Blockchains

Cryptocurrencies and Consortium Blockchains

Tero Keski-Valkama, Elisa Patronen

2017-02-2

What is Blockchain

- Blockchain is a collection of cryptotechnologies to achieve a distributed consensus about immutable, additive data in an untrusted environment.
    1. Blockchain is a sequence of records, or blocks, so that each block contains a hash digest of the previous block (which recursively contains the hash digest of the previous block and so on).
    2. A consensus mechanism with rules to determine which blocks are accepted to be the next block in the blockchain. Many solutions such as proof-of-work, proof-of-stake, proof-of-burn, Practical Byzantine Fault Tolerance, and hybrids.
    3. A discovery and broadcast infrastructure to relay transactions and blocks to peers and miners.
    4. Application-specific public key or other cryptography to prove identities of parties in transactions, wallets and so on.
    5. Microcode used to define the transaction semantics or smart contracts, such as Bitcoin Script, Solidity or Chaincode.
- In blockchain, a single valid block can be used to validate the whole chain of blocks to deep history so that anyone can make sure that nothing has been altered in the stored data, by checking that the hashes of the previous block always matches the content of the previous block.
- The consensus mechanism offers guarantees that all parties have a converging view in the blockchain regarding what is valid and what is not. It prevents changing the history and that the whole blockchain integrity is guaranteed.

There Shall Be No Blockchain But Bitcoin

click

Example of a Consortium Blockchain: Hyperledger Vision

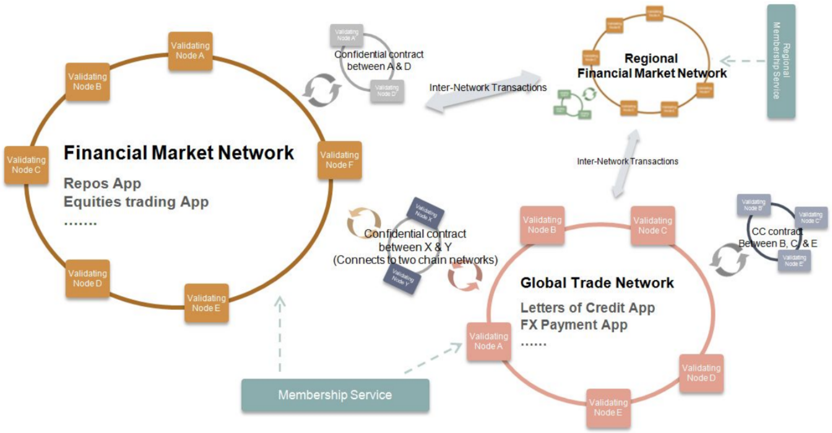

Financial Market Network
Repos App
Equities trading App
....
Validating Node A
Validating Node B
Validating Node C
Validating Node D
Validating Node E
Validating Node F
Confidential contract between A & D
Inter-Network Transactions
Regional Financial Market Network
Regional Membership Service
Inter-Network Transactions
Confidential contract between X & Y (Connects to two chain networks)
Global Trade Network
Letters of Credit App
FX Payment App
......
CC contract Between B, C & E
Membership Service

Figure: Hyperledger Vision[1]

[1] Hyperledger Whitepaper – academic fair use

Example of a Consortium Blockchain: Hyperledger Architecture

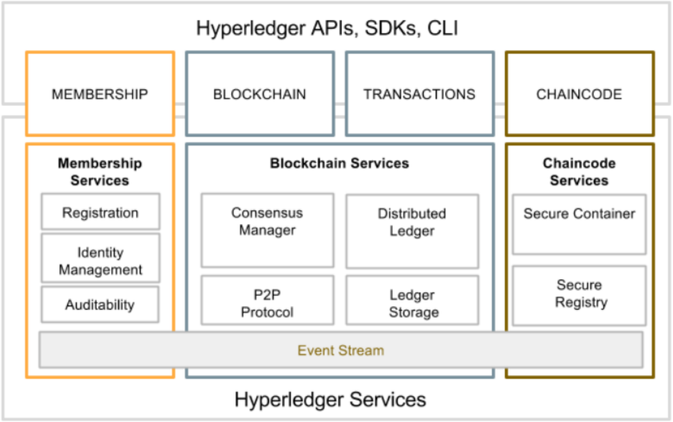


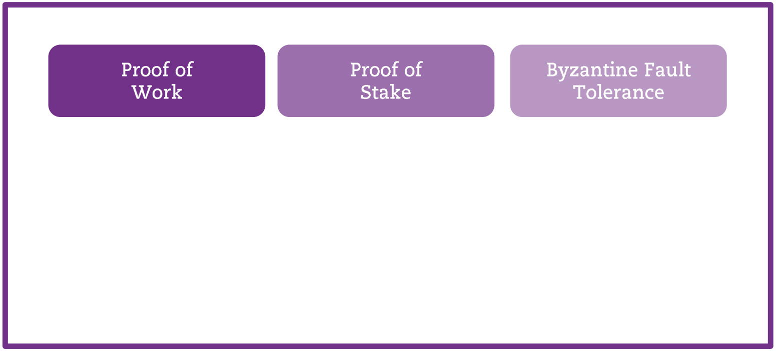
Figure: Hyperledger Architecture[2]

[2] Hyperledger Whitepaper – academic fair use

Comparison of Associated Technologies

	Distributed Database	Consortium Blockchain	Cryptocurrency Blockchain
Consensus mechanism	Simple parallel consistency	Byzantine Fault Tolerance	Proof-of-Work, Proof-of-Stake, or a hybrid
Requires a cryptocurrency	no	no	yes
Access	Closed	Controlled	Open
Peers	None	Validated	Untrusted

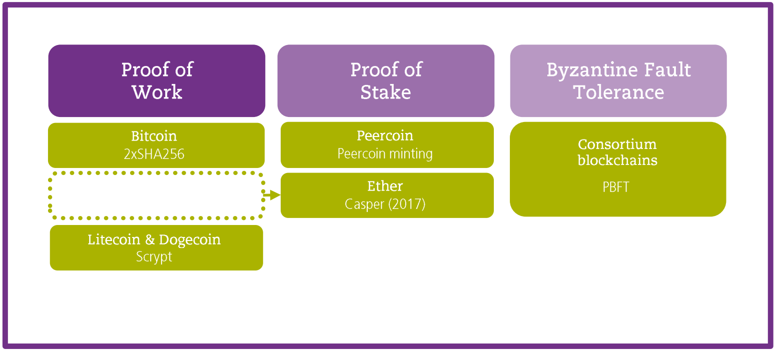
3 kinds of consensus algorithms



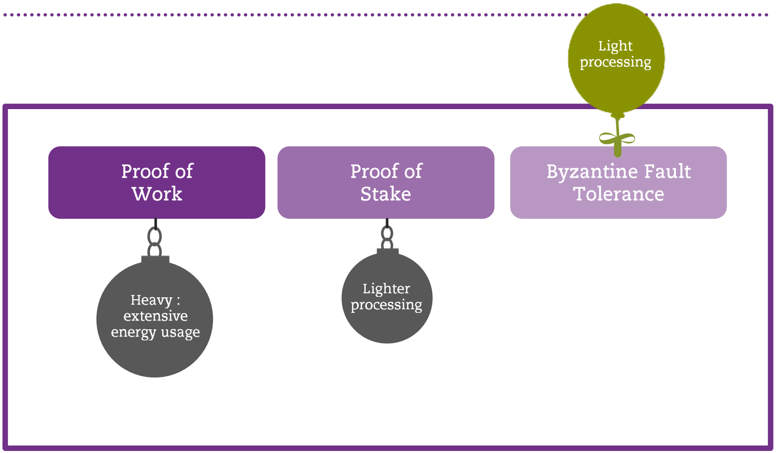
3 kinds of consensus algorithms

Proof of Work	Proof of Stake	Byzantine Fault Tolerance
Bitcoin 2xSHA256	Peercoin Peercoin minting	Consortium blockchains PBFT
Ether Ethash		
Litecoin & Dogecoin Scrypt		

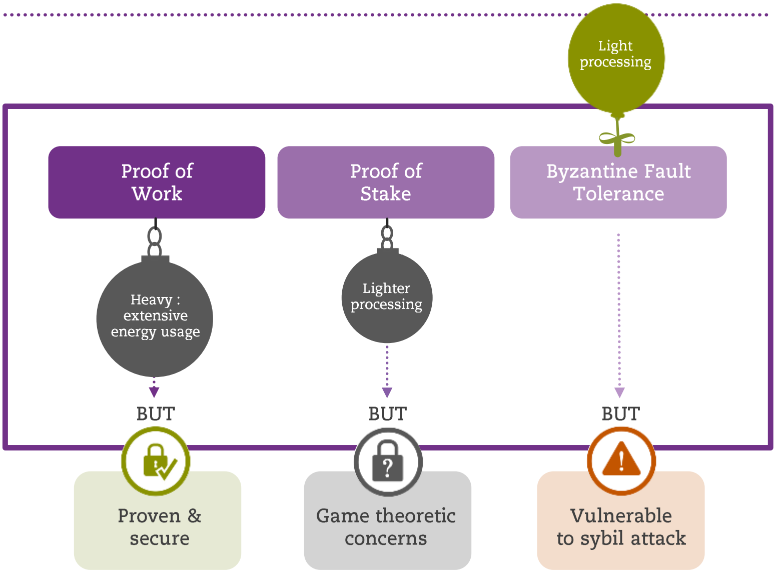
3 kinds of consensus algorithms



3 kinds of consensus algorithms



3 kinds of consensus algorithms



Consensus Mechanisms – Starting from Bitcoin

- Consensus is inherently a game theoretic concept in Byzantine systems, because the peers can try to cheat.
- In open ecosystems it must be made economically infeasible to break the rules or the goals of the system. This leads to the requirement of having a cryptocurrency built into the system. In practice, a validating peer gains cryptocurrency for processing transactions, and this cryptocurrency only has value if the whole system works.
- The Bitcoin network can process the maximum of 7 transactions per second with the current block size limit of 1 MB.
- Calculating Bitcoin mining hashes requires about 1 W of power for 1 GH/s of computation for the most energy efficient ASIC implementations.
- The current hashrate of the Bitcoin network of 3,051,683,778 GH/s translates to a power of about 3 GW.
- In standard reindeers of 200 kg, this amounts to burning 2.25 reindeers of equivalent coal every second.
- In closed consortiums, it is feasible to get rid of peers behaving incorrectly, so expensive proof-operations can be avoided.

click

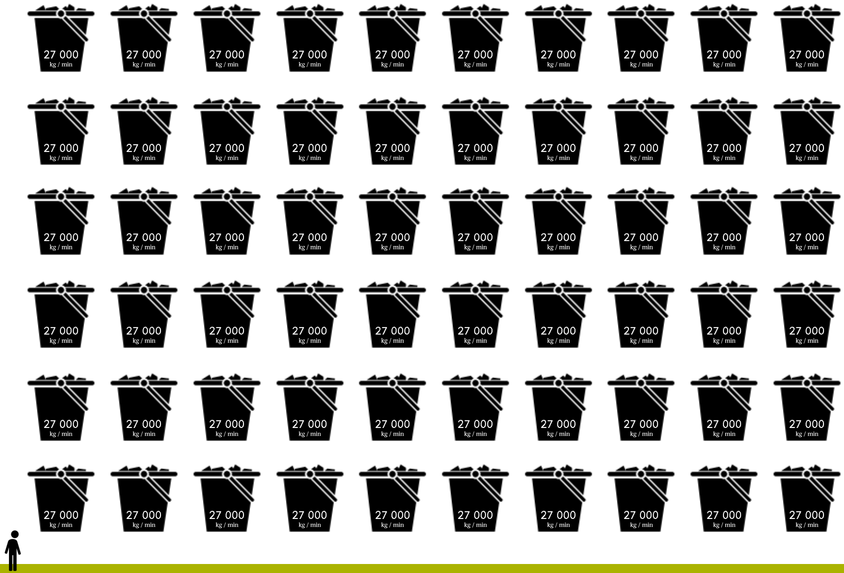
Bitcoin Network Burns

27 000 kg

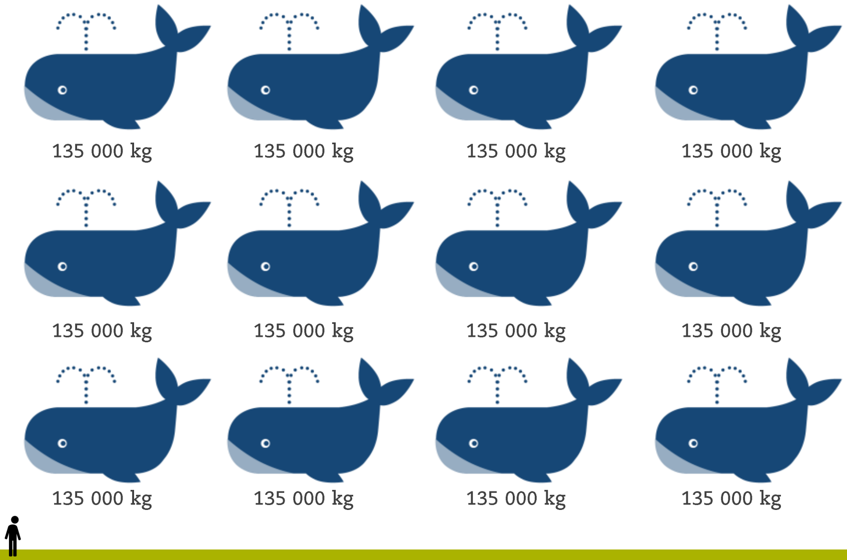
coal in only

1 minute

..Which means 1 620 000 kg per hour



..Or approximately 12 blue whales!



Proof of Work – Bitcoin, Litecoin, Dogecoin, etc.

- The point of Proof-of-Work is to prove that you have spent real resources in generating the block.
- Proof-of-work algorithms include for example Bitcoin double SHA256, or Dogecoin/Litecoin Scrypt.
- Bitcoin includes a double SHA-256 hash of the block in the blocks, and the block is only accepted if the hash value is lower than the difficulty limit. Hence, block hashes start with lots of zeros, for example: 0x000000000000000012fdce7dd73fddb087e66f4f6bb9672667b854282855669 for the block #451676
- Bitcoin Proof-of-Work does not require a lot of memory and can be easily implemented as an ASIC chip → all miners are based on cheap ASICs now, and the hashrate is basically limited by energy costs. These ASICs are special-purpose machines and cannot be used for any other purpose than mining Bitcoins.
- Litecoin and several other coins use Scrypt algoritm as Proof-of-Work. This algorithm requires more memory (128 kB to match a typical CPU L2 cache), and memory is difficult to implement on an ASIC. Litecoin and Dogecoin can be mined with general purpose GPUs and even CPUs, and even in browsers. This has an effect of moving the bottleneck towards more expensive, but ubiquitous general purpose hardware from simple energy use.

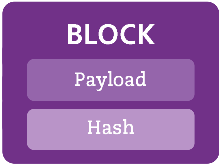
Proof of Stake – Ether after 2017, Peercoin

- Proof-of-Stake is a proposed alternative to energy wasting Proof-of-Work. Instead of proving you have done work, you prove you own a number of coins.
- Generally, for each block each coin gets a random chance of determining the next block.
- In 2017, Ethereum (Ether) moves to Proof-of-Stake algorithm, Casper. Some cryptocurrencies use a hybrid between Proof-of-Work and Proof-of-Stake.
- Game theoretic worries: If the miners have no stake, why would they play fair?

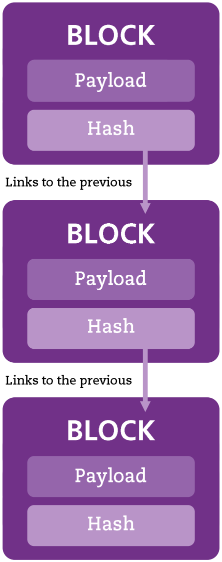
Byzantine Fault Tolerance

- Byzantine Fault Tolerance refers to a general game theoretic mathematical problem where distributed parties try to achieve consensus in spite of unreliable messaging and hostile actors.
- There are several algorithms and implementations with different characteristics.
- Practical Byzantine Fault Tolerance algorithm useful for consortium blockchains, but cannot be used for open blockchains.
- Byzantine Fault Tolerance algorithms do not generally consider an open system where new actors can join at will, and therefore they implicitly assume a kind of a Proof-of-Stake through association to the group.
- These algorithms generally need a centralized identity management to prevent a Sybil attack. Although it could be said that the centralized identity manager could freely perform a Sybil attack in these systems.

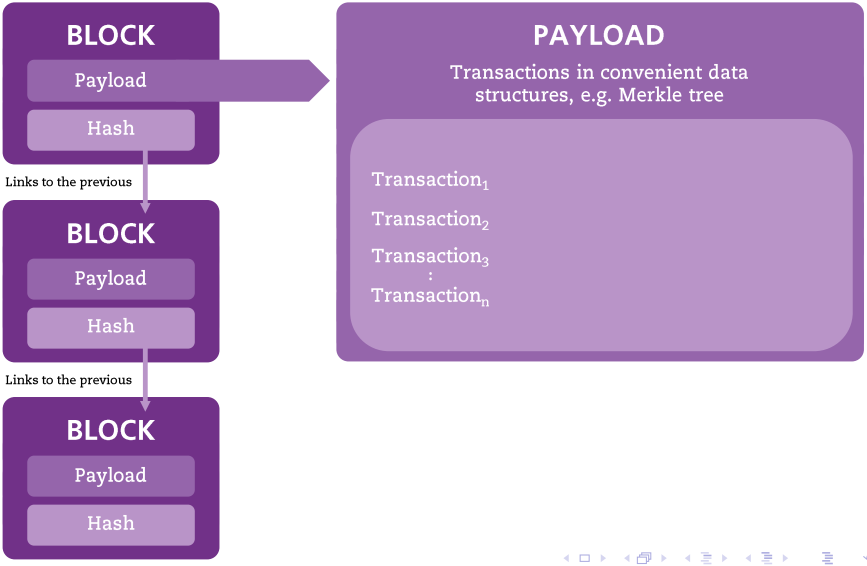
Inside of a blockchain



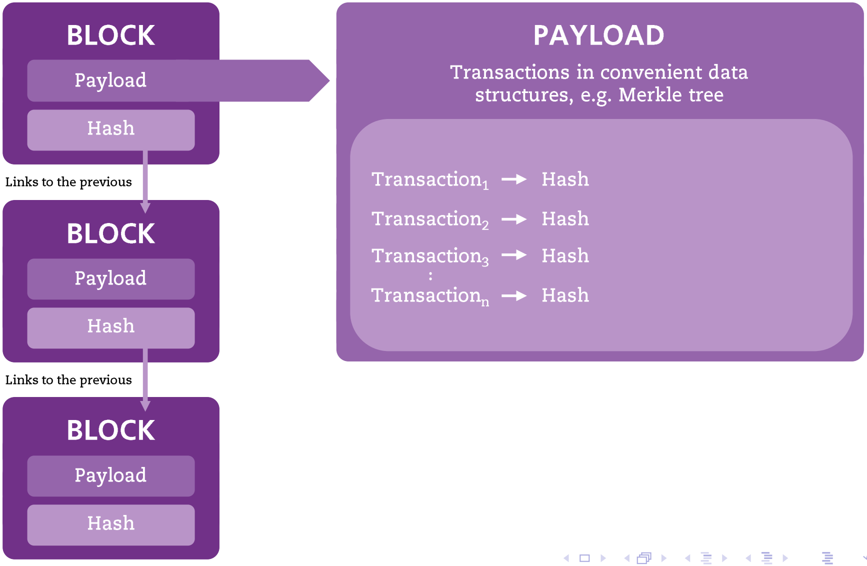
Inside of a blockchain



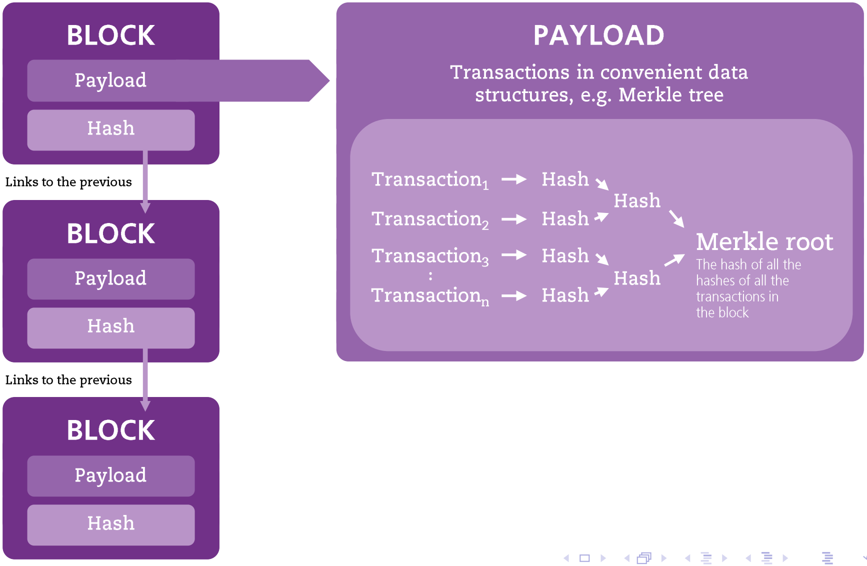
Inside of a blockchain



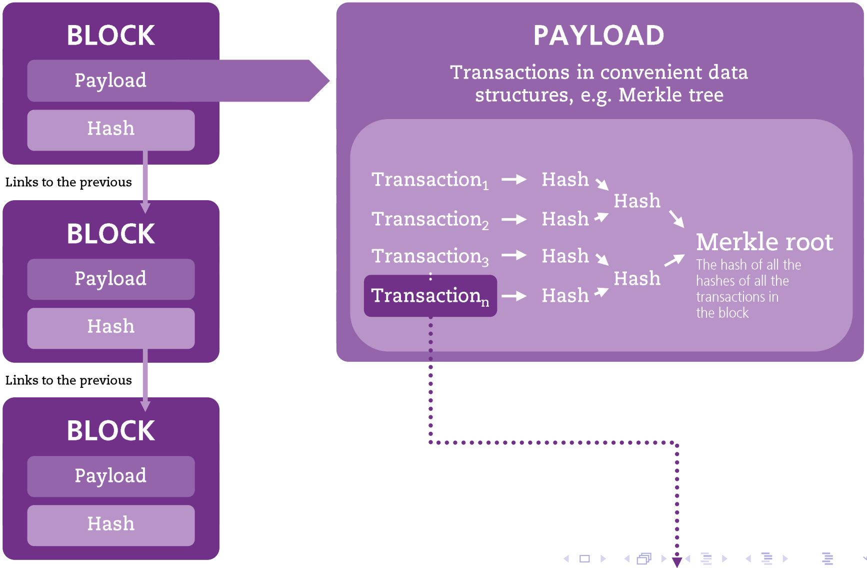
Inside of a blockchain



Inside of a blockchain



Inside of a blockchain



Transaction

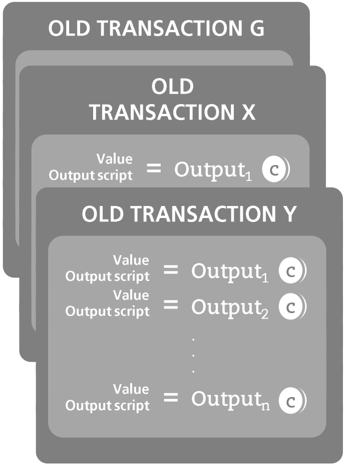
Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated

Transaction

Includes chaincode script that determines

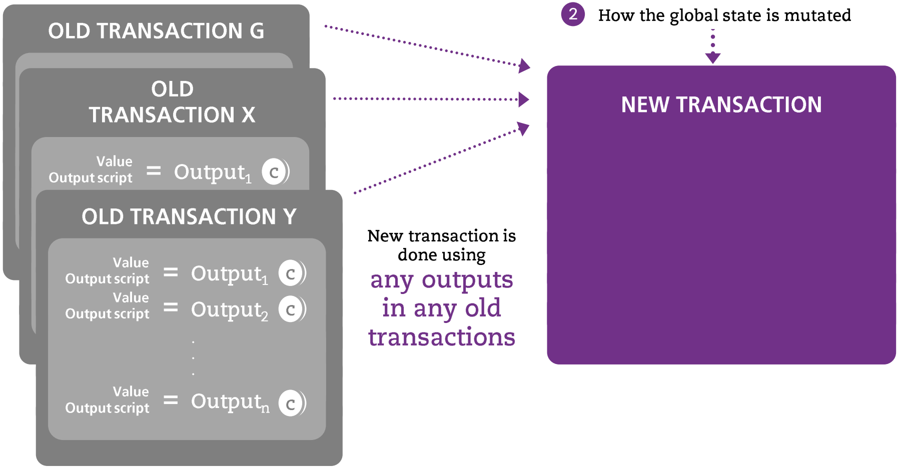
1. Validation rules
2. How the global state is mutated



Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated

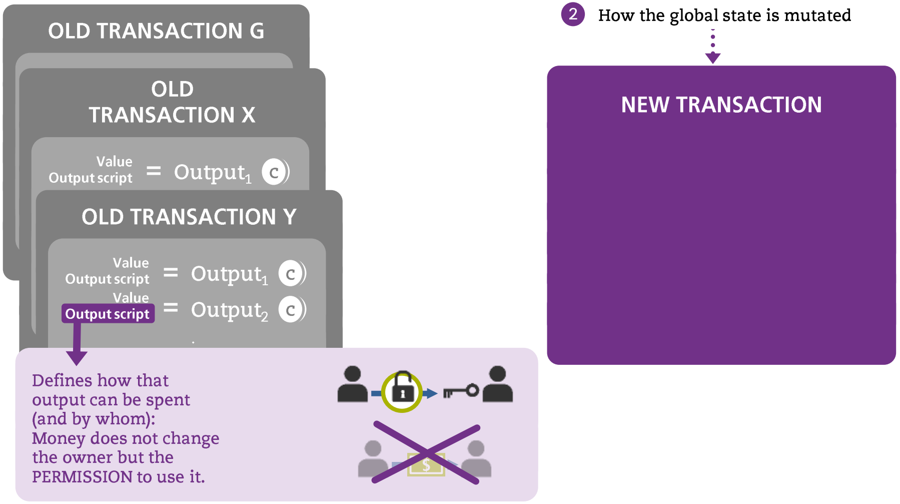


New transaction is done using **any outputs in any old transactions**

Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated

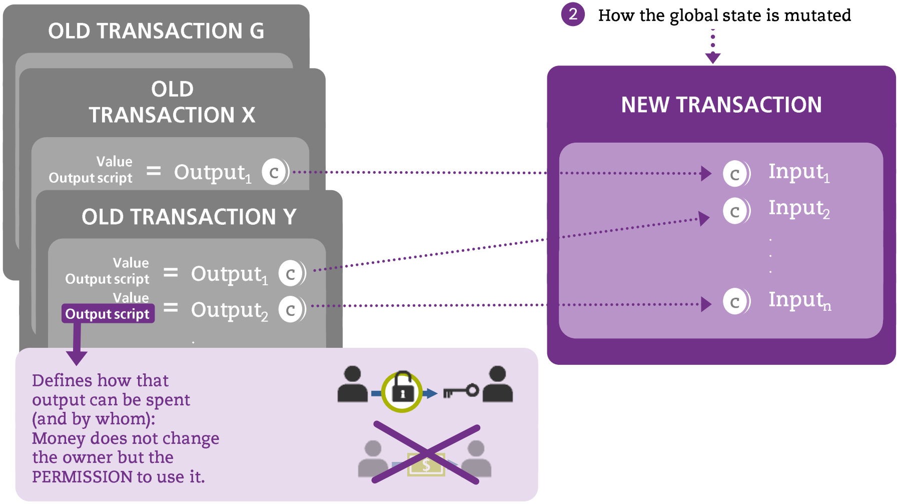


Defines how that output can be spent (and by whom): Money does not change the owner but the PERMISSION to use it.

Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated



Defines how that output can be spent (and by whom): Money does not change the owner but the PERMISSION to use it.

Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated

OLD TRANSACTION G

OLD TRANSACTION X

Value
Output script = Output_1 c

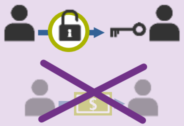
OLD TRANSACTION Y

Value
Output script = Output_1 c

Value
Output script = Output_2 c

.

Defines how that output can be spent (and by whom): Money does not change the owner but the PERMISSION to use it.



NEW TRANSACTION

Output reference
Signature script = c Input_1

Output reference
Signature script = c Input_2

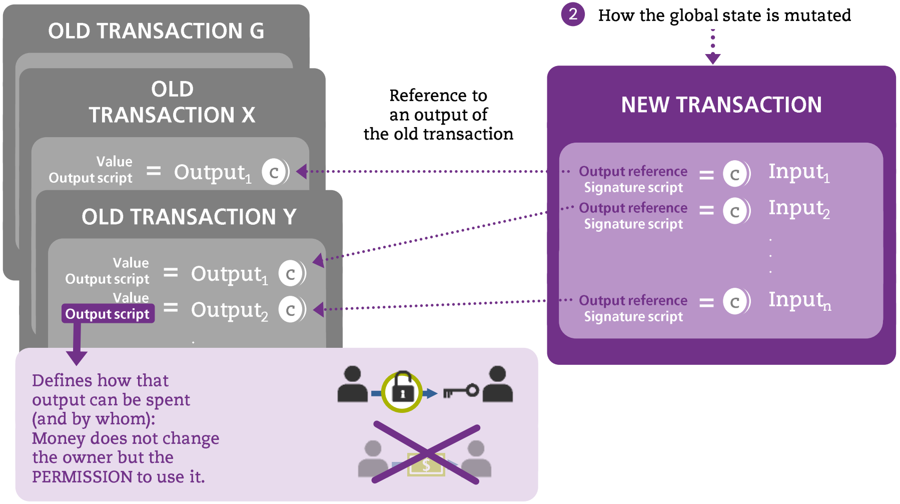
.
.
.

Output reference
Signature script = c Input_n

Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated

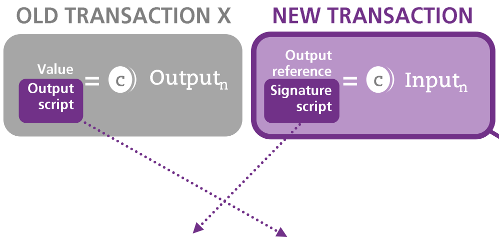


Defines how that output can be spent (and by whom):
Money does not change the owner but the PERMISSION to use it.

Transaction

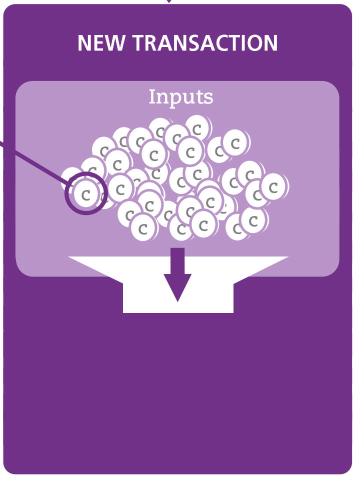
Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated



Signature script + output script

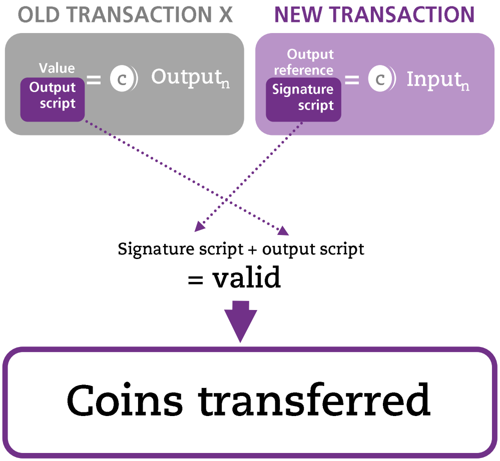
= valid

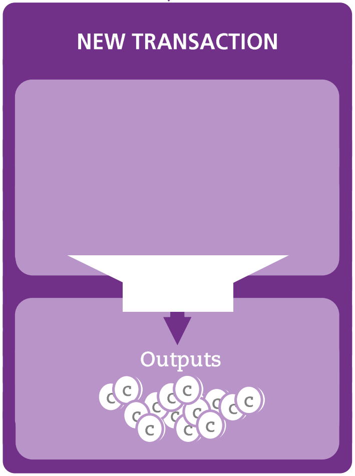


Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated

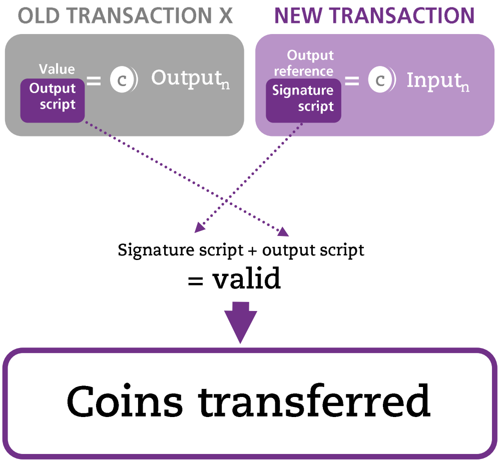


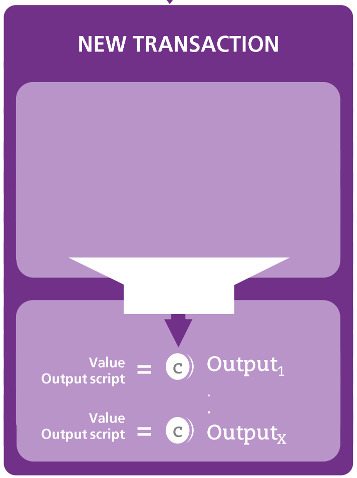


Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated





Comparison of Chaincode Languages

Constrained

- Bitcoin Script
- Allow complex transactions (e.g. multisig), but no smart contracts or general purpose computing.
- The execution time is limited to a specific maximum per transaction.
- A special transaction set limits the utility of the blockchain to a specific application.

Turing Complete

- Hyperledger Chaincode, Ethereum Solidity
- Allow smart contracts and general purpose computing. Even "world computer".
- Requires either transaction gas, a closed set of trusted peers, or whitelisted (non-Turing complete) transaction patterns.

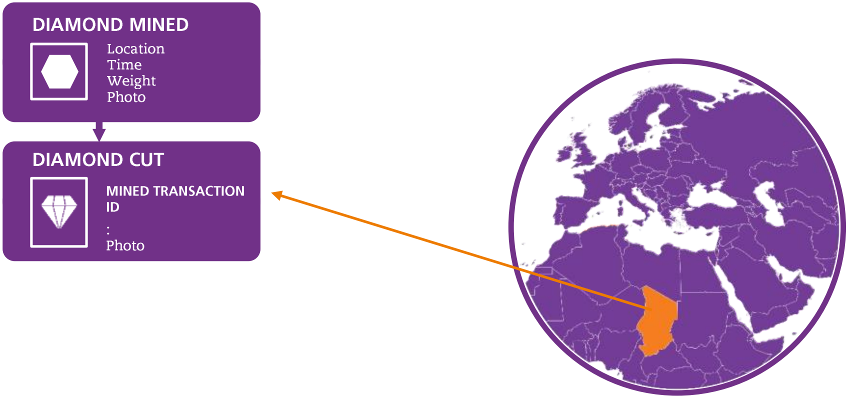
Diamond blockchain

DIAMOND MINED

Location
Time
Weight
Photo

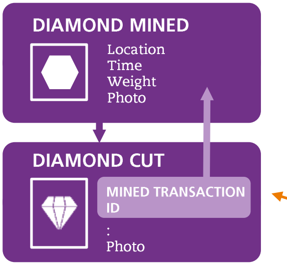
World with Countries and US, Canadian and Australian States - Single Color by FreeVectorMaps.com

Diamond blockchain



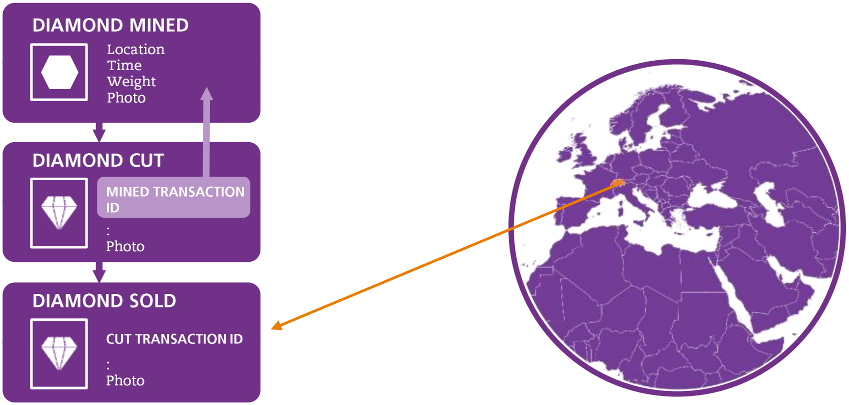
World with Countries and US, Canadian and Australian States - Single Color by FreeVectorMaps.com

Diamond blockchain



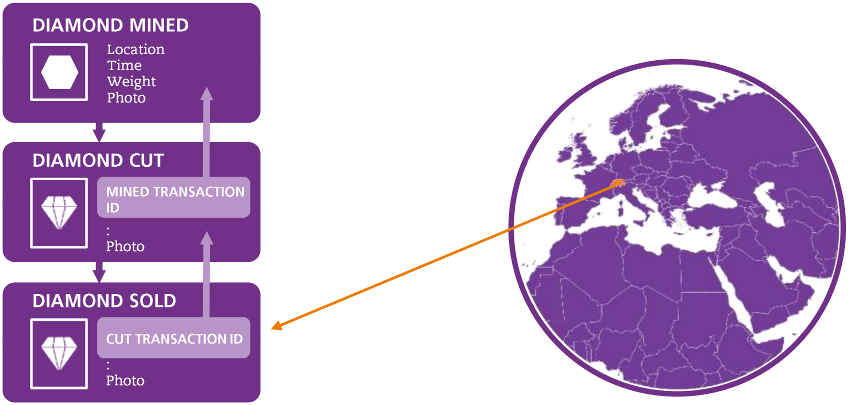
World with Countries and US, Canadian and Australian States - Single Color by FreeVectorMaps.com

Diamond blockchain



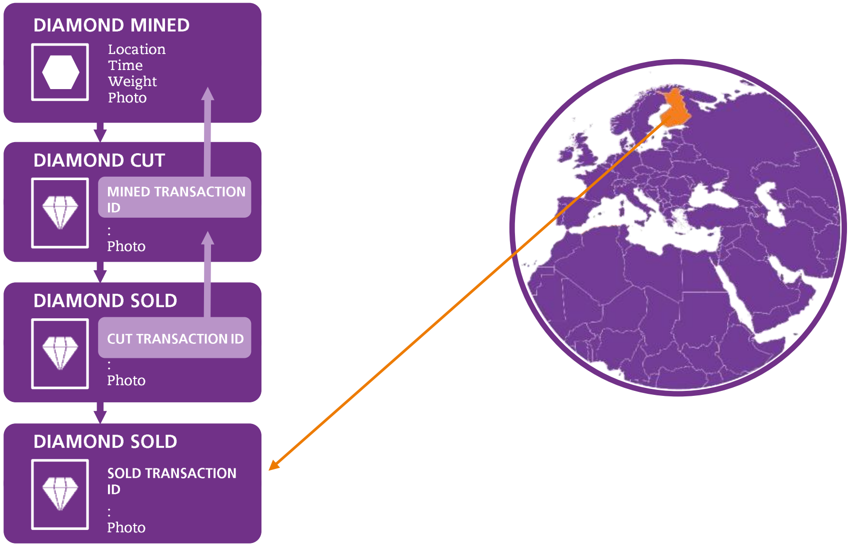
World with Countries and US, Canadian and Australian States - Single Color by FreeVectorMaps.com

Diamond blockchain



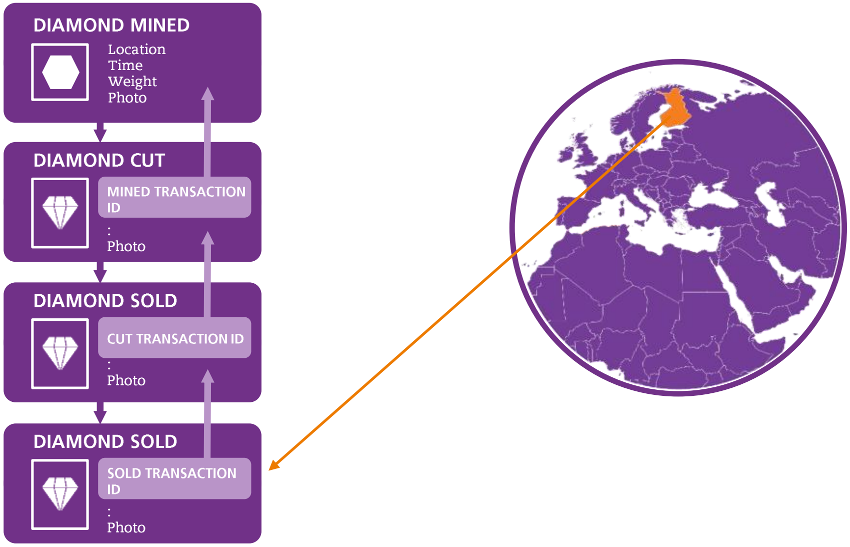
World with Countries and US, Canadian and Australian States - Single Color by FreeVectorMaps.com

Diamond blockchain



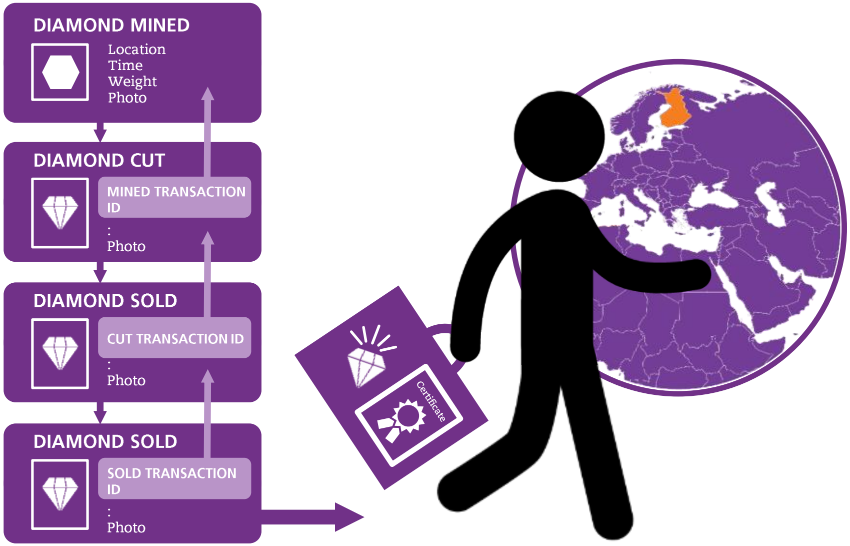
World with Countries and US, Canadian and Australian States - Single Color by FreeVectorMaps.com

Diamond blockchain



World with Countries and US, Canadian and Australian States - Single Color by FreeVectorMaps.com

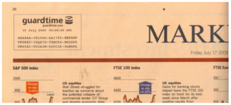
Diamond blockchain



World with Countries and US, Canadian and Australian States - Single Color by FreeVectorMaps.com

Guardtime KSI

- Estonian Guardtime offers a timestamp-hashing service based on Hash Calendar, which is a special type of a Merkle tree.
- Linked timestamping ties specific signing events together with time so that they cannot be altered without invalidating the whole chain.
- The service can be used to sign any data hash to irrevocably tie it to a specific time.
- The signature can then be used to prove that the hashed document existed at a claimed time.
- Applications include for example:
  - tamper-proofing logs, as a tampered log entry would not have a valid timestamp signature, as it did not exist at the claimed time.
  - Providing proof that a specific event happened at a certain point of time (not later than a given time).
- The infrastructure is secured by using periodical hash calendar roots published through widely witnessed media such as Financial Times and Twitter.



26

guardtime
guardtime.com
15 July 2009 00:00:00 UTC
AAAAAA-CKLUOA-AAI7FX-HHPAWP
VRUBEC-7DQE7O-TEBCP4-MS5ES5
UHOSEC-UU2A3N-OCCCIR-PLM4PG

MARK

Friday July 17 2009

S&P 500 index

US equities
Wall Street struggled for traction as concerns about the potential collapse of commercial lender CIT Group and gloomy economic data

FTSE 100 index

UK equities
Gains for banking stocks helped leave the FTSE 100 index on track for its best week since March after positive results from

Links

- Princeton course book: Bitcoin and Cryptocurrency Technologies
- Guardtime KSI
- Hyperledger Whitepaper
- Chainfrog Oy