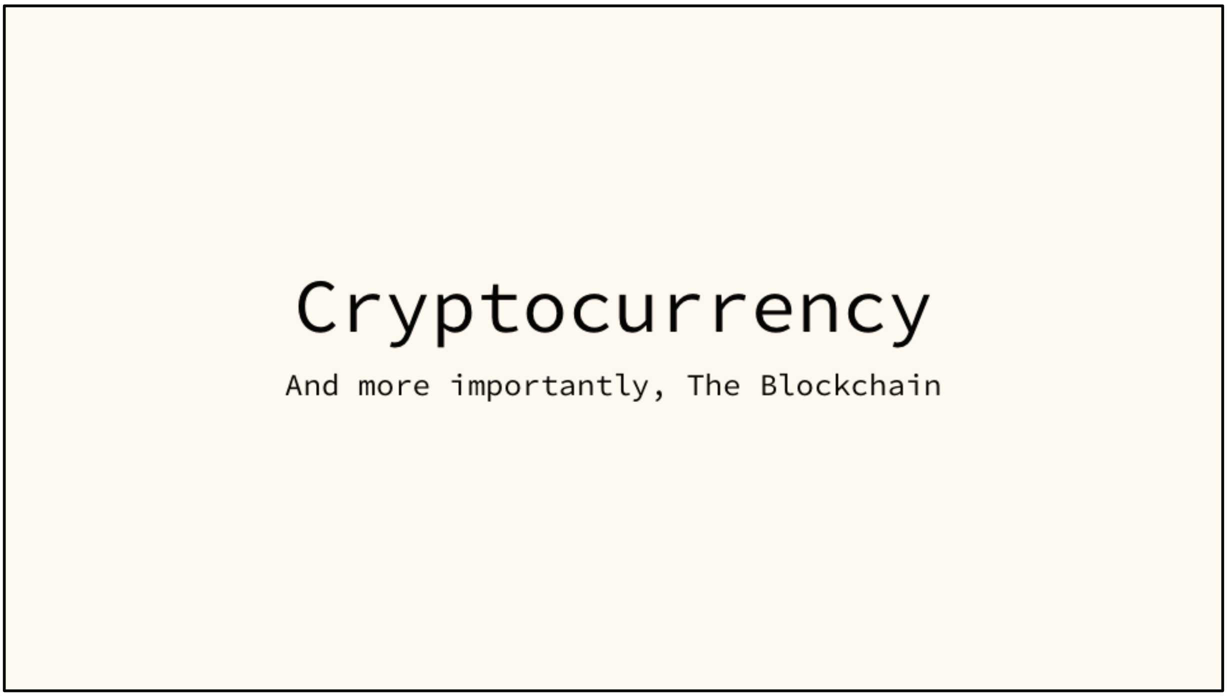
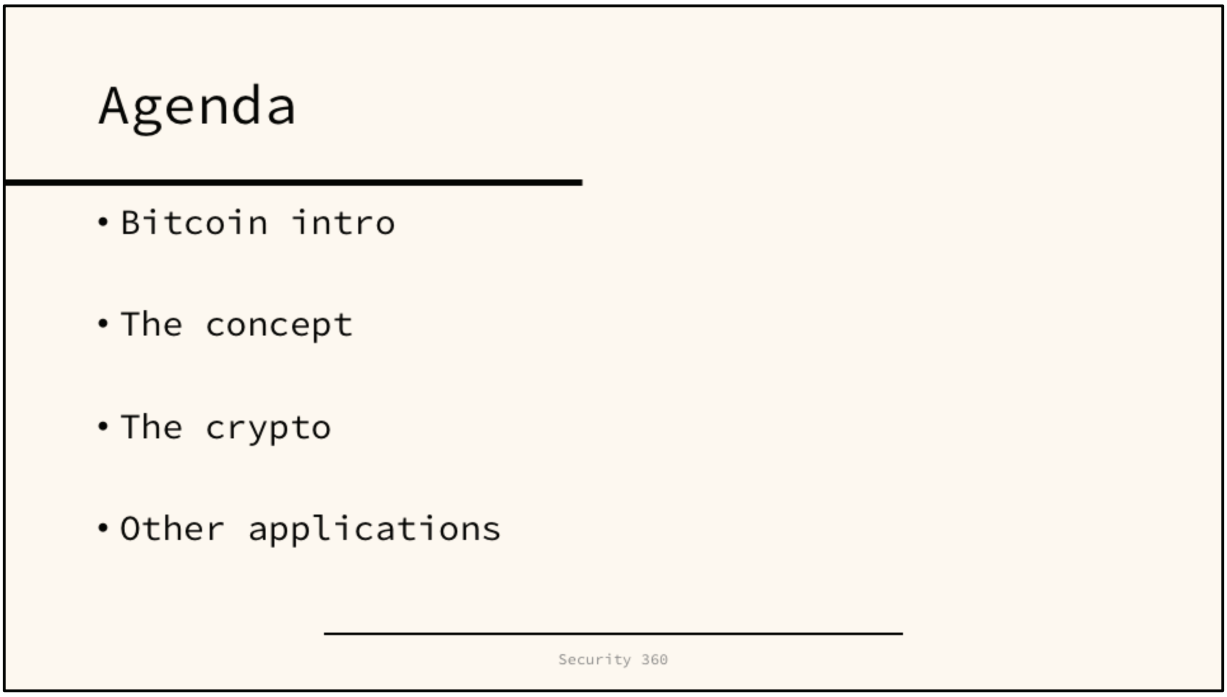


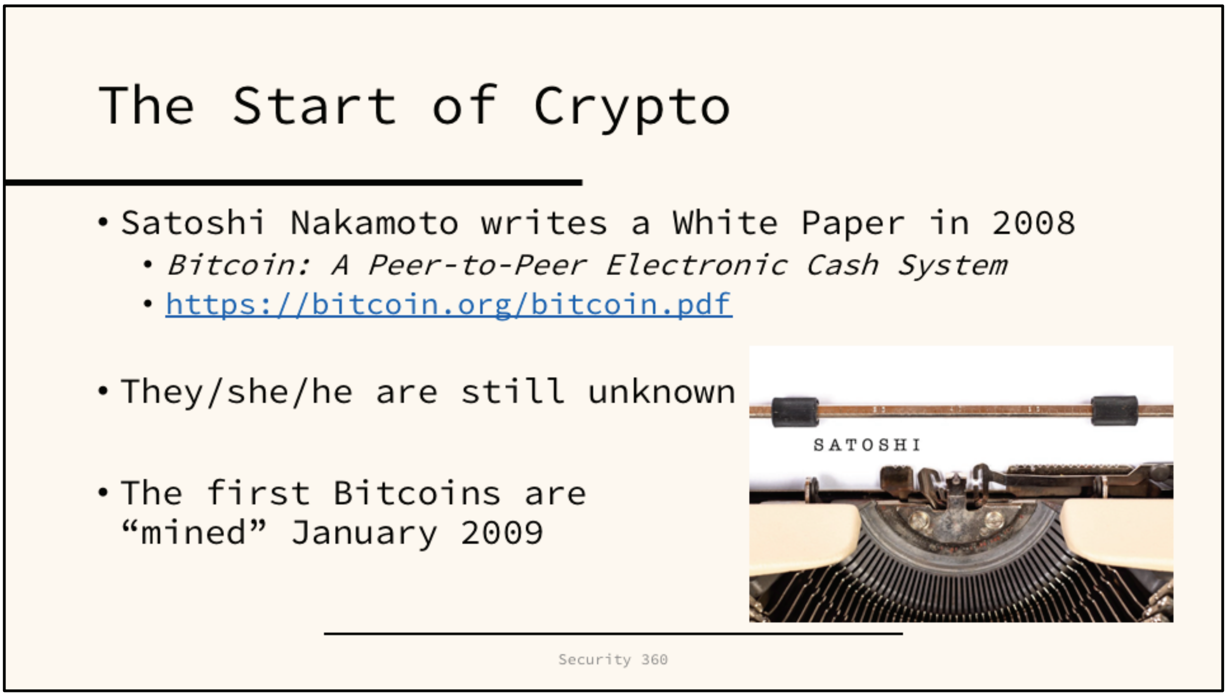
Cryptocurrency

And more importantly, The Blockchain



Agenda

- Bitcoin intro
- The concept
- The crypto
- Other applications



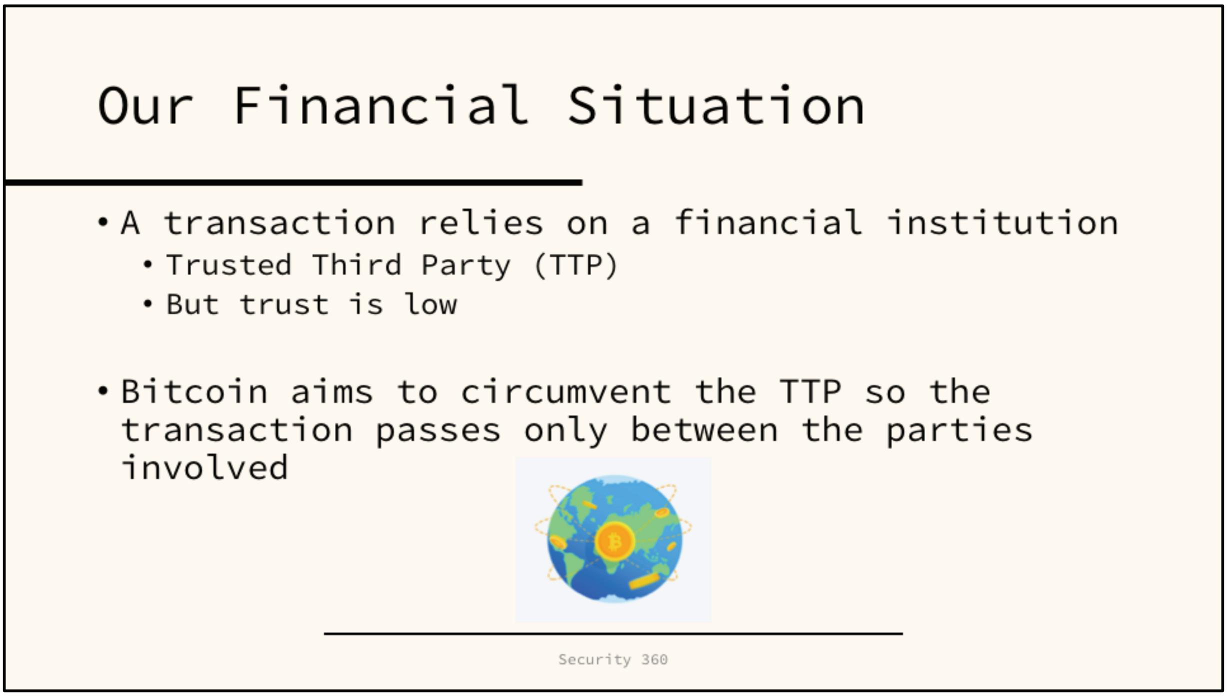
The Start of Crypto

- Satoshi Nakamoto writes a White Paper in 2008
  - *Bitcoin: A Peer-to-Peer Electronic Cash System*
  - https://bitcoin.org/bitcoin.pdf
- They/she/he are still unknown
- The first Bitcoins are “mined” January 2009

Security 360

"Satoshi (Trending Twitter Topics from 12.04.2019)" by trendingtopics is licensed under CC BY 2.0

"Das Milliardenspiel: Opener" by Bastian J. Schiffer is licensed under CC BY-NC-ND 4.0



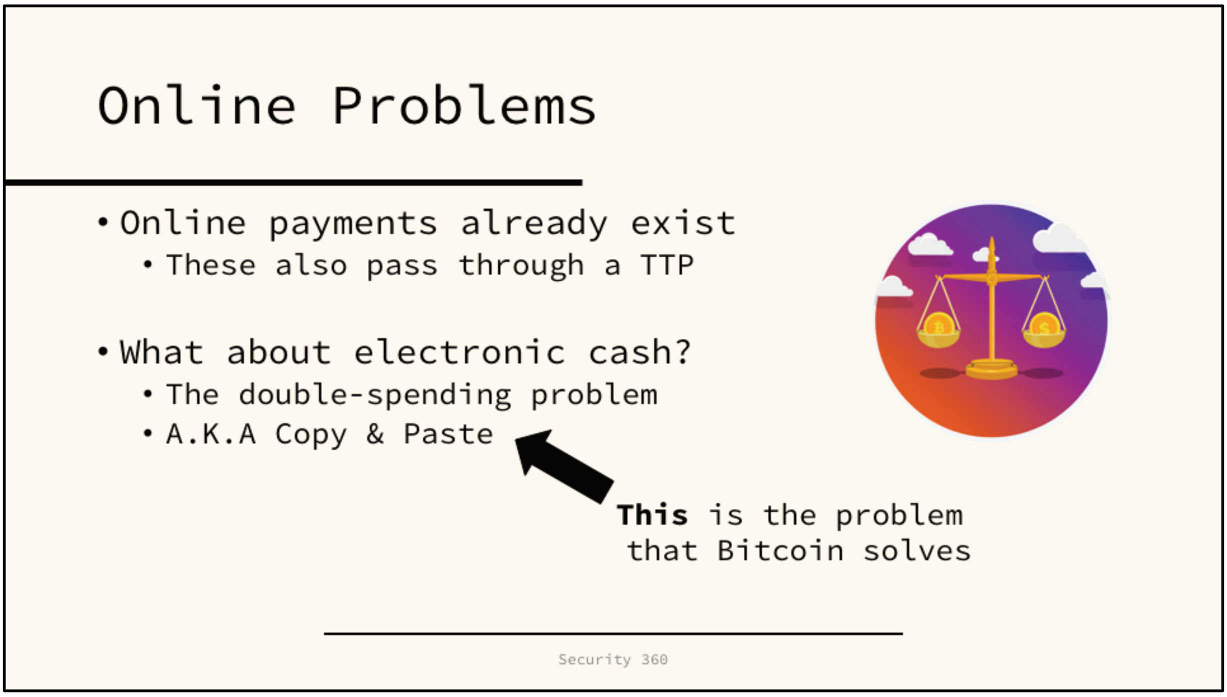
Our Financial Situation

- A transaction relies on a financial institution
  - Trusted Third Party (TTP)
  - But trust is low

- Bitcoin aims to circumvent the TTP so the transaction passes only between the parties involved

Security 360

"Bitcoin Illustrations Freebies" by Loredana Papp-Dinea, Mihai Baldean, Milo Themes is licensed under CC BY-NC-ND 4.0



Online Problems

- Online payments already exist
  - These also pass through a TTP
- What about electronic cash?
  - The double-spending problem
  - A.K.A Copy & Paste

This is the problem that Bitcoin solves

Security 360

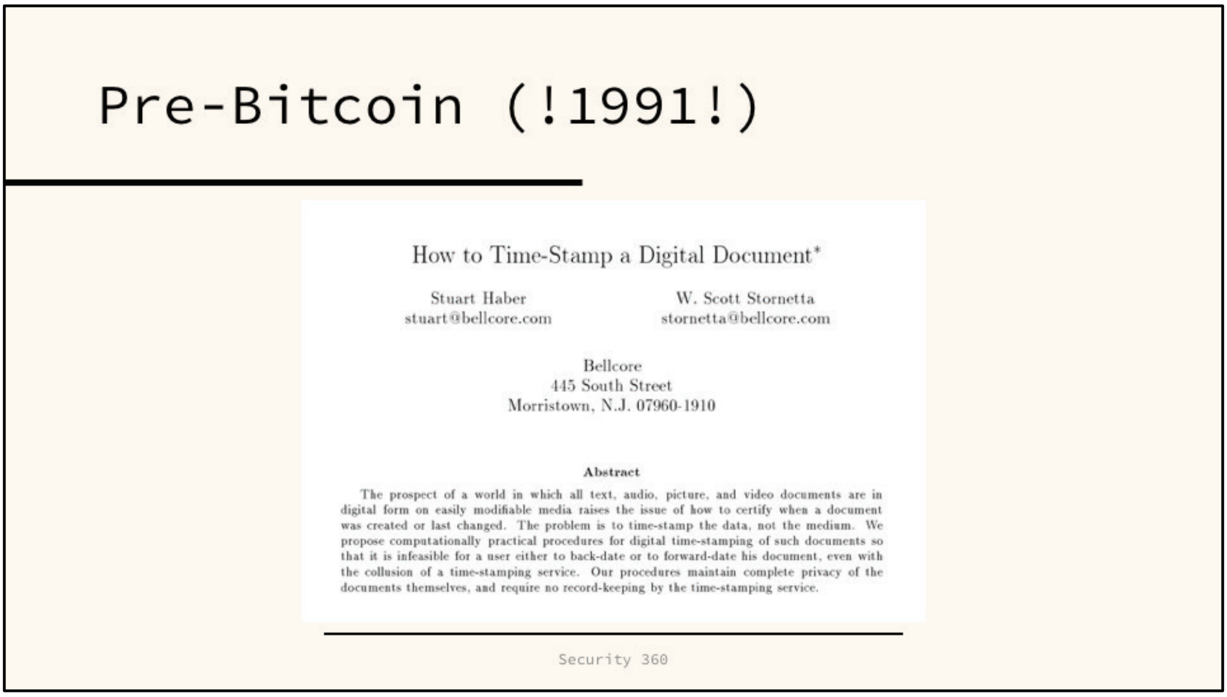
"Bitcoin Illustrations Freebies" by Loredana Papp-Dinea, Mihai Baldean, Milo Themes is licensed under CC BY-NC-ND 4.0

The Bitcoin Solution

“The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work”
– Satoshi Nakamoto, Bitcoin White Paper

A.K.A

The Blockchain



Pre-Bitcoin (!1991!)

How to Time-Stamp a Digital Document*

Stuart Haber
stuart@bellcore.com

W. Scott Stornetta
stornetta@bellcore.com

Bellcore
445 South Street
Morristown, N.J. 07960-1910

Abstract

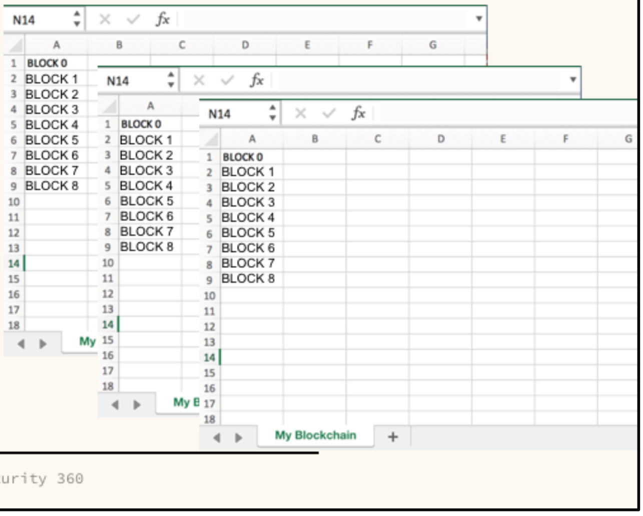
The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service.

Security 360

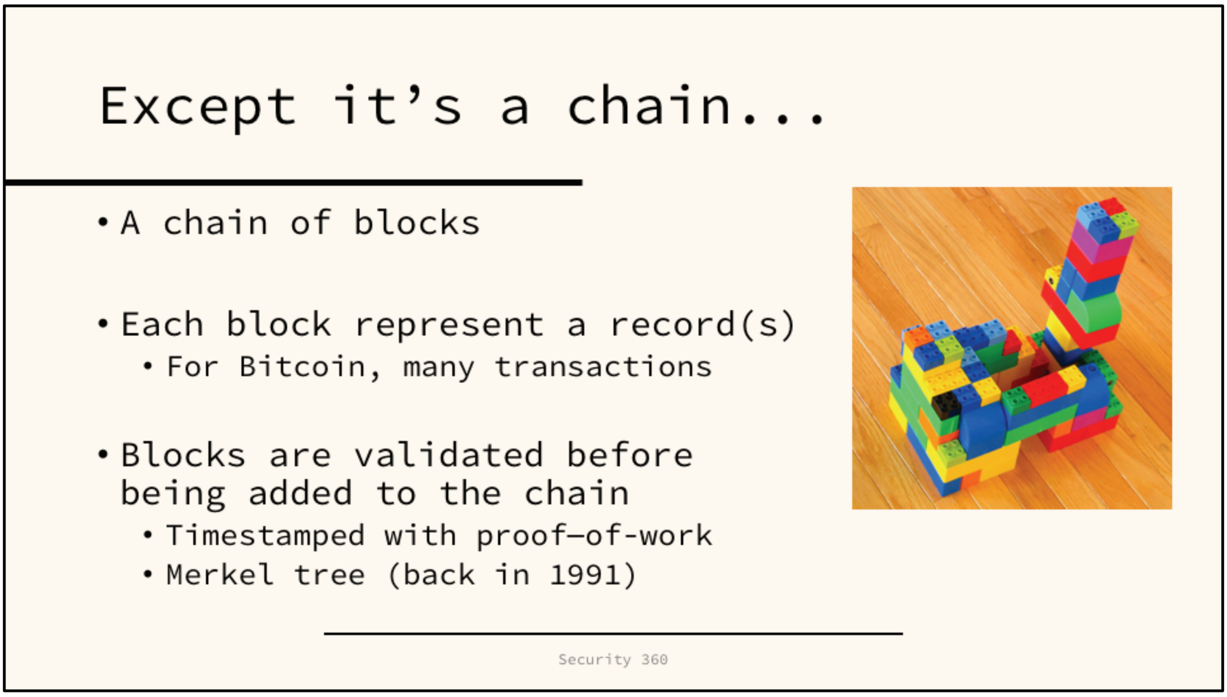
https://www.anf.es/pdf/Haber_Stornetta.pdf

Bitcoin P2P Network

- Imagine a database
- Update it constantly
- Replicate it across a network of peers
- Keep in sync

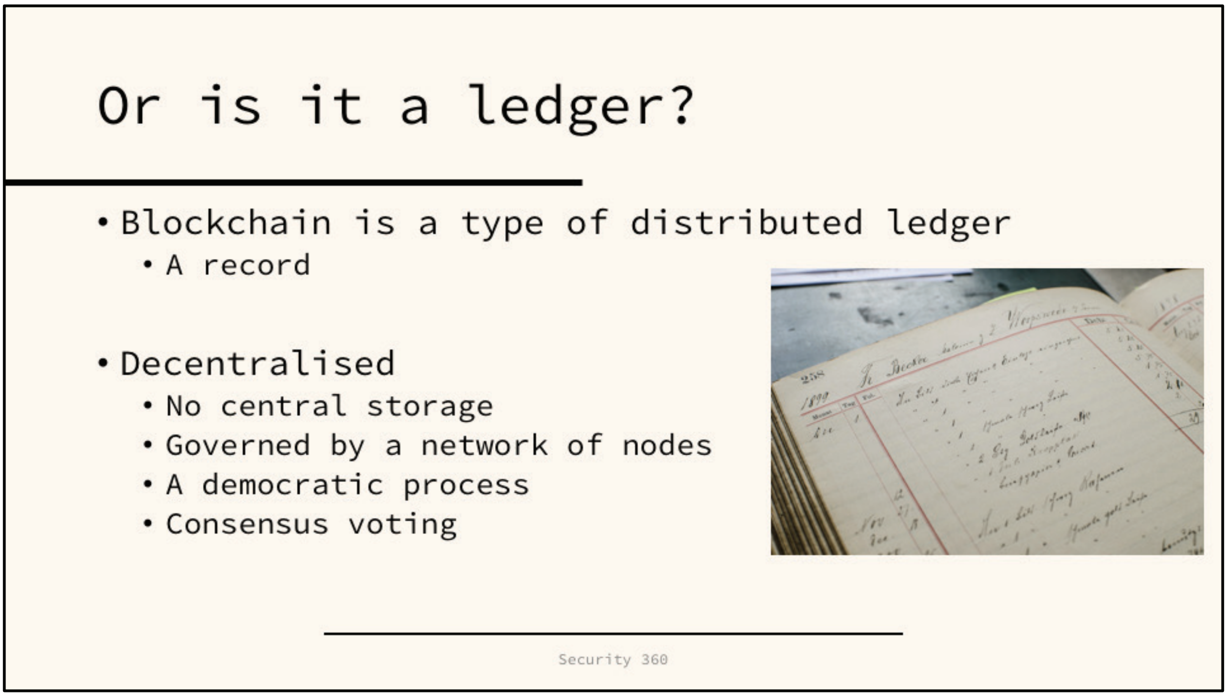


	A
1	BLOCK 0
2	BLOCK 1
3	BLOCK 2
4	BLOCK 3
5	BLOCK 4
6	BLOCK 5
7	BLOCK 6
8	BLOCK 7
9	BLOCK 8



Except it’s a chain...

- A chain of blocks
- Each block represent a record(s)
  - For Bitcoin, many transactions
- Blocks are validated before being added to the chain
  - Timestamped with proof–of-work
  - Merkel tree (back in 1991)

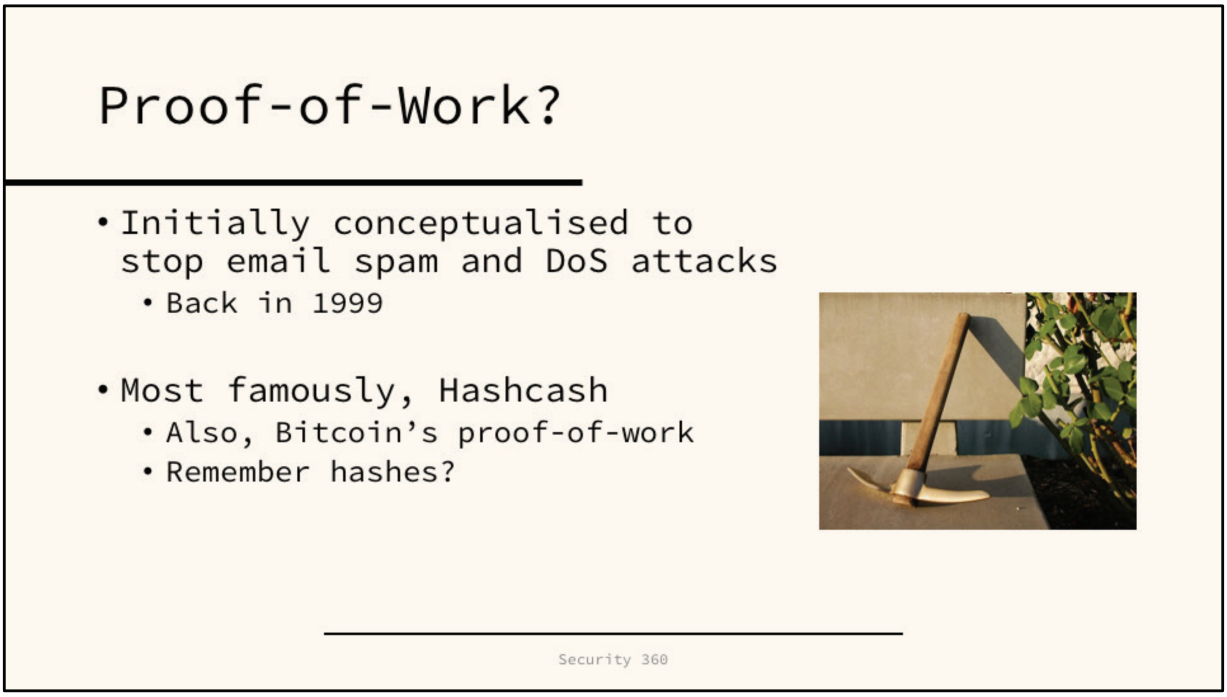


Or is it a ledger?

- Blockchain is a type of distributed ledger
  - A record
- Decentralised
  - No central storage
  - Governed by a network of nodes
  - A democratic process
  - Consensus voting

Security 360

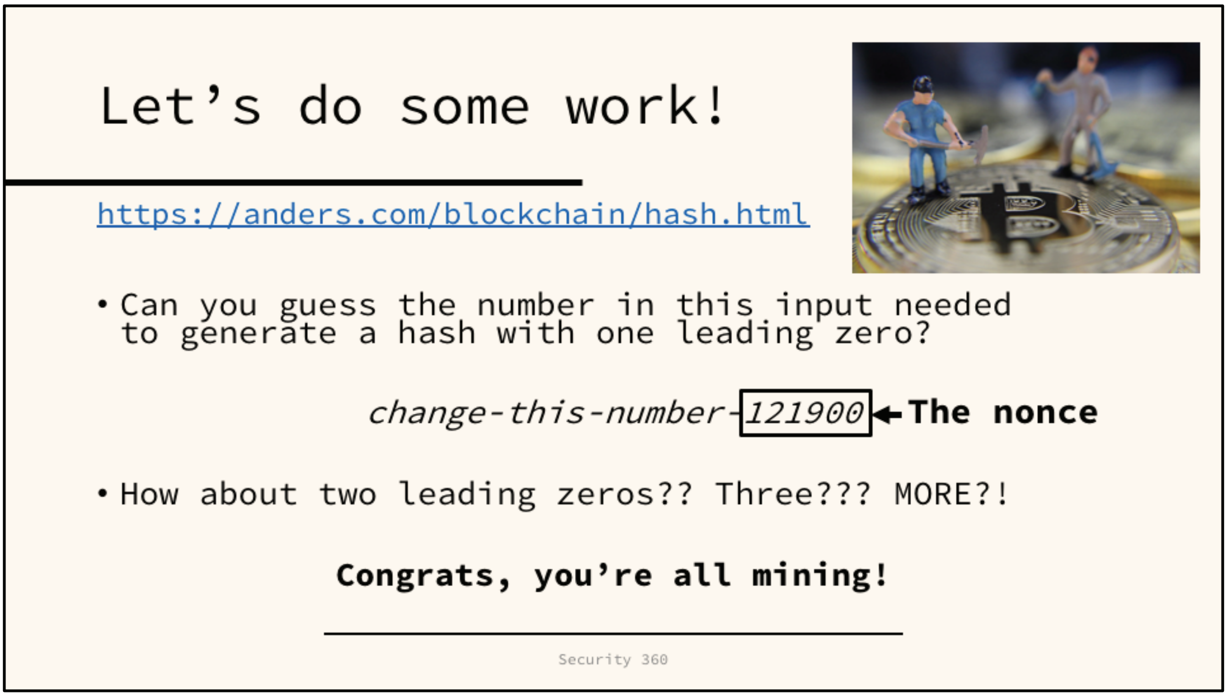
""1 Tube Krapplack" Buchandlung Netzel Worpswede - Kassenbuch, Eintrag Paula Becker" by r berndt is licensed under CC BY 2.0



Proof-of-Work?

- Initially conceptualised to stop email spam and DoS attacks
  - Back in 1999
- Most famously, Hashcash
  - Also, Bitcoin’s proof-of-work
  - Remember hashes?

Security 360



Let’s do some work!

https://anders.com/blockchain/hash.html

- Can you guess the number in this input needed to generate a hash with one leading zero?

change-this-number-121900 ← **The nonce**

- How about two leading zeros?? Three??? MORE?!

Congrats, you’re all mining!

Security 360

"Cryptocurrency Mining, Bitcoin mining stock photo" by Crypto360 is licensed under CC BY 2.0

The Genesis Block

- Block #0
- 10 leading zeros
- Mined by Satoshi
- Reward 50 Bitcoins!
- 03.01.2009

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

"Four Bitcoins laid on wood planks" by QuoteInspector is licensed under CC BY-ND 2.0

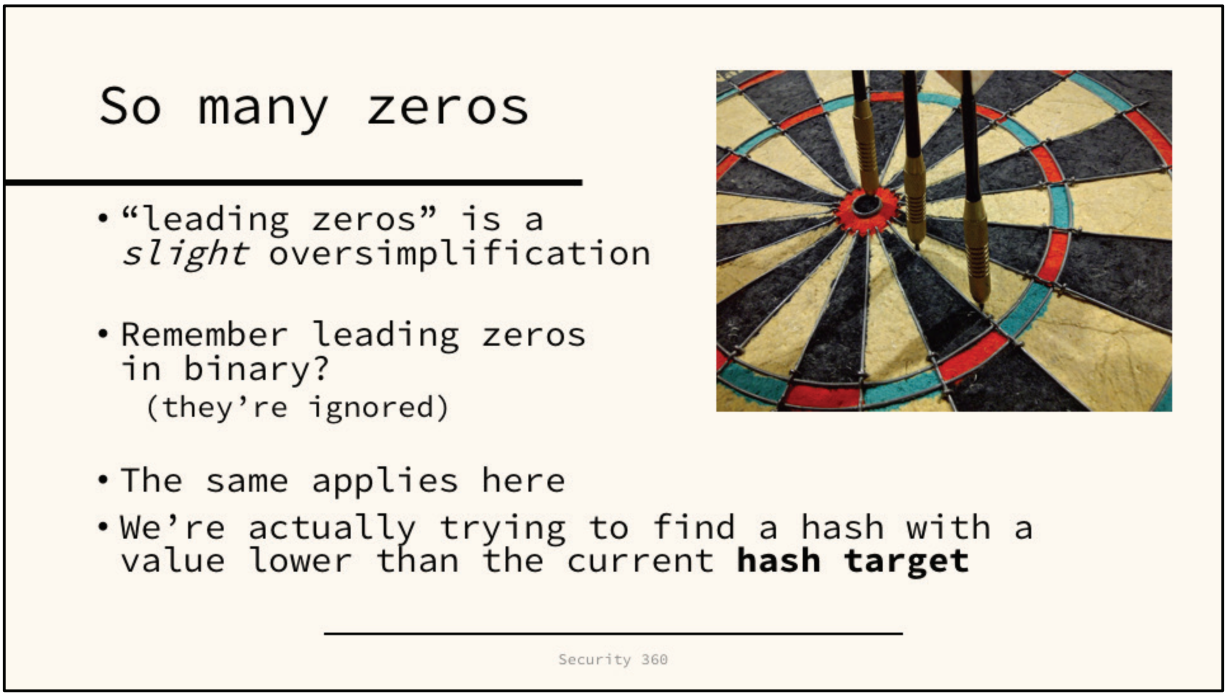
Blocks Today

- Block #580000
- 19 leading zeros
- Mined by a farm
- Reward 12.5 Bitcoins

```
00000000000000000003a93e72663961c2449dd1c92a004d39a6ff0df4ac72a3
```

Security 360

"Four Bitcoins laid on wood planks" by QuoteInspector is licensed under CC BY-ND 2.0

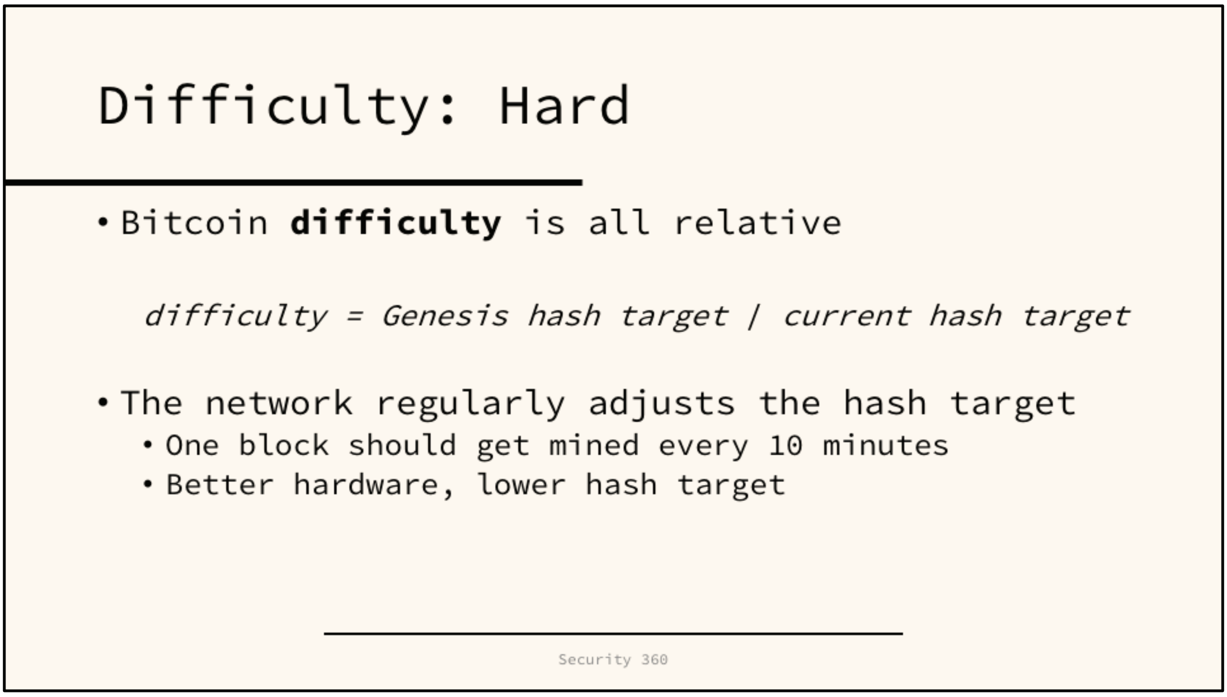


So many zeros

- “leading zeros” is a *slight* oversimplification
- Remember leading zeros in binary?
  (they’re ignored)
- The same applies here
- We’re actually trying to find a hash with a value lower than the current **hash target**

Security 360

"Bulls-eye" by Janna Wandler is licensed under CC BY-ND 2.0



Difficulty: Hard

- Bitcoin **difficulty** is all relative

  difficulty = Genesis hash target / current hash target

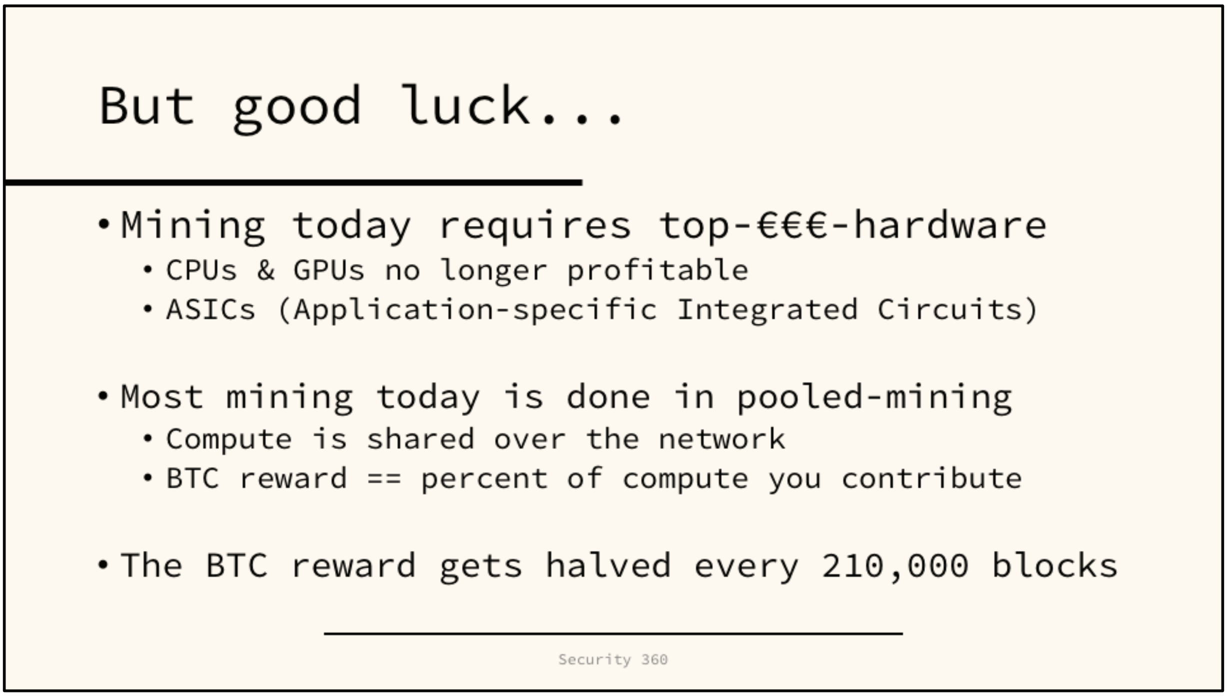
- The network regularly adjusts the hash target
  - One block should get mined every 10 minutes
  - Better hardware, lower hash target

What if I get one?

- It gets added to the chain, of course
  - Along with all transactions since the last block
- And, as a reward for being successful
  - You can add a transaction to yourself for **12.5BTC**!!!
  - **The coinbase**

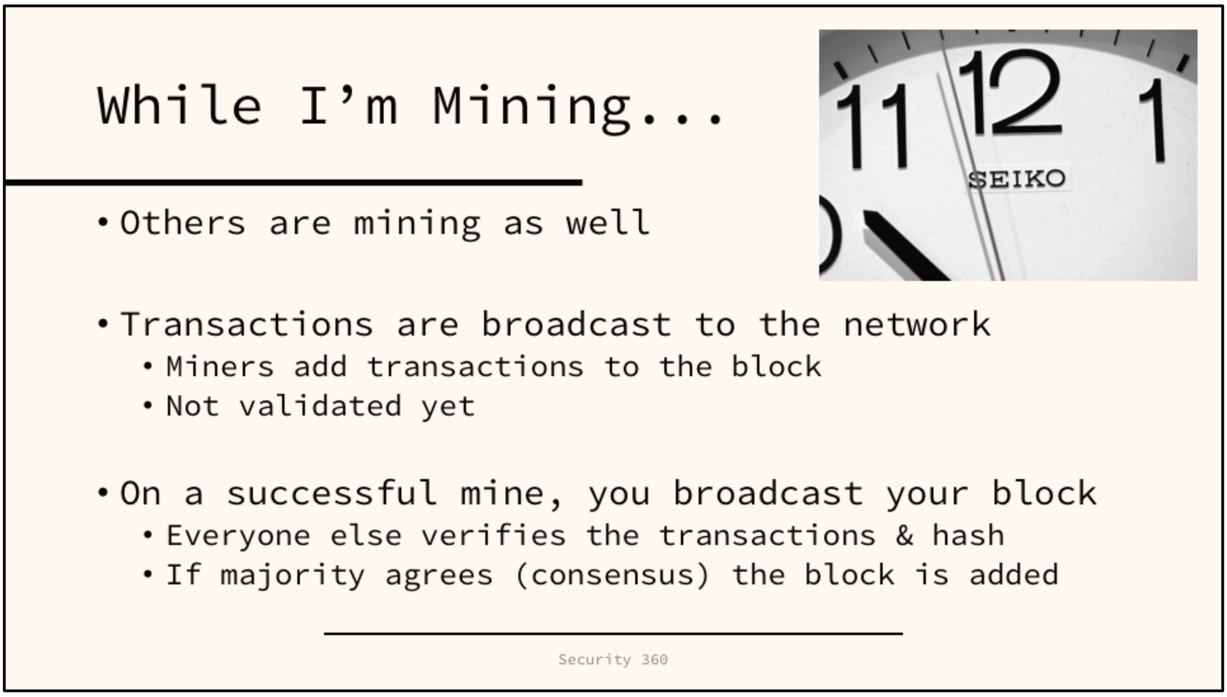
Security 360

"Bitcoin Illustrations Freebies" by Loredana Papp-Dinea, Mihai Baldean, Milo Themes is licensed under CC BY-NC-ND 4.0



But good luck...

- Mining today requires top-€€€-hardware
  - CPUs & GPUs no longer profitable
  - ASICs (Application-specific Integrated Circuits)
- Most mining today is done in pooled-mining
  - Compute is shared over the network
  - BTC reward == percent of compute you contribute
- The BTC reward gets halved every 210,000 blocks



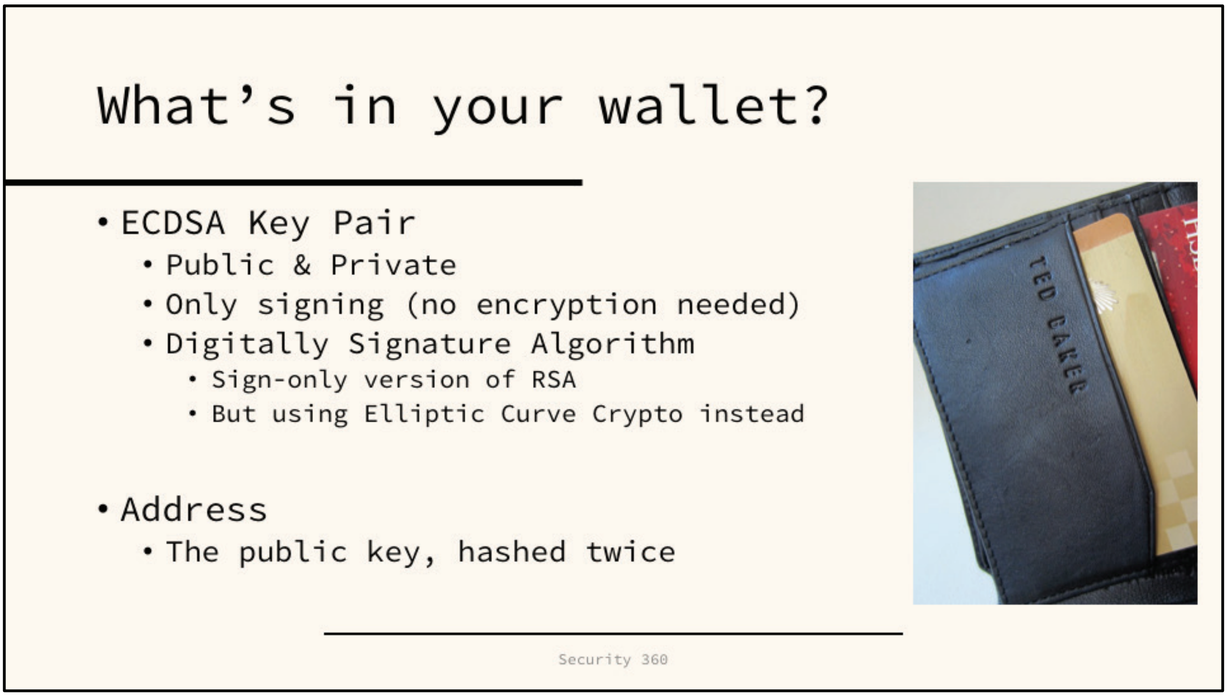
While I’m Mining...

- Others are mining as well
- Transactions are broadcast to the network
  - Miners add transactions to the block
  - Not validated yet
- On a successful mine, you broadcast your block
  - Everyone else verifies the transactions & hash
  - If majority agrees (consensus) the block is added

Security 360

Why it works? Too much Work!

- Modifying a block is not trivial
  - Modifying a block requires the proof-of-work to be done again
  - The input to compute the proof-of-work hash includes a reference to the block before it
  - So **ALL** the blocks after the modified block need their proof-of-work done again

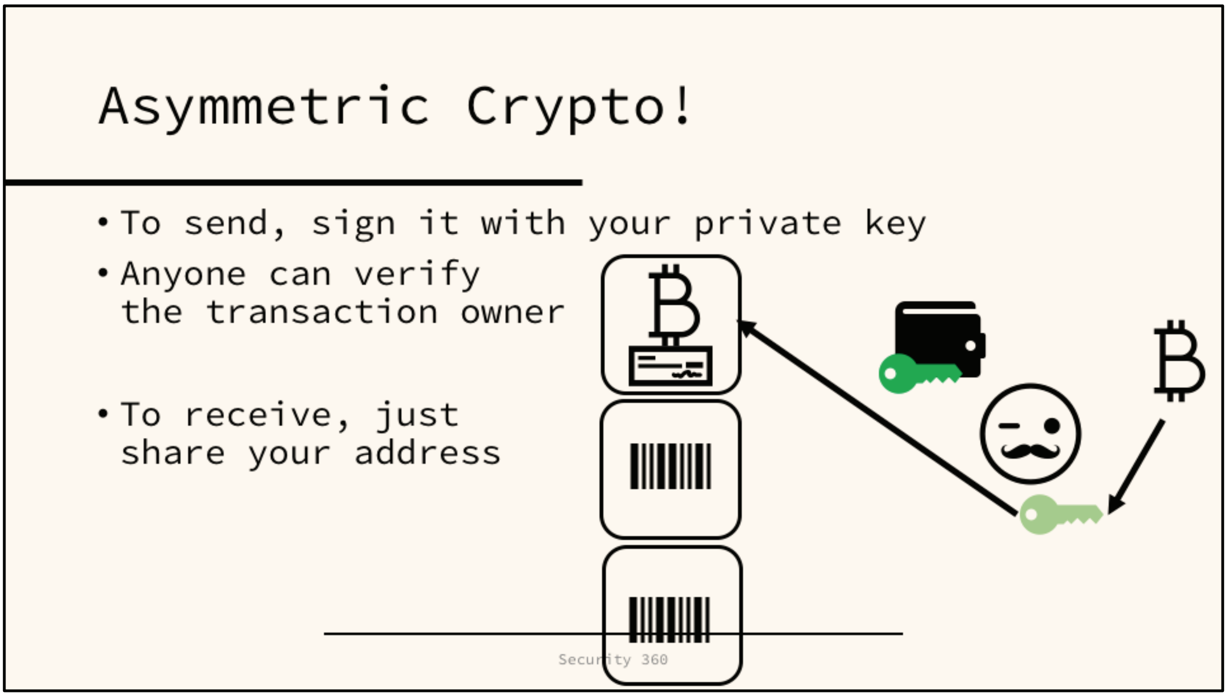


What's in your wallet?

- ECDSA Key Pair
  - Public & Private
  - Only signing (no encryption needed)
  - Digitally Signature Algorithm
    - Sign-only version of RSA
    - But using Elliptic Curve Crypto instead
- Address
  - The public key, hashed twice

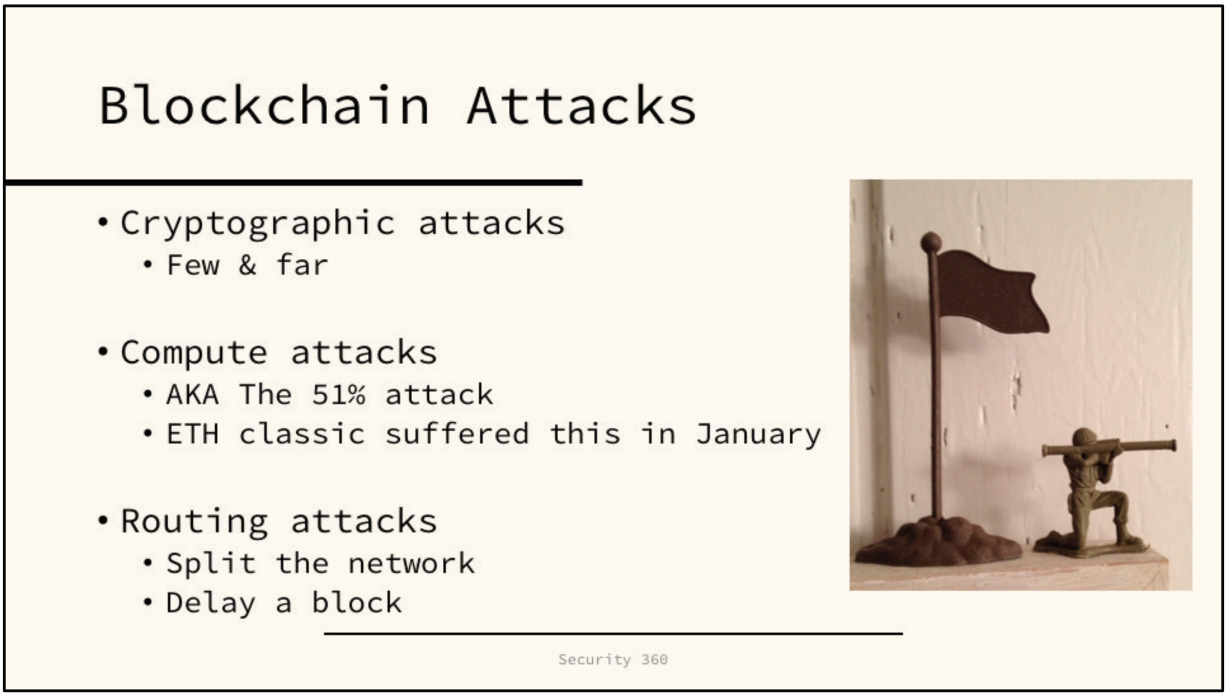
Security 360

"Credit Card in Wallet" by 401(K) 2012 is licensed under CC BY-SA 2.0



Asymmetric Crypto!

- To send, sign it with your private key
- Anyone can verify the transaction owner
- To receive, just share your address

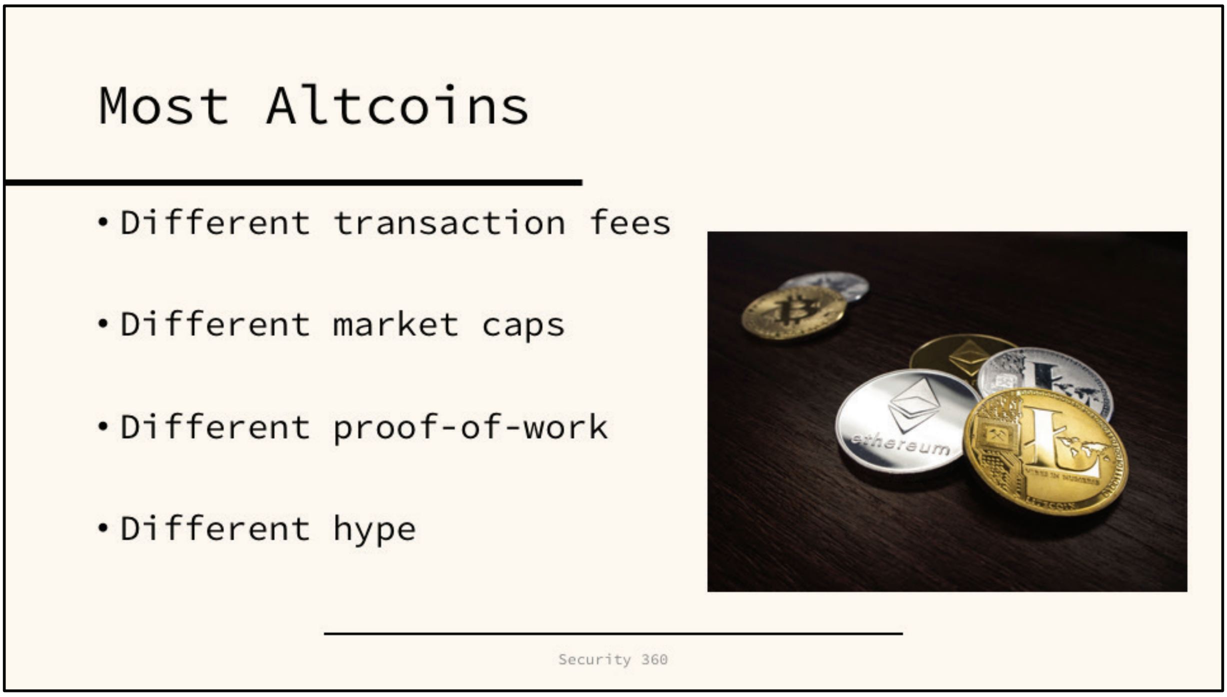


Blockchain Attacks

- Cryptographic attacks
  - Few & far
- Compute attacks
  - AKA The 51% attack
  - ETH classic suffered this in January
- Routing attacks
  - Split the network
  - Delay a block

https://btc-hijack.ethz.ch/files/btc_hijack.pdf

"Army men 2" by Ben Jolles is licensed under CC BY-NC 4.0

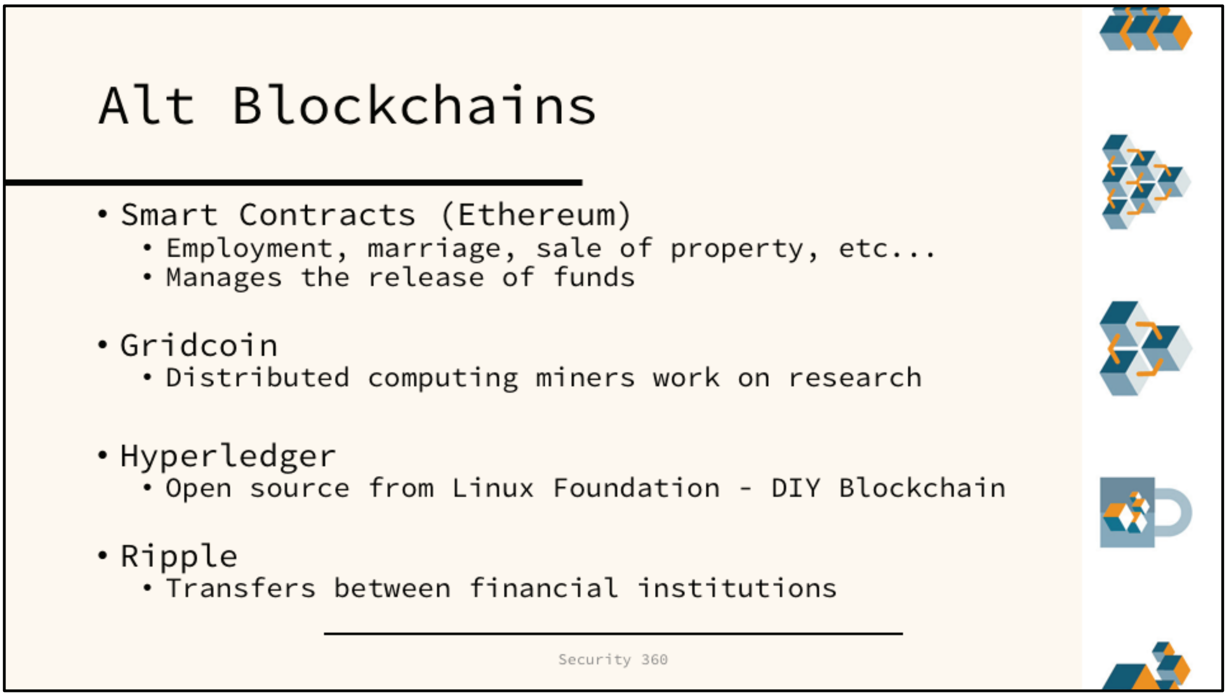


Most Altcoins

- Different transaction fees
- Different market caps
- Different proof-of-work
- Different hype

Security 360

"Altcoins - Alternative Cryptocurrencies" by orgalpari is licensed under CC BY 2.0



Alt Blockchains

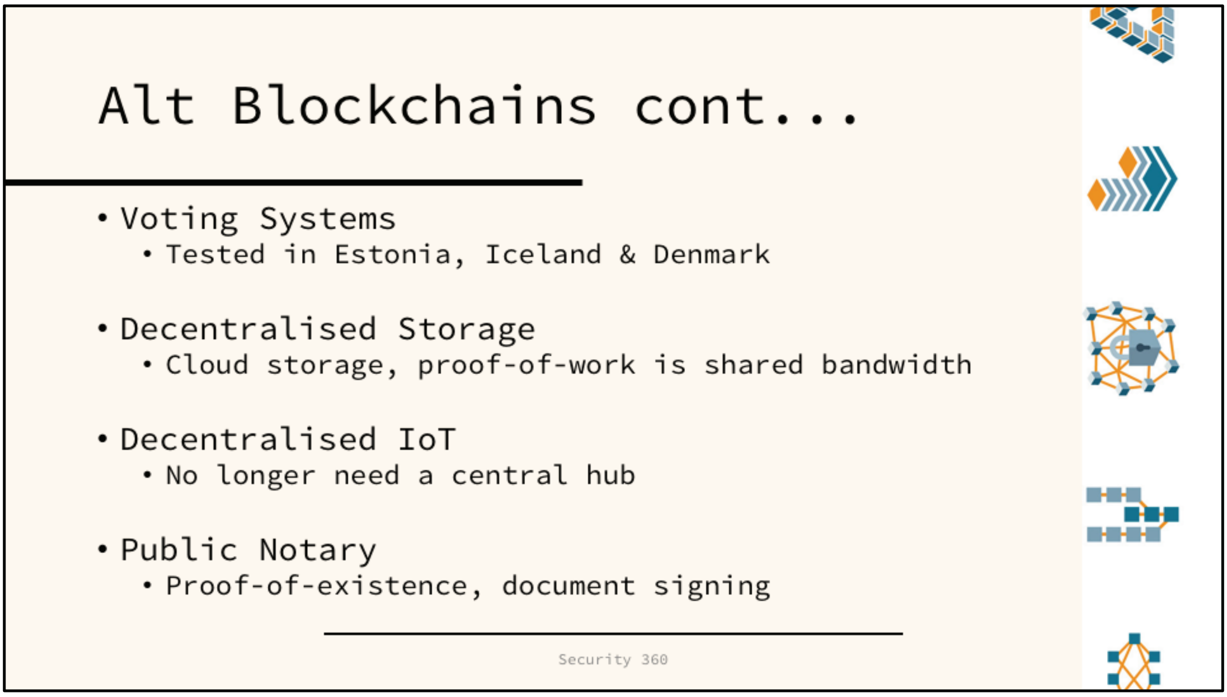
- Smart Contracts (Ethereum)
  - Employment, marriage, sale of property, etc...
  - Manages the release of funds
- Gridcoin
  - Distributed computing miners work on research
- Hyperledger
  - Open source from Linux Foundation - DIY Blockchain
- Ripple
  - Transfers between financial institutions

Security 360

"Oracle Blockchain icon" by Rick Byrne is licensed under CC BY-NC-ND 4.0

Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), p.71.

Pilkington, M., 2016. 11 Blockchain technology: principles and applications. *Research handbook on digital transformations*, *225*.



Alt Blockchains cont...

- Voting Systems
  - Tested in Estonia, Iceland & Denmark
- Decentralised Storage
  - Cloud storage, proof-of-work is shared bandwidth
- Decentralised IoT
  - No longer need a central hub
- Public Notary
  - Proof-of-existence, document signing

Security 360

"Oracle Blockchain icon" by Rick Byrne is licensed under CC BY-NC-ND 4.0

Pilkington, M., 2016. 11 Blockchain technology: principles and applications. *Research handbook on digital transformations*, *225*.

Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), p.71.