Blockchains, Distributed Ledgers, and more

Stefan Tilkov
@stilkov

INNOQ

Blockchain (noun) \ ˈbläkˈchān:
A slow, hard-to-scale, distributed immutable event log with a consensus approach based on turning a tree into a chain by converging on the branch with the most hashing power provably spent on it

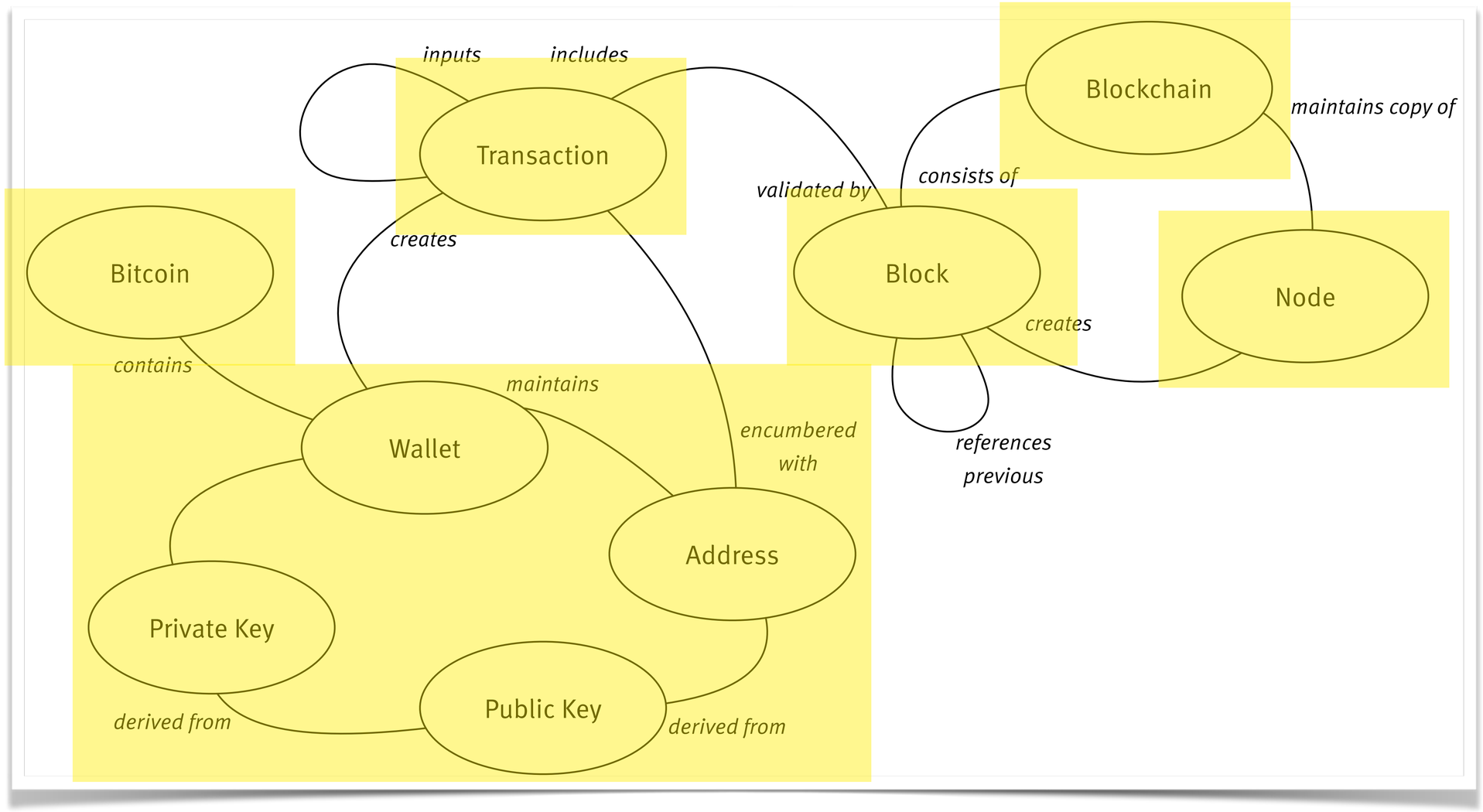
Ledger (noun) /ˈlɛdʒə/
a book or other collection of financial accounts

Distributed Ledger (noun) /ˈdɪstrɪbjuːtíd ˈlɛdʒə/
A blockchain not called a blockchain because
(a) it doesn't actually chain blocks or
(b) you think blockchains are uncool

@stilkov

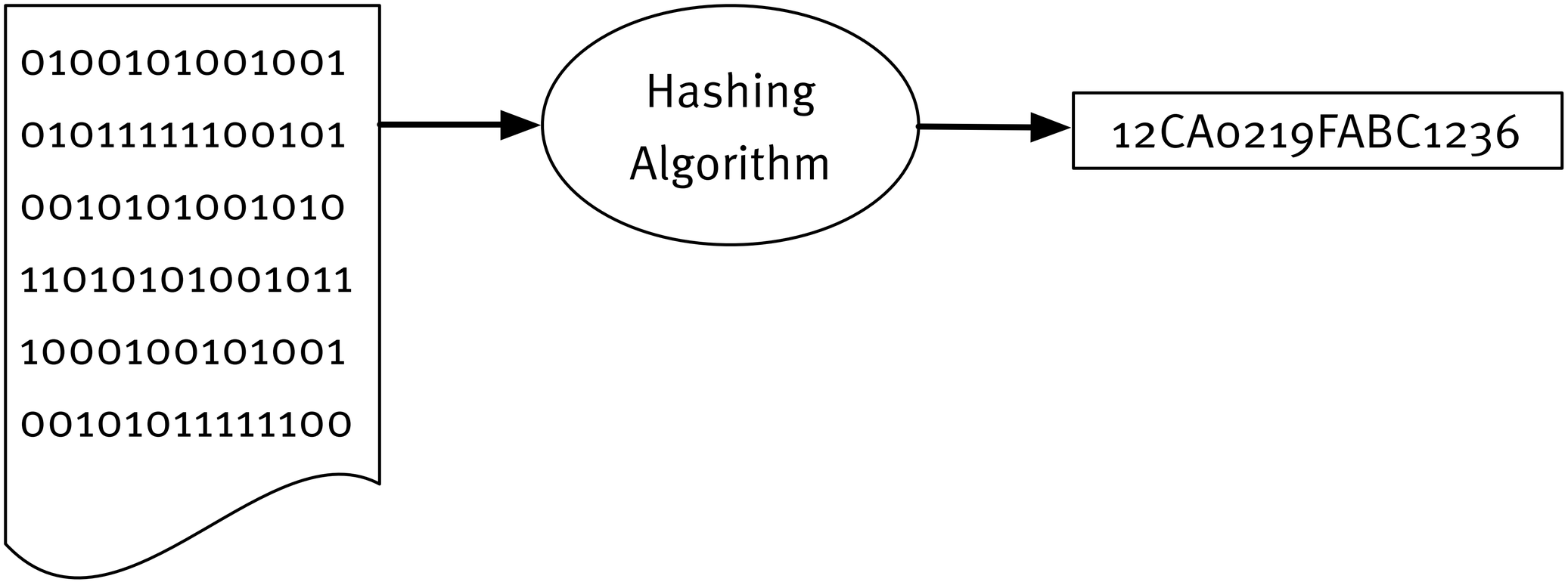

bitcoin

Bitcoin: Vocabulary

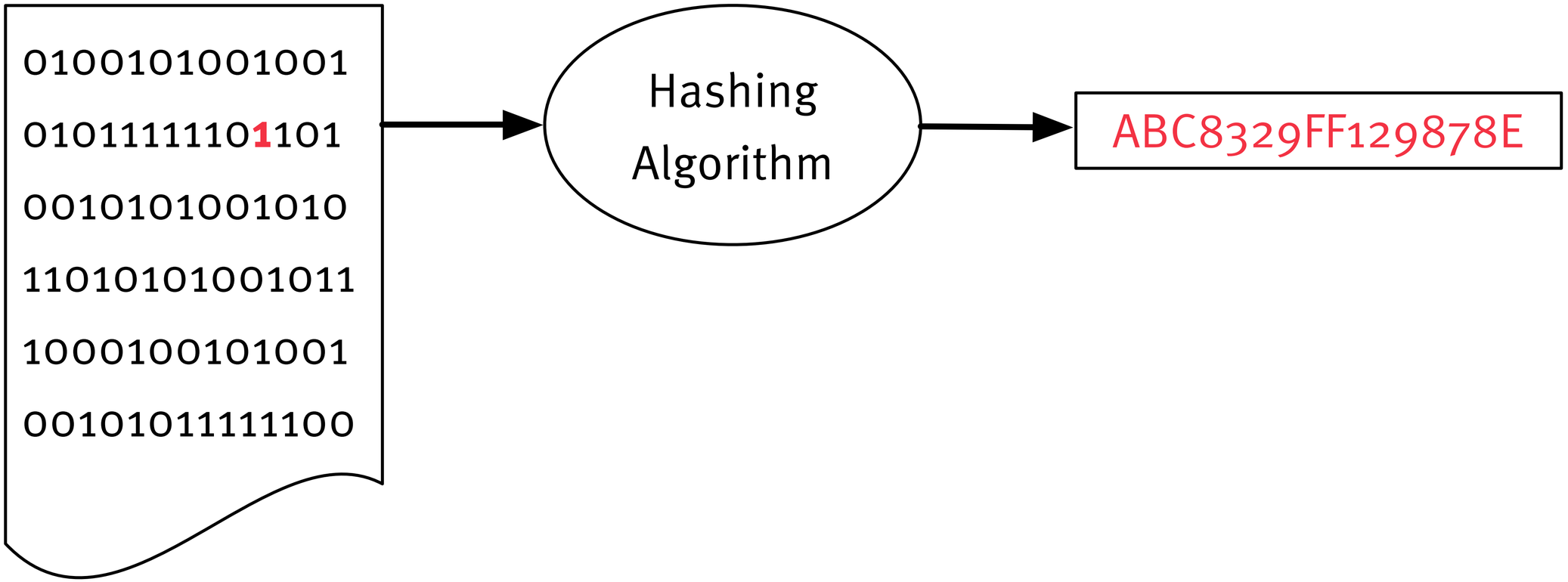


Consensus and Byzantine Failure Tolerance

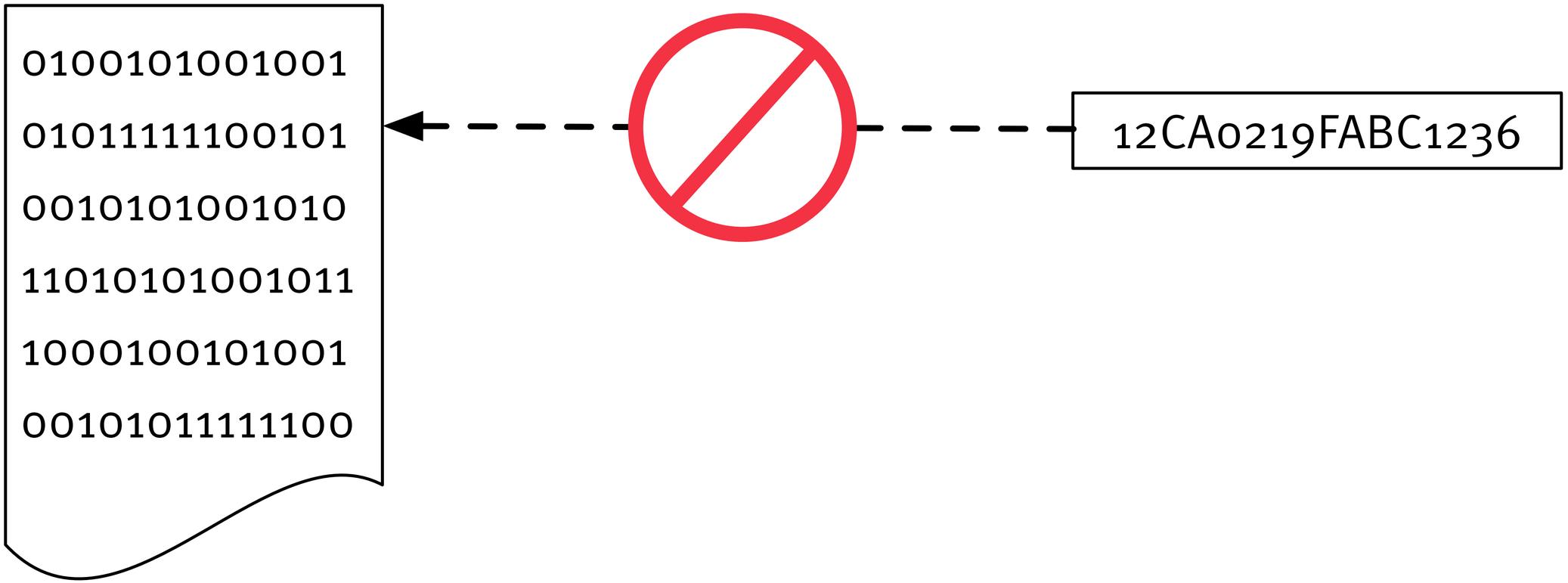
Hashing and Proof-of-work (PoW)



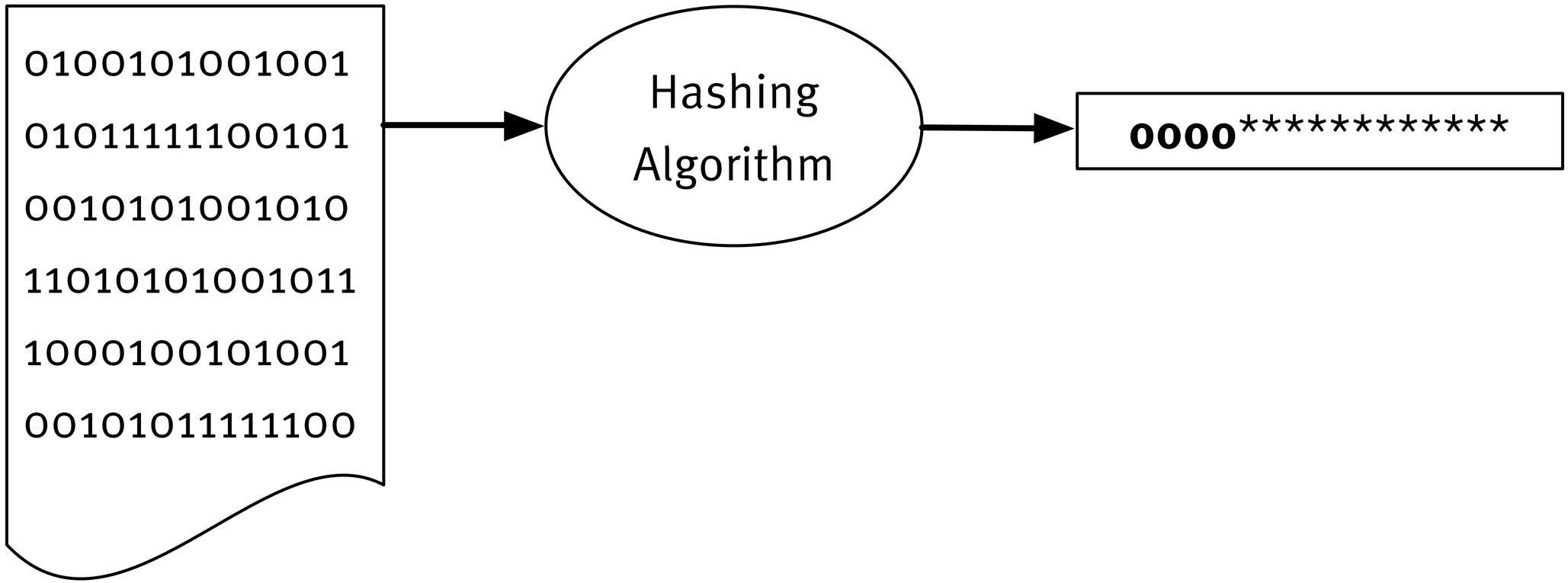
Hashing and Proof-of-work (PoW)



Hashing and Proof-of-work (PoW)



Hashing and Proof-of-work (PoW)



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

@stilkov

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

Proof-of-work alternatives

- Proof-of-stake (PoS)
- Proof-of-authority (PoA)
- Proof-of-service (PoSe)
- Proof-of-capacity (PoC)
- Proof-of-elapsed-time (PoET)
- ...

Permissioned vs. Public

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

ethereum

@stilkov

Criteria
a.k.a.
"So you think you need a blockchain ..."

Do you really need decentralization?

- Is there a single trusted organization?
- Do you trust it to not be malicious?
- Do you trust in its competency and security practices?
- Do you trust its longevity?

You don’t need a blockchain.

Are you suspicious about history?

- Can you trust available information is correct?
- Can you trust it hasn't been tampered with?
- Can you trust it's complete?

You don't need a blockchain.

Do you want to invite everyone?

- Do you have control over who can participate?
- Do you have a separate onboarding process?

You don’t need proof of work.

Is identity/authority problematic?

- Do you trust that participants are who they say they are?
- Can you be sure they have the authority to do what they do?
- Is there a trusted arbitrator?

You don't need proof of work.

Do you have doubts about processes?

- Can you trust computation followed the rules you expected?
- Can you trust code is correct?
- Can you trust code hasn't been tampered with?

You don't need smart contracts.

Do you have nothing to hide?

- Is all the data supposed to be private?
- Is data only supposed to be visible to a subset of your users?
- Is pseudonimity an insufficient solution?

You can't store your data in a (public) blockchain.

Criteria

- Do you really need decentralization?
- Are you suspicious about history?
- Do you want to invite everyone?
- Is identity/authority problematic?
- Do you have doubts about processes?
- Do you have nothing to hide?

Examples

Property Management

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

Obligations

- Taxation
- Emission fees
- Debt
- Clean energy fares
- …

Insurance and finance

- Claim regulation
- Ownership transfer
- Shared sign-off
- Intra-bank clearing
- Asset management
- Risk management/sharing
- …

E-Commerce

- Provenance tracking
- Virtual Marketplaces
- Participation models
- Loyalty programs
- …

Other use cases

- Tracking of certifications
- Fully automated payment (charging, usage fees)
- Public records of GPS tracking
- Safe auditing with legitimate (limited) law enforcement access
- …

Summary

You probably don't need a blockchain

If you need one, carefully select something that matches your needs

Beware of snake oil vendors

Explore the benefits and disrupt :)

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

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

More at: https://blockchain.innoq.com

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

@stilkov