CMU Computer Club Talk Series

Introduction to Bitcoin

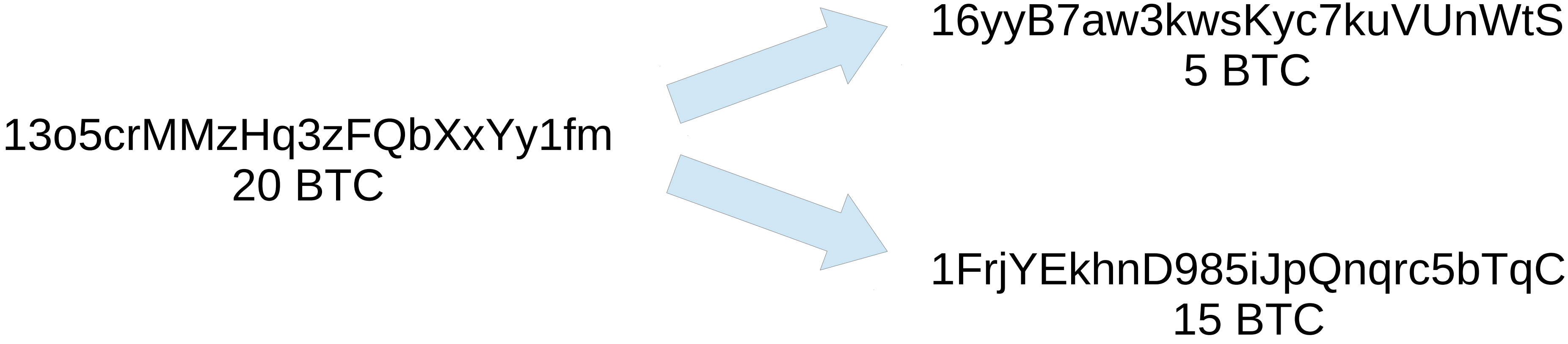
We would like to thank Green Hills Software for sponsoring this talk series.

Green Hills make the world's highest performing compilers, most secure real-time operating systems, revolutionary debuggers, and virtualization solutions for embedded systems.

Unspent Transaction Outputs (UTXO)

Key (address)	Balance
13o5crMMzHq3zFQbXxYy1fm	20.00000000
18VCnYccjarZUgENcXmaYVq	2.71828182
1Fmgf5cXfrGYv4b5TVkfYD8M	1.50000000
12f9hYjXWgCDAUm6mhgG38	0.29780000
1YTBss8vgm1dpxFJpWKu8ri2	0.00200000
1Tx9zZRZG28rCZ6t3yQKRTH	0.00100000

Bitcoin transaction



13o5crMMzHq3zFQbXxYy1fm
20 BTC

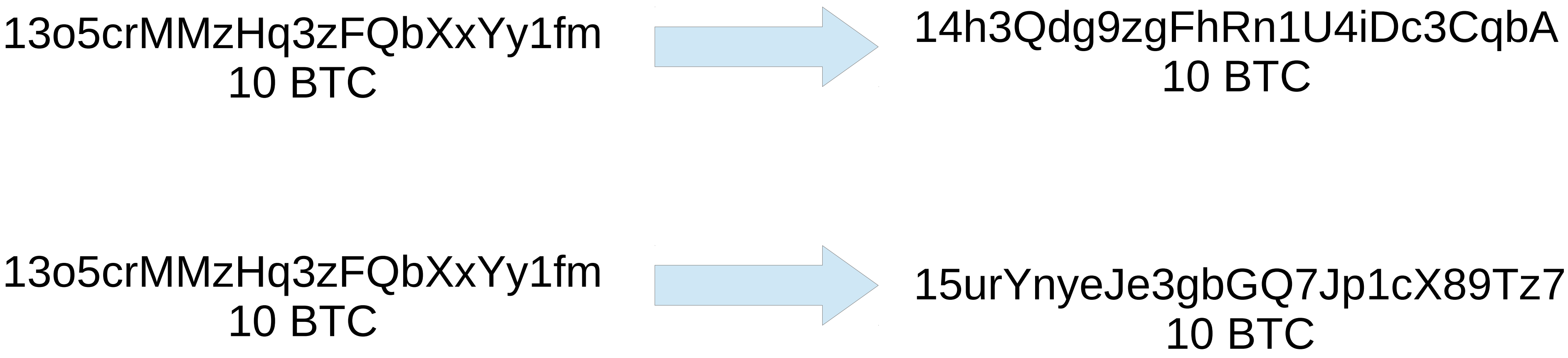
16yyB7aw3kwsKyc7kuVUnWtS
5 BTC

1FrjYEkhnD985iJpQnqrc5bTqC
15 BTC

Unspent Transaction Outputs (UTXO)

Key (address)	Balance
1FrjYEkhnD985iJpQnqrc5bTqC	15.00000000
16yyB7aw3kwsKyc7kuVUnWtS	5.00000000
18VCnYccjarZUgENcXmaYVq	2.71828182
1Fmgf5cXfrGYv4b5TVkfYD8M	1.50000000
12f9hYjXWgCDAUm6mhgG38	0.29780000
1YTBss8vgm1dpxFJpWKu8ri2	0.00200000
1Tx9zZRZG28rCZ6t3yQKRTH	0.00100000

The double spending problem



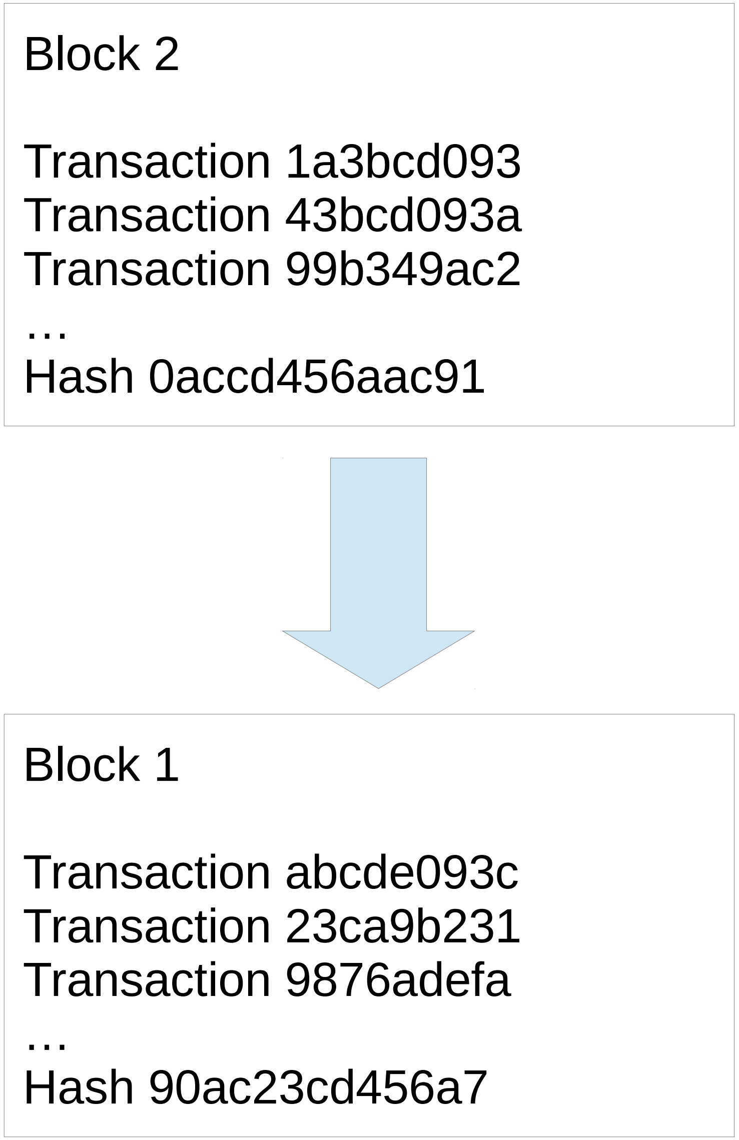
13o5crMMzHq3zFQbXxYy1fm
10 BTC

14h3Qdg9zgFhRn1U4iDc3CqbA
10 BTC

13o5crMMzHq3zFQbXxYy1fm
10 BTC

15urYnyeJe3gbGQ7Jp1cX89Tz7
10 BTC

Blocks



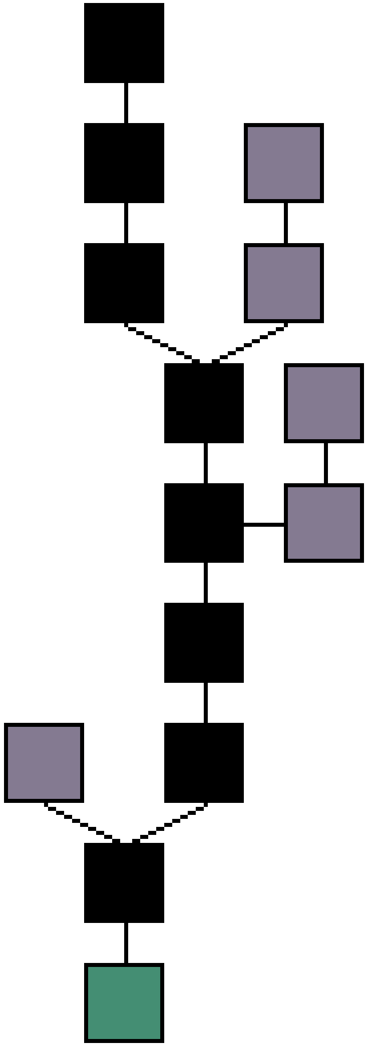
Block 2

Transaction 1a3bcd093
Transaction 43bcd093a
Transaction 99b349ac2
…
Hash 0accd456aac91

Block 1

Transaction abcde093c
Transaction 23ca9b231
Transaction 9876adefa
…
Hash 90ac23cd456a7

Blockchain



Bitcoin clients

- Full node
- Simplified Payment Verification (multibit, electrum)
- Web clients (blockchain.info)

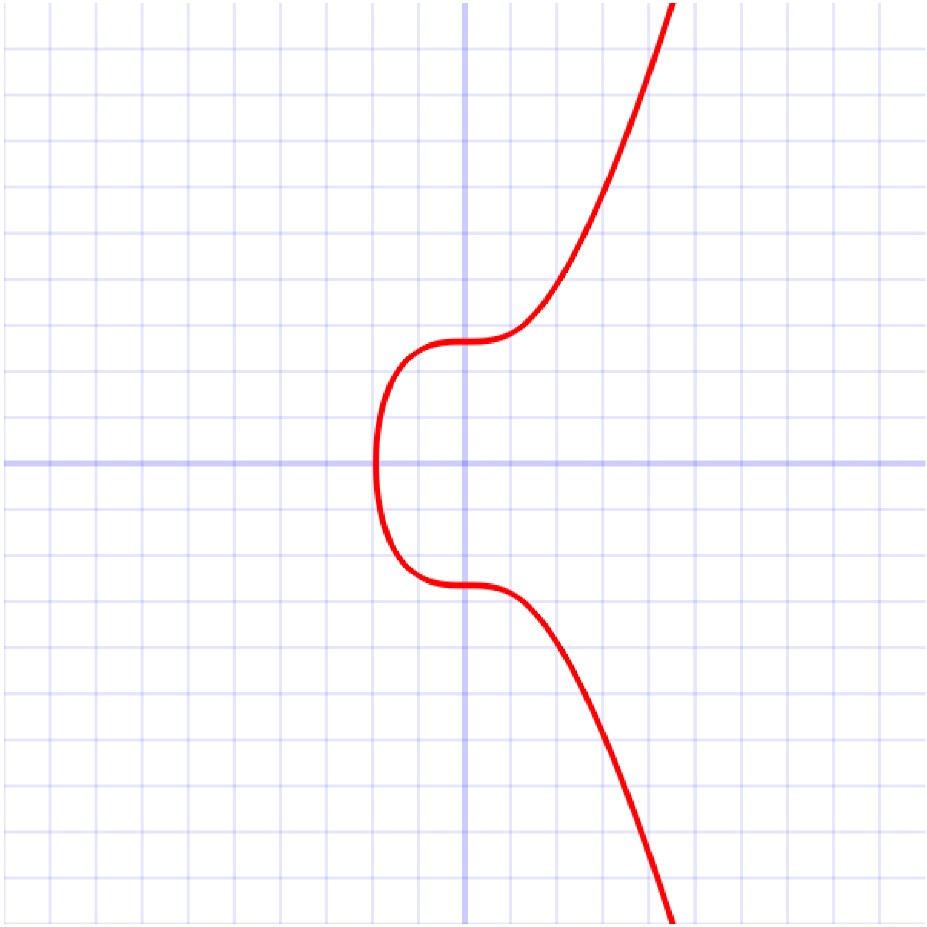
Getting Bitcoins

- Bank transfer
  Coinbase, Circle, Bitsimple
- P2P trading
  LocalBitcoins, Mycelium Trader, Bitcoin-Brokers, Bitcointalk.org
- Credit card by proxy
  amz2btc.com, Purse.io, Brawker
- Sell things
  coinpost.com, cyptothrift.com

Structure of a bitcoin address

- Base-58 encoded (A-Z, a-z, 1-9, excluding I,l,O)
- 160-bit hash, 32-bit checksum
- 1xxxx – Hash of public key
- 3xxxx – Script hash

SECP256K1



$$y^2 = x^3 + 7$$

Generating Addresses

sha256("it's a secret to everybody")
= 1f1a27b03ccaddef305483caf8dae0437
7e7093daee64508801829fb3bc71b0b

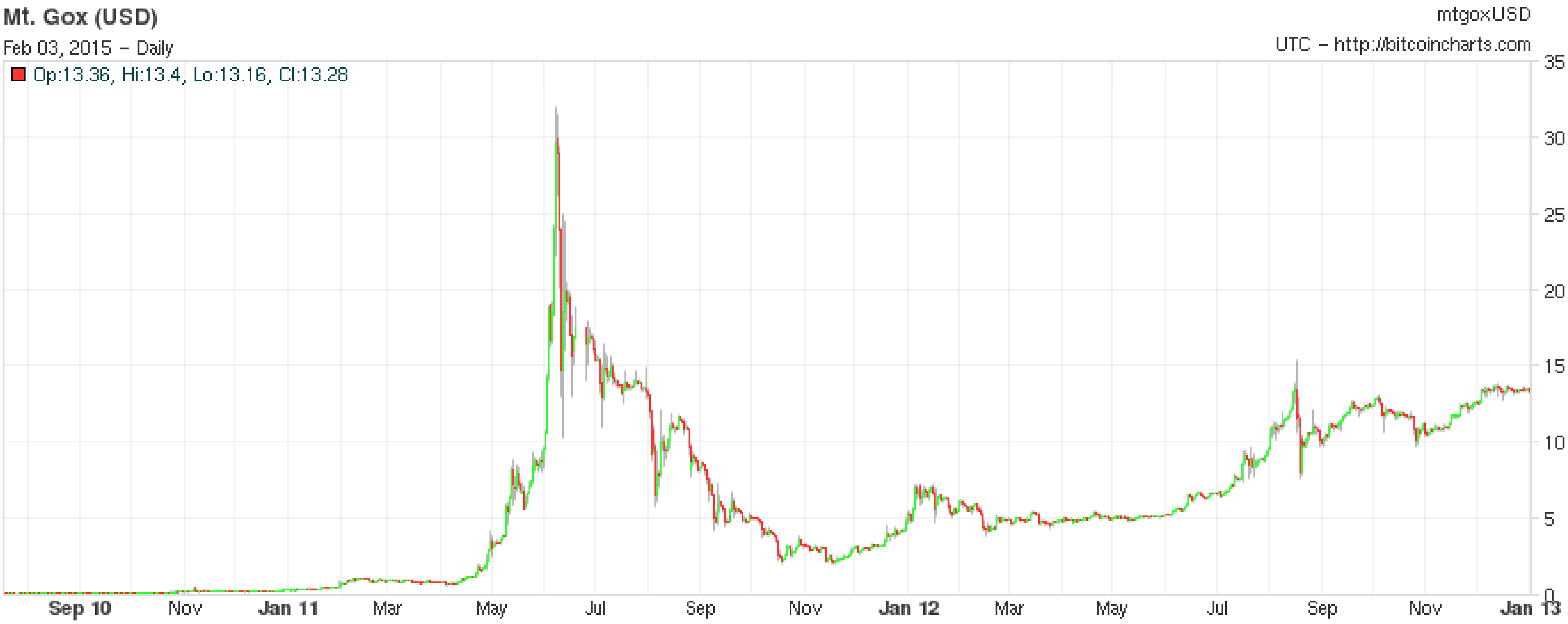
Public key (uncompressed)
19BZ1b3GifduLP22DmHP3np7W8nMBgdRuh

Public key (compressed)
1DXa95Vgrw1xsTSaZXL6MJt4qbBy4ZwAUm

Bitcoin History

- In May 2010, Laszlo offered 10,000 bitcoins for 2 pizzas.
- The value of those bitcoins has increased significantly since then.

Bitcoin Price in USD, 2010-2012


Mt. Gox (USD)
Feb 03, 2015 – Daily
mtgoxUSD
UTC – http://bitcoincharts.com
🟥 Op:13.36, Hi:13.4, Lo:13.16, Cl:13.28
Sep 10
Nov
Jan 11
Mar
May
Jul
Sep
Nov
Jan 12
Mar
May
Jul
Sep
Nov
Jan 13