Blockchain
(a.k.a. the slowest, most fascinating “database” you’ll ever see)

GOTO Amsterdam

13 June, 2017

Stefan Tilkov, @stilkov

innoQ

I don’t know Blockchain

and so can you

1.

Bitcoin

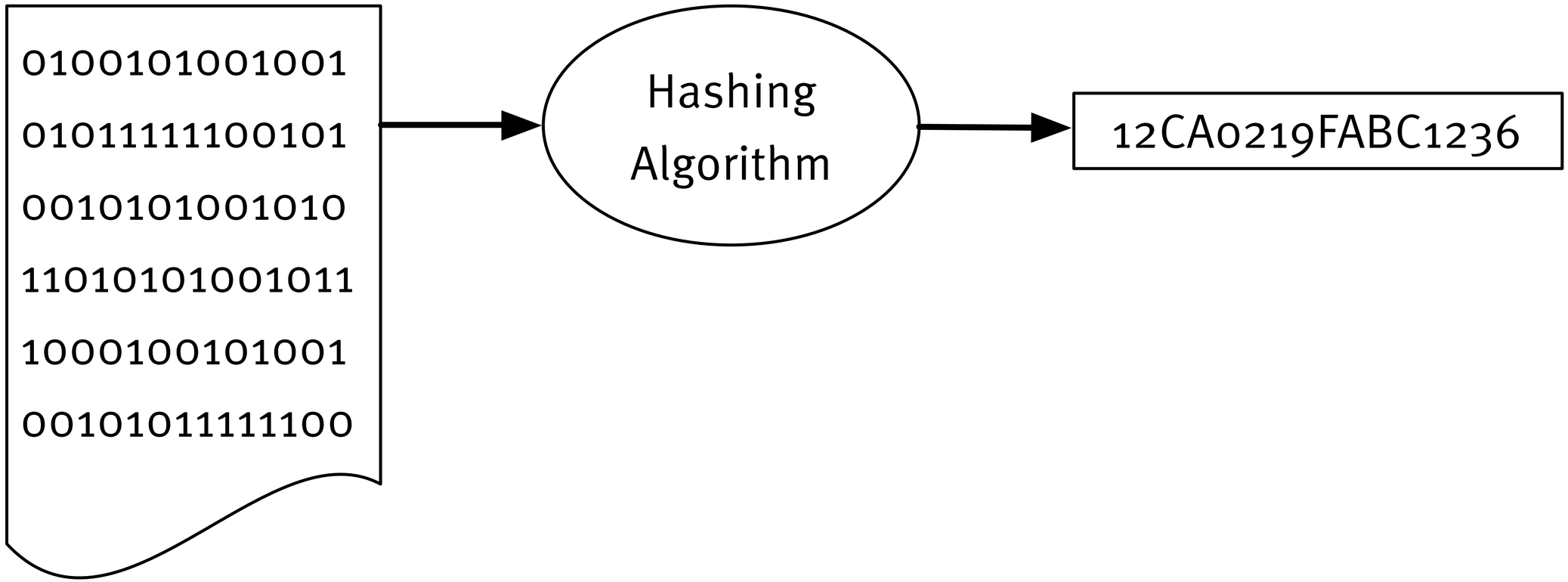
- Practical application of cryptography to
  - maintain a pseudonymous, global history of transactions
  - with guaranteed consistency
  - without centralization or intermediaries
  - resistant to forgery and fraud
- Created in 2009 by Satoshi Nakamoto
- Most successful crypto-currency to date

Cryptography?

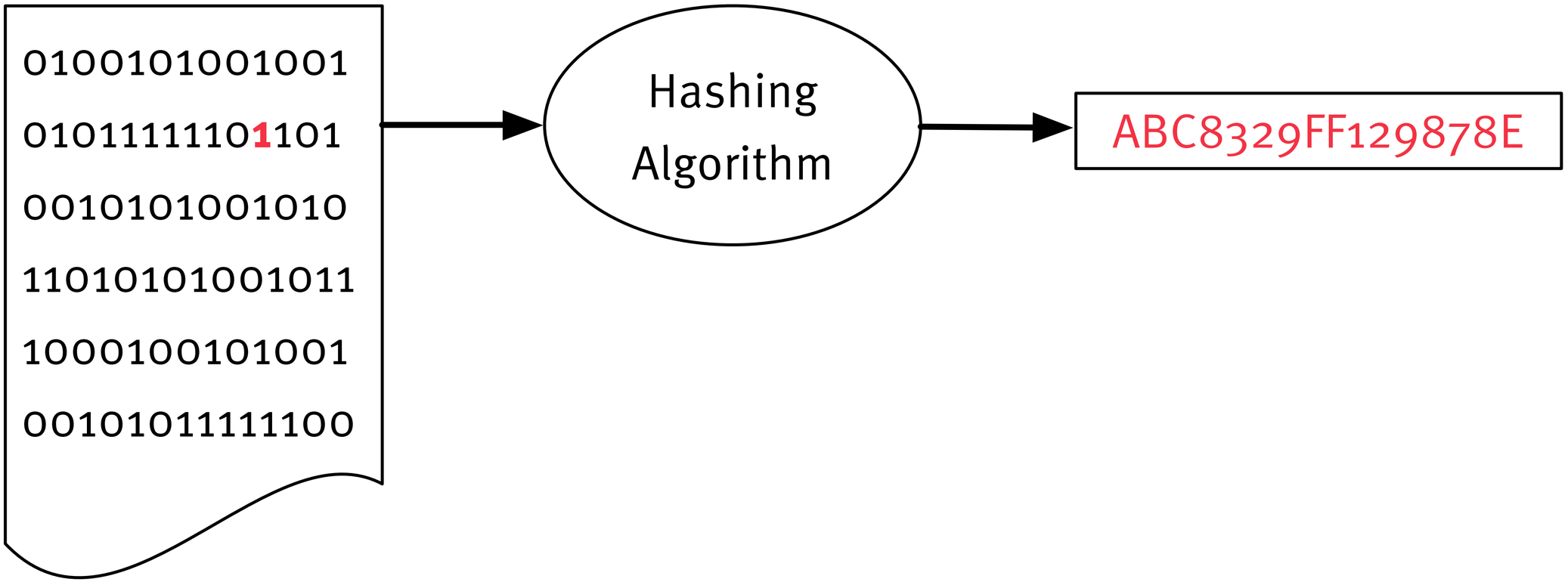
Oh no!

Don’t worry.

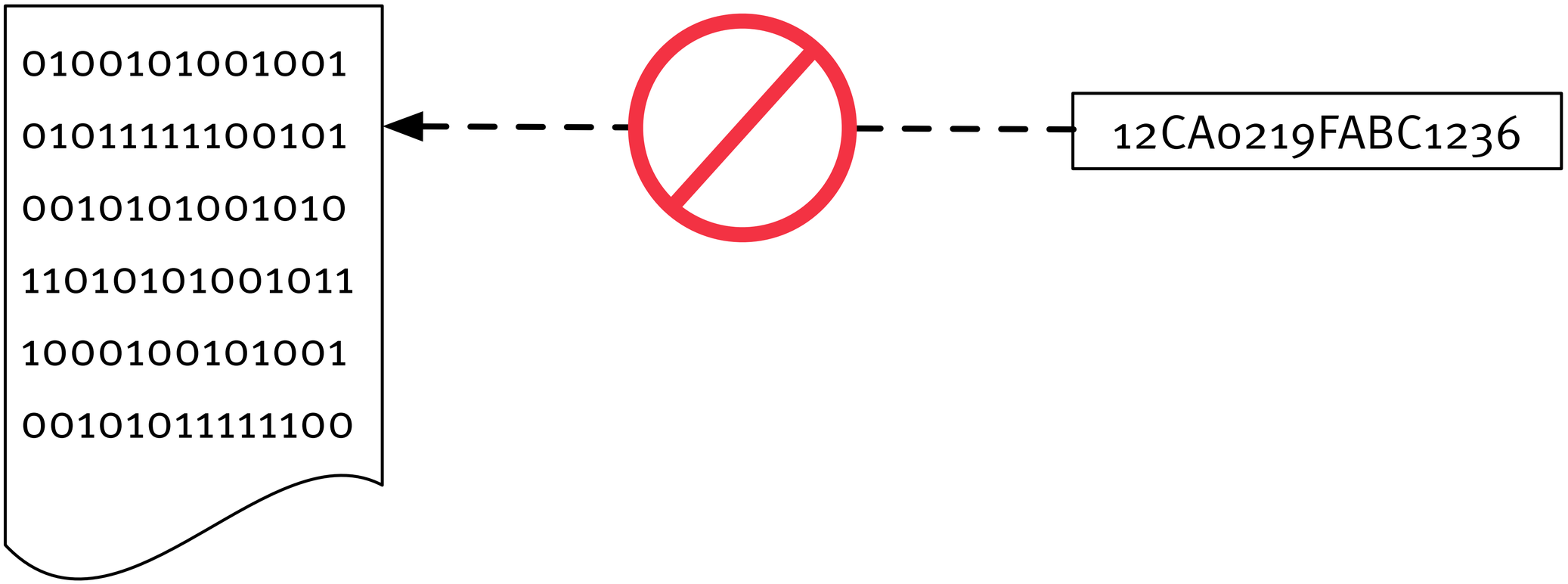
Hashing


0100101001001
0101111100101
0010101001010
1101010100101 1
1000100101001
0010101111100
Hashing
Algorithm
12CA0219FABC1236

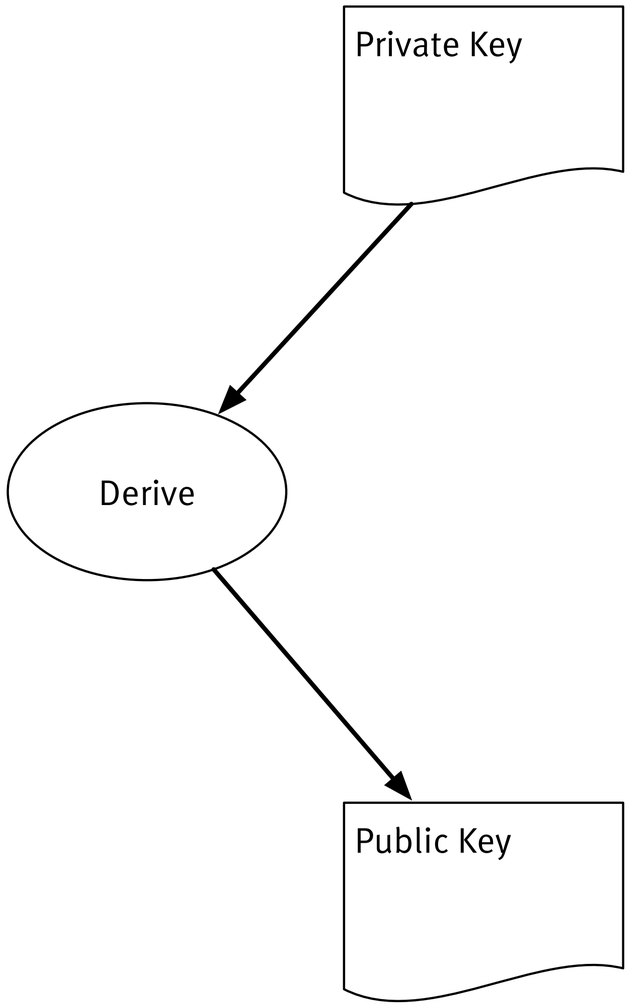
Hashing


0100101001001
0101111110 1 1101
0010101001010
11010101001011
1000100101001
00101011111100
Hashing
Algorithm
ABC8329FF129878E

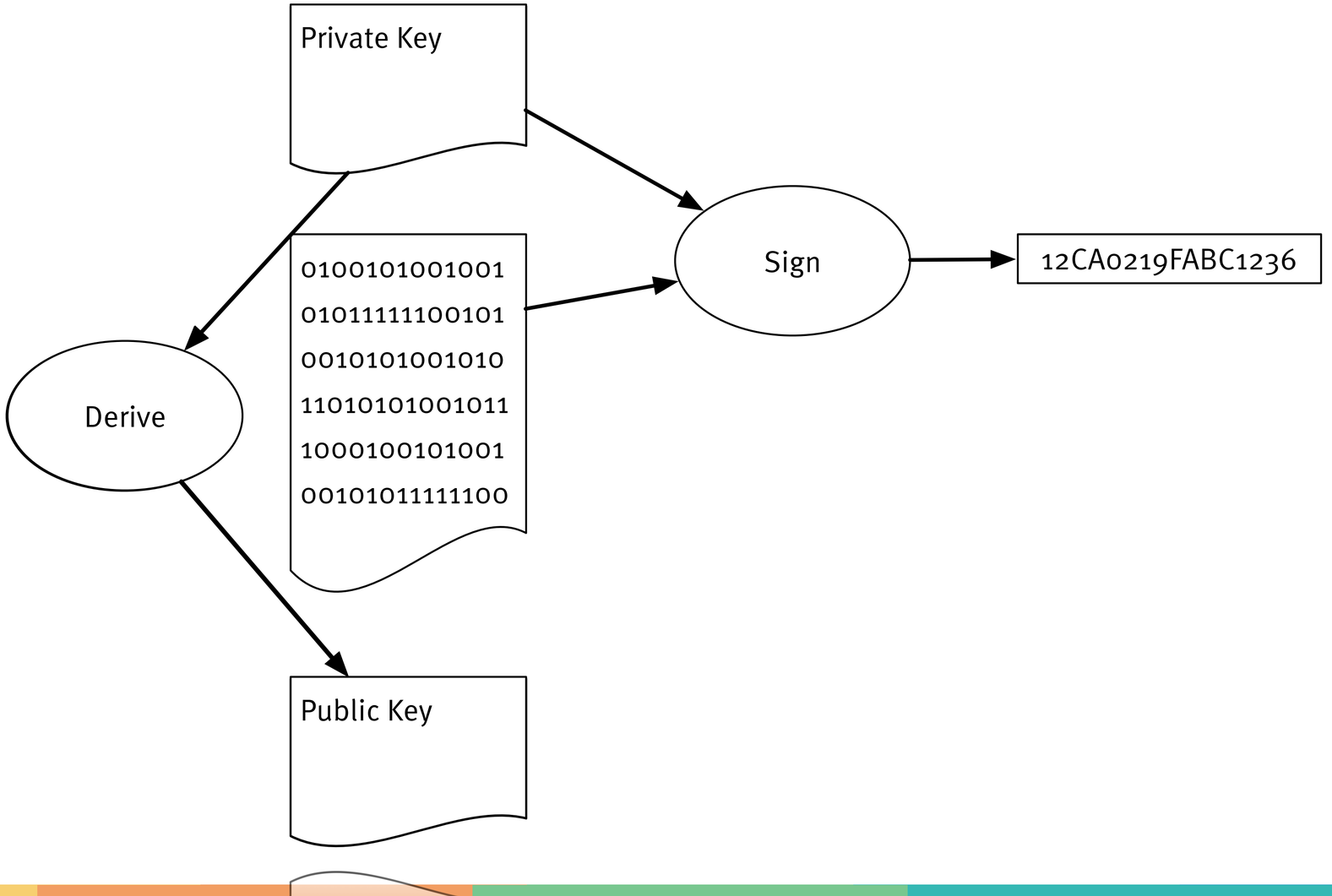
Hashing


0100101001001
0101111100101
0010101001010
11010101001011
1000100101001
00101011111100
12CA0219FABC1236

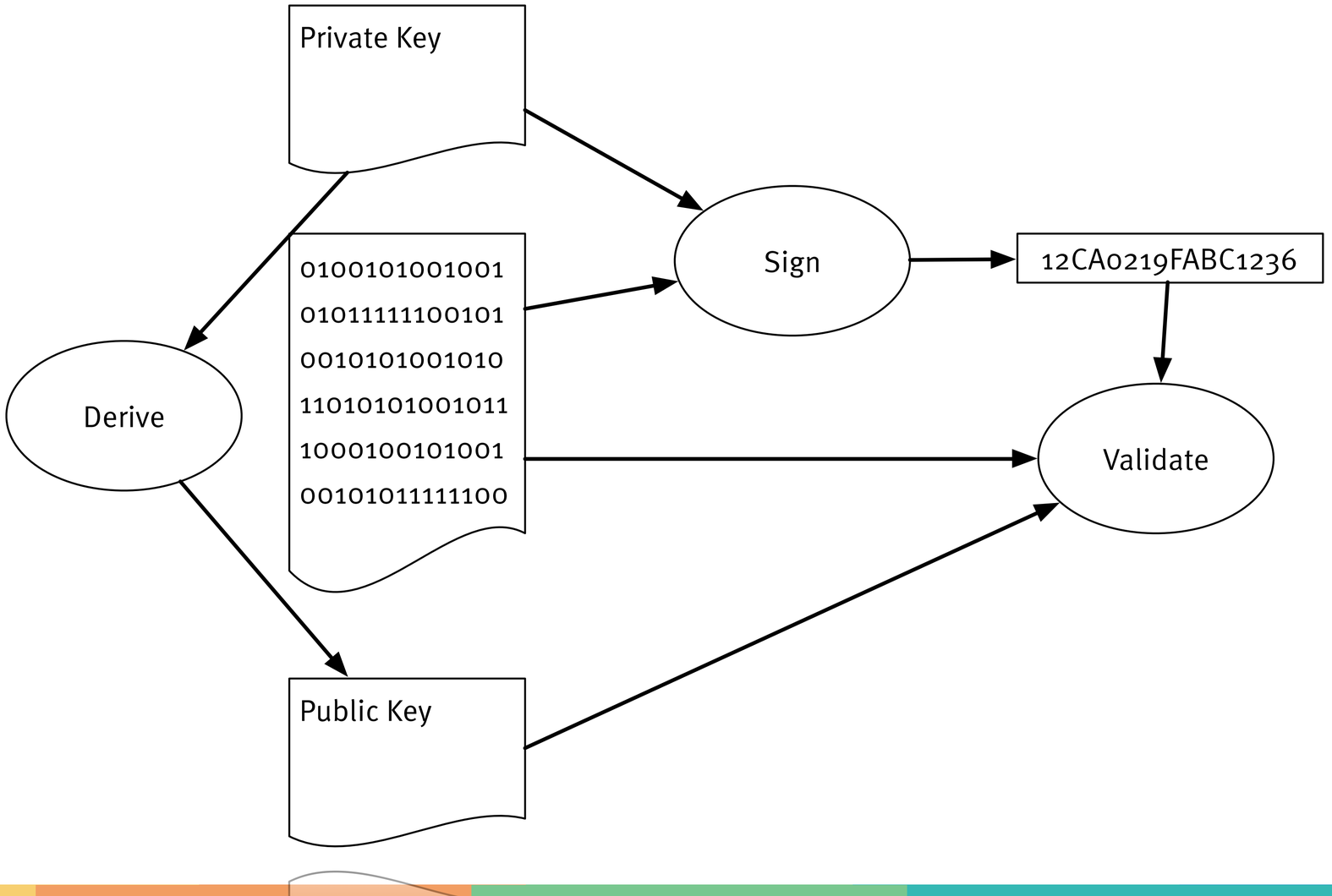
Public & Private Keys



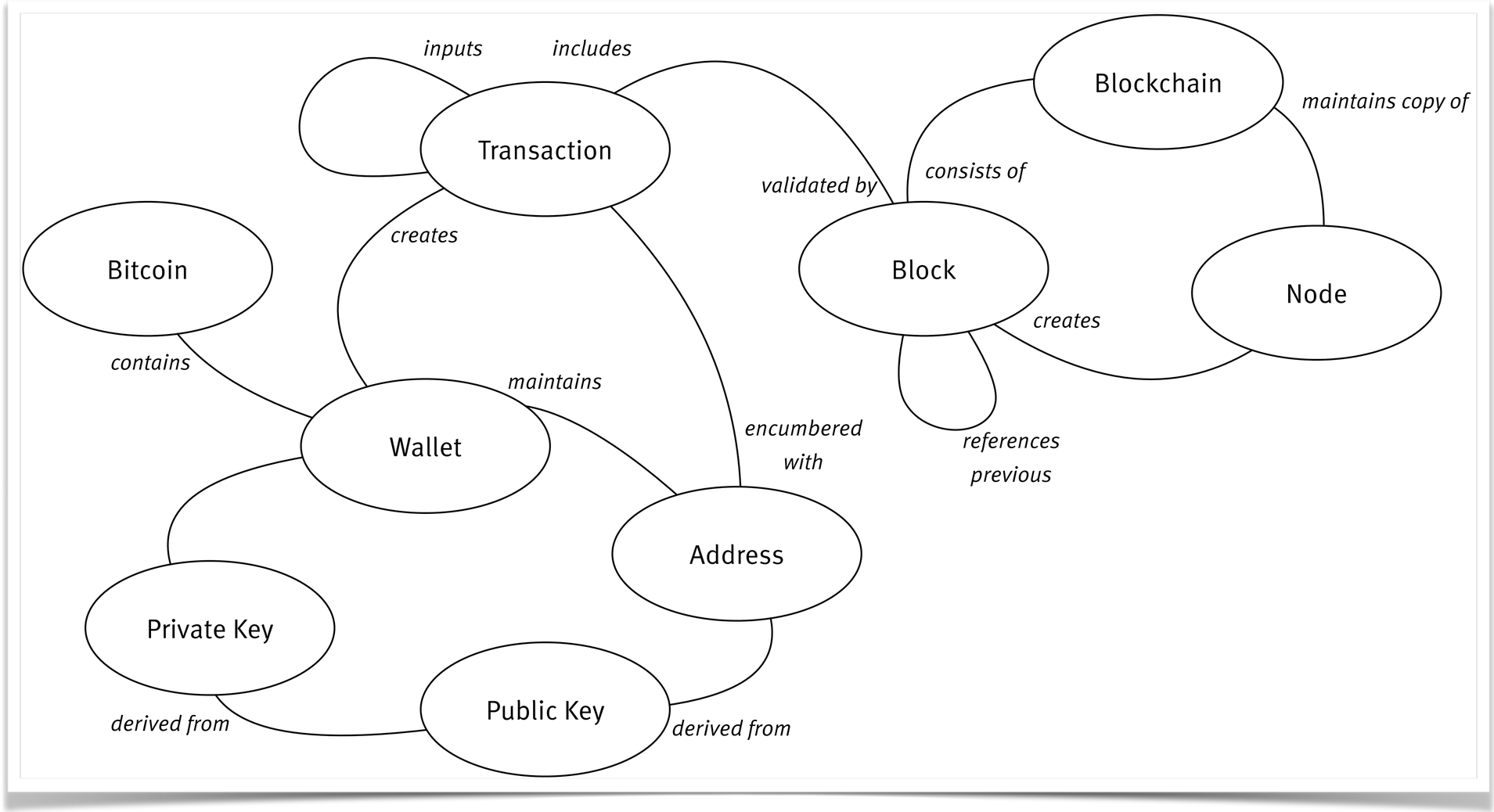
Public & Private Keys



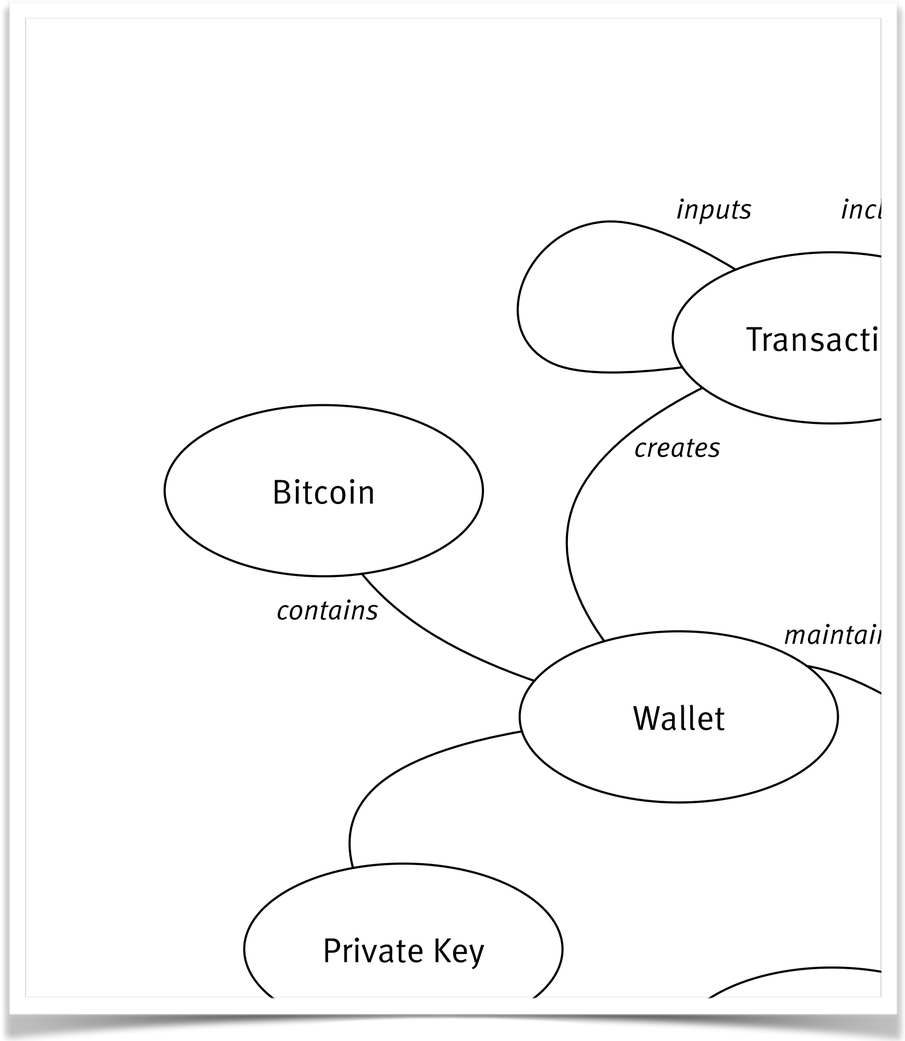
Public & Private Keys



Bitcoin: Vocabulary

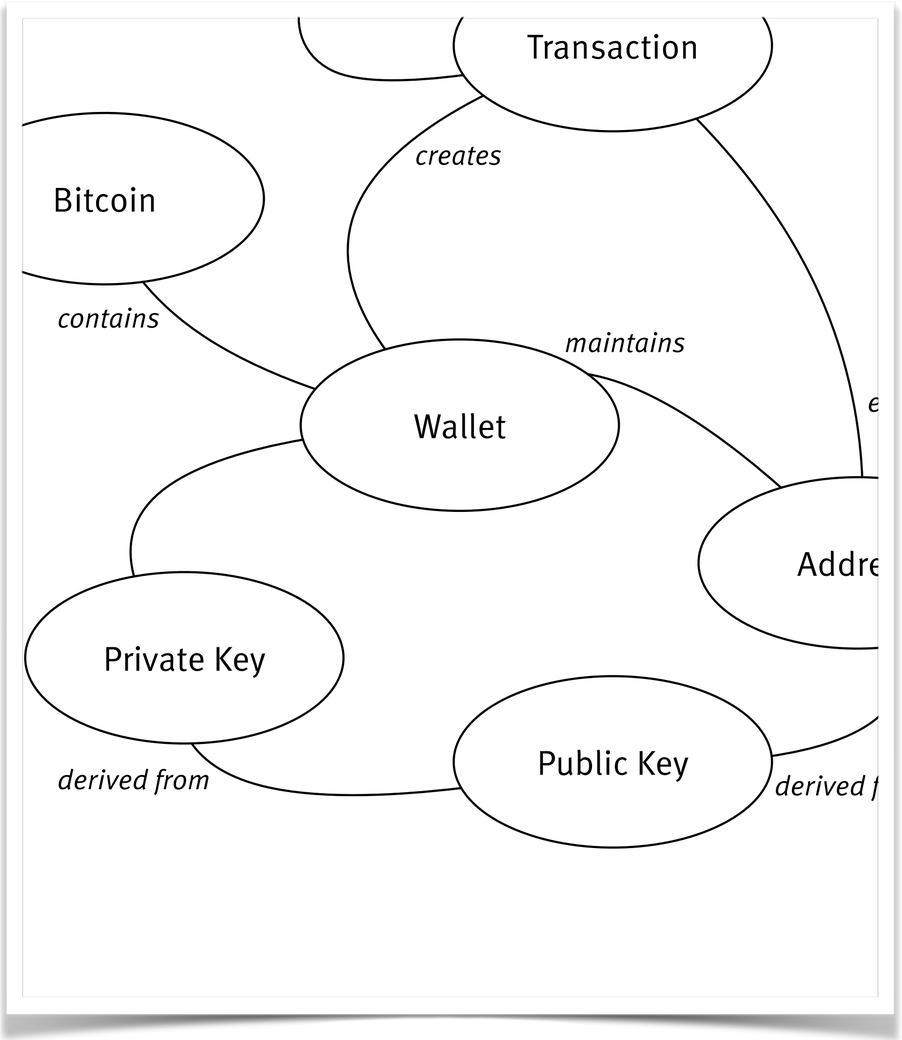


Bitcoin



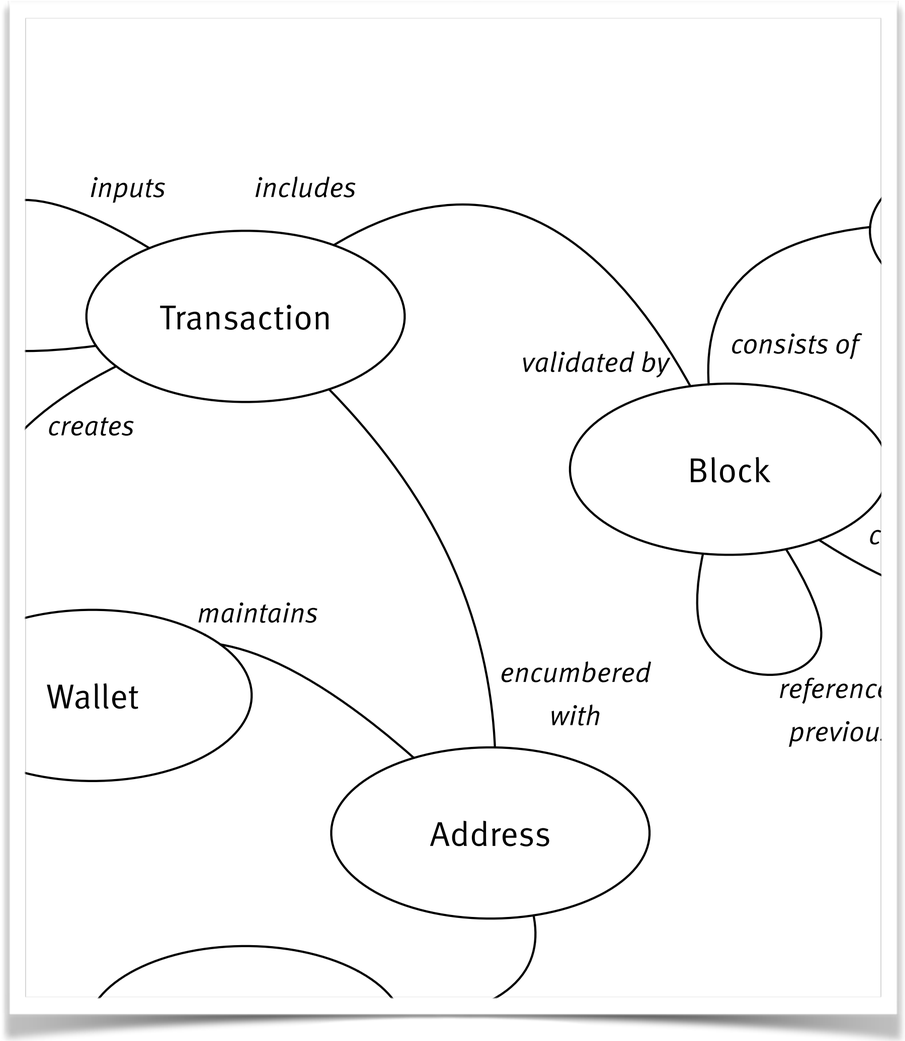
- The technology
- The currency
- Created via “mining” (coinbase tx)
- 1 Bitcoin (BTC) = 1,000 mBTC = 1,000,000 uBTC = 1,000,000,000 Satoshi
- Coins are maintained as part of transactions (not anonymous)

Bitcoin: Wallet



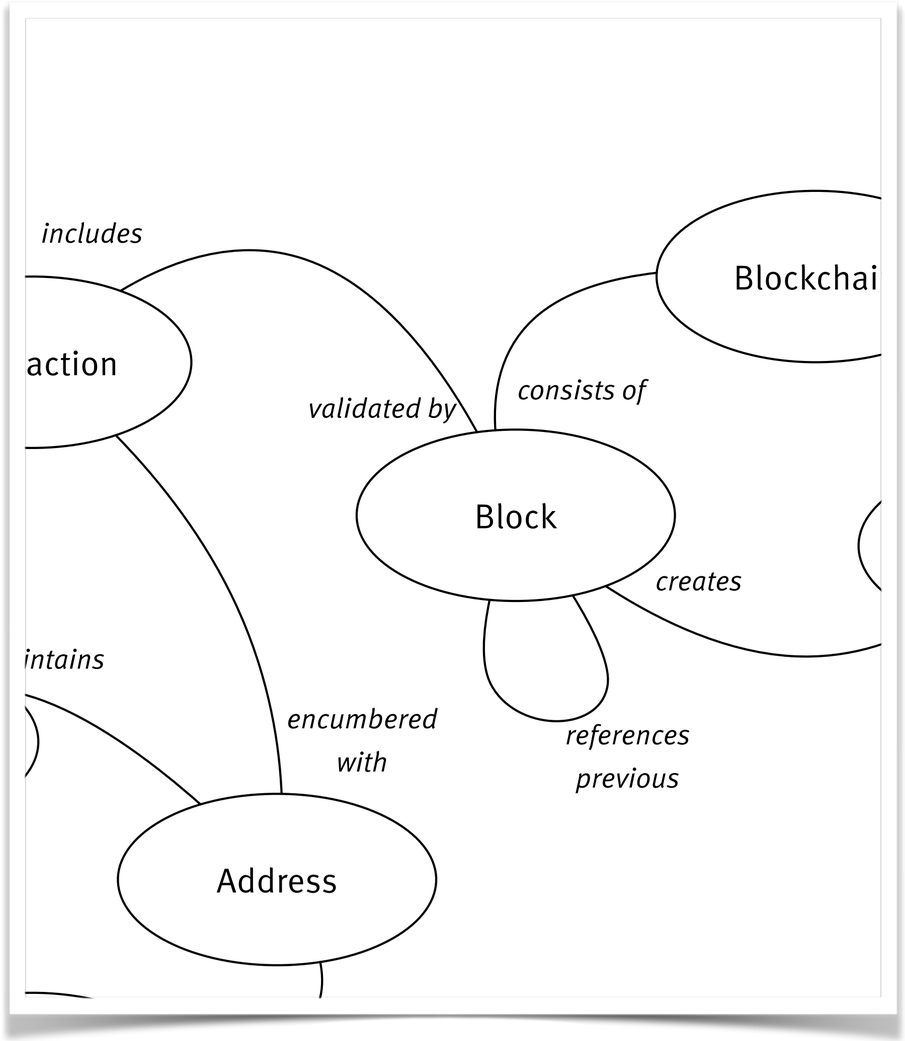
- Maintains private keys, public keys, addresses
- Used to sign transactions (sort of)
- Implementations for mobile devices, Mac, Windows, Linux
- “Online wallets” a.k.a. “a very bad idea”
- Offline wallet

Bitcoin: Transactions



- Multiple inputs (unspent transaction output, UTXO)
- Inputs can only be spent by owner
- Multiple outputs
- “Unspent” outputs are “encumbered” with recipient key
- Can be sent to any node
- Will be included in (validated by) block

Bitcoin: Blocks

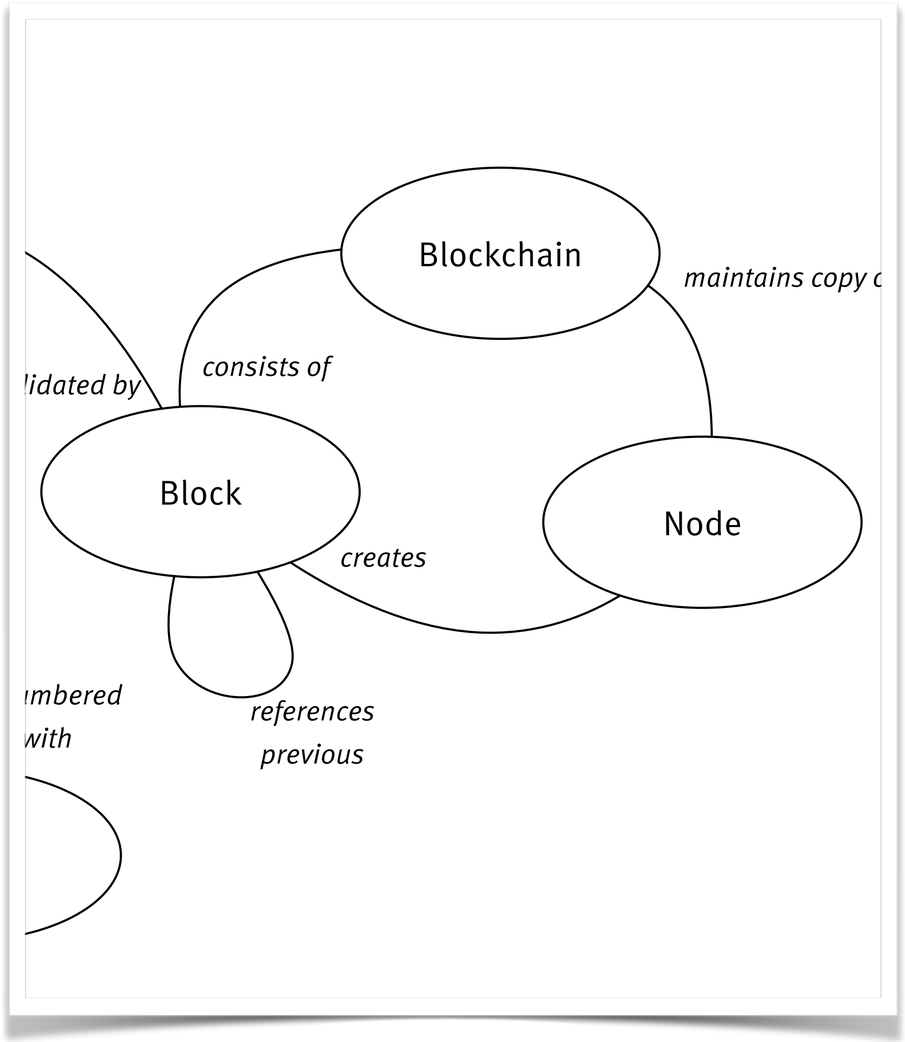


- Reference transactions
- Include proof of work
- Reference previous block
- Number of blocks relate to level of trust

Bitcoin: Mining & proof of work

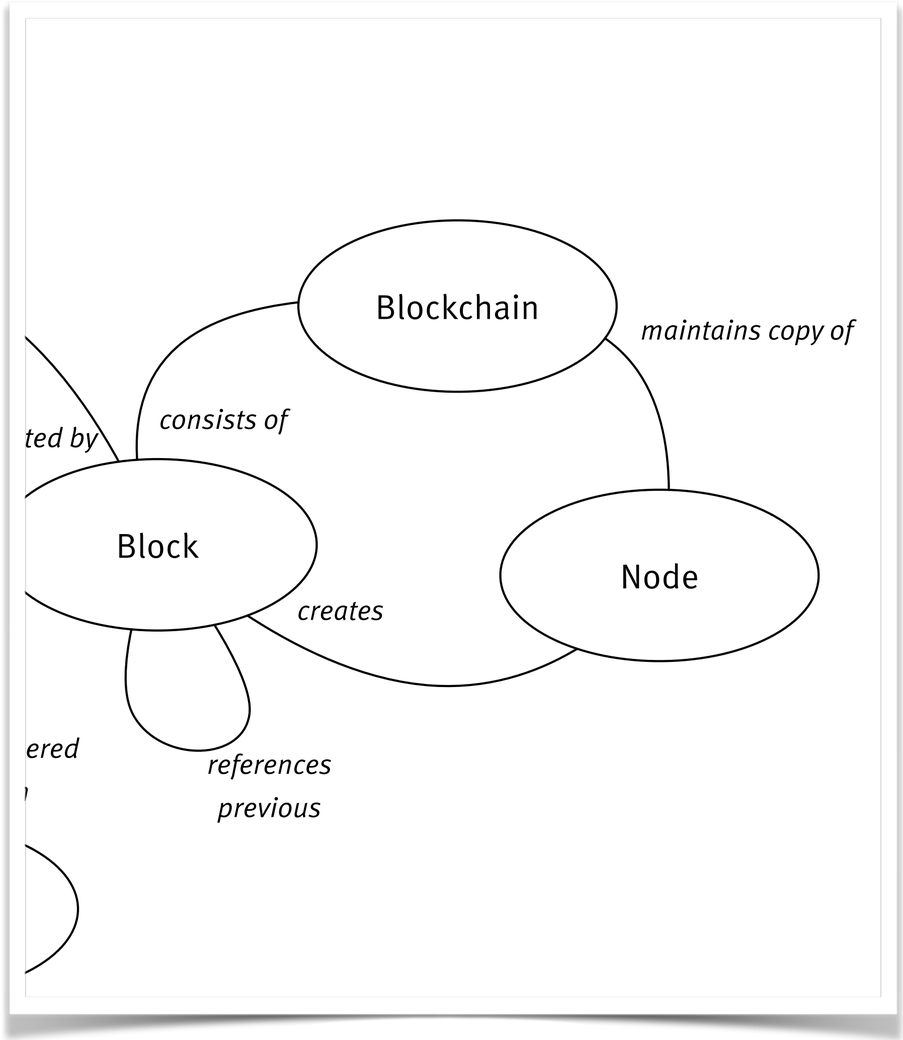
- Proof: Find a SHA256 input that meets network “difficulty target”)
- Cheaper to play by the rules than to cheat
- Difficulty adjusted over time
- Only way for new bitcoins to get introduced
- Optional transaction fee

Bitcoin: Nodes



- Form a peer-to-peer network
- Relay messages
- Validate transactions and blocks
- Maintain a copy of the blockchain

Bitcoin: Blockchain



- Linked list of all blocks ever created
- Can and will be validated by every node
- History of every transaction ever performed
- Not actually a ledger

Bitcoin: Validation/Consensus

- Blocks chain – the more blocks reference a block, the better
- Transactions considered immutable after 6 blocks
- Consensus by means of “longest chain”

Bitcoin: Script

- Intentionally limited scripting
- P2SH (“pay to script hash”) address (as opposed to P2PKH)
- Usage e.g. for multi-signature (joint accounts)
- Challenge: To spend, provide valid input to script
- Base script: Ensure recipient has correct private key

2.

ethereum

Ethereum vs. Bitcoin

- Blockchain as technical basis
- Currency: Ether
- 1 Block approx. every minute
- Currently *proof of work*, change to *proof of stake* planned
- Platform for arbitrary contracts
- State as part of the blockchain

Ethereum: Contracts & Code

- Accounts can externally owned
- Accounts can be embodied by code (“contract account”)
- Contracts specify rules for interactions

“Here, run that code for me, will ya?”

Ethereum: Gas

- Computation requires payment (“gas”)
- Amount determined by caller
- Execution of instructions consumes gas

Ethereum: Programming

- Low-level byte code: EVM
- Multiple languages
  - LLL (Lisp-like, low-level)
  - Serpent (Pythonesque)
  - Solidity (similar to JavaScript, but statically typed)
- Executed by every node mining or validating blocks

3. Alternatives

Alternative approaches

- Altcoins (Litecoin, Namecoin, Dogecoin, Devcoin, Bytecoin, ...)
- Colored coin
- Metacoin
- Sidechains

Private (“permissioned”) ledgers

- Used internally or with trusted partners
- Lots of startups: clearmatics, Eris, Peernova, BigchainDB, ...
- OSS initiative: HyperLedger (Fabric, Sawtooth Lake)

4.
What’s cool about it?

Distributed Consensus

- Trustable, secure
- Immediate
- (Mostly) Unbreakable

Open access

- Anyone can participate
- No centralized control
- Globalized

- *Detour: Politics*

Disrupting intermediaries

- Intermediaries provide consistency as a service
  - Risk of monopolies
  - Expensive
  - Possibly influenced by politics
- Blockchain cuts out the middle man

Cost reduction for clearing

- Collaborations rely on clearing e.g. in finance, logistics, energy
- Reduced cost due to “permissioned” model (more trust)

5.
What about the bad parts?

Bitcoin: Fraud

- Every bitcoin theft due to exchanges
- Not a single successful attack on the blockchain itself
- Much less vulnerable than any other currency

Ethereum: Vulnerabilities

- TheDAO on Ethereum: 150 million USD investment
- Theft (?) of 60 million USD due to bug in contract code
- Ethereum Hard-fork

“If code is law, what’s wrong with bugs?”

Bitcoin: Scalability

- 1 block every ten minutes
- Current size limit: 1 MB – 5,000 tx – 600 sec – 8.3 tx/s
- Current visa tx rate: 5,000-50,000 tx/s
- Possible solutions:
  - Increase block size
  - “Segregated witness”

Bitcoin: Volatility

- Exchange rate with other currencies (real and crypto)
- Much more stable in recent months
- Will likely calm down even more
- Has hurt “the brand” significantly

6. Use Cases

Property Management

- Record (partial) ownership
- Trade property/shares
- Identity
- DRM
- Access Control
- Digital Assets

Obligations

- Emission fees
- Debt
- Clean energy fares

Distributed Autonomous Organizations

- Complex interactions among participants
- Multi-tiered
- Corporation contracts as code

Other use cases

- Fully automated payment (Charging, Usage fees “Maut”)
- Public records of GPS tracking
- Safe auditing with legitimate (limited) law enforcement access

7. Summary

(a.k.a. what I believe today)

Trusted, distributed, decentralized platforms will play a significant role in many industries

Don’t dismiss Bitcoin, Ethereum or public, permissionless blockchains in general just yet

Permissioned ledgers may be the future – or just an intermediate step to a new shared platform (similarly to the Internet)

The barrier to entry has never been this low – commercially as well as from a technical perspective

Disrupt or be disrupted

Thank you.

Questions?

Comments?

@stilkov

Stefan Tilkov

stefan.tilkov@innoq.com

Phone: +49 170 471 2625

innoQ

www.innoq.com

innoQ Deutschland GmbH

Krischerstr. 100
40789 Monheim am Rhein
Germany
Phone: +49 2173 3366-0

Ohlauer Straße 43
10999 Berlin
Germany
Phone: +49 2173 3366-0

Ludwigstr. 180E
63067 Offenbach
Germany
Phone: +49 2173 3366-0

Kreuzstraße 16
80331 München
Germany
Phone: +49 2173 3366-0

innoQ Schweiz GmbH

Gewerbestr. 11
CH-6330 Cham
Switzerland
Phone: +41 41 743 0116