Nikolai Smirnov and Laurence Squires

Cryptocurrency

What is it?

- Digital medium of exchange (currency)
- Encryption techniques regulate generation of units of currency
- First cryptocurrency – Bitcoin 2009


much coin how money so crypto
wow
very currency wow
mine v rich

Benefits:

- International
- Freedom in Payment
- Anonymous
- Less Risk (irreversible, hard to fraud)

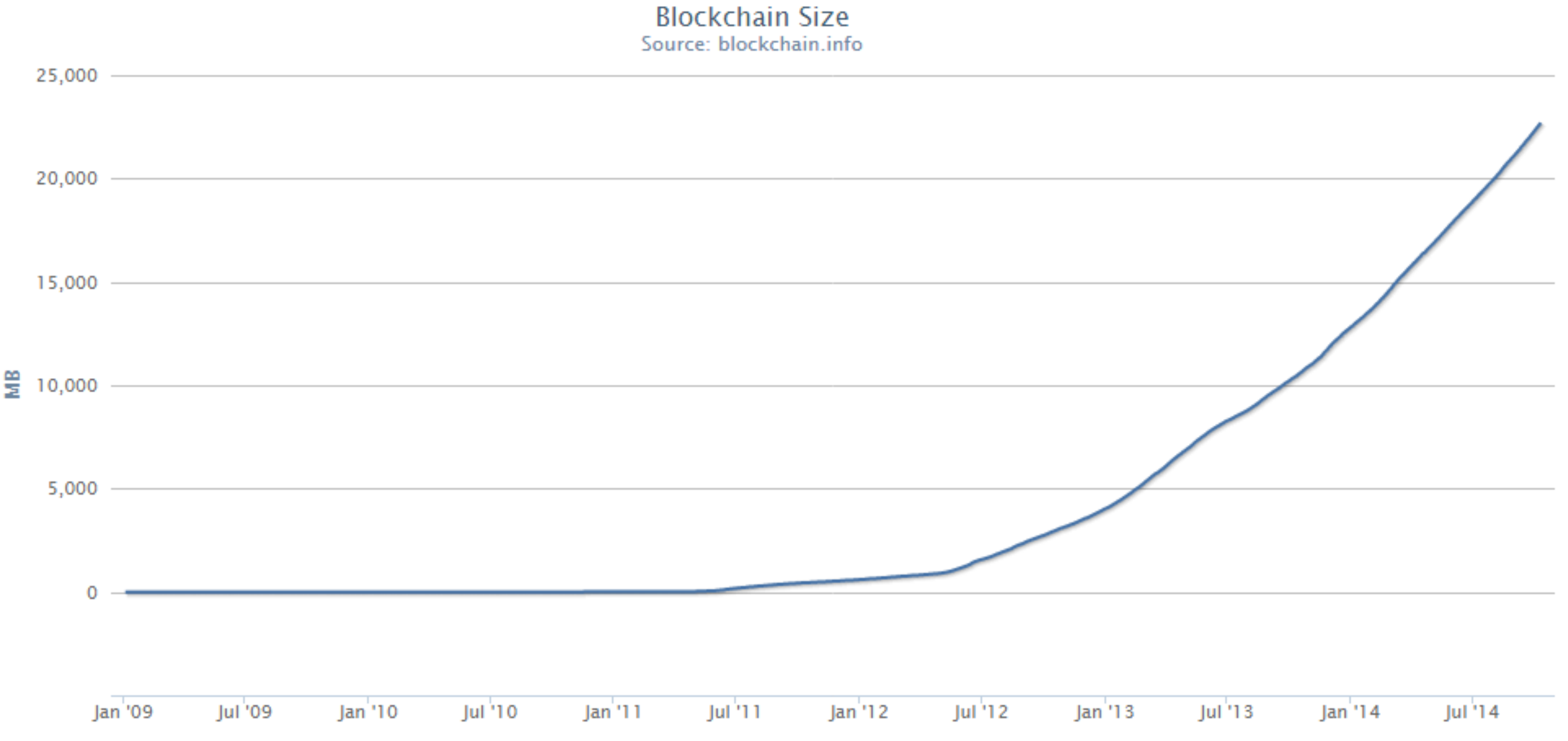
How it works:

- ‘Miners’ go through a ‘script’. Eventually they will find a valid chain of letters and numbers that can become a coin.

- Designed to be resource-intensive and difficult to limit ‘blocks’.

Mining process:

- **Public ledger** of financial transactions in bitcoin – **block chain**
- Servers form a public network which allows people to send each other bitcoin by validating the transactions, adding them to their copy of the ledger and broadcasting this addition
- Miners compile recent transactions into '**blocks**' and try to solve a computationally difficult puzzle
- By completing this puzzle, it 'seals' the ledger behind layers of computational work and adds a new 'block' to the block chain.
- Prevents fraudsters from hacking the ledger


Blockchain Size
Source: blockchain.info
MB
25,000
20,000
15,000
10,000
5,000
0
Jan '09
Jul '09
Jan '10
Jul '10
Jan '11
Jul '11
Jan '12
Jul '12
Jan '13
Jul '13
Jan '14
Jul '14

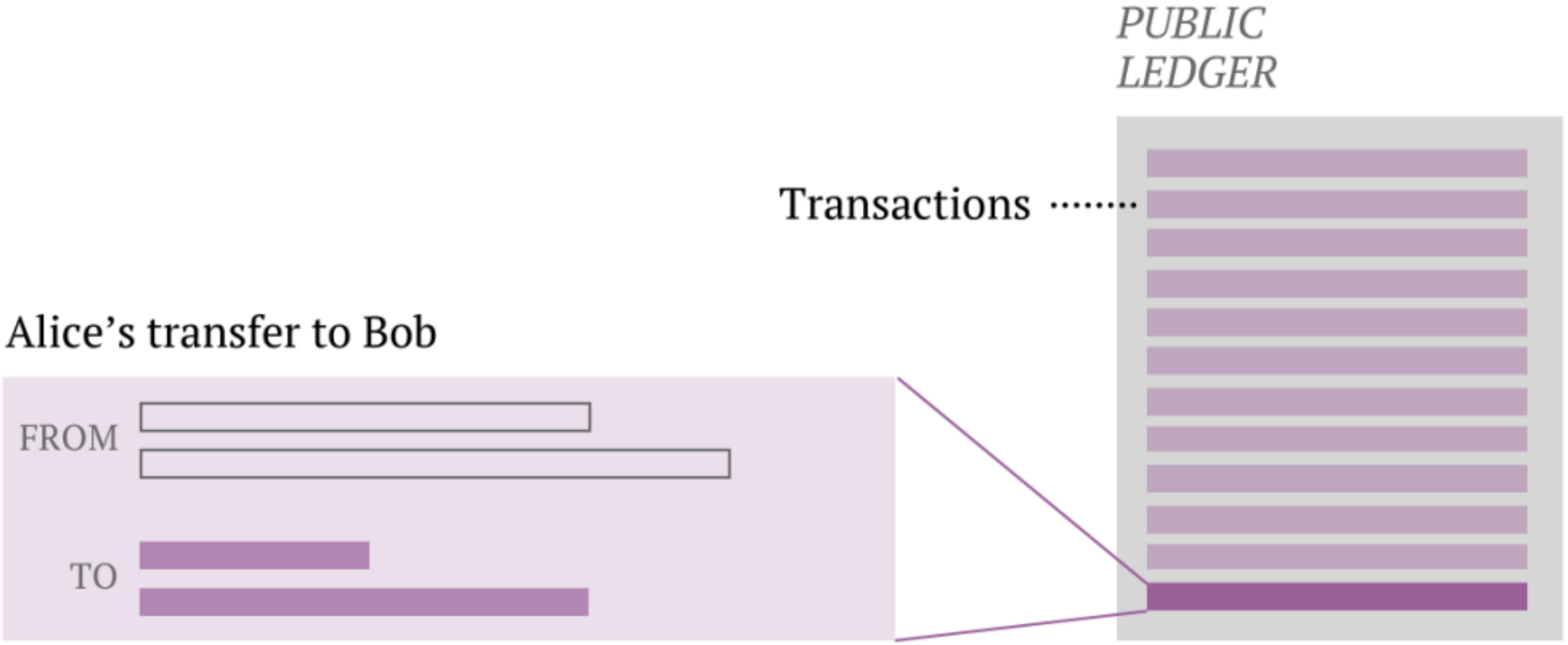
Mining process:

- First miner to do so receives a reward of 25 bitcoins (halved every 210,000 blocks)
- Provides incentive for people to mine
- "Within cryptocurrency systems the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners: members of the general public using their computers to help validate and timestamp transactions adding them to the ledger in accordance with a particular timestamping scheme" - Wikipedia

Transaction:

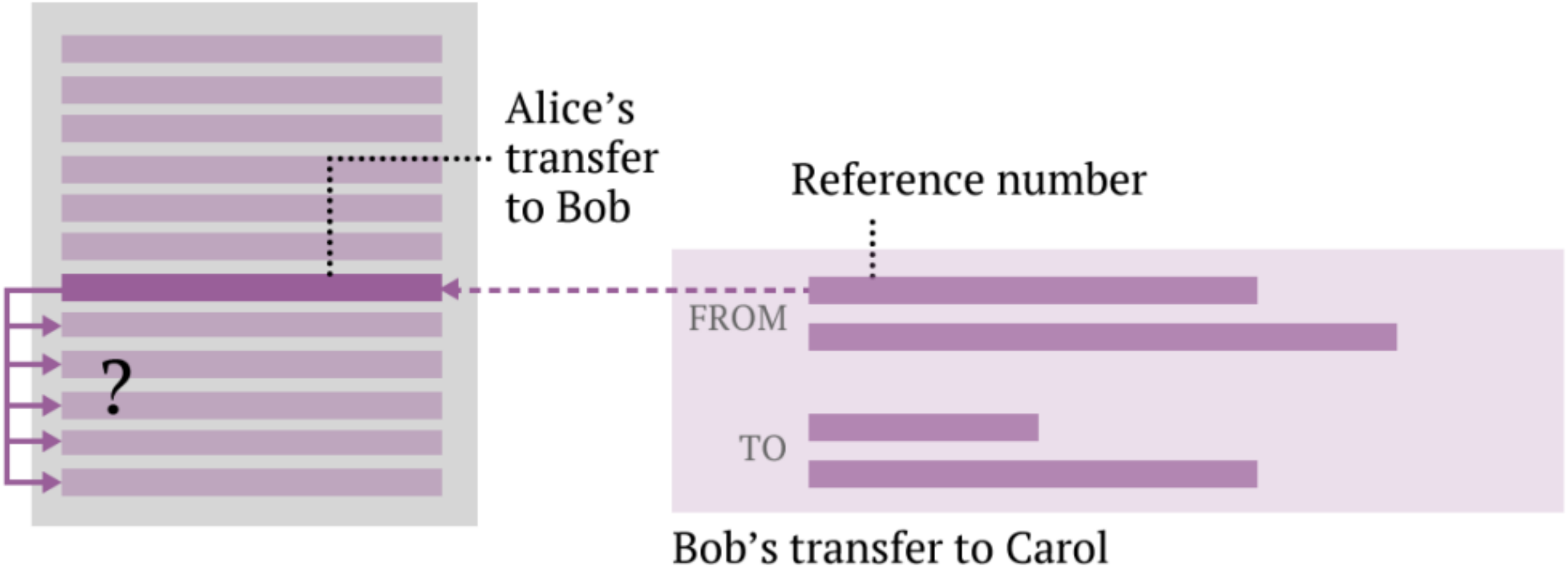
- No accounts to keep anonymity
- Keys to access money
- Alice sends Bob one bitcoin
- Transfer is encoded into a chunk of text that includes the amount and Bob’s address.

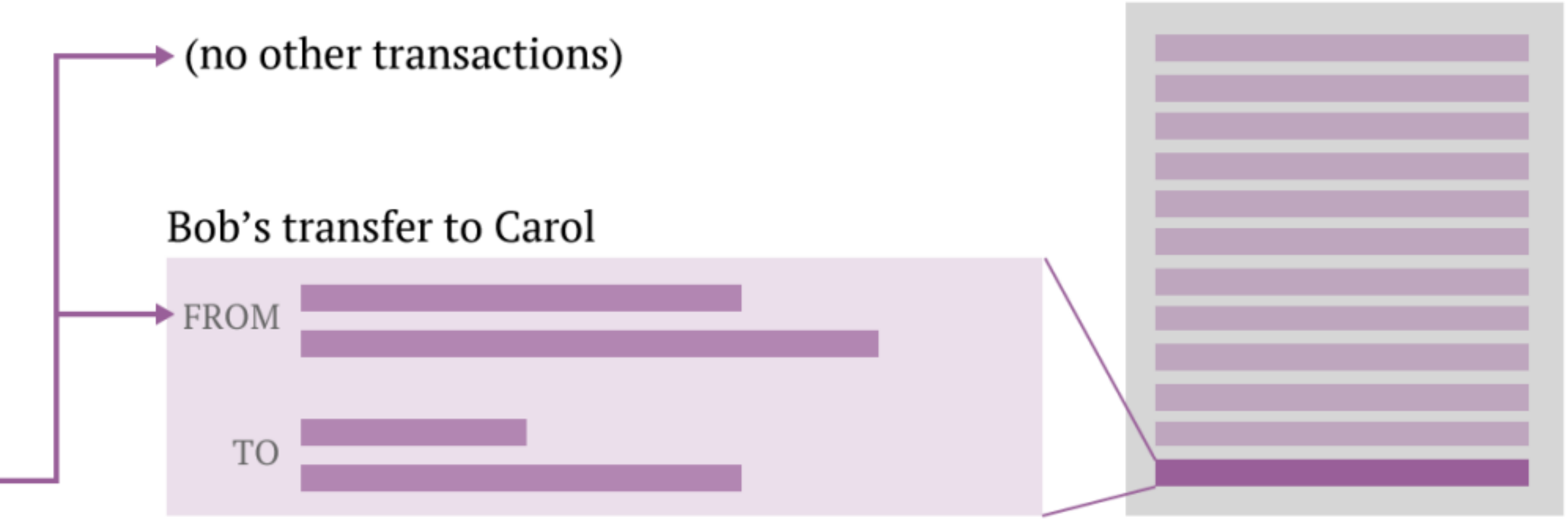
```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```


PUBLIC
LEDGER
Transactions
Alice's transfer to Bob
FROM
TO

Transaction

- Bob then continues to send Carol one bitcoin
- He creates a transaction to Carol's address
- Transaction sent out to all miners
- Miners make sure Bob hasn't spent the bitcoin already (prevents double spending)


Alice's
transfer
to Bob
Reference number
FROM
TO
?
Bob's transfer to Carol


(no other transactions)
Bob’s transfer to Carol
FROM
TO

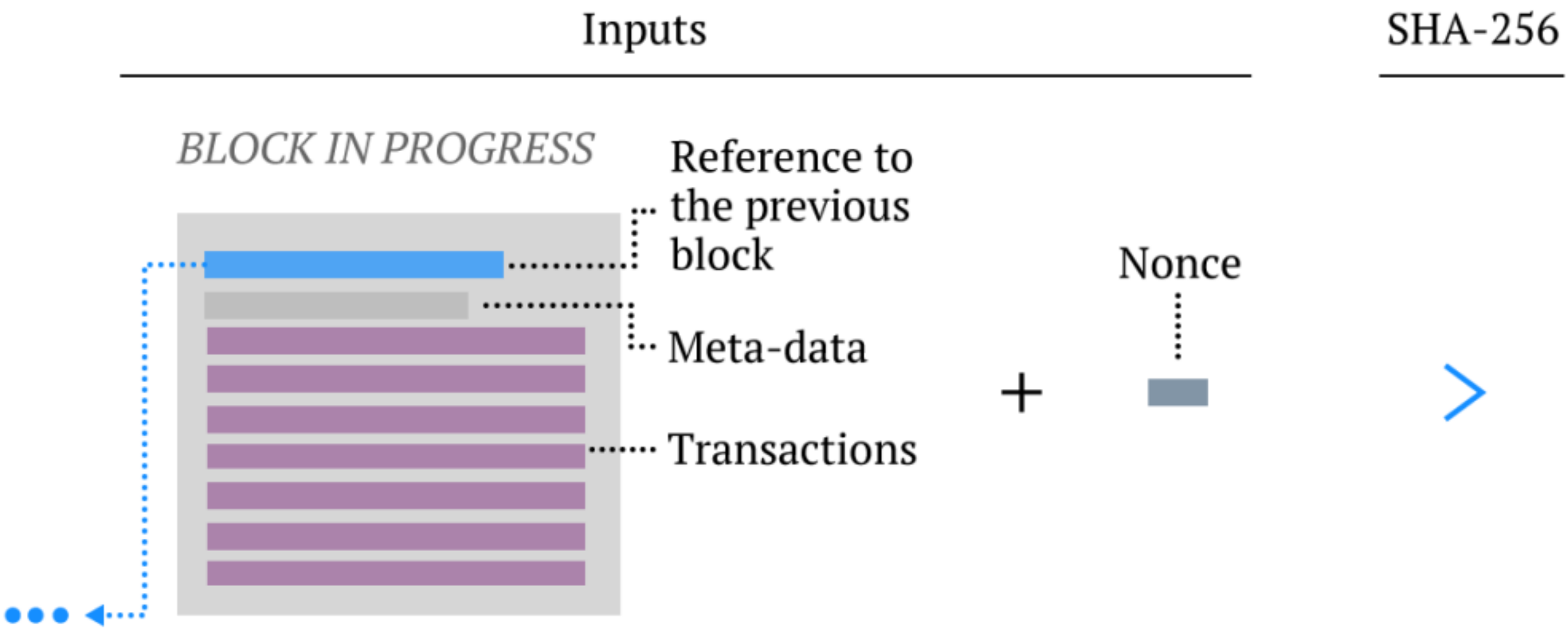
Ledger:

- Ledger broken into blocks
- Transaction logs containing 10 minutes of bitcoin activity each
- Contain reference to previous block (creates a chain)

Hash Function

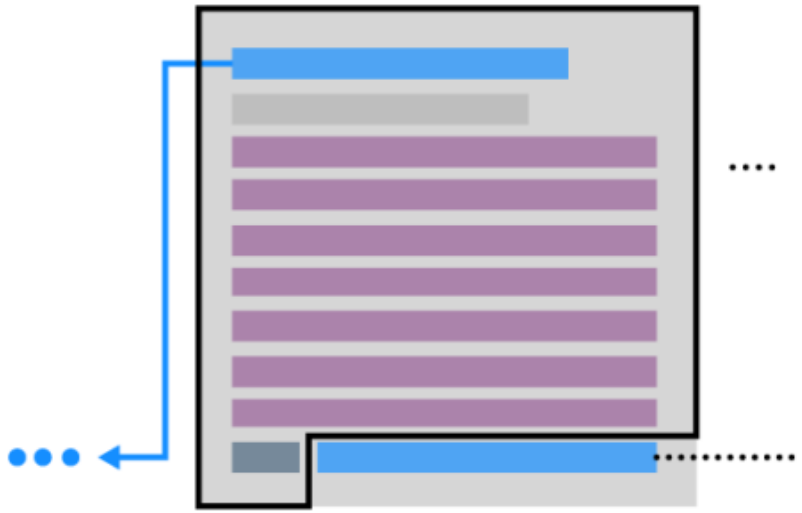
- Each block sealed/protected with cryptography
- Requires an algorithm called a hash function
- Takes an input to produce an output
- Output **always** a predetermined length
- **Impossible** to find unambiguous original input
- Slight variation in input leads to a completely different output
- Hash function that bitcoin uses is **SHA-256**
- Always produces a string 64 characters long
- Developed by NSA.

Input	SHA-256	Hash
The quick brown fox jumps over the lazy dog	>	d7a8fbb307d78094 69ca9abcb0082e4f 8d5651e46d3cdb76 2d02d0bf37c9e592
The quick brown fox jumps over the lazy dog.	>	ef537f25c895bfa7 82526529a9b63d97 aa631564d5d789c2 b765448c8635fb6c


Inputs
SHA-256
BLOCK IN PROGRESS
Reference to the previous block
Meta-data
Transactions
Nonce

Hash function

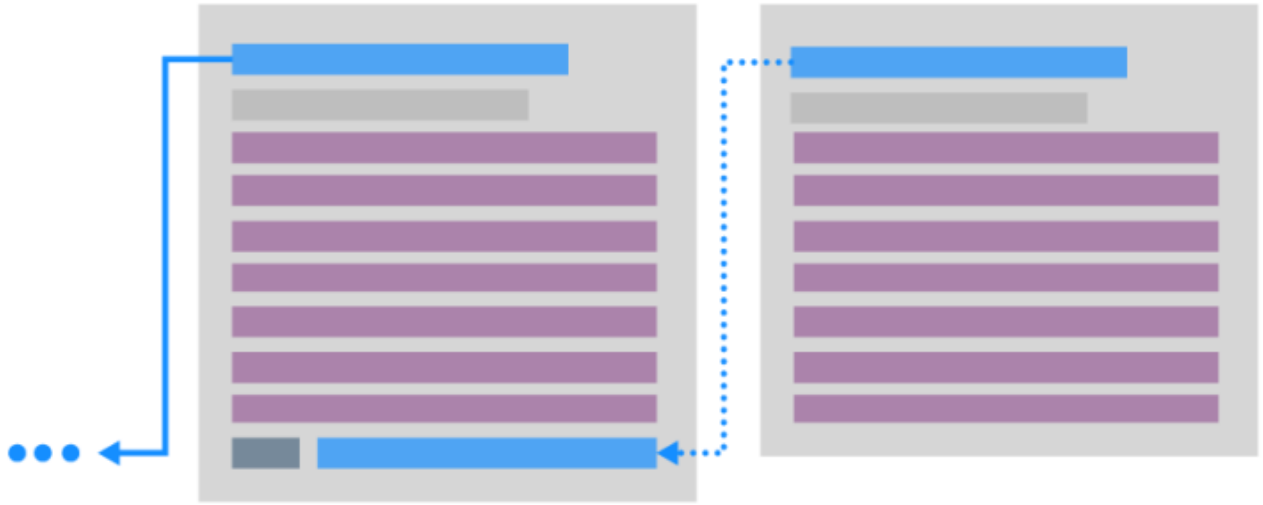
- Goal to find hash that at least has a certain number of leading zeroes
- 000009ff7ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069
- Difficulty adjustable
- Every 2016 blocks (approx. 2 weeks) difficulty reset
- Adjusted so that average time to find solution takes 10 minutes
- Guarantees constant security, regardless of amount of miners



If you take a hash of all these inputs...

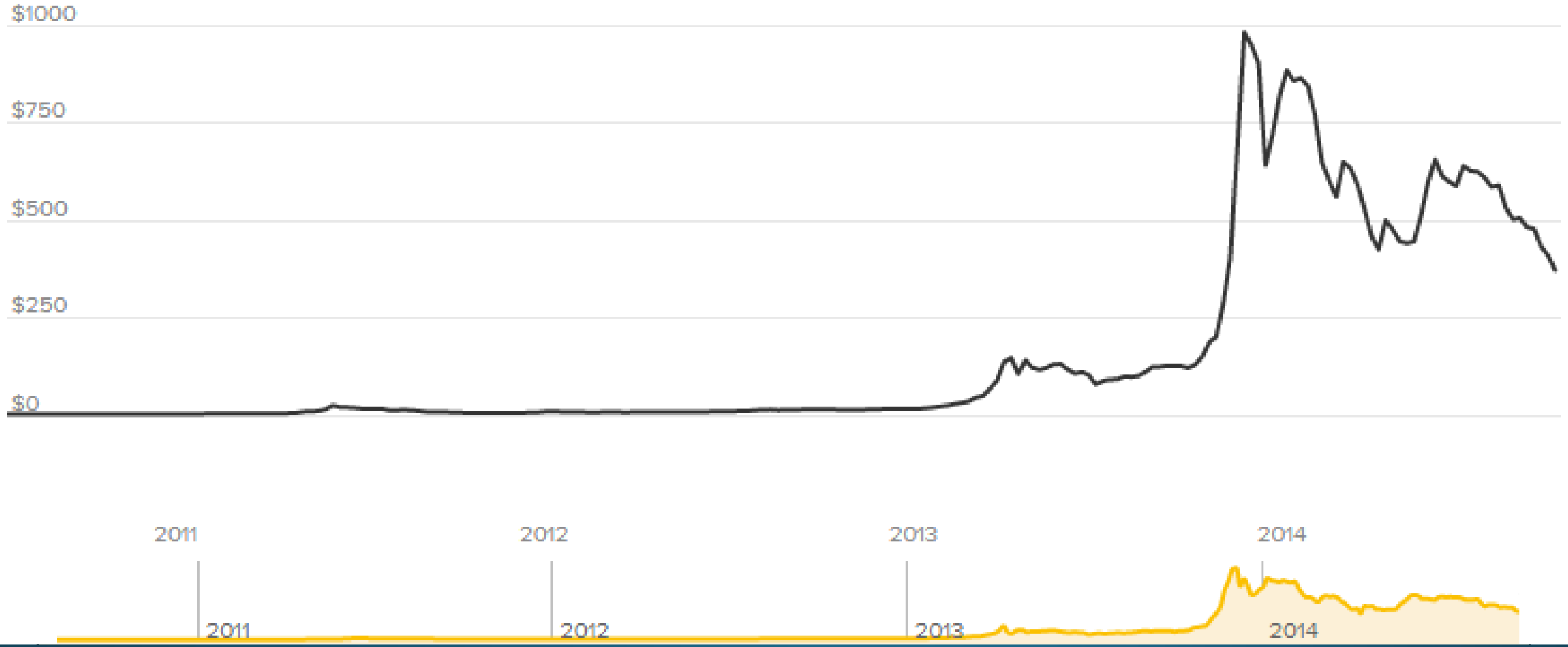
...do you get this output?

If yes, then start a new block



Hacking

- Hacker wants to change transaction 60 minutes ago, to spend bitcoins again
- Modifies record for transaction
- Solves a new proof-of-work, finding a new nonce
- Continues to rebuild an alternative chain going forward
- Requires more computational power than miners combined
- 51% attack
- More computational power than google


$1000
$750
$500
$250
$0
2011
2012
2013
2014
2011
2012
2013
2014


Bitcoin Difficulty
Maximum difficulty per day
250M
200M
150M
100M
50M
0
Jul 09
Jan 10
Jul 10
Jan 11
Jul 11
Jan 12
Jul 12
Jan 13
Jul 13

Difficulty History

Date	Difficulty	Change	Hash Rate
Sep 25 2014	34,661,425,924	16.20%	248,116,151 GH/s
Sep 13 2014	29,829,733,124	8.75%	213,529,547 GH/s
Aug 31 2014	27,428,630,902	15.03%	196,341,788 GH/s
Aug 19 2014	23,844,670,039	20.86%	170,686,797 GH/s
Aug 08 2014	19,729,645,941	5.30%	141,230,307 GH/s
Jul 25 2014	18,736,441,558	8.08%	134,120,673 GH/s
Jul 12 2014	17,336,316,979	3.08%	124,098,191 GH/s
Jun 29 2014	16,818,461,371	24.93%	120,391,236 GH/s
Jun 18 2014	13,462,580,115	14.51%	96,368,902 GH/s
Jun 05 2014	11,756,551,917	12.44%	84,156,677 GH/s
May 24 2014	10,455,720,138	18.10%	74,844,960 GH/s
May 12 2014	8,853,416,309	10.66%	63,375,223 GH/s
Apr 29 2014	8,000,872,136	14.64%	57,272,474 GH/s
Apr 17 2014	6,978,842,650	14.04%	49,956,502 GH/s
Apr 05 2014	6,119,726,089	22.23%	43,806,706 GH/s
Mar 24 2014	5,006,860,589	17.80%	35,840,504 GH/s
Mar 13 2014	4,250,217,920	11.39%	30,424,245 GH/s
Feb 28 2014	3,815,723,799	21.92%	27,314,015 GH/s
Feb 17 2014	3,129,573,175	19.39%	22,402,357 GH/s
Feb 05 2014	2,621,404,453	19.49%	18,764,744 GH/s
Jan 24 2014	2,193,847,870	22.59%	15,704,175 GH/s
Jan 13 2014	1,789,546,951	26.16%	12,810,076 GH/s
Jan 02 2014	1,418,481,395	20.12%	10,153,885 GH/s
Dec 21 2013	1,180,923,195	30.01%	8,453,378 GH/s

Mining methods:

- CPU mining
- GPU mining
  - 3200 32-bit instructions/clock vs 4 32-bit instructions/clock
- Application-specific integrated circuit (ASIC)
- Mining services (cloud mining)
- Pools
  - **https://www.dogepool.net/**

Antminer S3+, 453GH/s, £349.00

ASIC Block Erupter, 336MH/s, £20.00

Bitcoin creation:

- Reward halved every 210,000 blocks
- Bitcoins will never exceed 21 million
- Expected to cap in 2140.

Projected Bitcoins Long Term

Block	Reward Era	BTC/block	Year	Start BTC	BTC Added	End BTC	BTC Increase	End BTC % of Limit
0	1	50.00000000	2009.007	0.00000000	10500000.00000000	10500000.00000000	infinite	50.00000006%
210000	2	25.00000000	2013.000	10500000.00000000	5250000.00000000	15750000.00000000	50.00000000%	75.00000008%
420000	3	12.50000000	2016.993	15750000.00000000	2625000.00000000	18375000.00000000	16.66666667%	87.50000010%
630000	4	6.25000000	2020.986	18375000.00000000	1312500.00000000	19687500.00000000	7.14285714%	93.75000010%
840000	5	3.12500000	2024.978	19687500.00000000	656250.00000000	20343750.00000000	3.33333333%	96.87500011%
1050000	6	1.56250000	2028.971	20343750.00000000	328125.00000000	20671875.00000000	1.61290323%	98.43750011%
1260000	7	0.78125000	2032.964	20671875.00000000	164062.50000000	20835937.50000000	0.79365079%	99.21875011%
1470000	8	0.39062500	2036.956	20835937.50000000	82031.25000000	20917968.75000000	0.39370079%	99.60937511%
1680000	9	0.19531250	2040.949	20917968.75000000	41015.62500000	20958984.37500000	0.19607843%	99.80468761%
1890000	10	0.09765625	2044.942	20958984.37500000	20507.81250000	20979492.18750000	0.09784736%	99.90234386%
2100000	11	0.04882812	2048.934	20979492.18750000	10253.90520000	20989746.09270000	0.04887585%	99.95117198%
2310000	12	0.02441406	2052.927	20989746.09270000	5126.95260000	20994873.04530000	0.02442599%	99.97558604%
2520000	13	0.01220703	2056.920	20994873.04530000	2563.47630000	20997436.52160000	0.01221001%	99.98779307%
2730000	14	0.00610351	2060.913	20997436.52160000	1281.73710000	20998718.25870000	0.00610426%	99.99389658%
2940000	15	0.00305175	2064.905	20998718.25870000	640.86750000	20999359.12620000	0.00305194%	99.99694833%
3150000	16	0.00152587	2068.898	20999359.12620000	320.43270000	20999679.55890000	0.00152592%	99.99847420%
3360000	17	0.00076293	2072.891	20999679.55890000	160.21530000	20999839.77420000	0.00076294%	99.99923713%
3570000	18	0.00038146	2076.883	20999839.77420000	80.10660000	20999919.88080001	0.00038146%	99.99961859%
3780000	19	0.00019073	2080.876	20999919.88080001	40.05330000	20999959.93410001	0.00019073%	99.99980932%
3990000	20	0.00009536	2084.869	20999959.93410001	20.02560000	20999979.95970001	0.00009536%	99.99990468%
4200000	21	0.00004768	2088.861	20999979.95970001	10.01280000	20999989.97250001	0.00004768%	99.99995236%
4410000	22	0.00002384	2092.854	20999989.97250001	5.00640000	20999994.97890001	0.00002384%	99.99997620%
4620000	23	0.00001192	2096.847	20999994.97890001	2.50320000	20999997.48210001	0.00001192%	99.99998812%

Wallet:

- File that contains private collection of keys
- Used to send transactions
- Stored on hard drive
- Generates bitcoin address


11:20
Bitcoin Wallet
Your Bitcoin Address:
1KGe NiDw zH5N
rdwN ETj3 hQEx
wr5H MN9e FW
BTC 2.08454166
worth about EUR 8.71338413
Received
Both
Sent
2012/05/04 → darkly - 11.50
2012/05/03 → 1DaTD... - 4.43348969
2012/05/03 → sodoku - 0.0105
2012/05/03 ← 1Gjq... + 15.46391753
2012/04/17 → darkly - 1.00
2012/04/06 → darkly - 9.00
Blockchain downloading, 4 days behind