Blockchains
Introduction to Blockchains

Christian Grothoff

Bern University of Applied Sciences

20.03.2026

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?

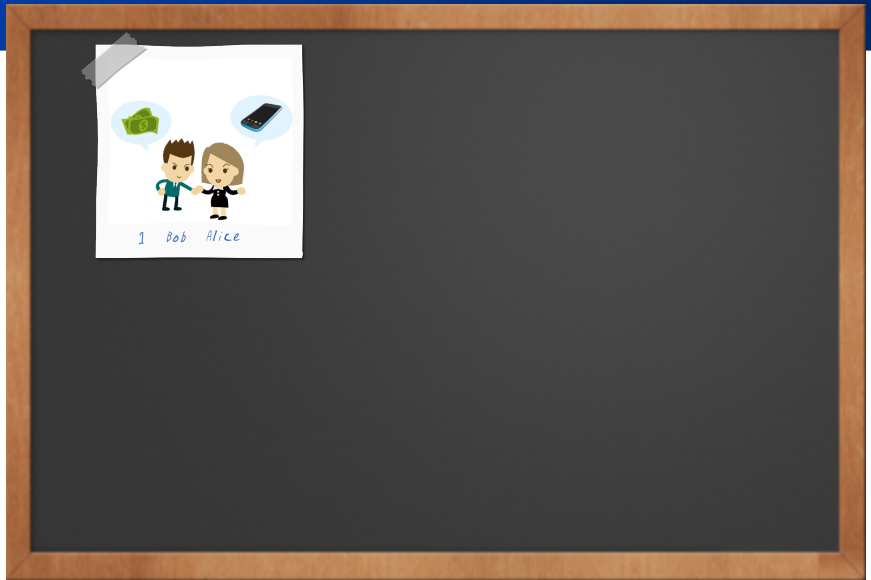
What are other applications for Blockchains?

Bonus: Depolymerization [3]

Blockchain[1]

[1] Illustrations by Alexandra Dirksen, IAS, TUBS [2]

Blockchain



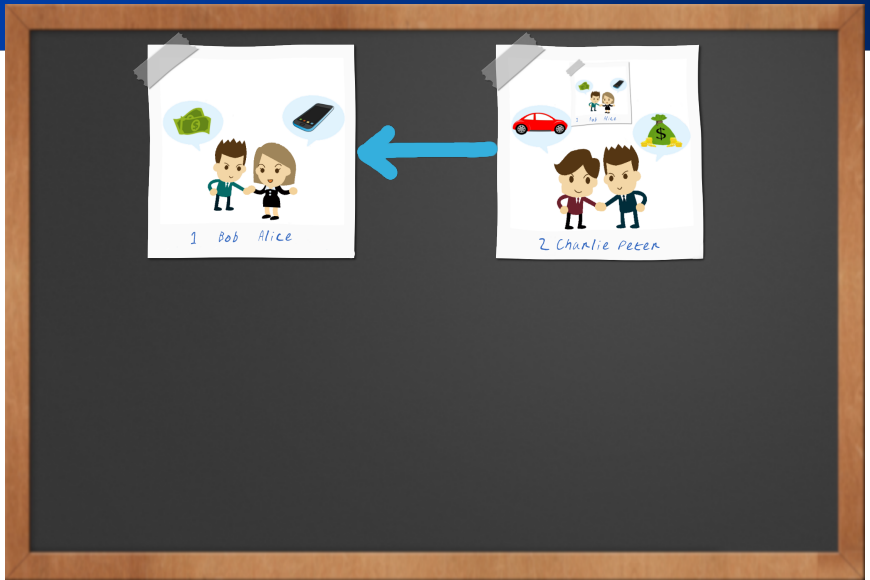
Blockchain

Blockchain

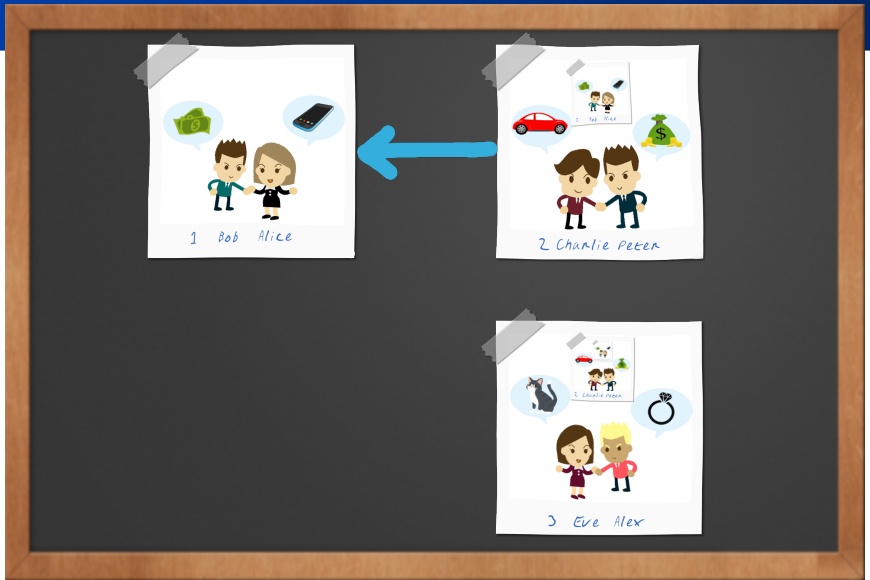
Blockchain

NGI TALER

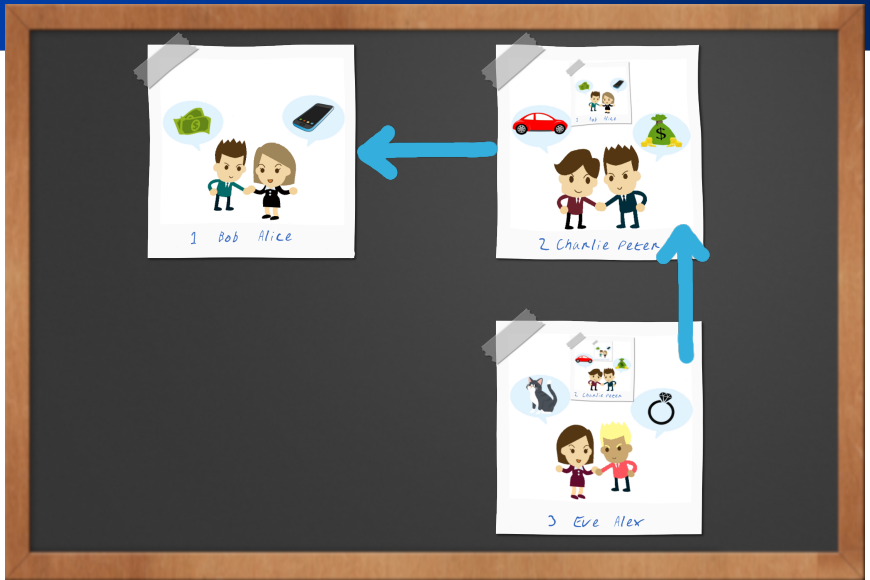
Blockchain



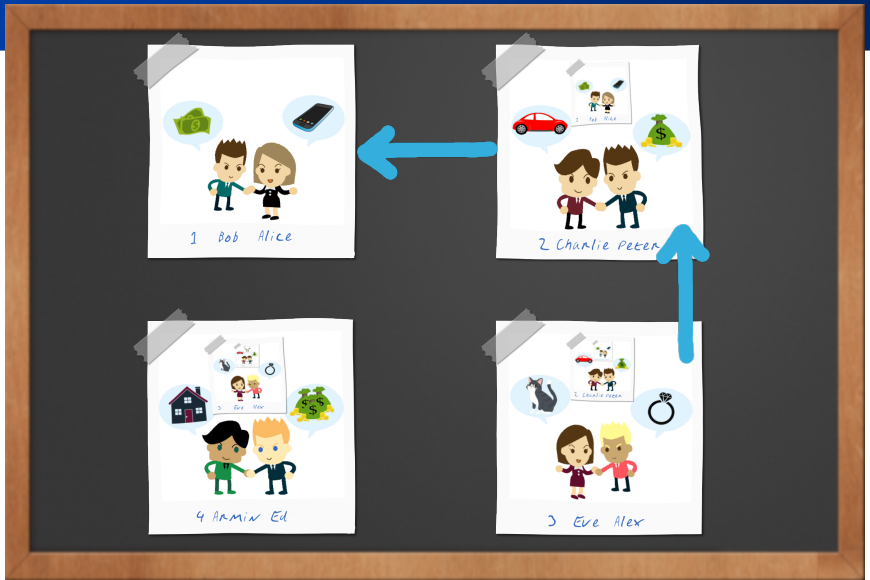
Blockchain



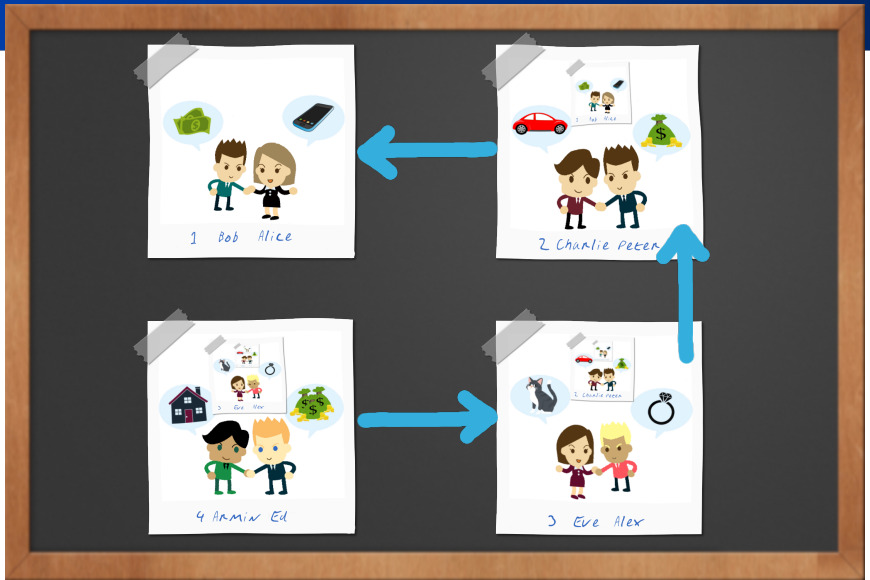
Blockchain



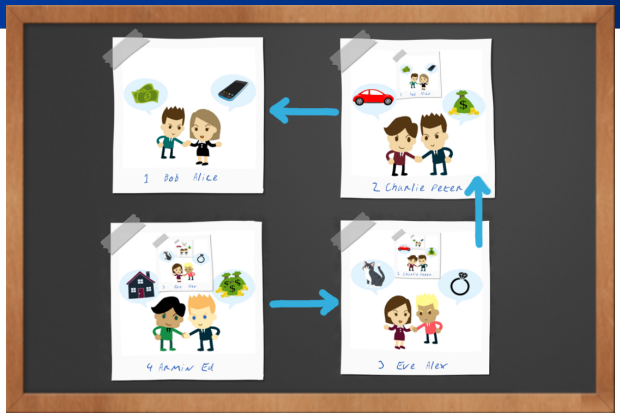
Blockchain



Blockchain

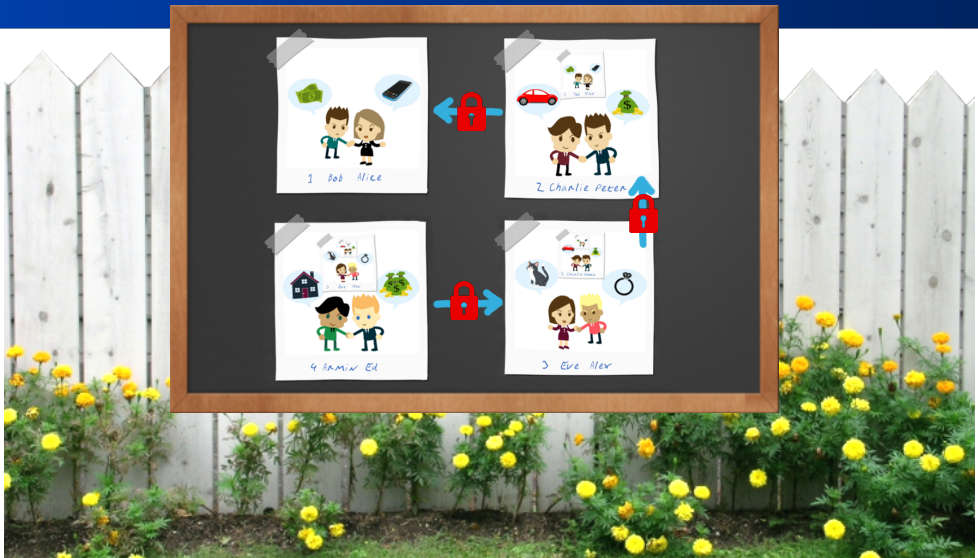


Advertised Blockchain “properties”



Immutability

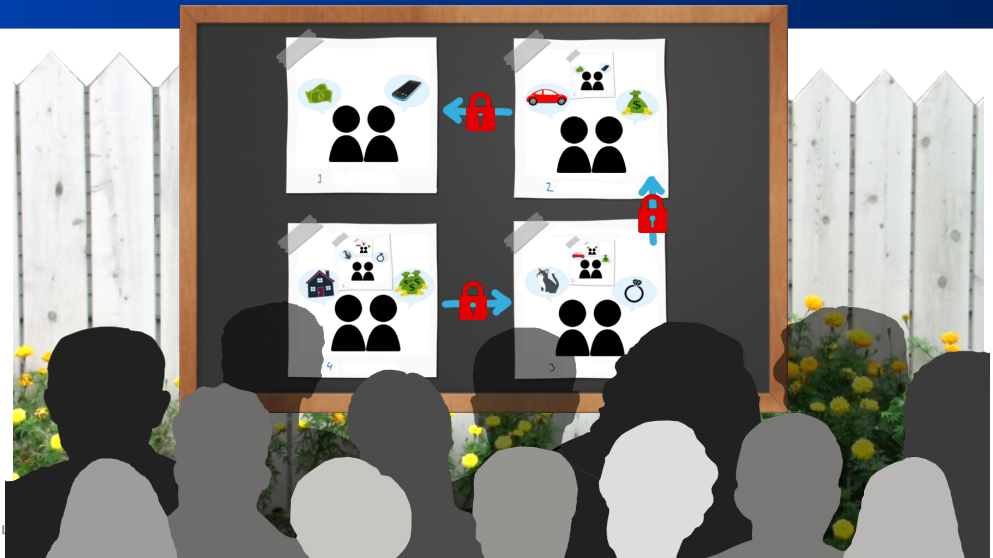
Transparency



Decentralisation

Autonomy

Anonymity

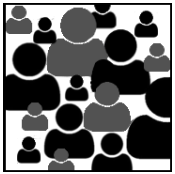


Summary: Blockchain “properties”

Im-
mutability

Trans-
parency

Anonymity



Decentralisation

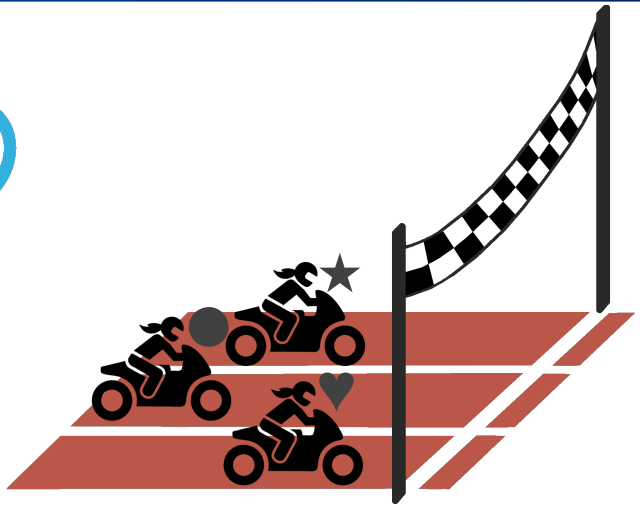
Autonomy

Irreversibil-
ity

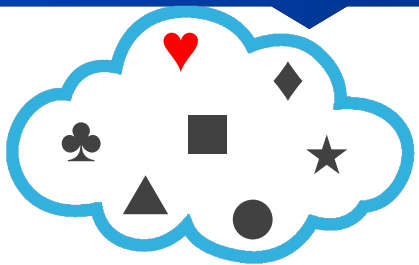
Who gets to append the next block?

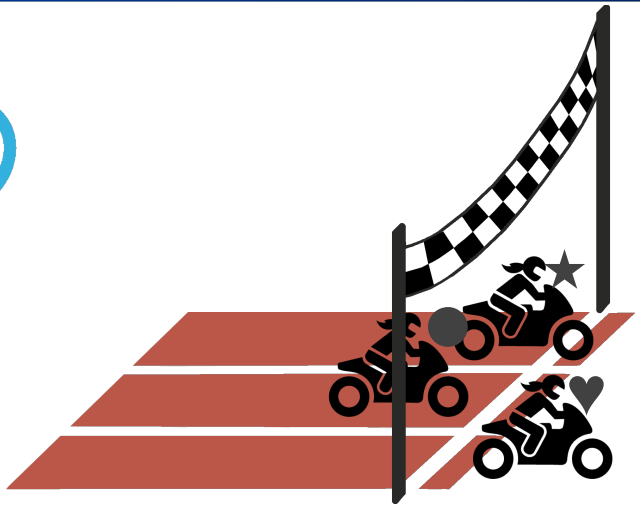
Proof of Work

Proof of Work

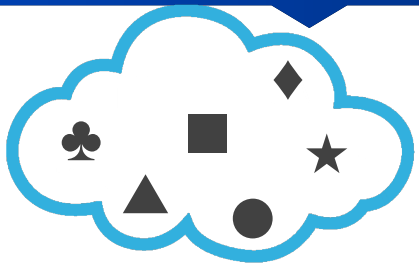


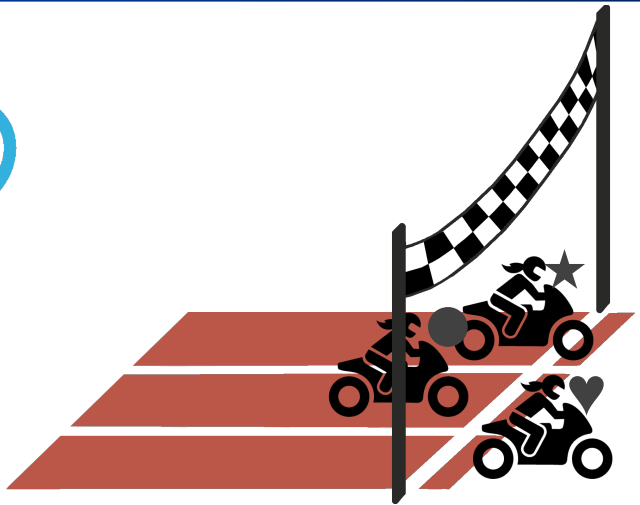
Proof of Work



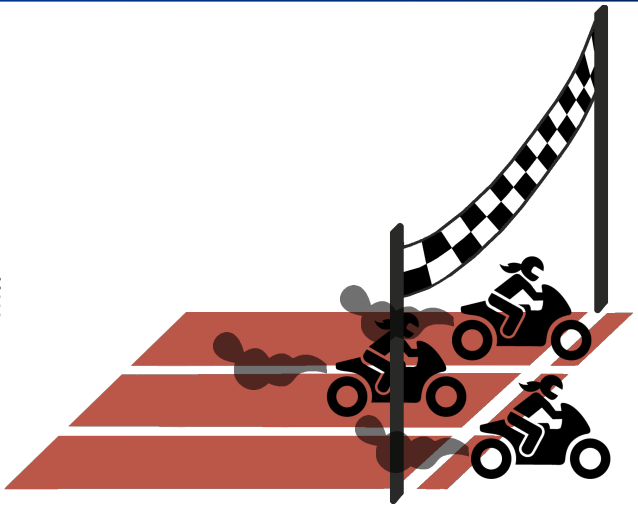


Proof of Work

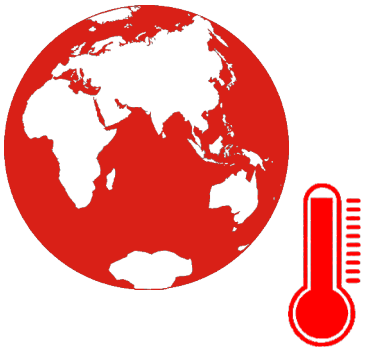


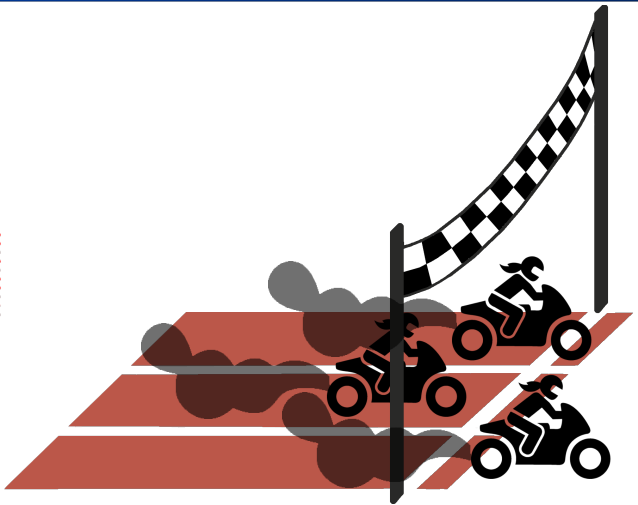


Proof of Work



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

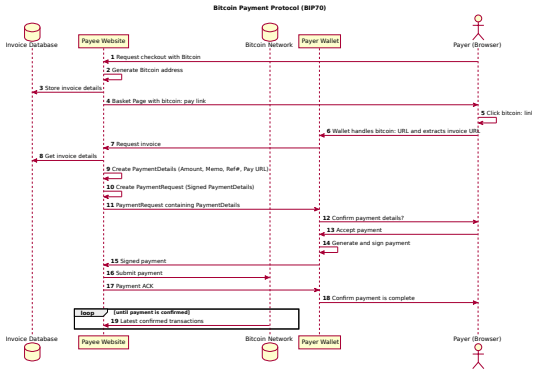
Rational Forking

Imagine:

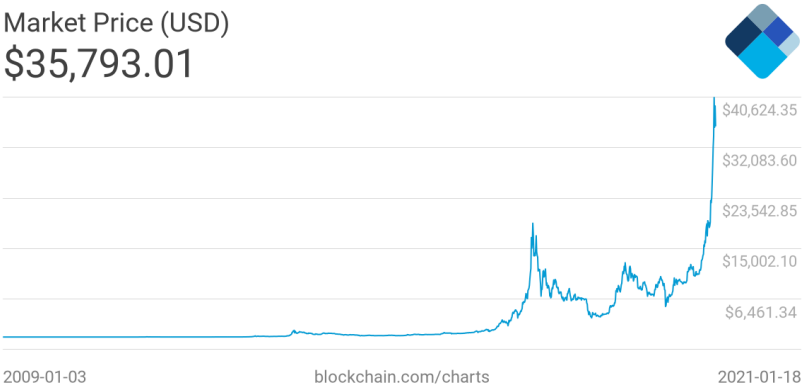
- The previous block had a transaction from *X* to *Y* over 100 BTC with a fee of 0.001 BTC, a block reward of 7.5 BTC and total transaction fees of 5 BTC.
- The next consistent blocks can be assumed to again have block rewards of 7.5 BTC and transaction fees of 5 BTC.
- The issuer *X* of the 100 BTC 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)



The Value of Bitcoin



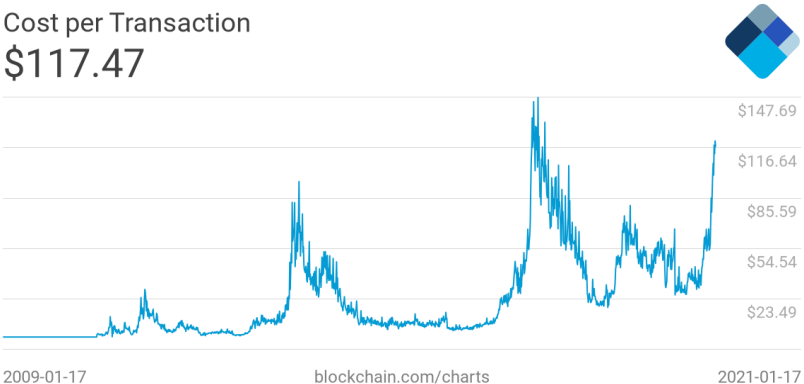
Mining

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



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

$\Rightarrow$ 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!

Blockchain Trilemma

Blockchains claim to achieve three properties:

- Decentralization: there are many participants, and each participant only needs to have a small amount of resources, say $O(c)$
- Scalability: the system scales to $O(n) > O(c)$ transactions
- Security: the system is secure against attackers with $O(n)$ resources

The Blockchain trilemma is that one can only have two of the three.

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

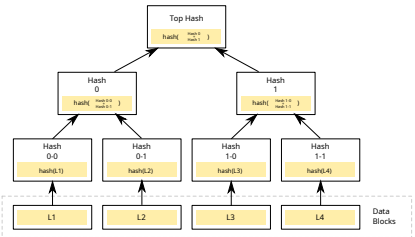
Security Goals for Time Stamping Services

- 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:



Bonus: Depolymerization

Blockchain based cryptocurrenc


BBC Home News Sport More
NEWS Menu
World Africa Asia Australia Europe Latin America
Middle East US & Canada
Kosovo bans cryptocurrency mining after blackouts
5 January


Environment Climate crisis Wildlife Energy Pollution
The Observer
How do we solve bitcoin's carbon problem?
The cryptocurrency consumes more energy than Norway. As countries consider copying China's ban, experts disagree on whether a greener version is possible


WIRED SUBSCRIBE
As Kazakhstan Descends Into Chaos, Crypto Miners Are at a Loss
The central Asian country became No. 2 in the world for Bitcoin mining. But political turmoil and power cuts have hit hard, and the future looks bleak.

Biggest cryptocurrencies

- **BTC** Bitcoin
- **ETH** Ethereum

Common blockchain limitations

- **Delay** block and confirmation delay
- **Cost** transaction fees
- **Scalability** limited amount of transaction per second
- **Ecological impact** computation redundancy
- **Privacy & regulatory compliance**

Related work

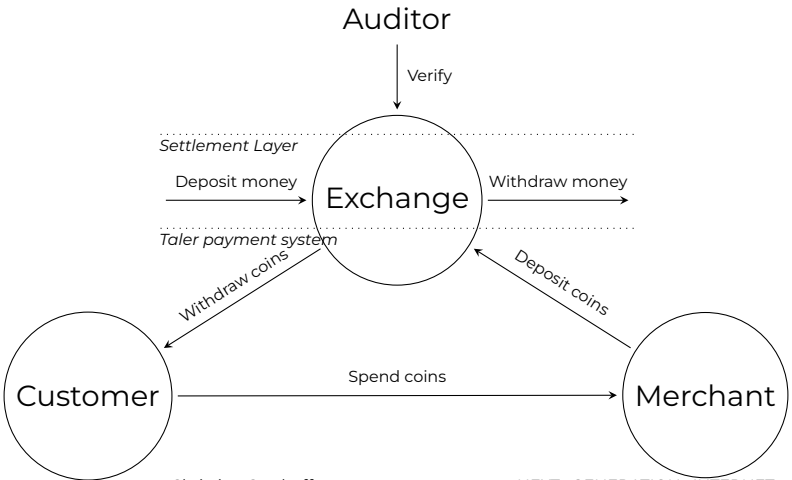
Centralization - Coinbase off-chain sending

+ Fast and cheap: off chain transaction
– Trust in Coinbase: privacy, security & transparency

Layering - Lightning Network

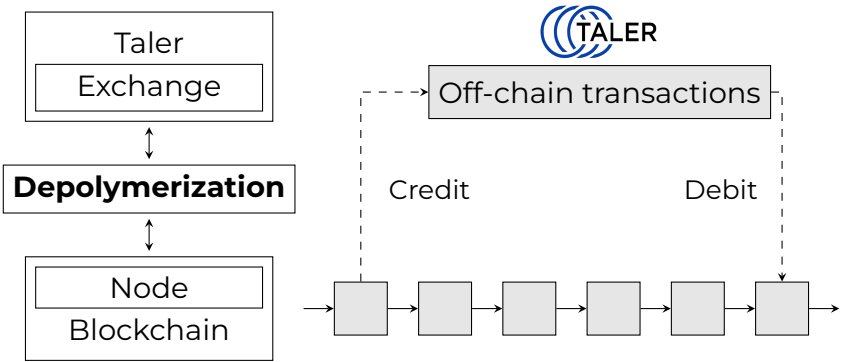
+ Fast and cheap: off-chain transactions
– Requires setting up bidirectional payment channels
– Fraud attempts are mitigated via a complex penalty system

Taler
Architecture

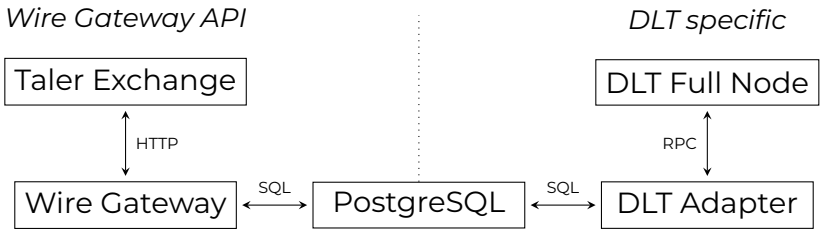


Project Depolymerization

Taler with blockchain settlement layer



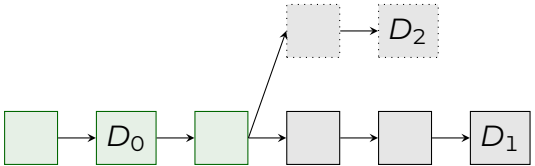
Depolymerization [3]
Architecture



- Common database to store transactions state and communicate with notifications
- Wire Gateway for Taler API compatibility
- DLT specific adapter

CAP & Bitcoin

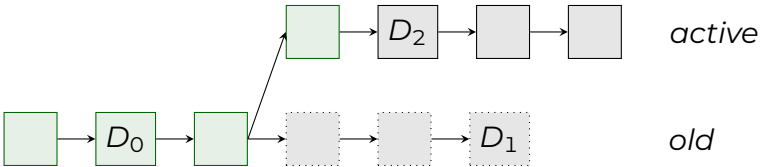
Chain reorganization



Bitcoin is inconsistent:

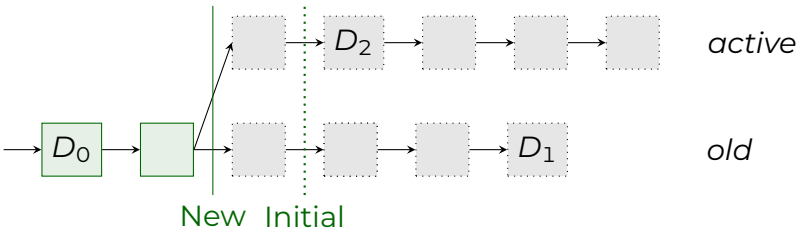
- Conflicting blocks can be mined at the same time
- This can happen by accident, or on purpose!
- Coins could be spent twice, once on each fork of the chain!
- Longest chain is considered “valid”

Handling blockchain reorganization

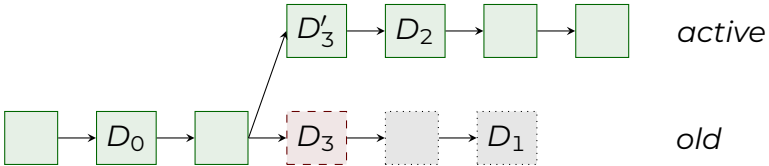


- As small reorganizations are common, Satoshi already recommended to apply a confirmation delay to handle most disturbances and attacks.
- If a reorganization longer than the confirmation delay happens, but it did not remove credits, Depolymerizer is safe and keeps running.

Adaptive confirmation



Handling blockchain reorganization



If a fork removed a confirmed debit, an attacker may create a conflicting transaction. Depolymerizer suspends operation until lost credits reappear.

Challenges

Taler Metadata

- Metadata are required to link a wallet to credits and allow merchant to link deposits to debits
- Putting metadata in blockchain transactions can be tricky

Storing metadata
Bitcoin

Bitcoin - Credit

- Transactions from code
- Only 32B + URI
- **OP_RETURN**

Bitcoin - Debit

- Transactions from common wallet software
- Only 32B
- **Fake Segwit Addresses**

Storing metadata
Ethereum

Smart contract?

- Logs in smart contract is the recommend way (ethereum.org)
- Expensive (additional storage and execution fees)
- Avoidable attack surface (error prone)

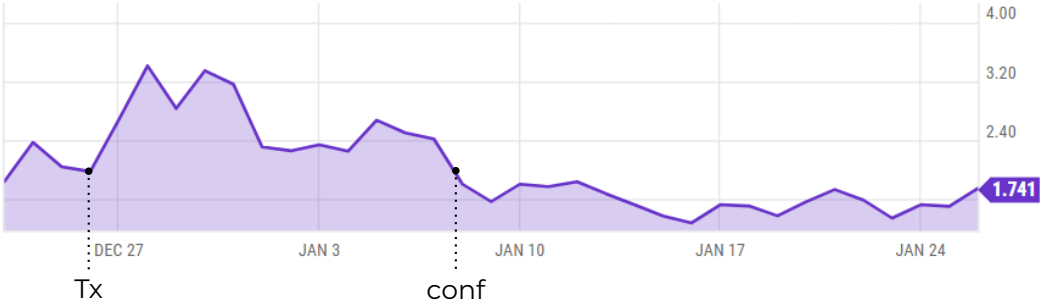
Custom input format

Use input data in transactions, usually used to call smart contract, to store our metadata.

Blockchain challenges

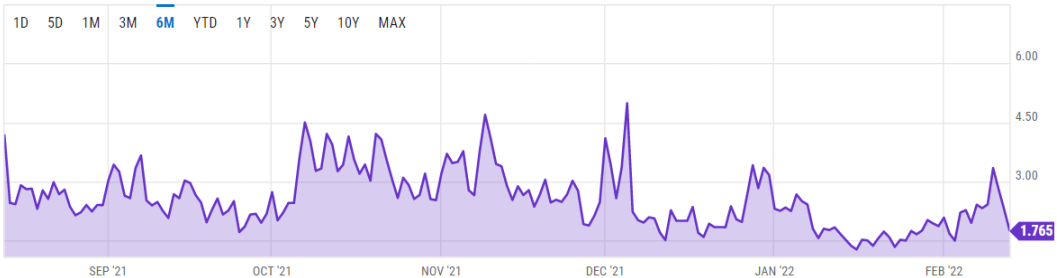
Transactions stuck in mempool

We want confirmed debits within a limited time frame.



Blockchain challenges

Transactions stuck in mempool



Bitcoin average transaction fee over 6 months (ychart)

Future work

- Support other blockchains
- Universal auditability, using sharded transactions history
- Multisig by multiple operators for transactions validation

Conclusion

Blockchains can be used as a settlement layer for GNU Taler with Depolymerizer.

- – Trust exchange operator or auditors
- \+ Fast and cheap
- \+ Realtime, ms latency
- \+ Linear scalability
- \+ Ecological
- \+ Privacy when it can, transparency when it must (avoid tax evasion and money laundering)

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]

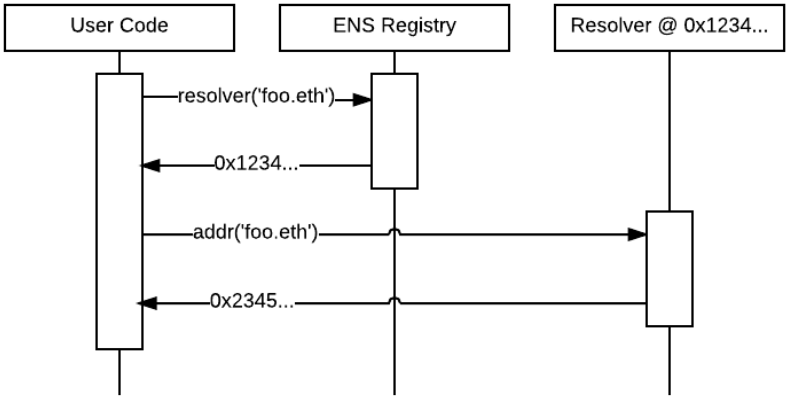
Let's have a smart contract in the Blockchain manage naming!

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]



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.


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

References II

- Antoine d'Aligny, Emmanuel Benoist, and Christian Grothoff.
  Project depolymerization: Tokenization of blockchains.
  In *4th Conference on Blockchain Research and Applications for Innovative Networks and Services*, September 2022.
- 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.