RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CRYP-W05

The Future of Bitcoin and Cryptocurrencies

MODERATOR: **Bart Preneel**

Professor
KU Leuven and iMinds
@CosicBe

PANELISTS:

Joseph Bonneau
Researcher
Stanford University and EFF
@josephbonneau

Greg Maxwell
CTO
Blockstream
@Blockstream

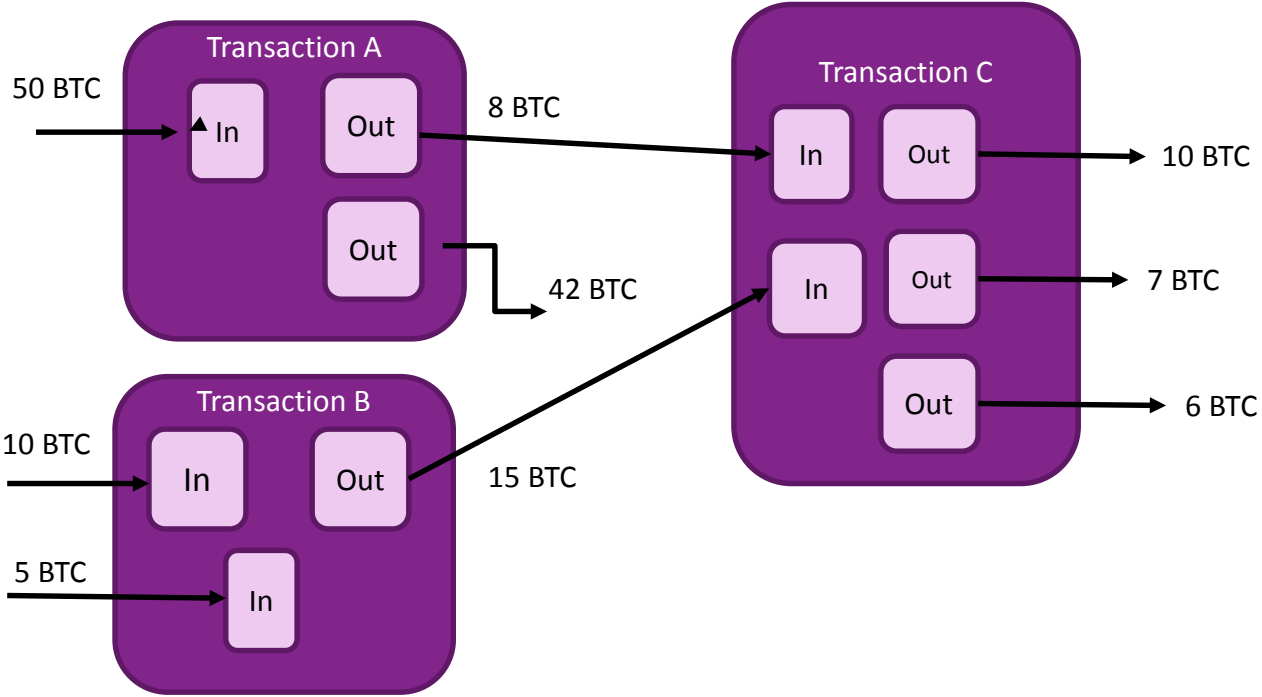
Adi Shamir
Professor
The Weizmann Institute

#RSAC

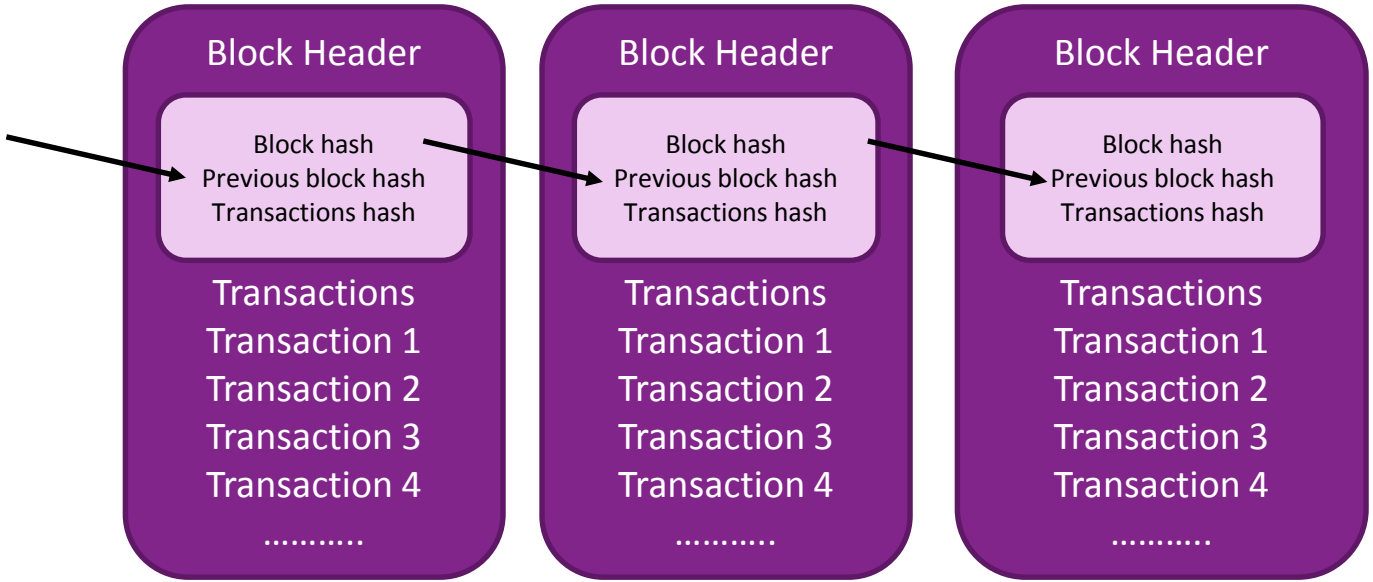
Bitcoin (°2008)

- **Digital currency with distributed generation and verification**
- **Transactions**
  - irreversible
  - inexpensive
  - over anonymous peer-to-peer network
  - broadcast within seconds and verified within 10 to 60 minutes by inclusion in hash chain
  - double spending prevention using a public decentralized ledger (block chain)
- **Pseudonymous** (believed by many to be anonymous)

Bitcoin Transaction



Bitcoin Ledger: the Blockchain



Increment counter in block header until block hash has many leading zeroes

Block #359391

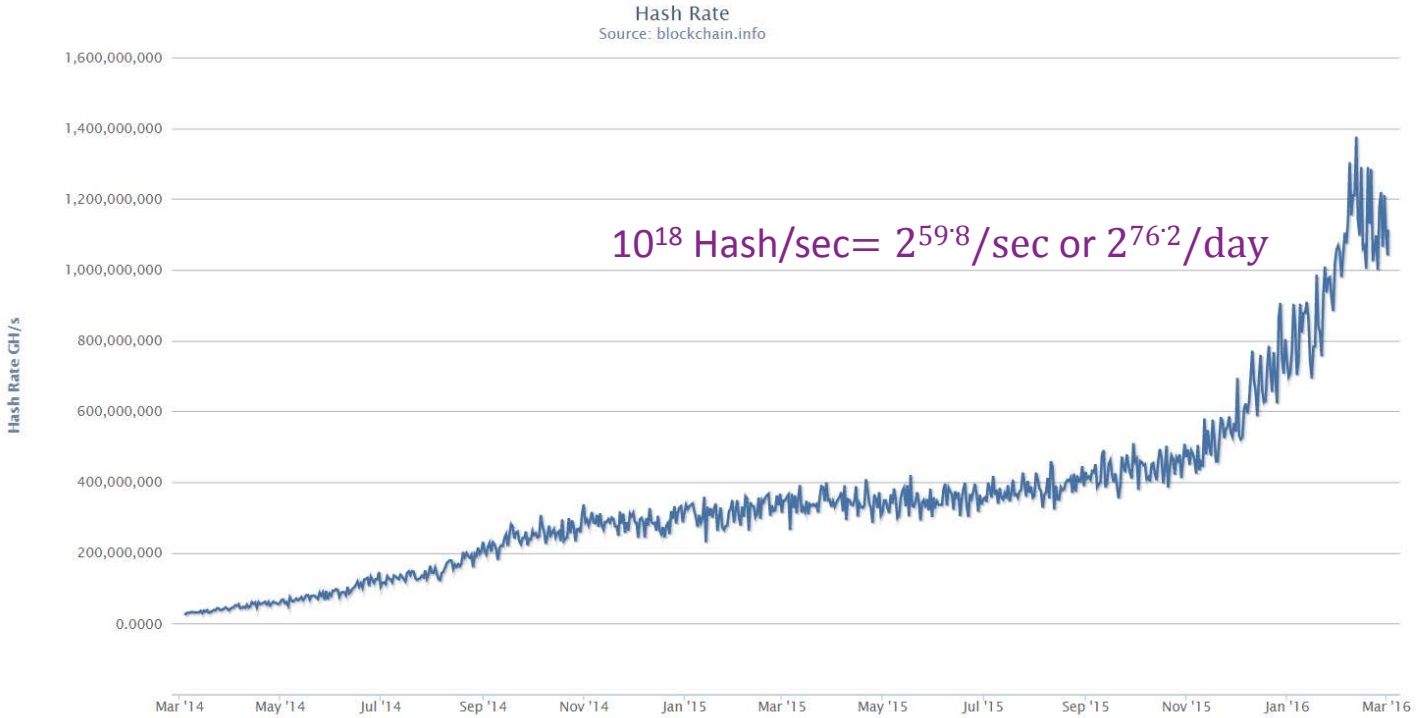
Summary	
Number Of Transactions	534
Output Total	5,027.57450746 BTC
Estimated Transaction Volume	1,557.11401964 BTC
Transaction Fees	0.02377486 BTC
Height	359391 (Main Chain)
Timestamp	2015-06-04 14:37:52
Difficulty	47,589,591,153.63
Bits	404167307
Size	368.591796875 KB
Version	3
Nonce	1031353973
Block Reward	25 BTC

Hashes	
Hash	00000000000000012bc7a8d83834654d71e95d7db09d398a45872807bec4b25
Previous Block	00000000000000136efacd3881239f9e42f8cedba375e07f80e4f776d94b95
Next Block(s)	
Merkle Root	e6d3ff8630fb4590c4167604acf42d06e12ff1ea004a42347d2abb64bca21c68

Mining Difficulty Level (https://blockchain.info/stats)

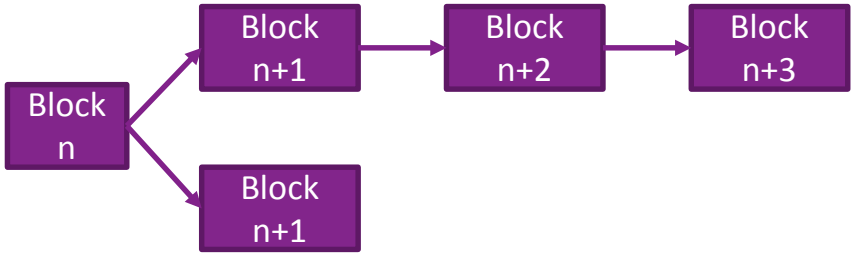
- Target: mining 1 block should take roughly 10 minutes
- Update level every 2016 blocks

Mining Hash Rate of Bitcoin Network



Block Chain Forks

- The block chain normally is one long chain
- Distributed nature of the network can lead to forks:



- Longest chain will become the main chain
- Transactions in orphan blocks are rebroadcast
- Transaction is typically accepted after it is included in 6 blocks (60 minutes)

Miners Revenue USD (https://blockchain.info/stats)

Market price in USD (https://blockchain.info/stats)

Market Capitalization (https://blockchain.info/stats)