NTNU

Norwegian University of Science and Technology

Bitcoin, Blockchains and Smart Contracts

Understanding the Crypto in Cryptocurrencies

Colin Boyd

Department of Information Security
and Communications Technology, NTNU

February 2019

NTNU

Outline

NTNU

Bitcoin origins

- Online proposal by Satoshi Nakamoto late 2008
- First Bitcoin blocks formed 2009
- Protocol defined by implementation in software
- No central authority
- Not linked to any fiat currency

NTNU

Interfacing with the Bitcoin blockchain

Several alternative methods to view and interact with the Bitcoin blockchain:

- Make a bitcoin node: install Bitcoin Core
- Toolkit: libbitcoin-explorer

  `https://github.com/libbitcoin/libbitcoin-explorer`
- Blockchain explorers
  - https://btc.bitaps.com
  - https://blockstream.info
  - https://www.blockchair.com
- Bitcoin testnet

NTNU

Digital signatures

- A digital signature is a bit string which authenticates a message
  - Private signing key is used to generate each signature
  - Public verification key is used to verify each signature
- Bitcoin uses a modern, efficient, standardised signature scheme (ECDSA with a specific curve)
- Bitcoin signatures are 512 bits in length
- Bitcoin addresses are public signature verification keys
- A typical Bitcoin address:

`1HnhWpkMHMjgt167kvgcPyurMmsCQ2WPgg`

NTNU

Bitcoin transactions

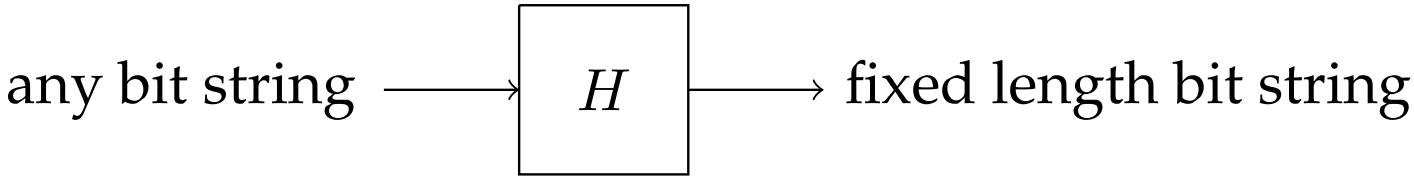
- Bitcoin transactions (payments) transfer value from one or more *input addresses* to one or more *output* addresses
- Each output specifies:
  - The address whose signing key will be used later to authorise spending of the output
  - The value of this output
- Each input specifies:
  - an output of an *earlier* transaction with its value
  - a signature of the current transaction by the owner of that input

NTNU

Valid transactions in Bitcoin

- A transaction that spends an already spent output is invalid (no double spending)
- The sum of input values to a transaction must not exceed the sum of output values
- Transactions are exchanged on the Bitcoin peer-to-peer network
- A set of transactions is sometimes hashed together into a *Merkle root*

Hash functions



- Example SHA-256: output looks like a random 256 bit string (64 hex digits)
- SHA-256 hash of an Ubuntu image (around 2GB file):

```
574870693753941 8ee5707bd538c4f5e
abae485d17aa49fb13ce2c9b70532433
```

NTNU

Hash collisions

— A collision for H is a pair or two messages $m_1 \neq m_2$ such that

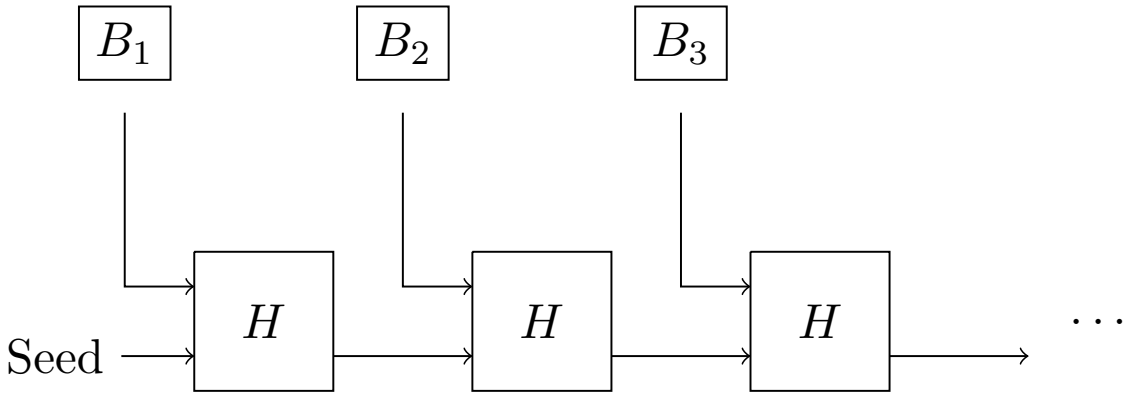
$$H(m_1) = H(m_2).$$

— Collisions must *exist*

Fact

For a good hash function collisions are too hard to find

Hash chains



— Sequence of hashes. Each new hash input includes the previous hash.

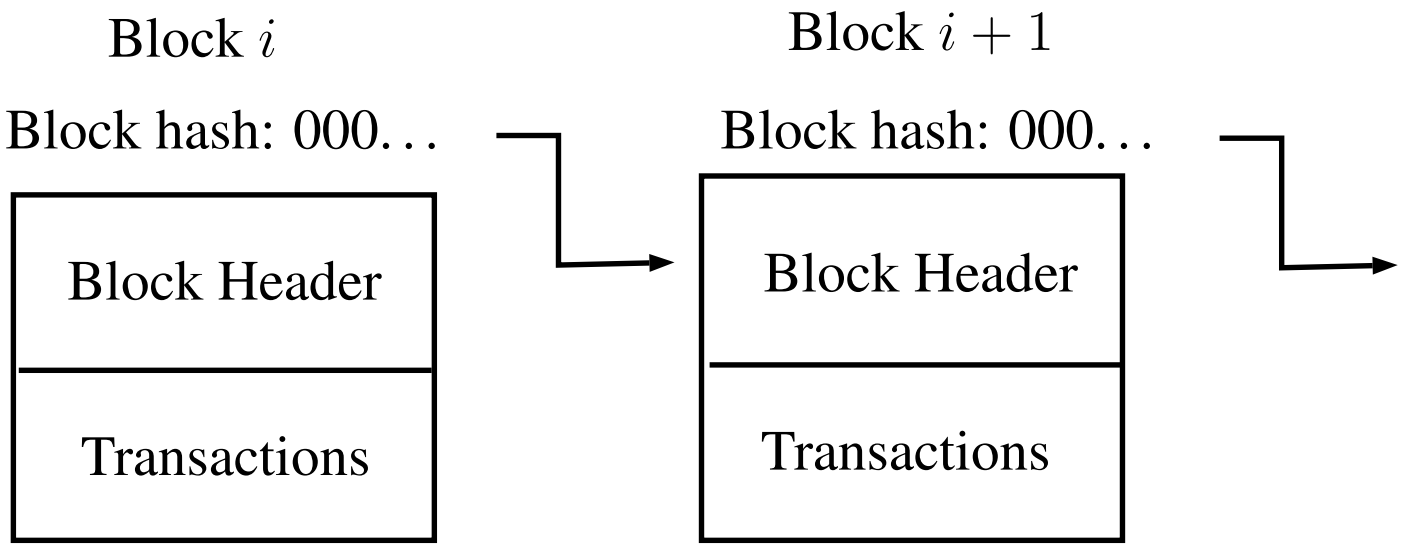
— Cannot change (add, delete nodes) without finding a collision

— Used in cryptography for a long time (micropayments, timestamping, . . .)

Bitcoin blocks

- A Bitcoin block consists of an 80-byte header and a set of transactions
- Each header includes the hash of the previous block header
- The Bitcoin blockchain started with block number 0, known as the *genesis block*

Chained blocks



Fact

The Bitcoin blockchain is a hashchain of blocks

Mining

- A block is valid if it has a hash with enough zero bits at the start
- The number of zero bits at the start of a valid block is defined by the current *difficulty*
- A *miner* attempts to construct a valid block by changing variables in the block until there are enough zero bits in the hash
- This is a *cryptographic puzzle* or *proof of work*. Only known way to solve the puzzle is by trial and error

Question

How many trials do we expect to need to construct a block with hash starting with 32 zero bits?

NTNU

Mining costs and rewards

- A *block reward* is given for each block mined until 21 000 000 bitcoins mined (around year 2040)
- When Bitcoin started the block reward was 50 Bitcoins, but it halves every 4 years
- Transactions include fees paid to miner

Fact

Consensus is built by the community accepting that the longest valid chain is the correct blockchain

DIY mining

AntMiner S9 ~13.0TH/s @ 0.098W/GH 16nm ASIC Bitcoin Miner

by Bitmain

20 customer reviews | 69 answered questions

Price: $515.00 + $189.82 Shipping & Import Fees Deposit to Finland Details

Free Amazon tech support included

- Bitcoin Mining Hash Rate: 13.0TH/s ±5%
- Power Consumption: 1273W ±10% (Power supply not included)
- Built-in web management portal - No separate host computer or software required
- Most Power Efficient Bitcoin Miner: 0.098 J/GH ±7%
- Power supply sold separately - AntMiner APW3++ power supply recommended if you have 220v+. EVGA SuperNova 1600 G2 recommended if you only have 110-120v power.

› See more product details

Used & new (11) from $399.00

Today all effective mining is done in *mining pools* – a huge industry

Industrial scale mining

NHO-toppens bønn til regjeringen: – Rydd opp i dette uhellet

Fjerning av strømrabatt for kryptosentre rammer hele datasenternæringen – ikke bare de som driver med utvinning av Bitcoin, hevder NHO-topp.

NHO frykter at store aktører ikke vil bygge datasentre i Norge når staten skiller på pris etter hva man bruker datasentrene til. Her fra datalagring i fjellhallen Green Mountain i Rennesøy. Illustrasjonsfoto.
FOTO: SEBASTIAN WINUM STORVIK/NRK

Ole-Fredrik Lambertsen
@olambertsen
Journalist

Oliver Rønning
@oroenning
Journalist

Publisert 24. nov. 2018 kl. 21:11

Source: nrk.no

NTNU

How much electricity does mining use?

- Bitcoin miner profits depend on:
  - capital cost of equipment
  - cost of electricity
  - value of Bitcoin
- Mining reward available per day for Bitcoin is $12.5 \times 144 \times$ Value of 1 Bitcoin:
  - $\approx$ \$6.3 million today
  - $\approx$ \$35 million December 2017
- Often estimated that Bitcoin energy consumption is similar to a small country:
  https://digiconomist.net/bitcoin-energy-consumption

Bitcoin as a global immutable ledger

- The Bitcoin blockchain contains many messages hidden in Bitcoin addresses or transactions
- Easy to add your own message
- Available as a notary service for around $1 per document

Question

Can this feature make it illegal to run a Bitcoin node?

NTNU

How anonymous is Bitcoin?

- Bitcoin addresses provide *pseudonymity*
- New addresses can be generated for every transaction
- Transaction inputs and outputs are public and *linkable*
- Some transactions, such as those with exchanges, are not permitted to be anonymous

Fact

Bitcoin transactions provide only weak anonymity

Monero and Zcash

- Some newer cryptocurrencies use cryptography to provide stronger anonymity, usually at a computational and/or storage cost
- Ring signatures:
  - someone from a user-defined set of signed the transaction
  - used in Monero
- Zero knowledge proofs:
  - provide proof that transaction is valid without revealing details
  - used in Zcash
- Zcash has been approved by financial regulators in New York (NYFDS)

NTNU

Smart contracts

- A set of formal conditions which trigger a payment when they are satisfied
- Bitcoin has a built-in scripting language
  - Powerful but limited language
  - Used in every transaction
  - Script must return TRUE in order to spend transaction output
- Developed further in Ethereum
  - Turing complete language
  - Contains both users accounts and contract accounts
  - Basis for many blockchain applications today
- Most large companies, such as IBM, are interested in using smart contracts in commercial applications

NTNU

Altcoins

- Hundreds of Bitcoin alternatives deployed today
- Commercial applications today typically using closed (*permissioned*) blockchains
- Other consensus mechanisms are being widely explored
  - Proof of stake
  - Sortition (see Algorand)
  - Byzantine agreement protocols

Conclusion

- Commonly stated that we are still at the start of the blockchain era
- Many different opinions on the likely impact of blockchains
- According to Meiklejohn top challenges are:
  - **Interoperability**: in a world of multiple ledgers, how should they be classified or standardised to allow interoperation?
  - **Cost-effectiveness**: can we avoid proof-of-work puzzles with their huge power costs?
  - **Privacy**: long-term privacy, selective privacy and anonymity all remain problematic
  - **Scalability**:
    - how to limit the size of blockchains?
    - can we split into realms of interest (sharding) to avoid checking all transactions?

NTNU

More information

- Mastering Bitcoin by Andreas M. Antonopoulos
  https://github.com/bitcoinbook/bitcoinbook
- Technical details of Bitcoin: en.bitcoin.it
- Software and wallets for Bitcoin: bitcoin.org
- Original Bitcoin paper of Satoshi Nakamoto:
  https://bitcoin.org/en/bitcoin-paper
- IBM Blockchain Blog
  https://www.ibm.com/blogs/blockchain/

Thanks for listening

Questions?