GOTO Amsterdam 2018

Blockchain Consensus: Let's All Just Agree

Stefan Tilkov
@stilkov

INNOQ

Classical Consensus

- Foundational theory: Replicated State Machines
- Two-phase commit
- View-stamped replication
- Paxos
- Raft
- Zab
- ...

Classical Consensus

- Low-latency, (partially) synchronous networks
- Widely used
- well-researched Safety, Liveness properties

Byzantine Failure Tolerance

Byzantine Failure

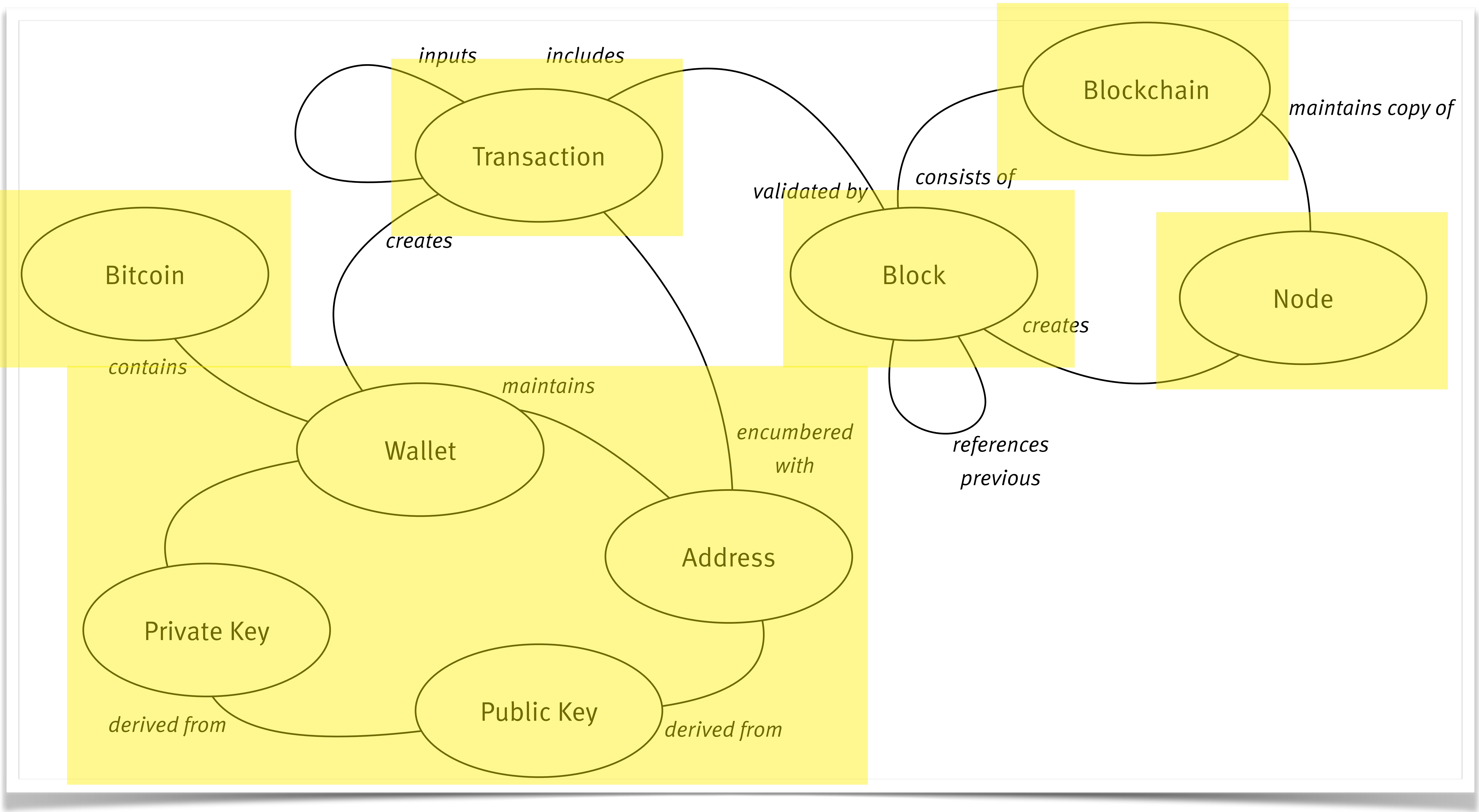
- Actors that are not only unreliable, but also
  - Erroneous
  - Malicious
- Key question: How many traitors to tolerate

Practical Byzantine Fault Tolerance (PBFT)

- Formally documented (M. Castro/B. Liskov, 1999)
- Implementations, e.g. BFT SMaRt
- Tolerates (n-1)/3 faulty replicas

- Scalability/Complexity O(n^2)
- Closed Group

Blockchain & Bitcoin

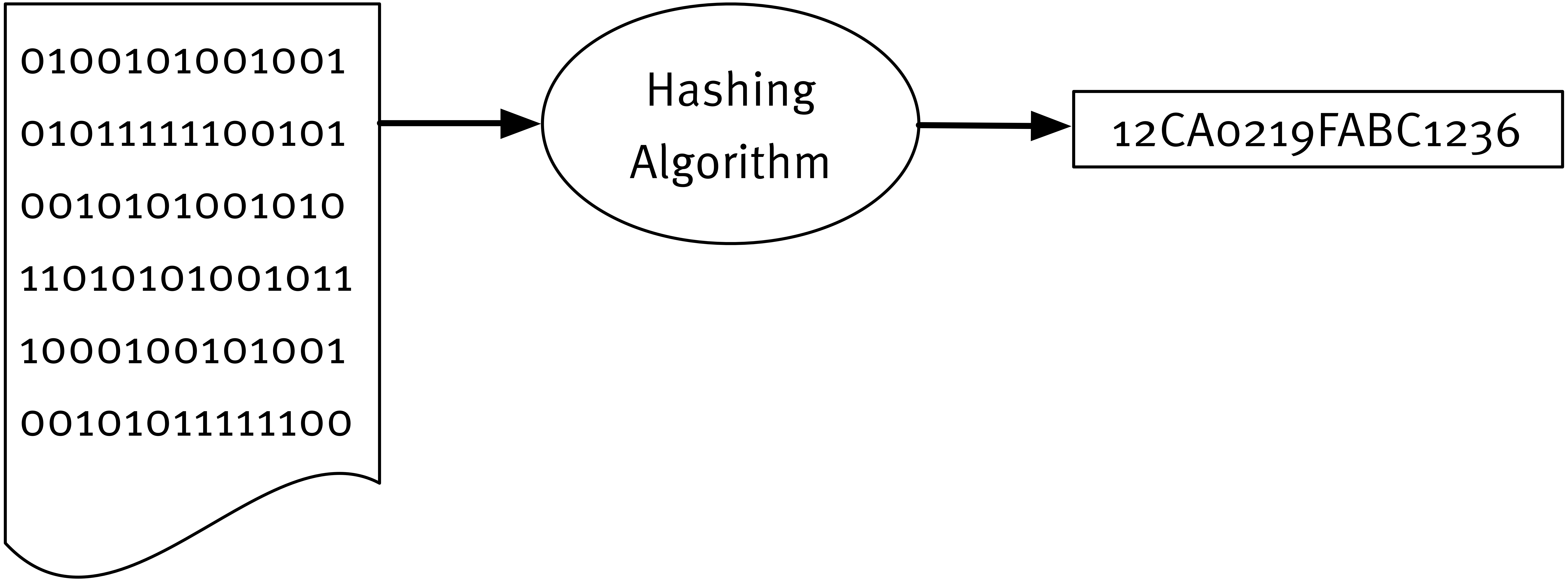


Bitcoin:
Nakamoto Consensus

Bitcoin: Nakamoto Consensus

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

Hashing

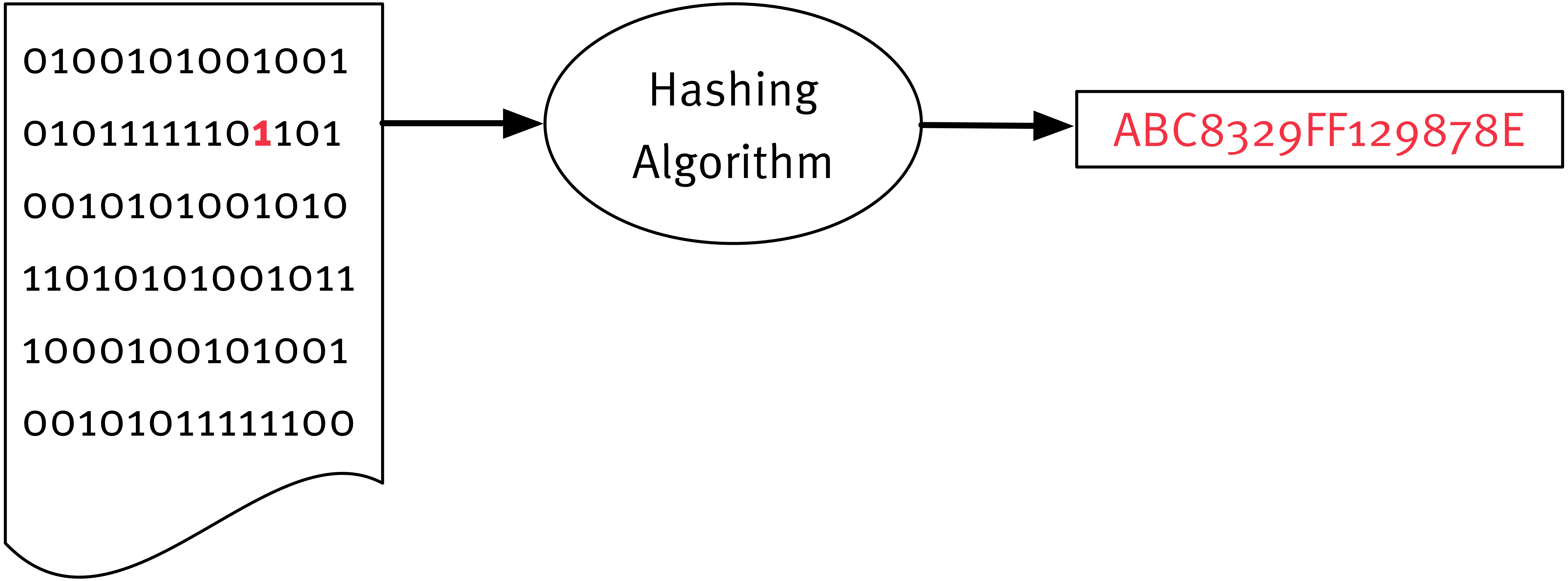


0100101001001
0101111100101
0010101001010
11010101001011
1000100101001
00101011111100

Hashing Algorithm

12CA0219FABC1236

Hashing



0100101001001

0101111110**1**101

0010101001010

11010101001011

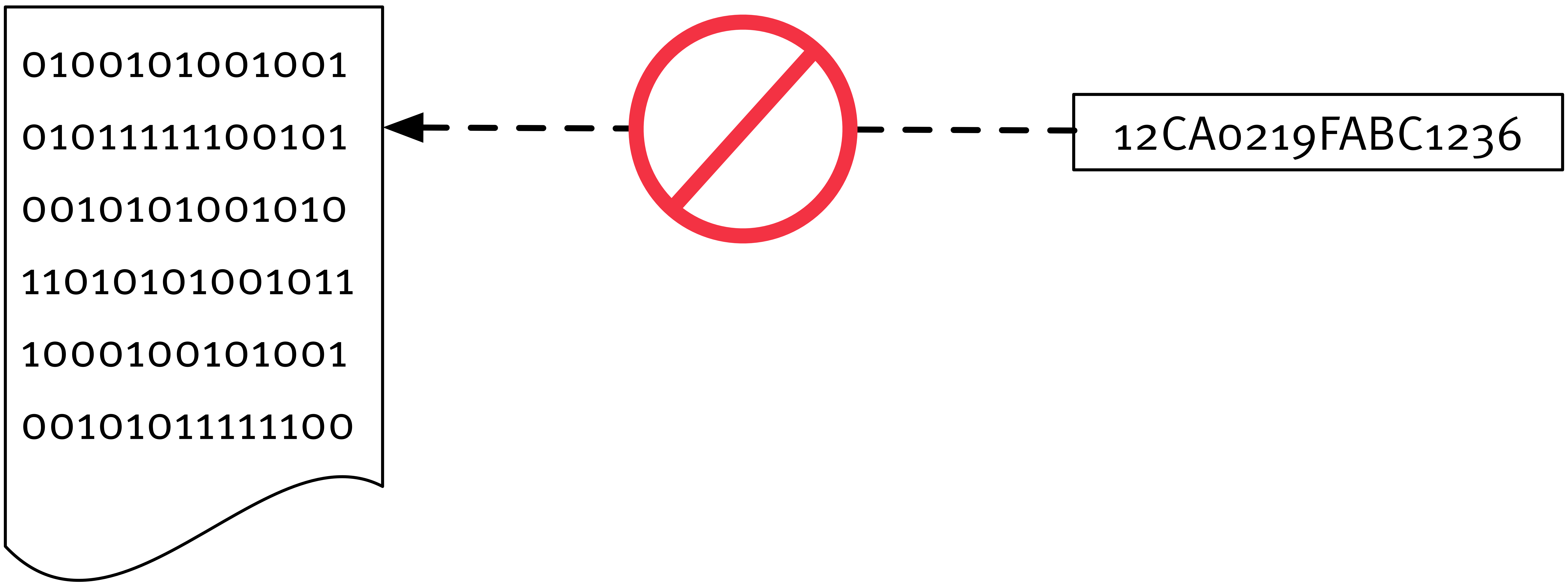
1000100101001

00101011111100

Hashing Algorithm

ABC8329FF129878E

Hashing



0100101001001

0101111100101

0010101001010

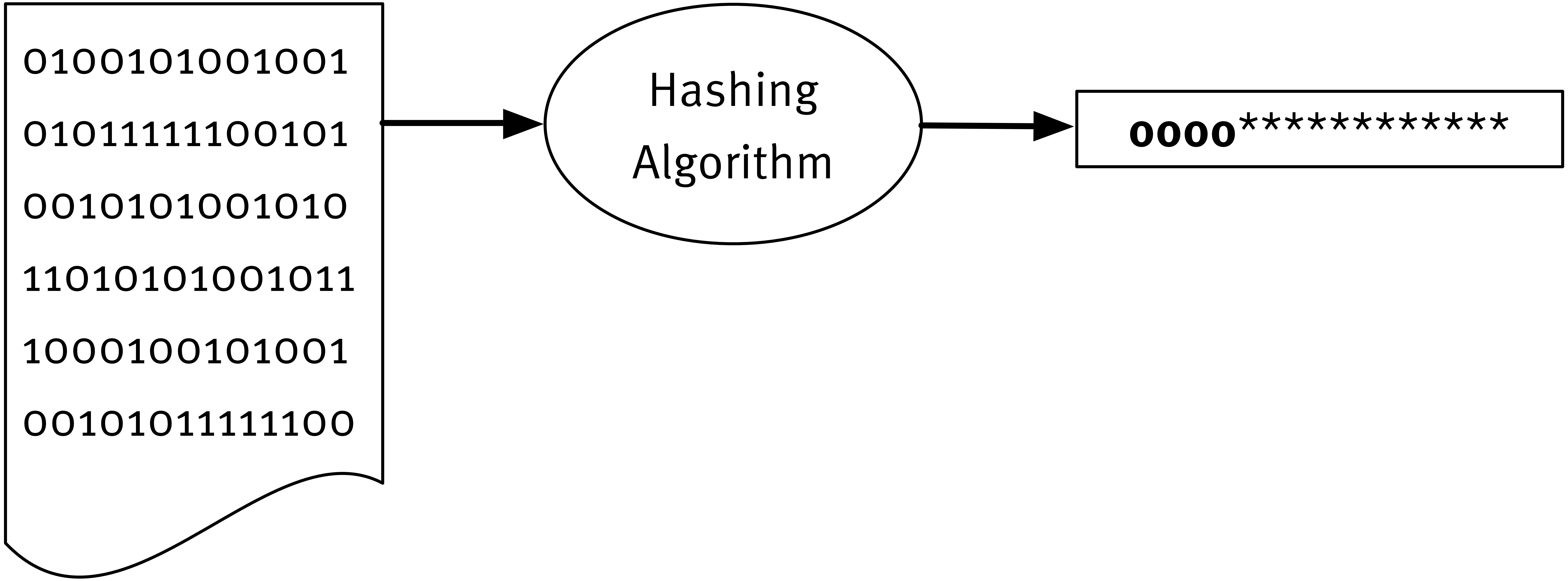
11010101001011

1000100101001

00101011111100

12CA0219FABC1236

Proof of Work (PoW)



0100101001001

01011111100101

0010101001010

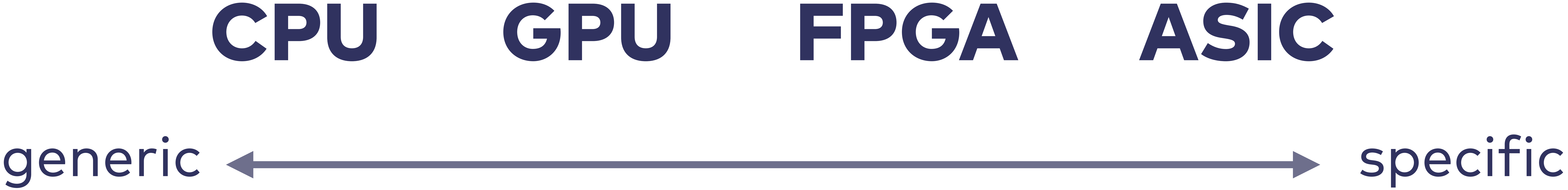
11010101001011

1000100101001

00101011111100

Hashing Algorithm

0000************



CPU **GPU** **FPGA** **ASIC**

generic ↔ specific

SHA-256^2

Scrypt

Ethash

X11

PoW Energy Discussion

Position 1: "Catastrophic"

- Continuously increasing demand
- The Netherlands: 106TWh/y
- Bitcoin: 65 TWh/y
- Little to no value, only speculation
- Use of cheap & dirty energy sources
- Completely useless hardware with limited shelf life

PoW Energy Discussion

Position 2: “No big deal”

- Demand will not increase linearly
- More useful than Christmas lights
- Transparent costs, as opposed to classical banking
- No need for multiple PoW chains
- Use of cheap & clean energy sources, excess energy
- ASIC-resistant algorithms

Problems to solve

Transaction Validation

Committee Selection

Consensus

Governance

Permissioned vs. Public

DB	e.g. Ripple	e.g. Dash	Bitcoin
Trusted, Known	**Untrusted, Known**	**Untrusted, Joined**	**Untrusted, Unknown**

Alternatives

Proof-of-stake

- Proof of commitment by owning/risking cryptocurrency
- Eligibility for voting and/or weight of vote determined by stake
- Hybrid model for transition period in Ethereum ("Casper, the FFG")
- Attacks: Nothing-at-stake, Long range
- Other examples: Cardano, EOS, NEO

PoS Variants

- On-chain: Validators anchored in blockchain, liveness (availability) over safety (consensus) (e.g. Casper)
- PBFT-based: Classical, safety over liveness (e.g. Tendermint)

Proof-of-service (PoSe)

- e.g. Dash: Bitcoin Fork, DAO model
- Adds “Masternode” concept
- Masternodes required to own 1000 Dash (>200k€)
- InstandSend, PrivateSend handled by masternodes
- 45%/45%/10% fee split miners/masternodes/funds

Proof-of-capacity (PoC)

- a.k.a. Proof-of-space
- used in e.g. Burst
- Pre-computed solutions to problem
- Hard to compute, easy to verify (e.g. hard-to-pebble graphs)

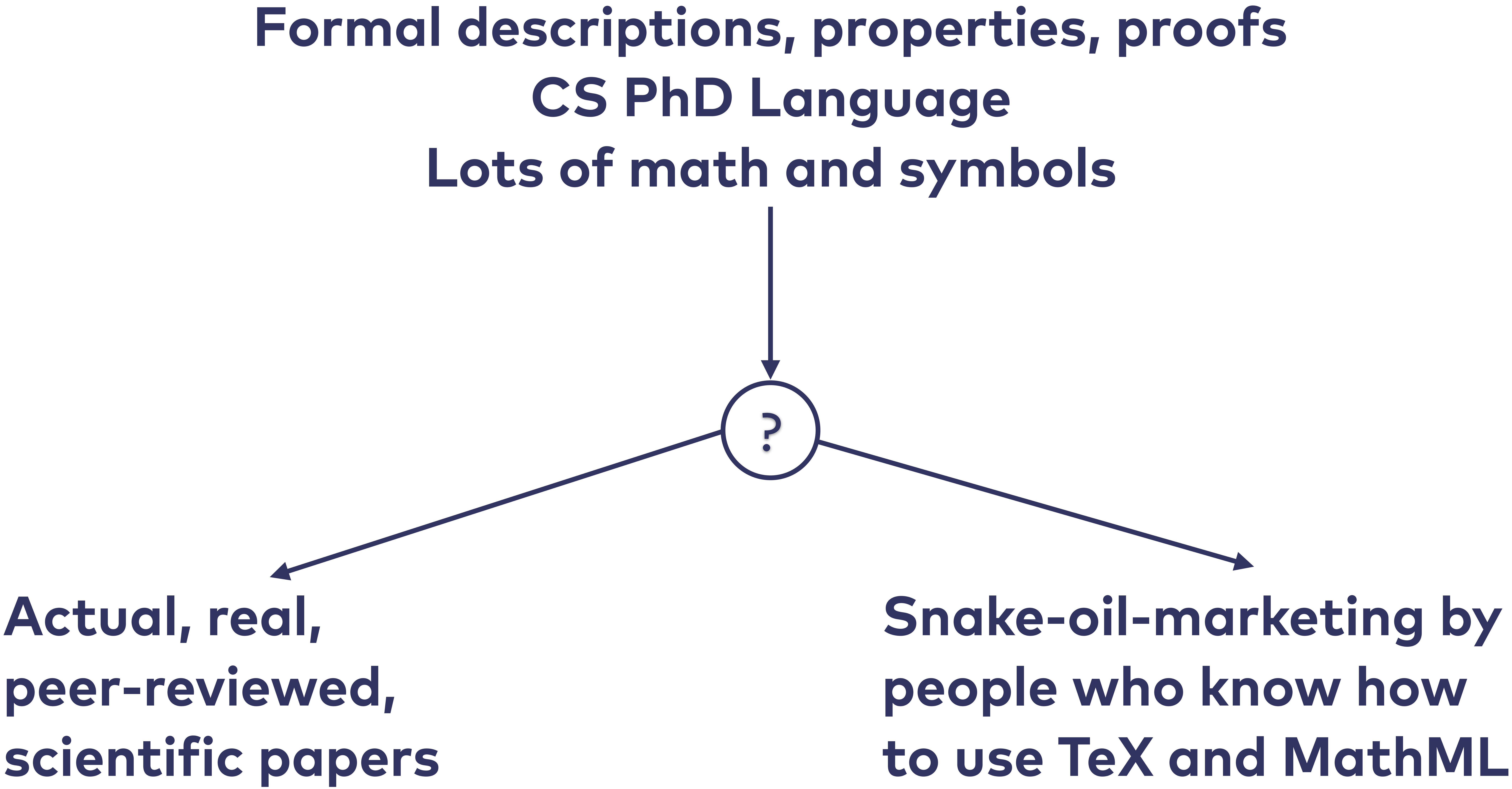
Proof-of-elapsed-time (PoET)

- Hyperledger Sawtooth
- Based on trusted hardware (e.g. Intel SGX)
- “Trusted lottery” based on wait time instead of PoW

XRP LCP, Cobalt

- Used by Ripple
- Unique Node List (UNL), maintained by users (clients)
- Currently mostly Ripple-owned validators
- Committee selection based on overlap
- Research led to better analysis for required overlap
- Cobalt as a new proposed protocol

Assessment Problem



Formal descriptions, properties, proofs
CS PhD Language
Lots of math and symbols

Actual, real,
peer-reviewed,
scientific papers

Snake-oil-marketing by
people who know how
to use TeX and MathML

Other Examples

- Hashgraph – Patented, strong marketing
- Avalanche – "Dropped" by "Team Rocket"
- Ouroboros – PoS, created by iohk,
  strong focus on academic cooperation

Summary

Proof of Work

a) sucks

b) works

Beware of alternatives with magic properties

Science may help

That's all I have.
Thanks for listening!
Questions?

Stefan Tilkov
@stilkov
stefan.tilkov@innoq.com
Phone: +49 170 471 2625

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

References

Overview

- Shehar Bano et al: SoK: Consensus in the Age of Blockchains (Paper), Morning Paper post by Adrian Colyer (Academic, many non-implemented papers and strategies referenced)
- Christian Cachin and Marko Vukolić: Blockchain Consensus Protocols in the Wild (Keynote text), Longer Version (focus on permissioned ledgers)
- Sigrid Seibold, George Samman: KPMG Whitepaper "Consensus Immutable agreement for the Internet of value", questionnaire results

Ethereum

- Vitalik Buterin and Virgil Griffith: Casper the Friendly Finality Gadget (Ethereums Proof-of-Stake algorithm, introduced in addition to PoW)

Ripple

- Brad Chase and Ethan MacBrough: Analysis of the XRP Ledger Consensus Protocol (original Ripple protocol)
- Ethan MacBrough: Cobalt: BFT Governance in Open Networks (proposed improved protocol for Ripple)

Burst

- Burst (Proof of Capacity) , Seán Gauld et al: The Burst Dymaxion (Mixing Tangle (like IOTA) with PoC blockchain)

Dash

- Evan Duffield et al: Transaction Locking and Masternode Consensus (PoS Masternodes, used for Governance, InstantSend, PrivateSend)

Avalanche

- Team Rocket: Snowflake to Avalanche: A Novel Metastable Consensus Protocol Family for Cryptocurrencies (new algorithm, hyped video)
- Review by Murat Demirbas (Prof at University of Buffalo), Interview with Emin Gün Sirer (Prof at Cornell)

Hashgraph

- Leemon Baird: Hashgraph Whitepaper (incl. marketing), technical paper

Sawtooth

- Jan Felix Hoops: An introduction to Public and Private Distributed Ledgers (Proof of elapsed time based on Intel's SGX extension)

Cardano

- Kiayias et al: Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol

Misc

- http://www.bailis.org/blog/safety-and-liveness-eventual-consistency-is-not-safe/

INNOQ

www.innoq.com

SERVICES

Strategy & technology consulting

Digital business models

Software architecture & development

Digital platforms & infrastructures

Knowledge transfer, coaching & trainings

FACTS

~125 employees

Privately owned

Vendor-independent

OFFICES

Monheim

Berlin

Offenbach

Munich

Zurich

CLIENTS

Finance

Telecommunications

Logistics

E-commerce

Fortune 500

SMBs

Startups