Blockchain

distributed ledgers

GOTO 2015 Copenhagen

Tamas Blummer

Chief Ledger Architect

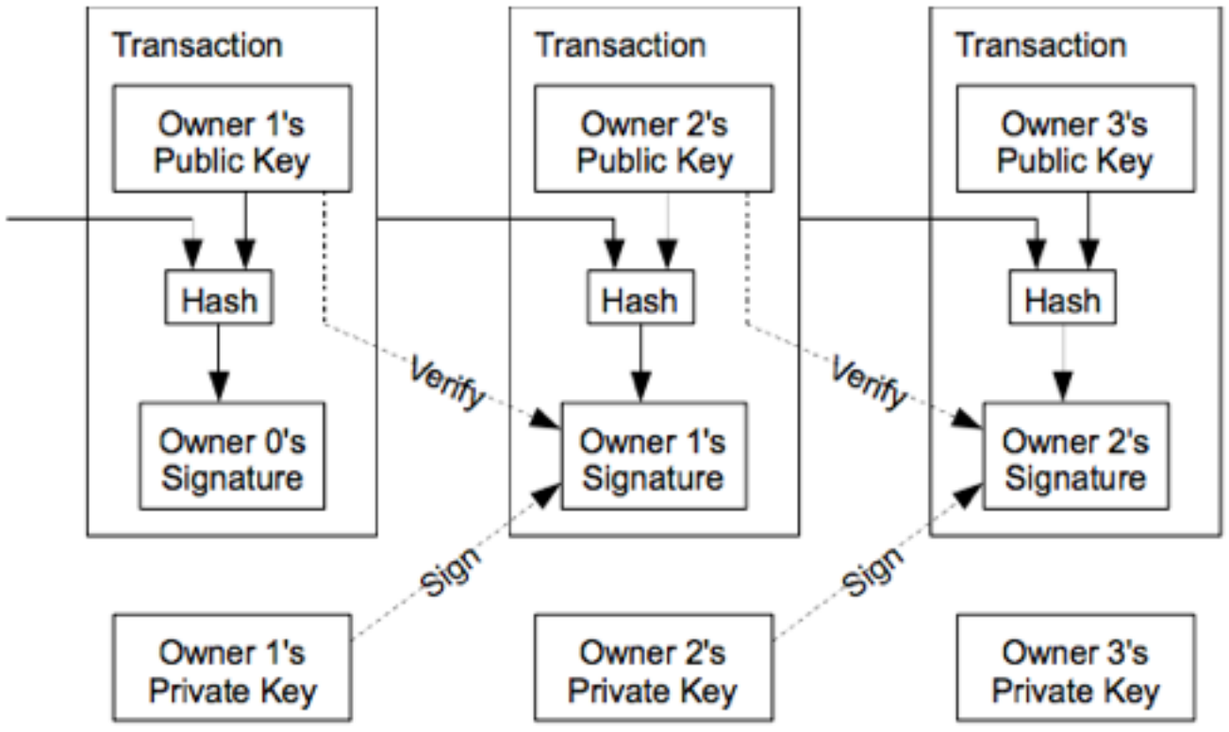
Digital Asset Holdings

tamas@digitalasset.com

What does it promise?

- Audit-ability
- Network wide consensus
- Privacy and Compliance
- Trust minimized execution
- Smart contracts

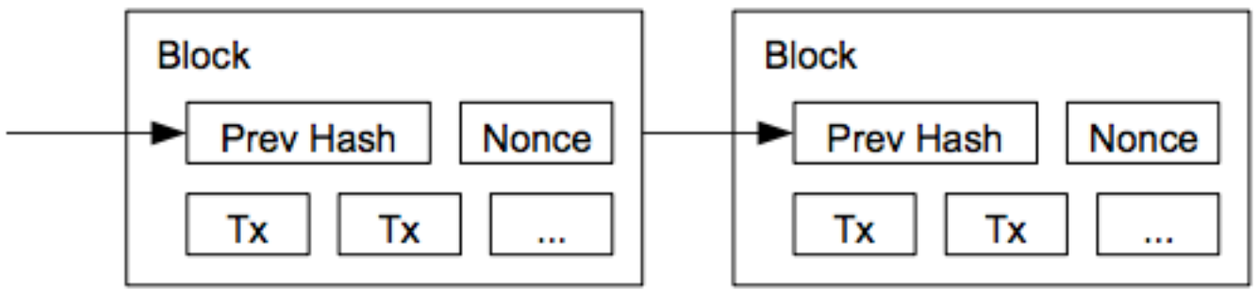
Audit-ability Transactions



A blockchain is an append only log for transactions.
Every transaction is digitally signed by the owner of its inputs.
The signature proves consistency and authenticity.

Audit-Ability

The Blockchain

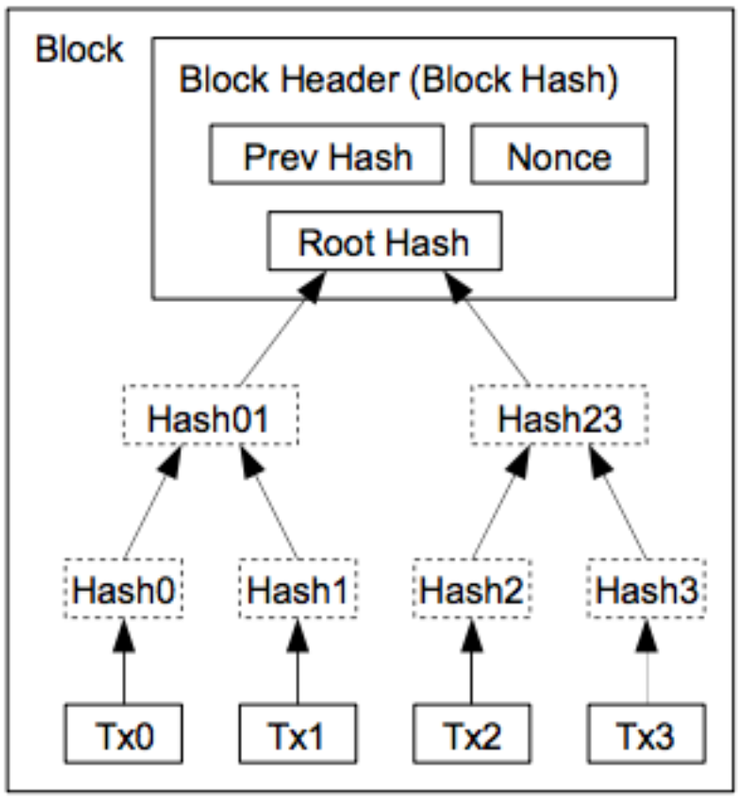


Transactions are collected into blocks.
The block's cryptographic hash includes that of its transactions and the hash of the previous block.

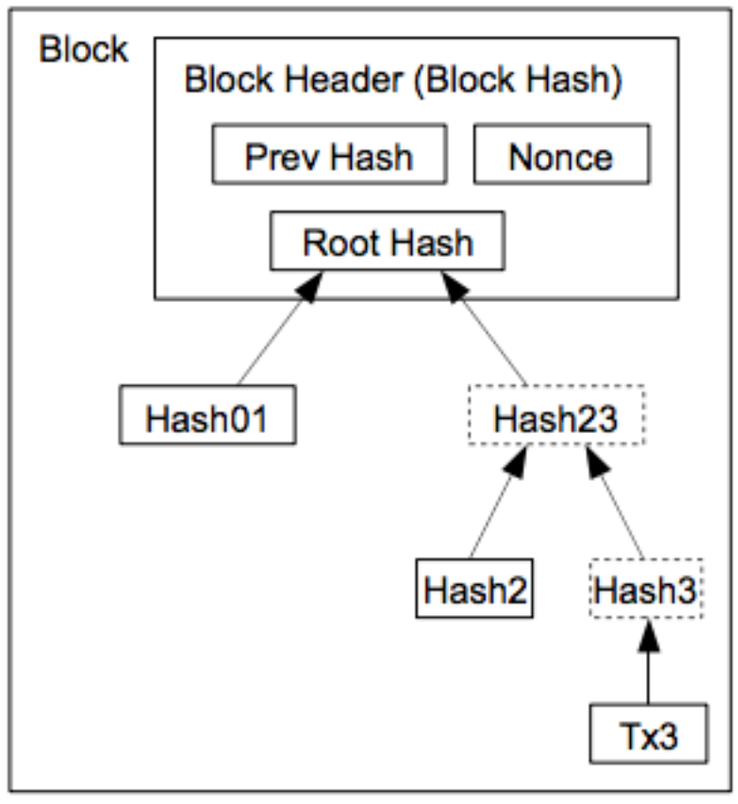
It is not feasible to change, add or remove any transaction without repeating the work invested into hashing the block and all blocks after it.

Audit-ability

Compact Proof of Existence



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

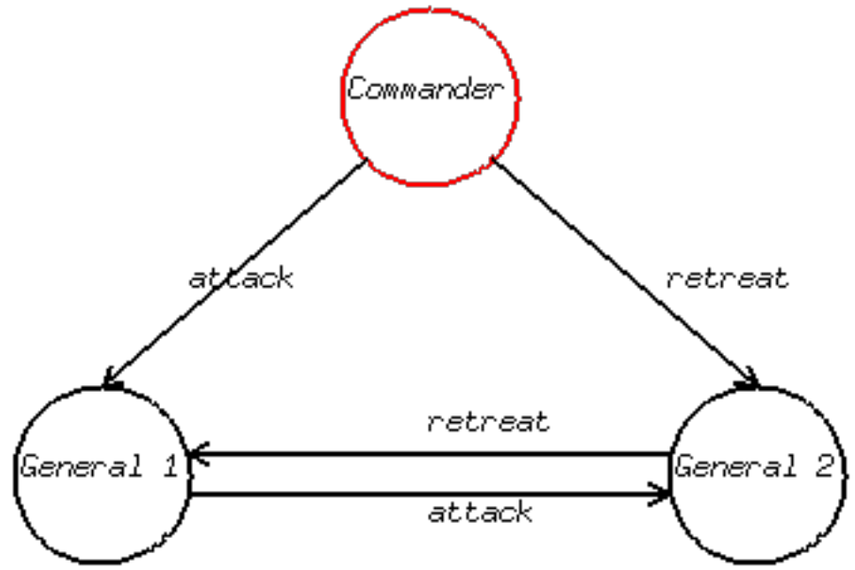
A compact proof of existence of a transaction in a block can be computed.

Network wide consensus
The limits

Nodes validating blocks of transactions vote on continuation of the chain, by

- Proof of Work aka. Nakamoto Consensus, means 1/2+ of computing power decides.

- Byzantine fault tolerant replication, means 2/3+ majority votes decides



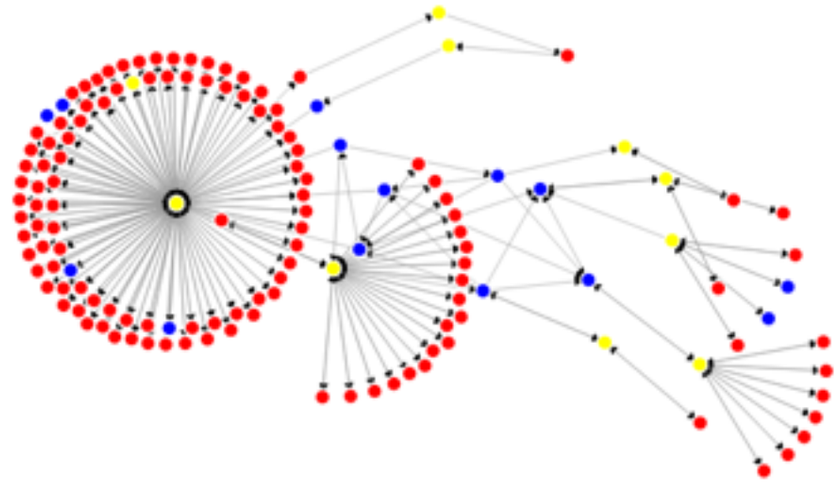
Network wide consensus
The Trade-Off

There is a practical trade-off between resilience against byzantine faults and computation power required.

In a network with known actors, hence a limited chance of faulty collusion, the consensus may be reached cheaply and efficiently.

Privacy

Concern: Efficiency promise of a shared ledger hurts privacy.



Remedies are

- Identities of sender and recipient are only known to those involved - no key re-use

- Transaction validity can be proven without knowing its details - zero knowledge proof.

Compliance

Concern: Privacy of transactions hurts oversight and regulations, repudiation.

Remedies:

- Deterministic identity generation may enable oversight of seemingly unrelated transactions. Homomorphic property of EC Key generation.

- Joint identities with arbitrators may provide for sufficient control and repudiation.

Trust-Minimized Execution

Consensus is built not only on order, but validity of transactions, where validity rules may be evaluated against a wider than transaction context.

Since transaction validating code is executed independently by all voting nodes, the result is a trust-minimized execution.

Results can not be influenced by a minority of network participants, especially not by making individual exceptions.

Revising past history of transactions becomes unattainable even for a bigger minority under time constraints for faulty behavior.

Payment Channels

Offsetting transaction pairs of trading partners that are valid to be committed to block chain may be instead hold and updated at high frequency.

The result is a secure payment (netting) channel without the time and size constraints of block chain inclusion.

Smart Contracts

Transactions that reallocate assets under control of a joint identity can implement atomic swap of ownership of assets.

Transaction validity rules that use external a wider context e.g. time point of inclusion into the blockchain, can implement and automated escrow.

“You should be taking this technology as seriously as you should have been taking the development of the Internet in the early 1990s,”

Blythe Masters,

CEO of Digital Asset Holdings