Block Reward

- *Wallet*
- *Merkle Tree*
- *UTXO*

Guessing random nummer (nonce)

hash of block + random nr < mining target

lower target == more difficult to guess (dynamic)



hash rate: sha256(block + nonce) , check within valid hash range?

POW alternatives - Proof of Stake, Proof of Importance

MINING – WHAT DOES IT PAY

block rewards:

Jan 2009 - Nov 2012: 50 BTC

Nov 2012 - Jul 2016: 25 BTC

Jul 2016 - Feb 2020: 12.5 BTC

Feb 2020 - Sep 2023: 6.25 BTC

etc etc

ant miner s9 (asic)

every 210.000 Blocks , about 4 years (block time: 10 min)

Miners get block rewards + fee,

Electricity costs in NL (feb 2018) , 1.500 EUR p BTC

ETHEREUM – BITCOIN 2.0

- *bitcoin has simple script(scrypt) - but no complex computations (not turing complete)*
- *bitcoin only internet money, not possible to create own logic (smart contracts)*
- *bitcoin only stores TX, Ethereum can store anything (sky is the limit)*
- *EVM; Ethereum Virtual Machine, solidity*
- *Gas: Eth is turing complete, for eg. loops (https://ethgasstation.info/)*
- *ICO's - funding*
- *etherscan.io , bijv https://etherscan.io/address/0xc0ADF1CCc703A0a3393892600883A1A91a4E38de#code*

SMART CONTRACTS & TOKENS

- *Differences Coins and Tokens (https://coinmarketcap.com/)*
- *Smart contract vs ERC 20 token (eth)*
- *Any change of state of contract is recorded as TX*
- *Alternatives: Lisk, NEO, (EOS, Cardano 3.0 ???)*

ERC-20 Interface spec

functions

- *totalSupply*
- *balanceOf*
- *allowance*
- *transfer*
- *approve*
- *transferFrom*

events:

- *Transfer*
- *Approval*

Nodig om met Wallet te kunnen communiceren

Smart Contract

contract someContract{}

ERC20 Token

contract someERC20Token is ERC20Interface{}

BLOCKCHAIN – IS GOOD FOR…

golden hammer (anti pattern)

Provenance *(herkomst)*

- *Tracking…no one can change just any record, all changes are recorded as TX, for eg transport, or money flows*
- *Transparency, all is open, this is good against corruption*
- *Ask yourself, why not use a regular database:*
  Database is centralised and maintained, you need to be able to trust this centralised party.

Consensus

- *Agreement by nodes. No* ***central*** *authority. Consensus driven by incentives (mining)*
- *No more need for middleman. Middleman often expensive and slow*
  for eg Western Union, you do not want this…and it is not needed
- *Information Silos…By centralised systems, inefficient storage and communication of data*

BLOCKCHAIN – IS GOOD FOR

Security and Immutability

- *In Bitcoin hashing is used for security…more is safer*
  Globally..no middleman. Proof of ownership…
  put product on blockchain…it is immutable,
  New global Infrastructure

- *Much safer..as not depended on 1 party*

High availability

- *Almost impossible to shut down, runs 24 x 7 (like torrent). Makes it suitable for missional critical systems,*
  there is always someone in the world who is up and running and making your ledger/contract available.
  global highly available database.

Finality

- *Transaction Finality; unless programmed nothing can be put back to original or changed…onc the (smart) contract is*
  created, everything is registered

- *Trustless businesses, but be aware you need good programmers…a fault in contract can lead to hacks*

BLOCKCHAIN – USE CASES (NON FINANCE)

Blockchain manufacturing

- *transparancy & accountability*
- *origin tracking*
- *real time data*
- *informational siloes*
- *certification and documentation*

Blockchain Healthcare

- *Send Information safe from 1 entity to the other*

Customer Loyalty

- *Liquiditeit by using tokens*
- *Airmiles can have real value…altcoins*

Real Estate

- *Waiting lists..people within organisation can put their family ahead…not possible with blockchain*
- *Corrupt countries….ownership is impossible to change as everything is recording on ledger*

BLOCKCHAIN – USE CASES

Insurrance

- *Fraud and Risk*
- *Inefficiency*
- *Explosion of Data*
- *No Global Track Record*

Evidence of facts by using blockchain in combination with IOT (sensors)
Proving you are a good driver or farmer (biological food)

Accountancy

- *Alle actions are registered…possibly the best audit-able system*

Advertising

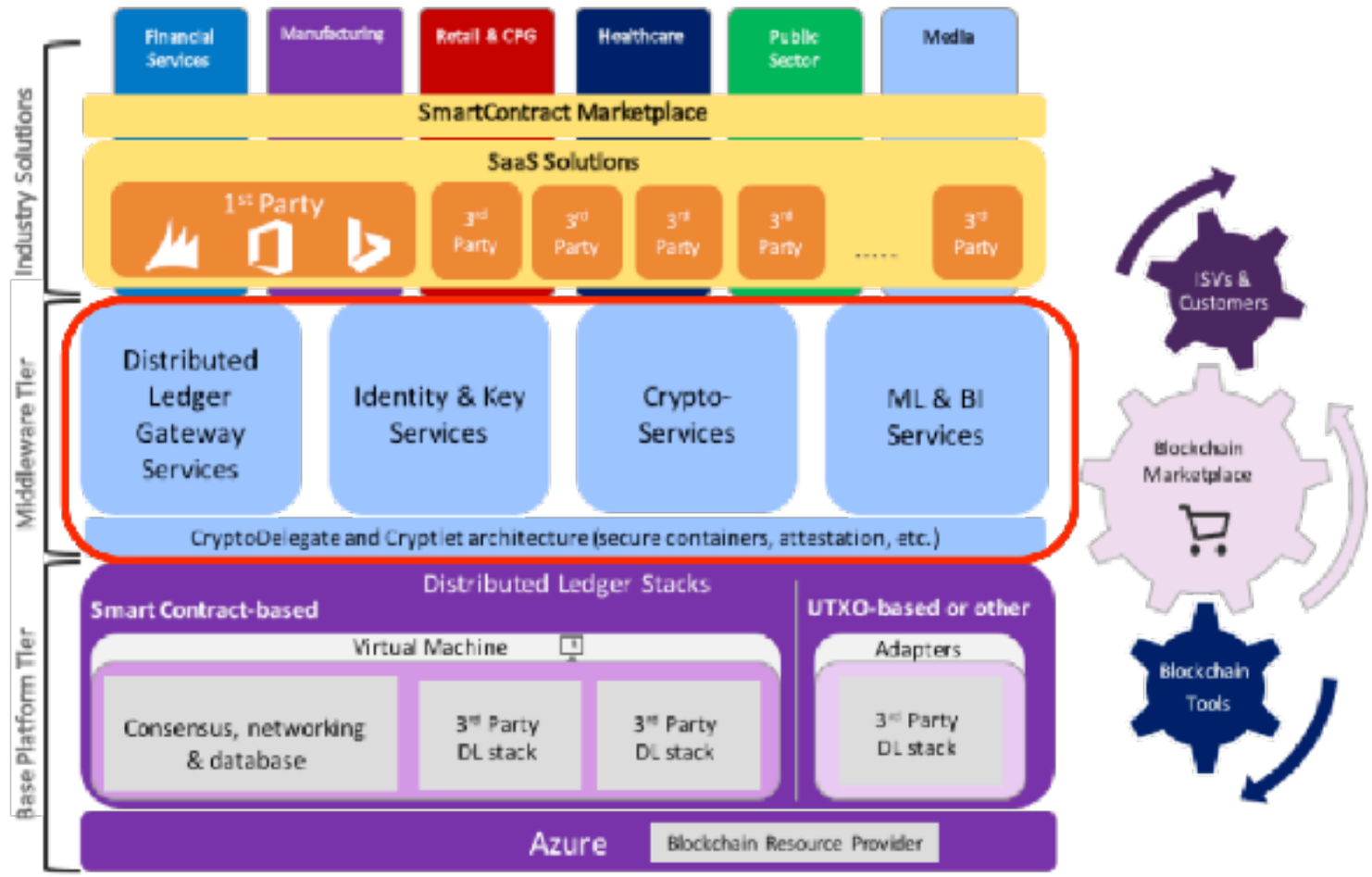
- *Lack of transparancy*
- *Fraud*
- *Immitations*
- *Middlemen*
- *Privacy*

For eg how many people actually saw the advertisement..currently no transparency

without middleman better transparant agreements can be made with customers
No middleman is for eg…make people watch personalised content and pay them for it (vice)

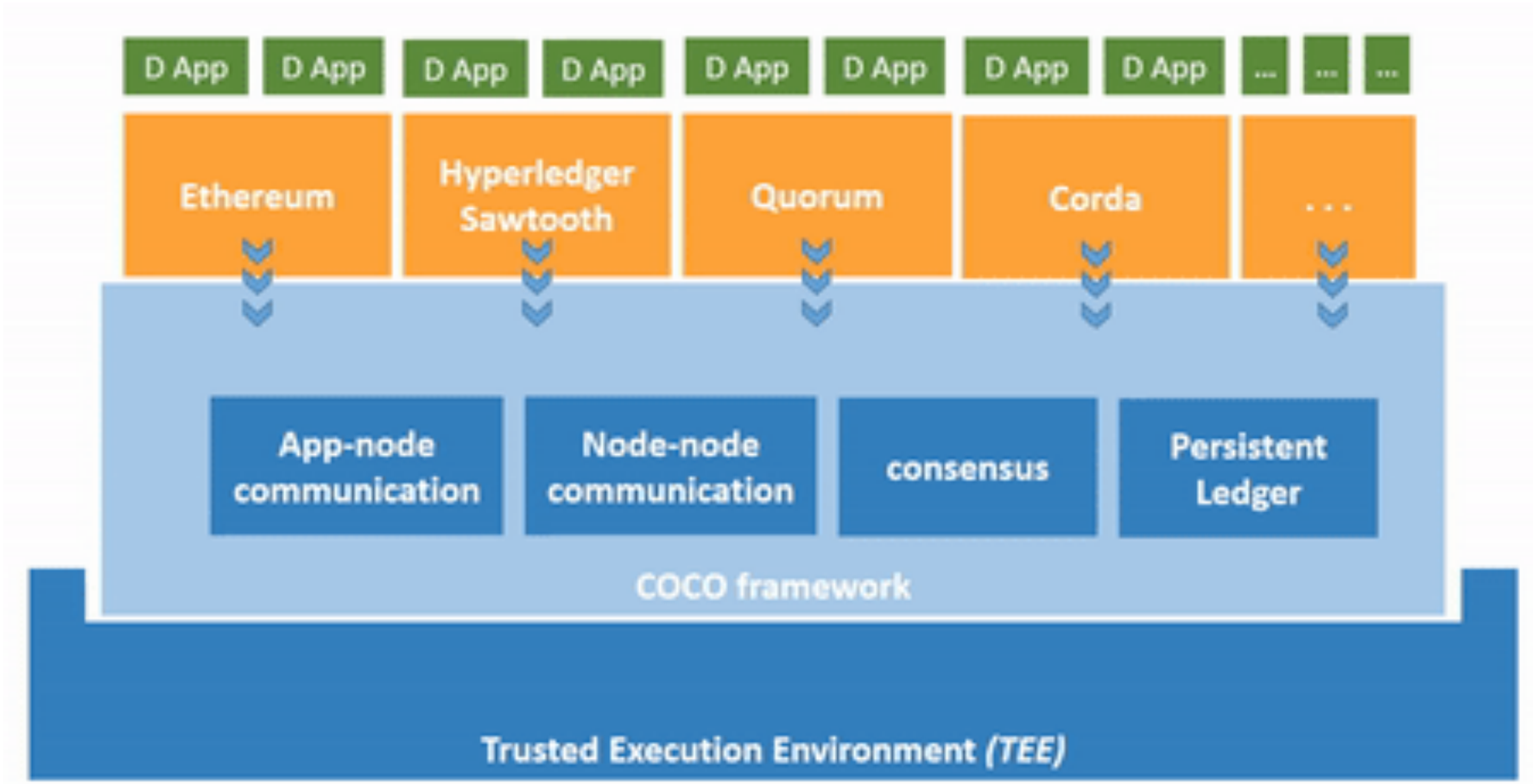
ENTERPRISE SMART CONTRACTS

- *Permission based Blockchain solutions*
- *Not perse public blockchain*
- *Emphasis on B2B solutions*
- *Re usable (secure) components*



AZURE – BLOCKCHAIN AS A SERVICE

- *Bletchley: dApp framework and integration with Paas/ Saas (vorige slide)*
- *Coco: Inter blockchain communication*
- *Alternatieven: Hyperledger (IBM), Stratis, Multichain & Quorum*



LAB – PGP

generate private key

openssl genrsa -out private.key

generate public key

openssl rsa -in private.key -pubout -out public.key

create text file

echo “hello world this is a demo” > sometekst.txt

encrypt file with public key

openssl rsautl -encrypt -pubin -inkey public.key -in sometekst.txt -out sometekst.cipher

decrypt file with private key

openssl rsautl -decrypt -inkey private.key -in sometekst.cipher

create SHA 256 Hash

echo “hello world” | openssl dgst -sha256

create fingerprint

openssl dgst -sign private.key -sha256 sometekst.txt >sometekst.signature

check fingerprint

openssl dgst -sha256 -verify public.key -signature sometekst.signature sometekst.txt

generate private key
openssl genrsa -out private.key

generate public key
openssl rsa -in private.key -pubout -ou

create text file
echo “hello world this is a demo” > so

encrypt file with public key
openssl rsautl -encrypt -pubin -inkey p
sometekst.cipher

LAB – CREATE SMART CONTRACT AND NET

https://openzeppelin.org/

solidity : http://remix.ethereum.org, documentation : http://remix.readthedocs.io/en/latest/

Meta mask

- *Install: https://metamask.io*
- *Create account, edit change name*
- *put ether on wallet: https://wiki.graveslab.org/ or http://faucet.ropsten.be:3001/*
- *Send eth from wallet to contract/ token*

Petshop demo - truffle framework

- *http://trufflframework.com/tutorials/pet-shop*

github: https://github.com/chrisvugrinec/blockchain-lab/