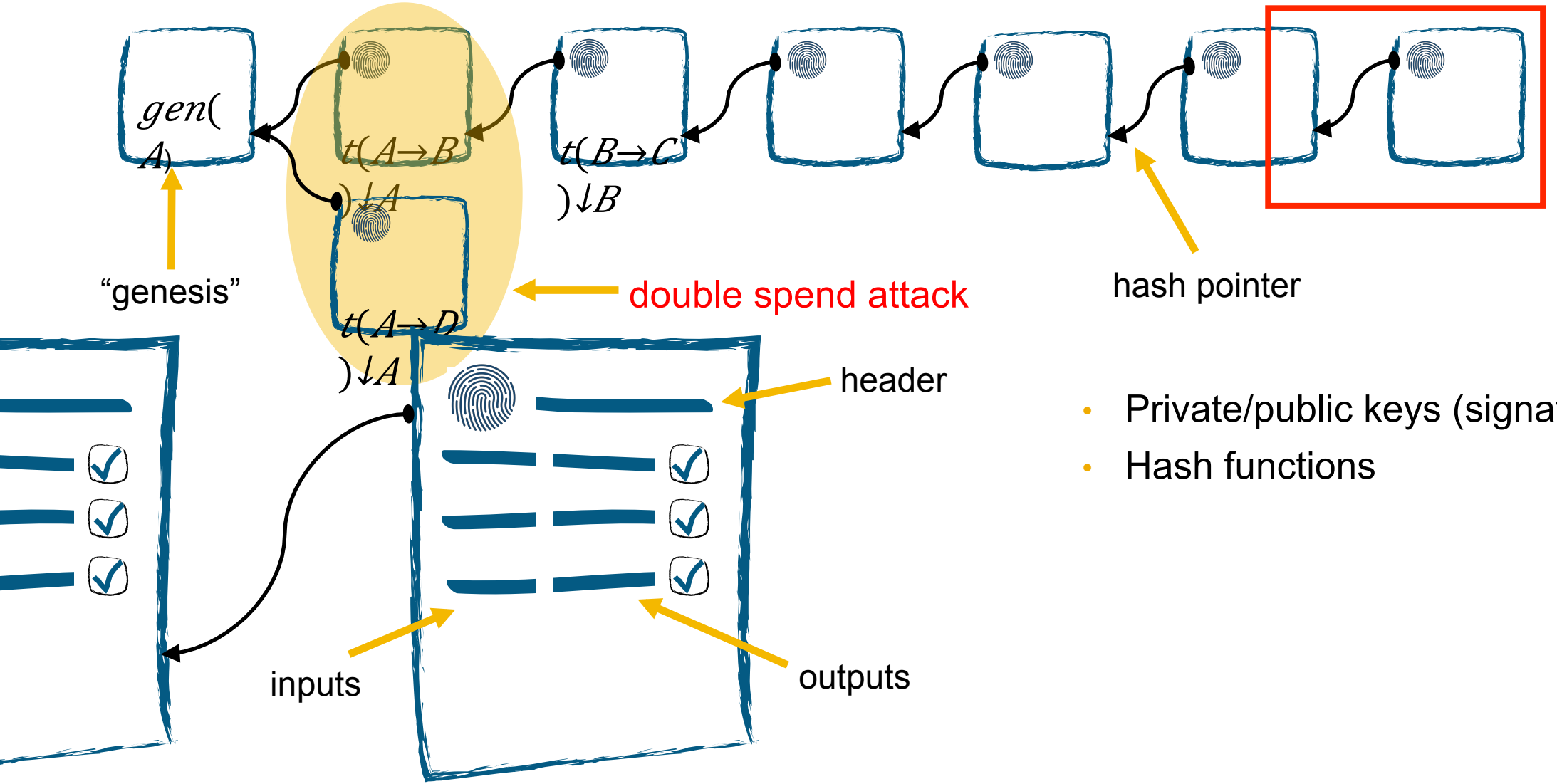
The *crypto* in cryptocurrencies



- Private/public keys (signatures)
- Hash functions

Consensus by proof-of-work

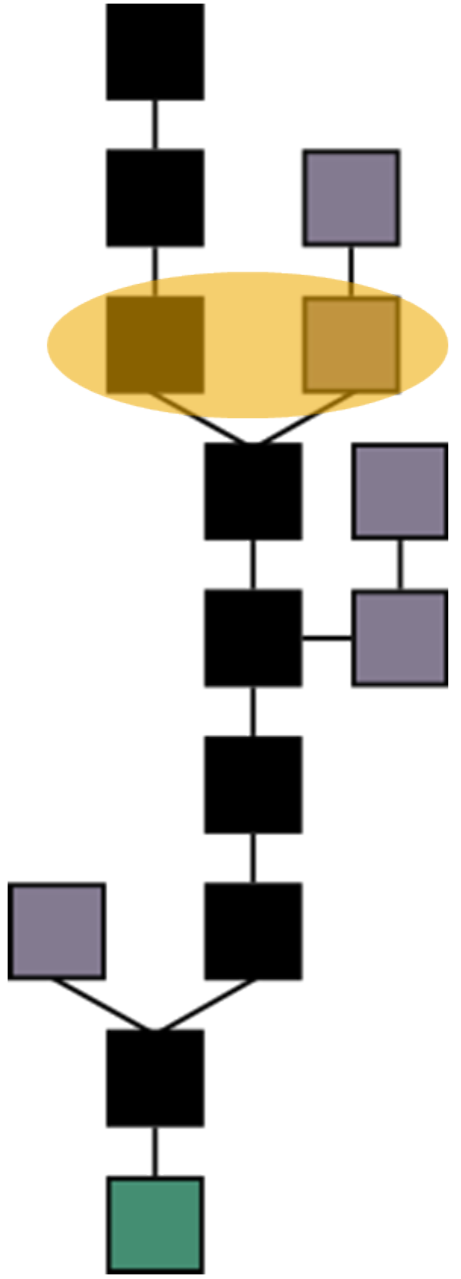
Bitcoin consensus protocol:

- New transactions are broadcast to all nodes
- Nodes collect new **valid** transactions into blocks
- **Lottery race** determines who gets write access
- Other nodes accept block if valid
- Nodes express their acceptance by building upon this block

Lottery race:

- Solve computational puzzle (mining):
- $H(nonce||prevhash||tx||...||tx) < \epsilon$
- Winner's block is added
- Longest valid chain wins (majority wins)

Incentive: Winner gets a reward



Overview: Smart contracts in Blockchains

A **smart contract** is a piece of code embedded in the Blockchain and being executed by each validator.

It can represent a **business contract** and guarantees **automation of business rule execution**.

Smart contract is a new concept and creates challenges:

- Code is Law philosophy is not the same as human interpretation of law
- Decentral code execution requires a new development paradigm

Recap: Cryptocurrencies

Decentralization

- Open peer-to-peer network
- No trust between participants
- No central authority
- “Miners” validate protocol
- Influence by hash-power
- Tamper-proof hash chain

Consensus

- Block creation lottery
- Poof-of-Work via hash puzzle
- Longest chain wins
- Probabilistic consensus
- Mining incentives

Limitations

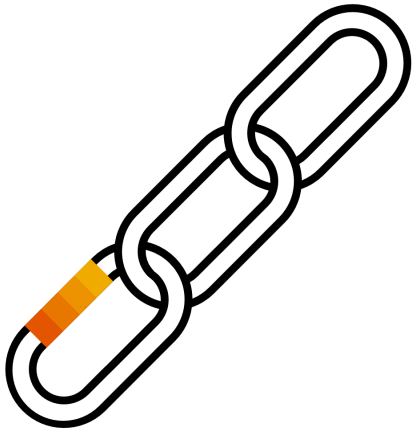
- Proof-of-Work expensive
- Low throughput
  (max 7 txs/s in Bitcoin)
- Full replication required

Blockchain terms demystified

Bitcoin

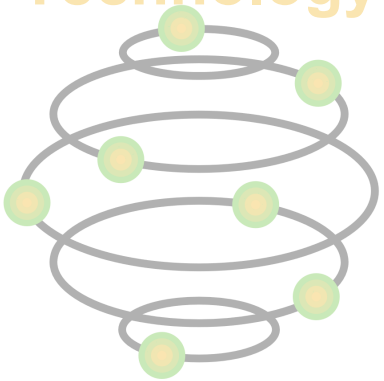
Cryptocurrency; encryption techniques are used to verify the transfer of funds; operating independently of a (central) bank.

Blockchain



Architectural concept that enables the decentralized, secure, direct, digital transfer of values and assets.

Distributed Ledger Technology



Distributed ledger; consensus of replicated, shared digital data spread across multiple sites, countries, or institutions. No central administrator or centralized data storage.

Blockchain deployment options

Public

Open for everyone to participate and read/write.

Permissionless Blockchain

Consortium

Access and permissions controlled by pre-selected set of nodes

Permissioned Blockchain

Overview: Blockchain consensus algorithms

- A **consensus** algorithm as part of a blockchain is used to guarantee a consistent state of the shared ledger/journal of transactions.
- **Public blockchains** use e.g. **Proof-of-Work** for a consistent block creation in a network with anonymous participants.
- **Consortium blockchains** use consensus algorithms to solve the concurrency write problem with known participants.

Blockchain Platform:	Bitcoin/Ethereum	Multichain	Hyperledger	…
	Proof-of-Work: For each block a crypto-graphical puzzle must be solved that requires massive computer power. Assuming 51% good nodes the blockchain history can not be changed.	**Round-Robin Block Creation**: One validator per block, working in a round-robin type of fashion. All validators are known and have permissions to create blocks. In private blockchain sufficient as participants are well known.	**Practical Byzantine Fault Tolerance (PBFT):** It is a consensus algorithm that tolerates the failures known of a minority of nodes. The majority of nodes determines the valid blocks.	