Topic 4.4 • Applications

Bitcoin

CO 487/687 • Fall 2024

Prof Douglas Stebila

UNIVERSITY OF WATERLOO

Overview of Bitcoin

What is electronic cash?

- Electronic cash is an electronic payment system modeled after our paper cash system.

- Some features of paper cash:
  - Recognizable (as legal tender)
  - Portable (easily carried)
  - Transferable (without involvement of the financial network)
  - Divisible (has the ability to make change)
  - Unforgeable (difficult to duplicate)
  - Untraceable (difficult to record where money is spent)
  - Anonymous (no record of who spent the money)

- Many of these features are not available with credit cards, wire transfers, or other more "standard" forms of electronic payment.

Basic concepts

- There are (up to) three parties in an electronic payment system:
  - A payer or buyer or consumer
  - A payee or seller or merchant
  - A financial network or central authority
- The electronic representation of cash is called a token or (electronic) coin.
- A device that stores or accesses coins is called a card or a wallet
- We distinguish between on-line and off-line payments:
  - On-line payments: Seller must communicate with the central authority in real-time at point of sale.
  - Off-line payments: No real-time communication is required.

Security properties of electronic cash

- For the payer:
  - Payer anonymity during payment.
  - Payment untraceability so that others cannot tell whose money is used in a particular payment.

- For the payee and (if it exists) the central authority:
  - Unforgeable coins: forging a valid-looking coin should be infeasible.
  - No double-spending: A coin cannot be used more than once for making a payment.

Other desirable properties for electronic cash

- Off-line payment system is preferable to on-line
- Payment mechanism should be cheap
- Payment mechanism should be efficient
- Cash should be transferable
- Cash should be divisible

Digital cash

- invention of digital cash
- lots of academic research

- ecash start-up (failed)
- more academic research

- academics give up on digital cash

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

https://bitcoin.org/bitcoin.pdf

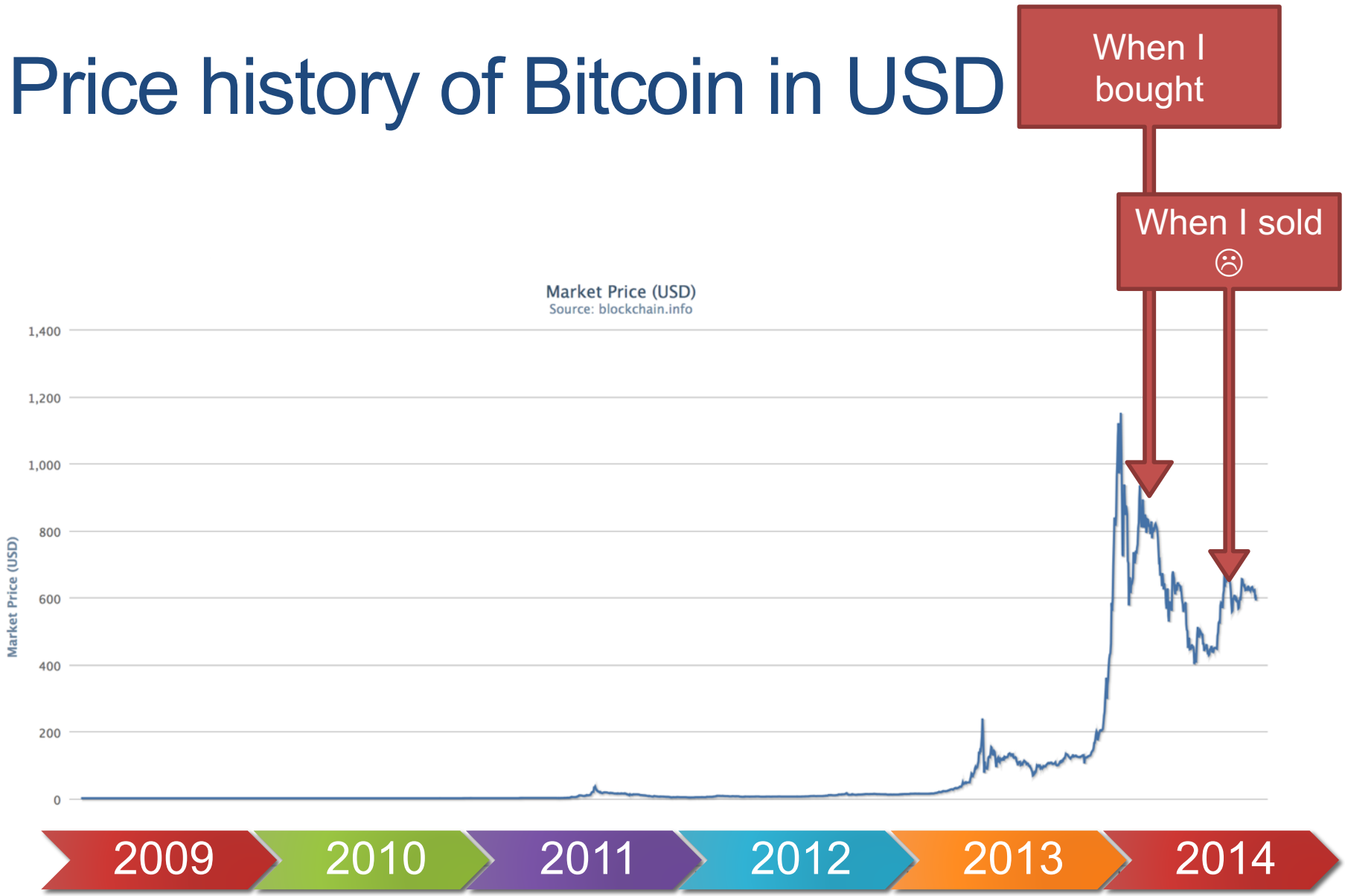
Bitcoin overview

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, http://bitcoin.org/bitcoin.pdf

- Paper published: October 31, 2008 (by Nakamoto)
- Code published: January 1, 2009 (by Nakamoto)
- The identity of Satoshi Nakamoto is not publicly known.

- Bitcoin relies on cryptography for its security, and uses no central authority.
- Coins are initially created by "mining."
- Owners are identified by their public keys.
- The miner is the initial owner of a coin.
- An owner A can transfer a coin to another owner B by signing (via a digital signature) the coin together with B's public key.
- Double spending is prevented by a "blockchain" which requires proof of work to compute.

Price history of Bitcoin in USD



https://blockchain.info/charts/market-price

Price history of Bitcoin in USD

What is Bitcoin?

Bitcoin is a decentralized distributed system for establishing a public ledger of transactions.

Basic idea

1. There's a public ledger that everyone can read with everyone's balance.
2. Alice wants to pay Bob 3 units.
3. Alice requests to put a transaction in the ledger saying "Alice pays Bob 3 units."
4. The maintainer of the ledger checks (a) that Alice has big enough balance and (b) that Alice really made the request, then records the transaction in the ledger.
5. Bob now has a higher balance.

Problems with the basic idea

No anonymity

- Use public keys rather than names.
- Use transaction references rather than accounts.

How to verify someone has authorization to spend from Alice's account?

- Use digital signatures to demonstrate ownership of currency from previous transaction.

Who maintains the ledger?

- Distributed ledger: incentivize community to maintain.

Transaction

"Alice pays Bob 3 units."

"Alice transfers control of 3 units to Bob."

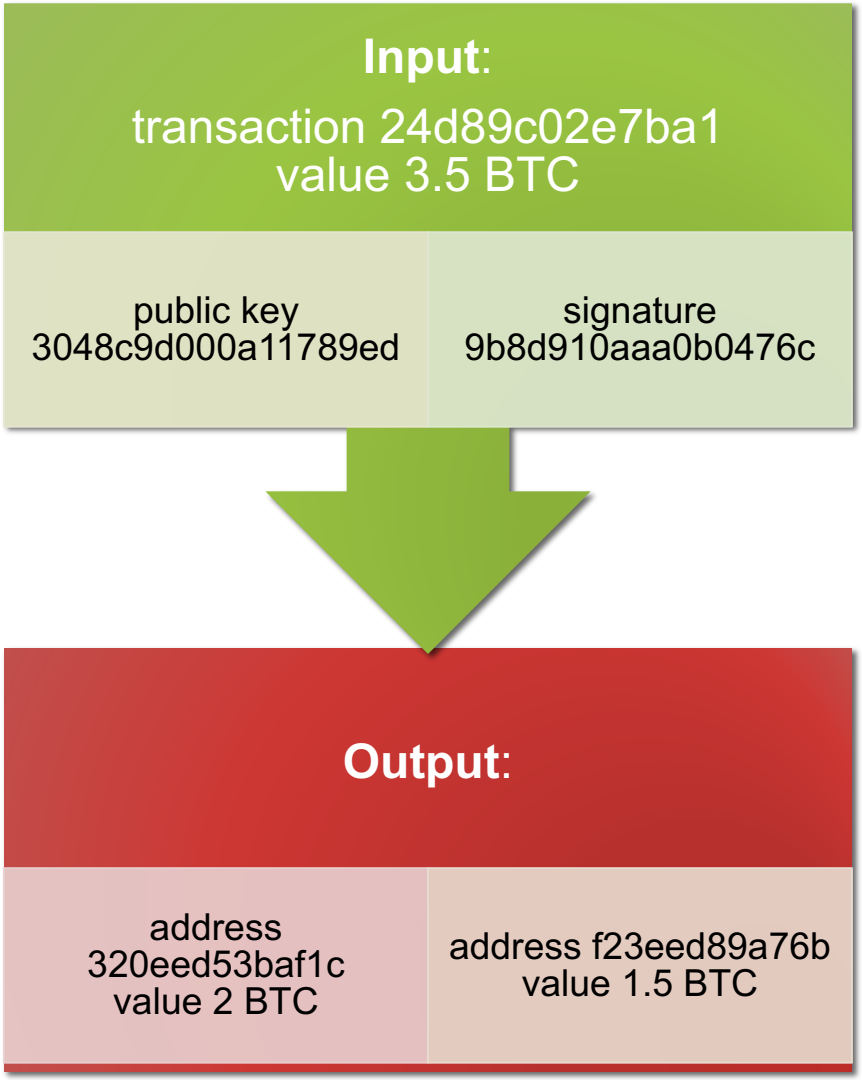
Input:

- Previous transaction ID.
- Public key used in previous transaction.
- Digital signature using based on previous transaction's public key.

Output:

- Bob's address
- # of units
  - Bitcoin address = hash of public key
- Should include own address to "make change"

Transaction



Public key:

- ECDSA public verification key used in address from previous transaction

Signature:

- signature of transaction using corresponding ECDSA private signing key

Bitcoin address:

RIPEMD-160(

SHA-256(ECDSA public key)

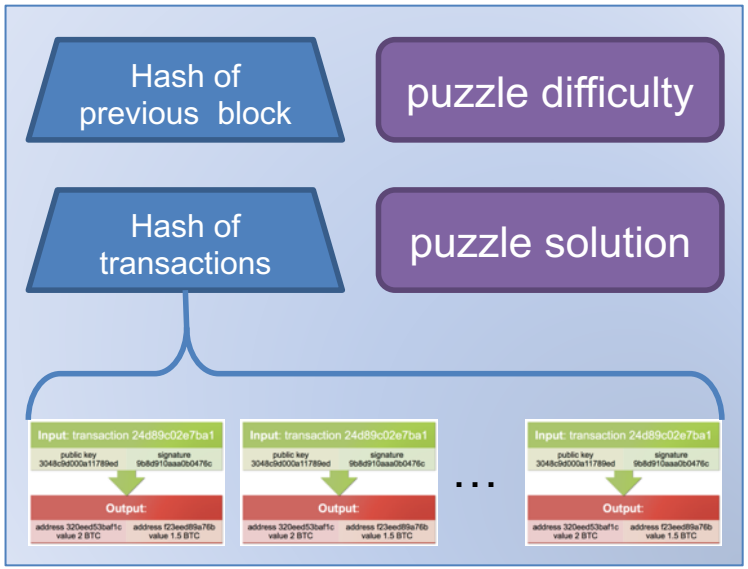
)

Block

Header

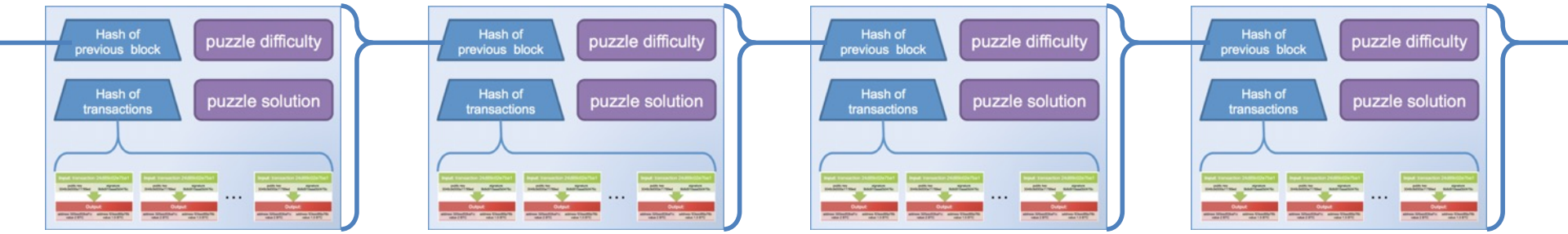
+

a list of transactions



Blockchain

A sequence of blocks = ledger of transactions



Which blockchain?

Blocks form a tree.

- Could have forks in the tree.
- Only the longest chain is considered to be valid by the community.

Adding blocks to the chain

A block can only be added to the blockchain if the hash of the block is small.

- Users try to generate a block with a small hash.
  - ("cryptographic puzzle")

- Updating the blockchain requires work but maintains the public ledger.

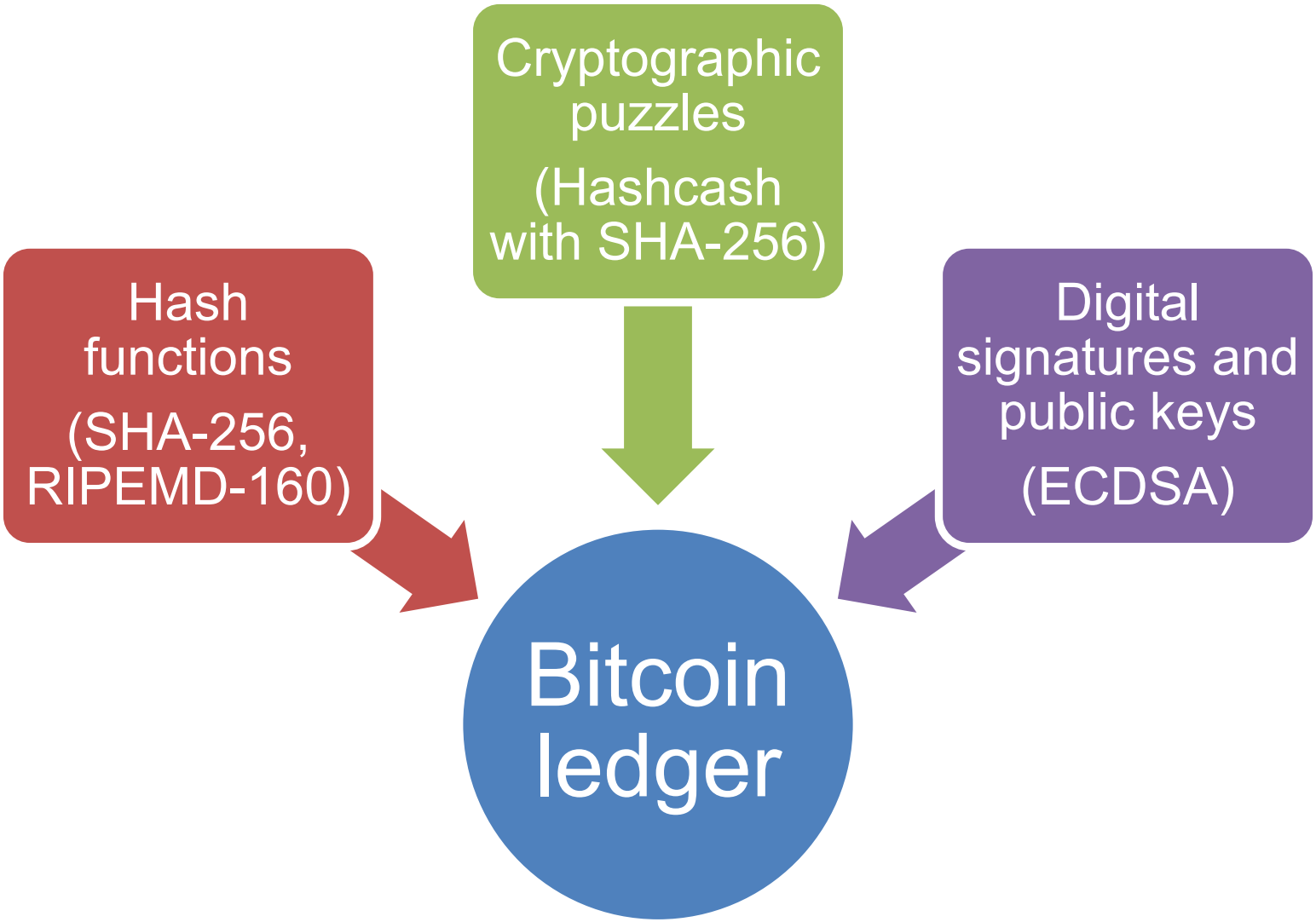
- Motivation: whoever constructs the block includes one transaction paying themselves 6.25 BTC ("**mining**")

Why people agree on a single ledger

Bitcoin designed so everyone is motivated to agree on a single public ledger

- If I am trying to add a block to the chain and I do so, I'm motivated to grow that chain because that chain has my reward.
- If I am trying to add a block to the chain but someone else beats me, the probability I'll find the next block is the same regardless of whether I use the new block or not.

Cryptographic ingredients



Cryptographic puzzles

Cryptographic puzzle

A "moderately hard" computational task.

Example:

- Let H be a hash function with 256 bits of output.
- Find a value x such that $H(x)$ starts with ~47 zeros.

"difficulty"

Analysis:

- Assume H is a random function (output bits are independent and identically distributed).
- Then for each different input x and each i, the probability that the ith bit of $H(x)$ is zero is ½.
- The probability that the first 47 bits of $H(x)$ are all zero is $1 / 2^{47}$.
- Need to try about 2^{46} different x values on average to find a satisfying value.

Hashcash cryptographic puzzle

Example:

- Let H be a hash function with λ bits of output.
  - Interpret output as an integer between 0 and $2^{\lambda}-1$
- Let s be a string.
- Let t be an integer.

- Find a value x such that $H(s \,||\, x) \leq t$.

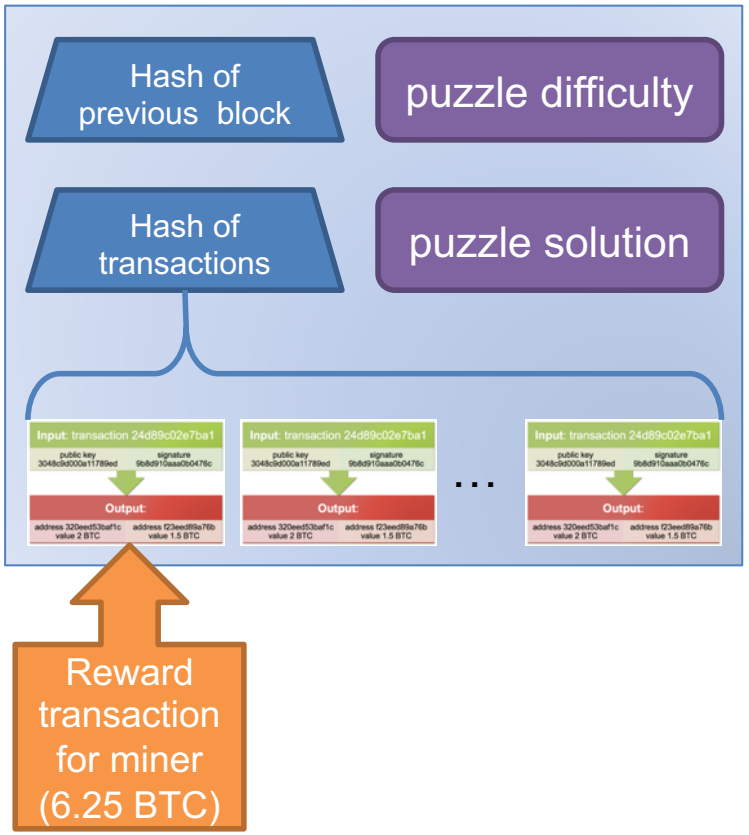
Puzzles in Bitcoin

Every miner is trying to construct a block header where

$H(H(\text{block header} \,||\, \text{solution})) \leq \text{difficulty target}$

H = SHA-256

Keep trying random solutions until one works



Bitcoin mining

Difficulty target adjusted every 2 weeks so that average block generation time is 10 minutes.

Current mining rate:

- 710 quintillion (approx. $2^{69.2}$ hashes) per second
  - https://www.blockchain.com/explorer/charts/hash-rate 2024/11/17

Mining pools

Since finding the solution to a new block is so unlikely individually, miners work together in pools.

If anyone in the pool finds the solution to the puzzle, the whole pool shares the reward.

How to split the reward?

- Just like Bitcoin mining, but with a higher difficulty target
- Pool miners submit whenever they find a hash less than the pool difficulty target
- Even if it's not a valid Bitcoin block, it still demonstrates that you are working hard
- Reward split based on number of submitted hashes

Alternative consensus mechanisms

Computation-bound puzzles

- e.g. Bitcoin
- Solving time primarily a function of CPU cycles
- Easy to run on low-memory GPUs or custom ASICs

Memory-bound puzzles

- e.g. Litecoin
- Solving requires significant amount of memory
  - e.g. using Scrypt function
- GPUs and ASICs may be less effective due to memory requirements

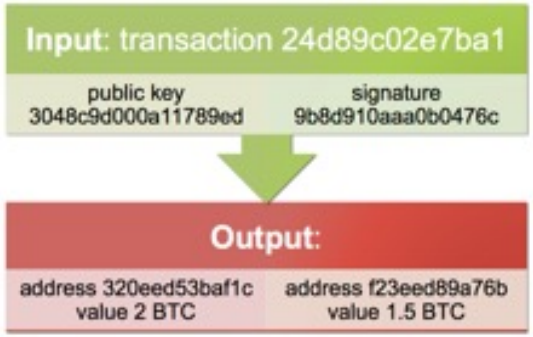
Proof-of-stake

- e.g. Ethereum since 2022
- Maintaining block chain delegated to participants in proportion to their holdings

Summary

Cryptographic parts of Bitcoin ledger

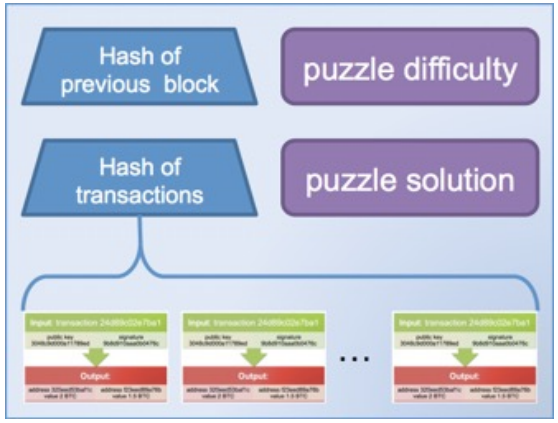
Transactions



Digital signatures for transaction approval (ECDSA)

Hashed public keys for addresses

Blocks



Hash used to collect transactions together

Cryptographic hash puzzle required to make block valid (Hashcash SHA-256)

Blockchain

Hash used to chain transactions together (SHA-256)

Only blocks in longest chain considered valid

Breaking Bitcoin via cryptography

Forge transactions

Breaking elliptic curve discrete logarithm with classical computers needs mathematical breakthrough.

Quantum computers can easily break ECDLP.

- "Just" need to build a quantum computer.

Mine faster

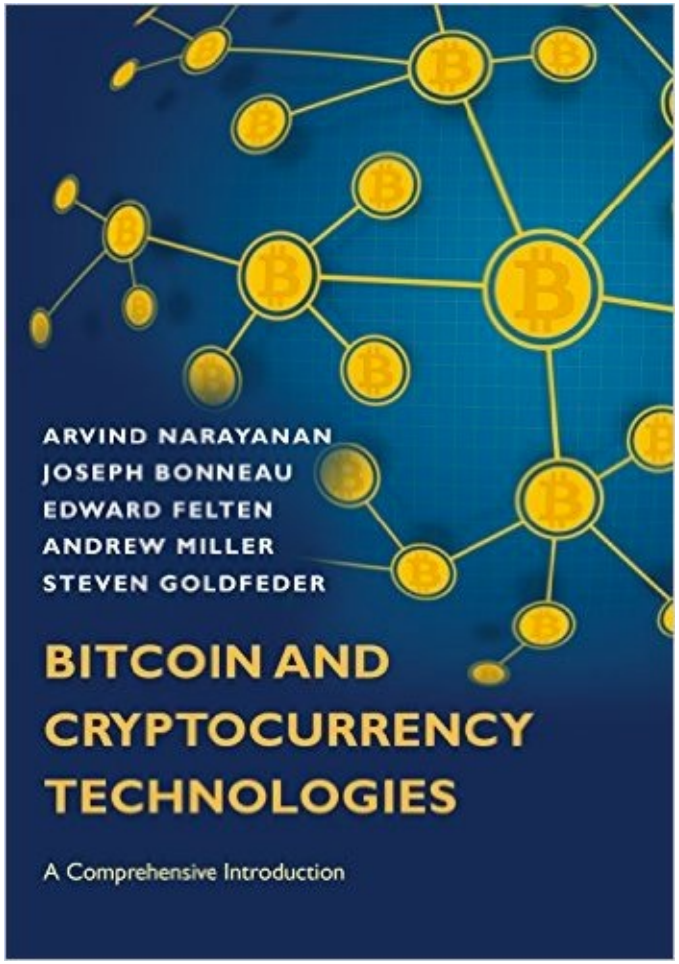
Figure out how to break partial preimage resistance / pseudorandomness of SHA-256.

Ethereum

- Second largest cryptocurrency
- Supports “smart contracts” which execute code
  - “If any 2 of the following 4 people authorize payment, release X funds to Alice.”
- Switched from proof of work to “proof of stake” as in Sept. 2022

- Created by **Vitalik Buterin**
- Started undergrad in math at Waterloo but dropped out in 2014 to work on Ethereum full-time

Further reading



http://bitcoinbook.cs.princeton.edu/

Original paper by Satoshi Nakamoto
https://bitcoin.org/bitcoin.pdf

Bitcoin wiki
https://en.bitcoin.it

Original Hashcash paper by Adam Back:
http://www.hashcash.org/papers/hashcash.pdf

crypto - Google Search

google.com/search?q=crypto&rlz=1C5CHFA_enCA928CA928&oq=crypto&gs_lcrp=EgZjaHJvbWUyBggAEEUYO...

Google

crypto

All News Images Videos Shopping Web Maps More Tools

This search may be relevant to recent activity: crypto ***mining***

Your Search activity | Feedback

Crypto.com
https://crypto.com

Crypto.com | Securely Buy, Sell & Trade Bitcoin, Ethereum ...

The World's Premier **Crypto** Trading Platform. Buy Bitcoin, Ethereum, and 350+ cryptocurrencies. Trade with 20+ fiat currencies and Apple/Google Pay.

Today's Cryptocurrency Prices · Crypto Earn · Crypto.com Exchange · OTC Portal

Wikipedia
https://en.wikipedia.org › wiki › Cryptocurrency

Cryptocurrency

A cryptocurrency, **crypto**-currency, or **crypto** [a] is **a digital currency designed to work through a computer network** that is not reliant on any central authority.

Top stories

News about crypto

Salon.com

The Crypto Revolution comes to Washington, with eye on regulatory reform

8 hours ago

Cryptocurrency

Software classification

A cryptocurrency, crypto-currency, or crypto is a digital currency designed to work through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it.
Wikipedia ›

Software In Genre: Zerocash, CryptoNote

Feedback

https://en.wikipedia.org/wiki/Crypto_naming_controversy
https://www.cryptoisnotcryptocurrency.com/