Blockchains

Introduction to Blockchains

Christian Grothoff

Bern University of Applied Sciences

31.05.2024

Learning Objectives

What is a Blockchain?

What properties are Blockchains claimed to have?

How does Proof-of-Work solve the Byzantine consensus problem?

Bitcoin and Payments: A good match?

What are other applications for Blockchains?

Blockchain[1]

[1] Illustrations by Alexandra Dirksen, IAS, TUBS [3]

Blockchain

Blockchain

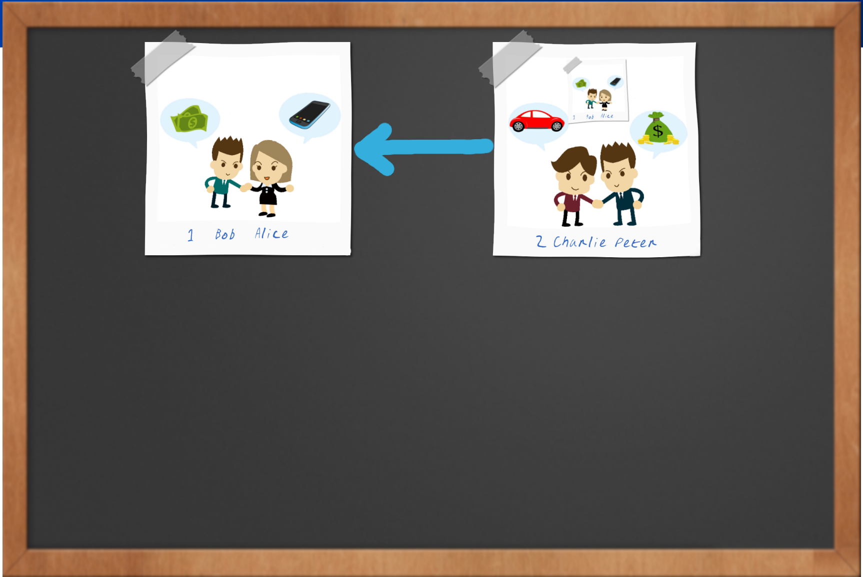
Charlie
Peter

Blockchain

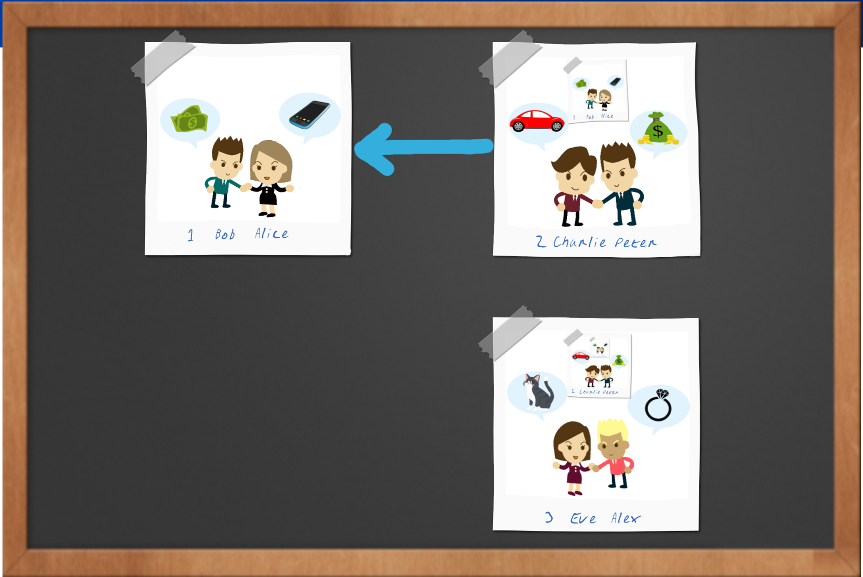
Blockchain

1 Bob Alice
2 Charlie Peter
1 Bob Alice

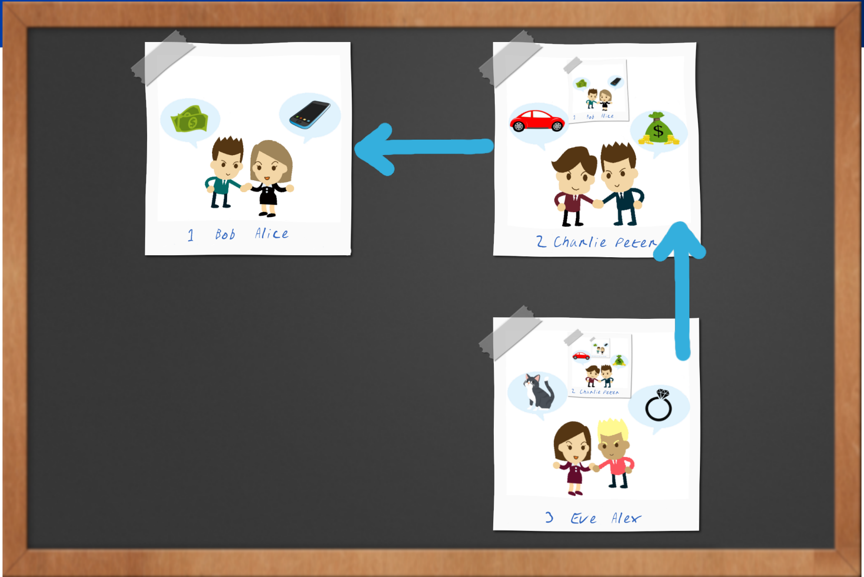
Blockchain



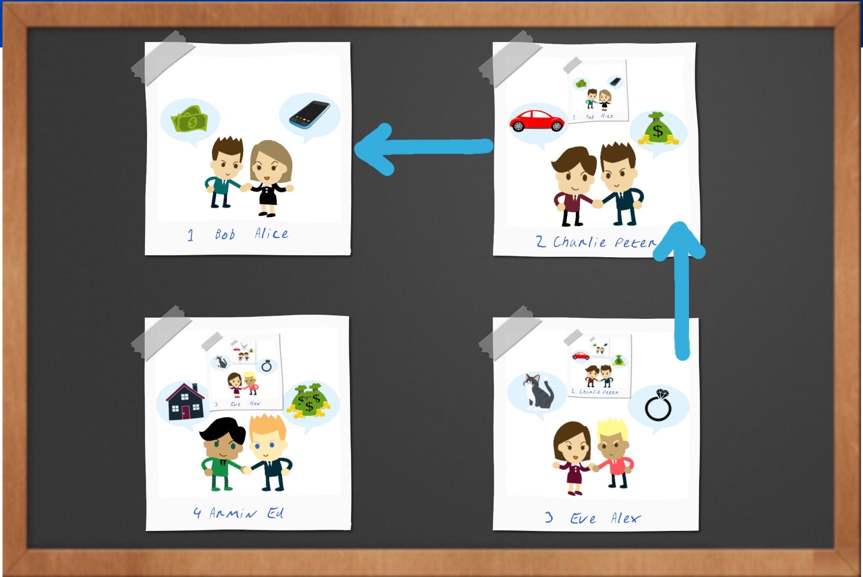
Blockchain



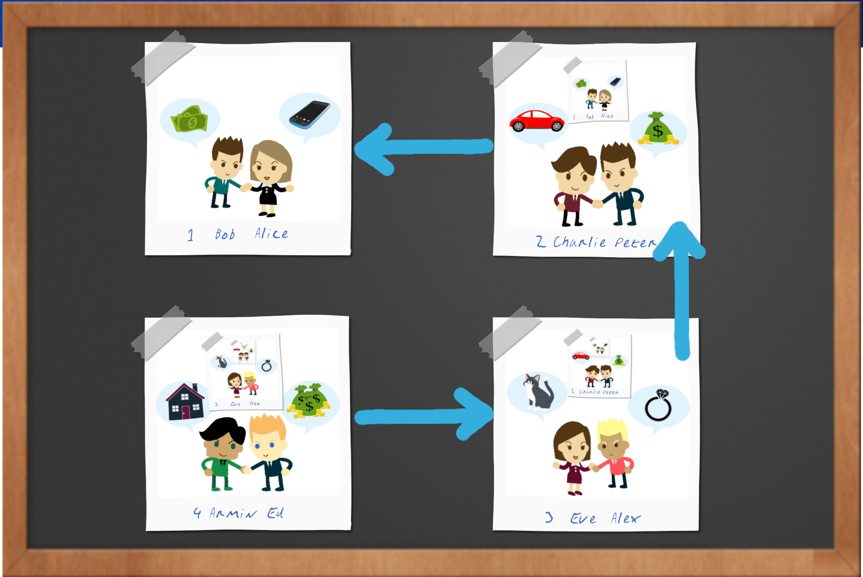
Blockchain



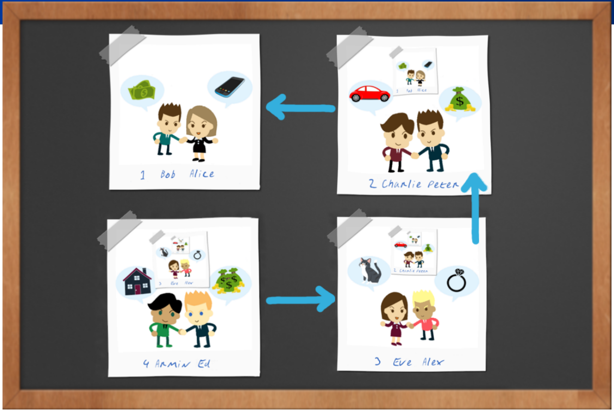
Blockchain



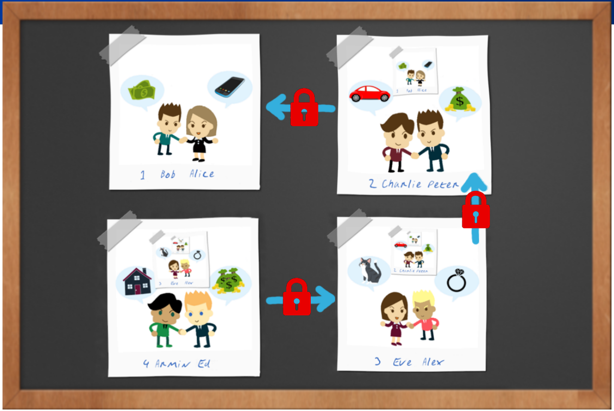
Blockchain


1 Bob Alice
2 Charlie Peter
1 Bob Alice
3 Eve Alex
2 Charlie Peter
4 Armin Ed
3 Eve Alex

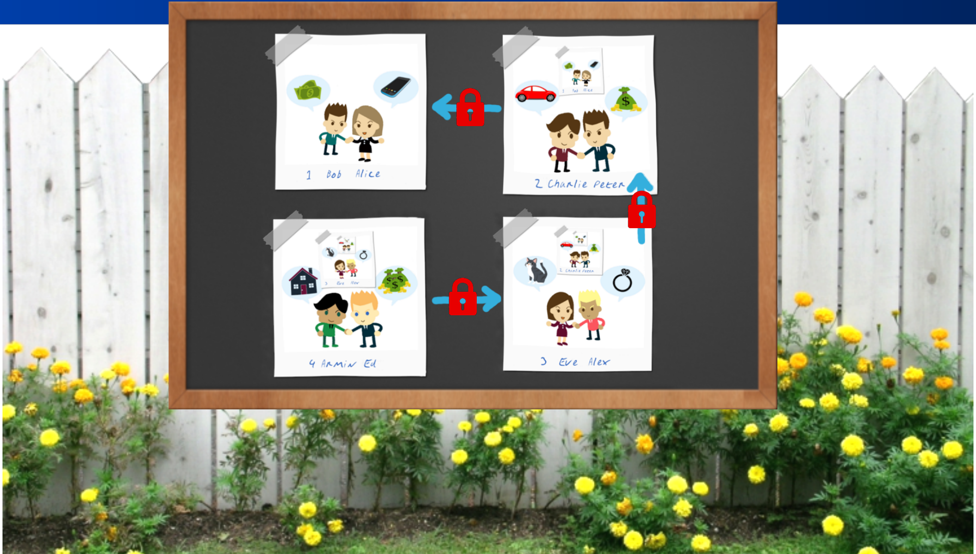
Advertised Blockchain “properties”



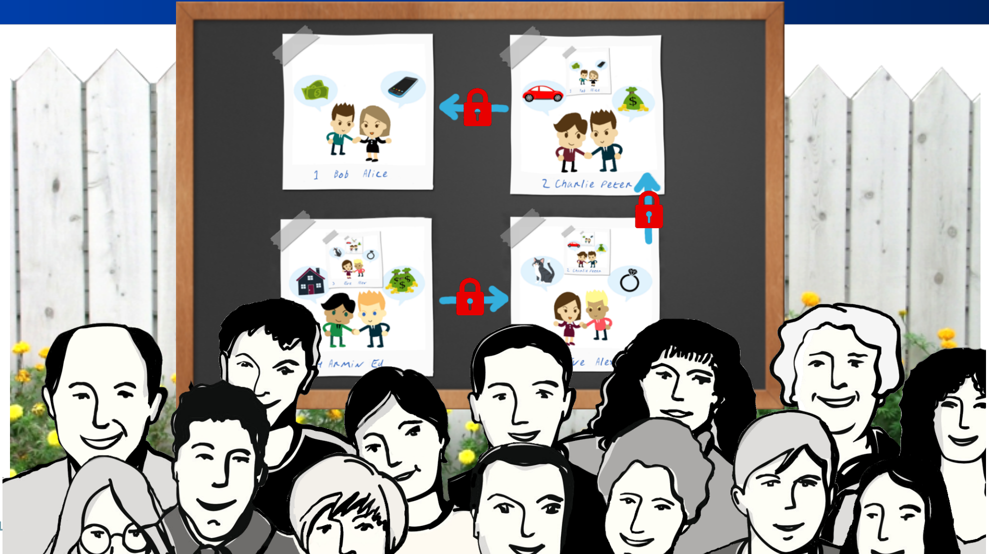
Immutability



Transparency



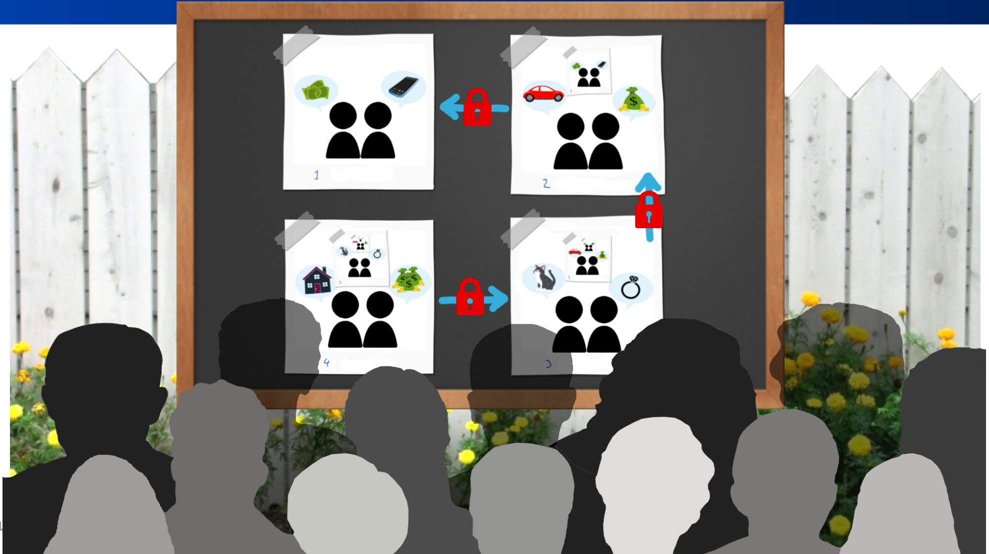
Decentralisation



Autonomy

1 Bob Alice
2 Charlie Peter
4 Armin Ed
3 Eve Alex

Anonymity

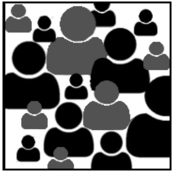


Summary: Blockchain "properties"

Immutability

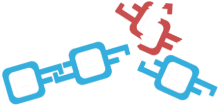
Transparency

Anonymity



Decentralisation

Autonomy

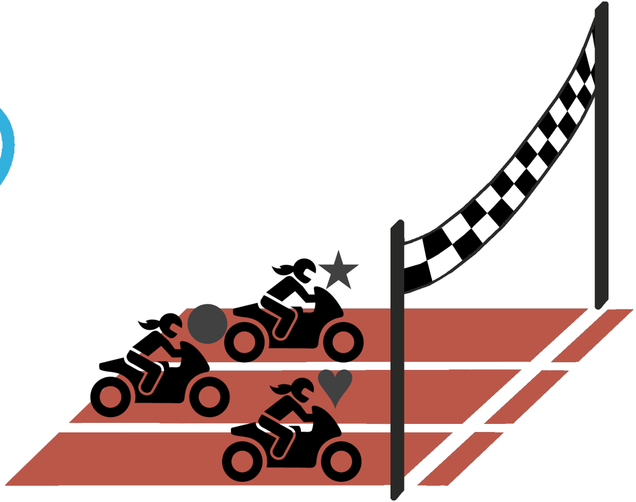


Irreversibility

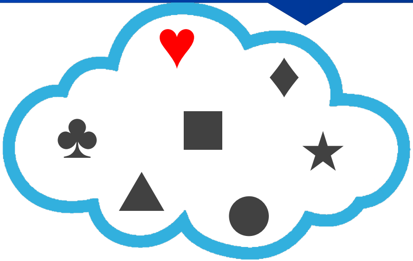
Who gets to append the next block?

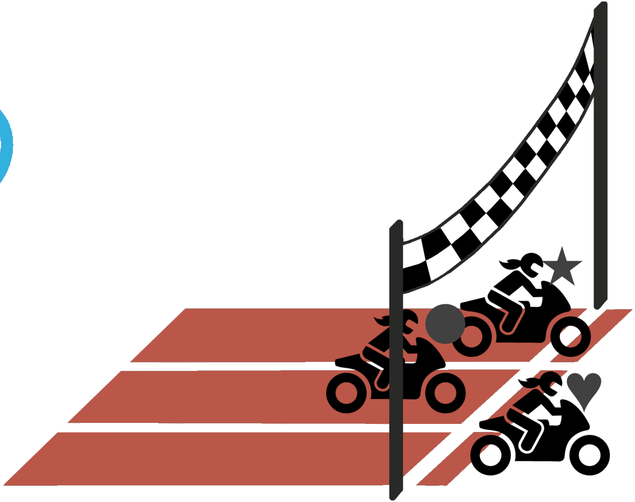
Proof of Work

Proof of Work

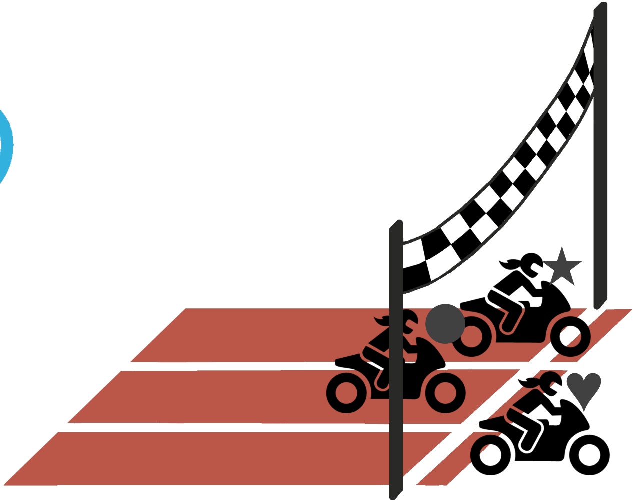


Proof of Work

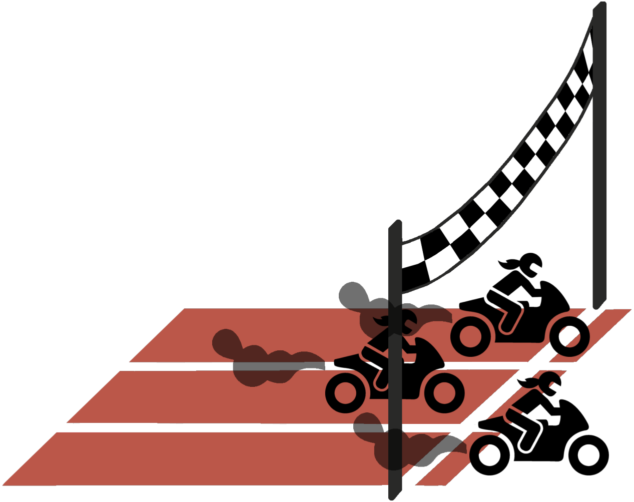




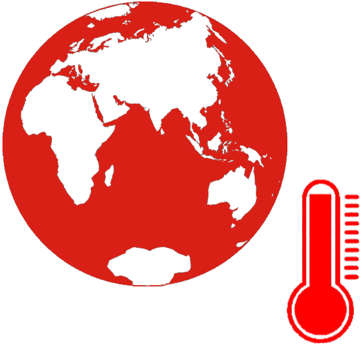
Proof of Work

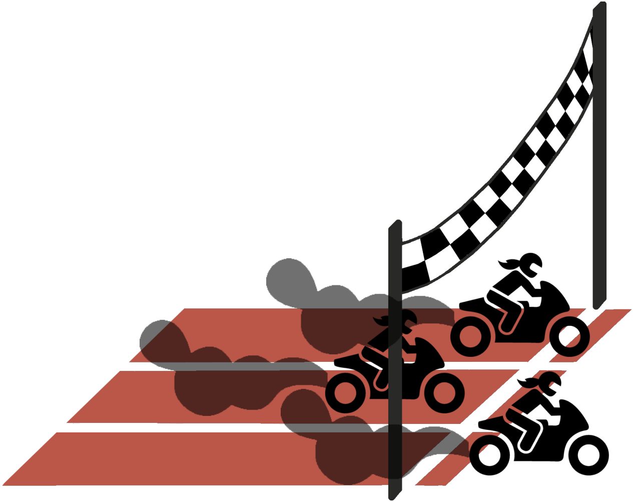


Proof of Work



Proof of Work





Bitcoin for Payments

Bitcoin claims to be a *payment system* using a Blockchain:

- Public keys identify accounts, private keys used to send money from the account into other accounts.
- Set of internally consistent transactions form each block
- Each block includes a transaction creating fresh coins and transferring applicable fees to block creator
- Computational difficulty adjusts to mining power. A new block is mined in $\approx$ 10 minutes
- Amount of bitcoin money supply created per block is exponentially decreasing

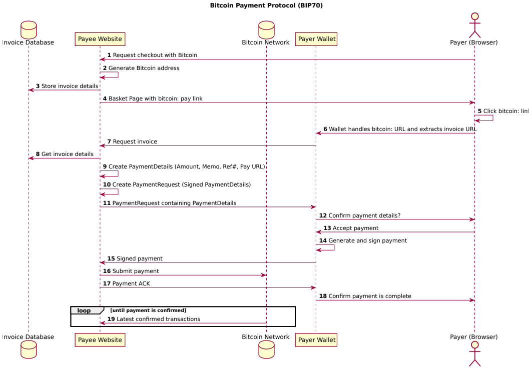
Rational Forking

Imagine:

- The previous block had a transaction from X to Y over 100 BTC with a fee of 0.001 BTC, a block reward of 7.5 BTC and total transaction fees of 5 BTC.
- The next consistent blocks can be assumed to again have block rewards of 7.5 BTC and transaction fees of 5 BTC.
- The issuer X of the 100 BTC transaction now signs a conflicting transaction where 50 BTC go to Z with a 25 BTC transaction fee.

What is the **rational** behavior for a miner M?

Bitcoin Payment flow (by W3C Payment Interest Group)



Bitcoin Payment Protocol (BIP70)

Invoice Database

Payee Website

Bitcoin Network

Payer Wallet

Payer (Browser)

1 Request checkout with Bitcoin

2 Generate Bitcoin address

3 Store invoice details

4 Basket Page with bitcoin: pay link

5 Click bitcoin: linl

6 Wallet handles bitcoin: URL and extracts invoice URL

7 Request invoice

8 Get invoice details

9 Create PaymentDetails (Amount, Memo, Ref#, Pay URL)

10 Create PaymentRequest (Signed PaymentDetails)

11 PaymentRequest containing PaymentDetails

12 Confirm payment details?

13 Accept payment

14 Generate and sign payment

15 Signed payment

16 Submit payment

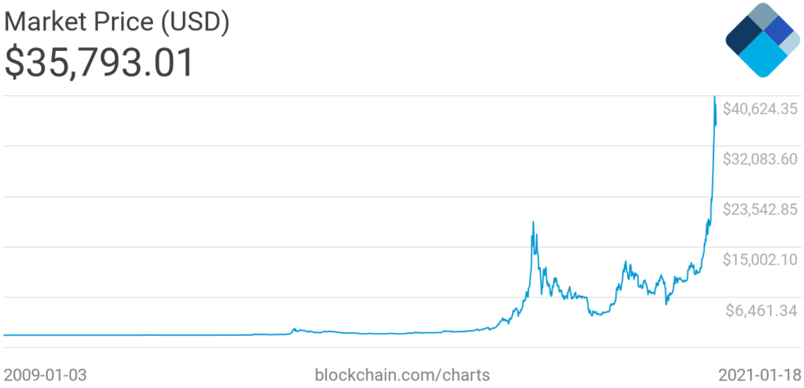
17 Payment ACK

18 Confirm payment is complete

loop **[until payment is confirmed]**

19 Latest confirmed transactions

The Value of Bitcoin



Market Price (USD)

$35,793.01

blockchain.com/charts

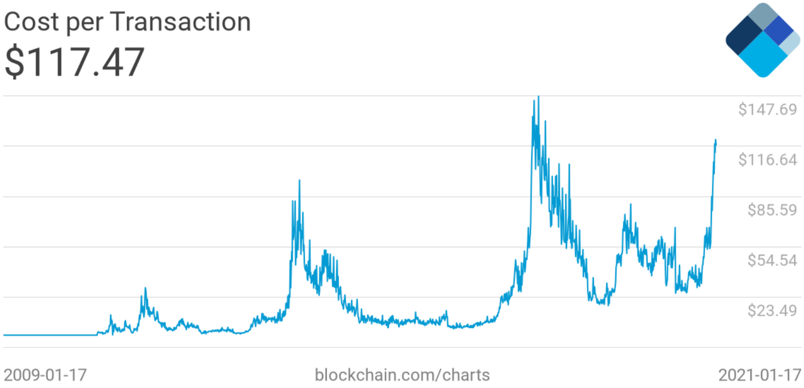
Mining

Mining requires:

- Learning pending transactions from peers
- Selecting a subset of of transactions which is valid (no double spending) by computing current account balances against the entire history
- Finding a hash collision (with adaptive difficulty)
- Propagating the new block to other miners

Usually specialized systems are used for finding hash collisions.

Mining cost



blockchain.com/charts

Current average transaction value: ≈ 1000 USD

Bitcoin performance

- Privacy: all transactions happen in the clear in public view
- Latency: transactions take 1h to kind-of be confirmed
- Storage: grows linearly forever, no garbage collection
- Power: Bitcoin mining consumes more than the Netherlands today
- Rate: Network handles at most about 7 transactions per second
- Accountability: use of public keys as addresses enables criminal use

⇒ Bitcoin fever lasting for years. Why?

Altcoins

- Dogecoin: same as Bitcoin, just named after a dog meme (an idea that is obviously worth billions!)
- Zcash: uses ZKSNARKs[2] to hide transactions (criminal activity on Bitcoin was too low)
- Ethereum: run Turing-complete virtual machine logic in the blockchain to enable "smart" contracts and arbitrary applications, not just payments (is "Accelerando" an utopia or dystopia?)
- Polkadot: use side-chains to improve scalability

[2] ≈ 1-15 minutes CPU time to create new transaction needed!

James Mickens on Blockchains

James W. Mickens is an American computer scientist and the Gordon McKay Professor of Computer Science at Harvard John A. Paulson School of Engineering and Applied Sciences at Harvard University. His research focuses on distributed systems, such as large-scale services and ways to make them more secure.

At the Digital Initiative's Future Assembly on April 6, 2018, he presented "Blockchains Are a Bad Idea: More Specifically, Blockchains Are a Very Bad Idea."

https://www.youtube.com/watch?v=15RTC22Z2xI (2018)

Break

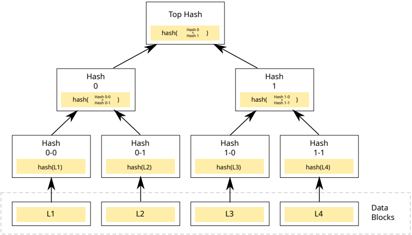
Security Goals for Time Stamping Services

- Document must have existed at the timestamp
- Modifications must be detected
- Document must have been created after the timestamp
- Validation of timestamp proof possible forever
- Non-repudiation
- No trusted third party (see [1, 4] for protocols with trusted third party)
- Availability

Blockchain-based Time Stamping Services

- `https://originastamp.com/`: Bitcoin&Ethereum, 100 timestamps $10
- `https://blockchainsign.io/`: Ethereum, 1 timestamp $5
- `https://guardtime.com/`: private KSI Blockchain (!?)

Key idea:



Security Goals for Name Systems

- Query origin anonymity
- Data origin authentication and integrity protection
- Zone confidentiality
- Query and response privacy
- Censorship resistance
- Traffic amplification resistance
- Availability

Approaches Adding Cryptography to DNS

- DNSSEC
- DNSCurve
- DNS-over-TLS (DoT)
- DNS-over-HTTPS (DoH)
- RAINS
- GNU Name System (GNS)

Namecoin

No need for a trusted third party: put the records into the Blockchain!

Or rather, put the public key of the owner and signed updates into it.

Plus, expiration rules.

Ethereum Name System[3]

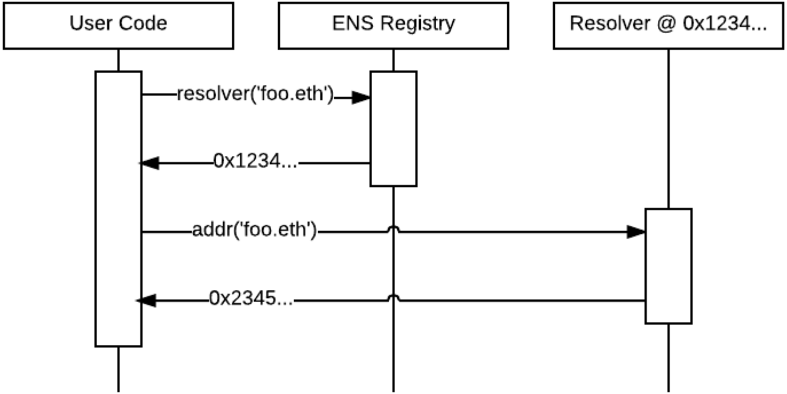
Let's have a smart contract in the Blockchain manage naming!

Blockchain contains smart contract and data who controls which name.

Contract allocates names under `.eth` using auctions.

[3] https://ens.domains/

Ethereum Name System[4]



[4] https://ens.domains/

Handshake Name System[5]

Incremental improvements over Namecoin and ENS:

- New blockchain with “HNS” utility tokens
- Compact proofs: resolvers do not need the full chain
- Pre-reserved names (ICANN TLDs, top-100k Alexa domains)
- Air-drop to “stakeholders” to boost adoption

[5] `https://handshake.org/`

References I

- C. Adams, P. Cain, D. Pinkas, and R. Zuccherato.
  Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
  RFC 3161 (Proposed Standard), August 2001.
  Updated by RFC 5816.
- David Chaum, Christian Grothoff, and Thomas Moser.
  How to issue a central bank digital currency.
  In *SNB Working Papers*, number 2021-3. Swiss National Bank, February 2021.

References II

- Alexandra Dirksen.
  A blockchain picture book.
  https://media.ccc.de/v/35c3-9573-a_blockchain_picture_book), 12 2018.

- D. Pinkas, N. Pope, and J. Ross.
  Policy Requirements for Time-Stamping Authorities (TSAs).
  RFC 3628 (Informational), November 2003.

Acknowledgements

Co-funded by the European Union (Project 101135475).

Co-funded by
the European Union

Co-funded by SERI (HEU-Projekt 101135475-TALER).

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union.

Neither the European Union nor the granting authority can be held responsible for them.