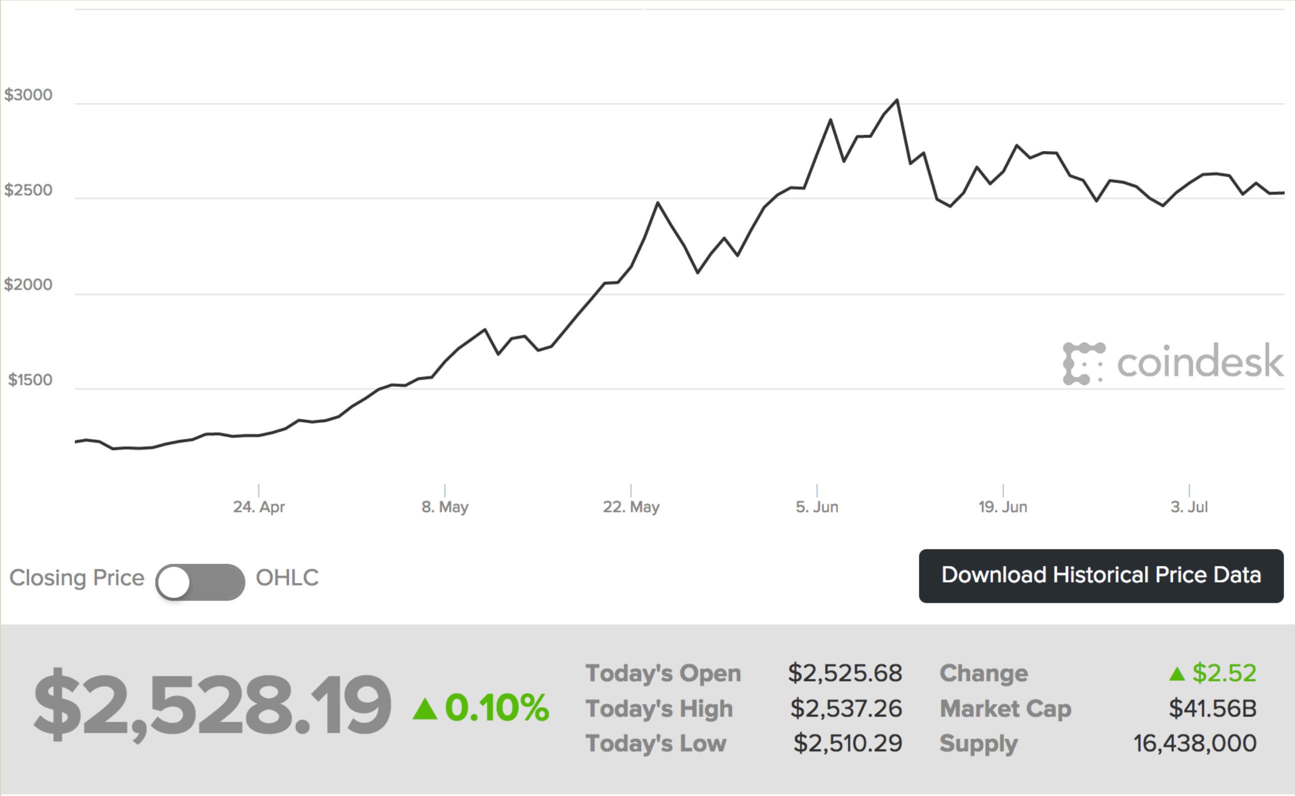
BITCOIN

AND OTHER CRYPTOCURRENCIES

Milo Trujillo

WHAT IS BITCOIN?

- Decentralized currency
- Fiat currency
- Often considered a commodity
- Based on Blockchain…



$2,528.19 ▲0.10%

Today's Open	$2,525.68	Change	▲ $2.52
Today's High	$2,537.26	Market Cap	$41.56B
Today's Low	$2,510.29	Supply	16,438,000

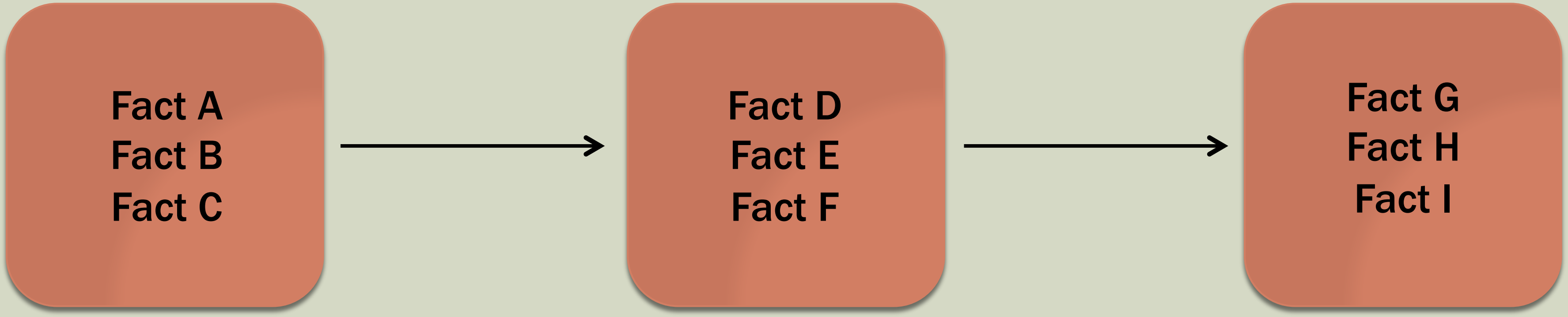
WHAT IS A CURRENCY?

- Something quantitative that can be exchanged
- Must know how much currency a person has
- Must prevent spending currency you don’t have

- One solution: Make a ledger of all monetary transactions, ever

WHAT IS THE BLOCKCHAIN?

- How do we know who has how much currency?
  - Public transaction history
- How do we prevent spending the currency of others?
  - Bitcoin wallets, strict chronological transactions



Fact A
Fact B
Fact C

Fact D
Fact E
Fact F

Fact G
Fact H
Fact I

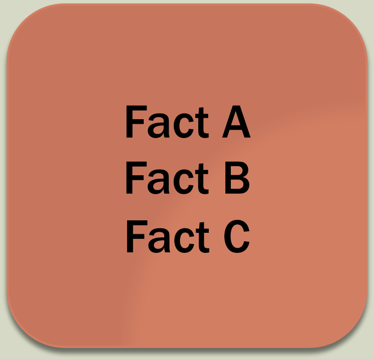
WHAT IS A BITCOIN WALLET?

- Public / Private keypair
- Public key is username
- Private key signs all transactions to authorize
- Nothing "stores" your bitcoins
  - Blockchain tracks how much currency allocated for each wallet

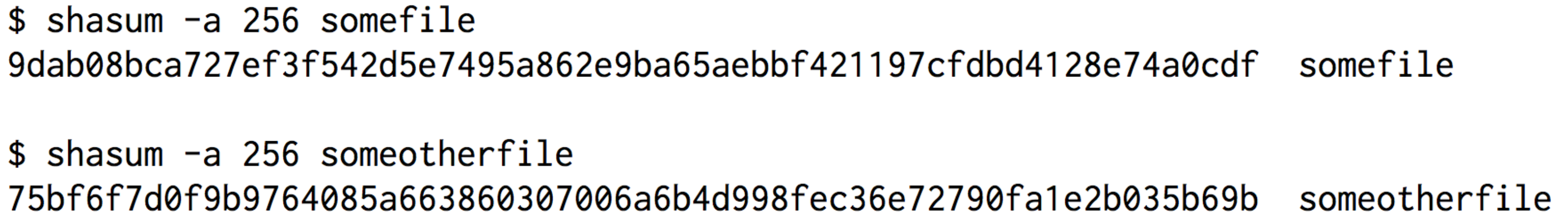
- Example:
  - Alice sends 5 BTC to Bob (using Bob's public key as a username), signs message with Alice's private key to authorize

WHAT IS IN A BLOCK?

1. All “facts” (transactions)
2. Identifier of the previous block
3. Random string
4. SHA256 hash of parts 1,2,3



Fact A
Fact B
Fact C



```
$ shasum -a 256 somefile
9dab08bca727ef3f542d5e7495a862e9ba65aebbf421197cfdbd4128e74a0cdf  somefile

$ shasum -a 256 someotherfile
75bf6f7d0f9b9764085a663860307006a6b4d998fec36e72790fa1e2b035b69b  someotherfile
```

WHAT'S THAT HASH FOR?

- To be accepted in to the blockchain, the block needs:
  - Part 2 (last block's identifier) must be correct
  - Part 4 (sha256 of parts 1,2,3) must start with *n* leading zeroes

If n=5:

Rejected Hash:

f56d11cb12191d
479f89062844e
e79c0a899549e
c234022d35431
d3c6fa5f40d

Accepted Hash:

000007e68c86f
72084cb7b10b6
bb5f12f698ce4a
d92acedce2bb95
a246e82016

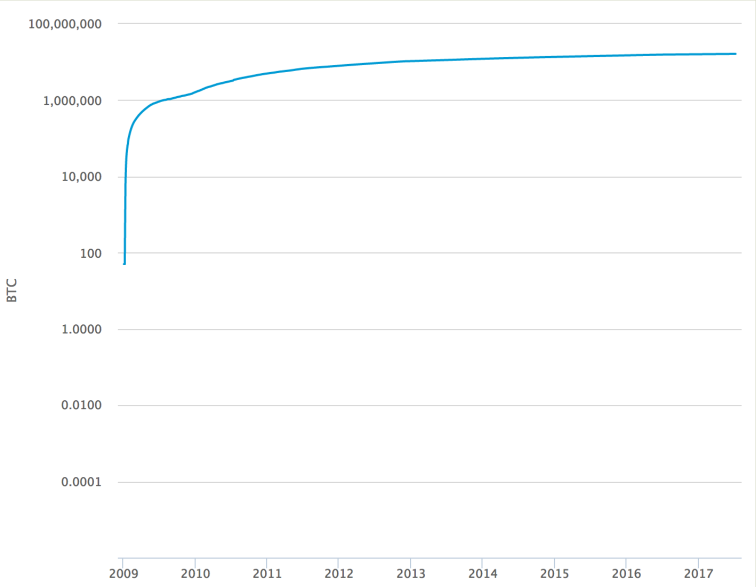
Note: SHA256 is specific to bitcoin – most cryptocurrencies use different hash

BITCOIN MINING

- Making a valid block equivalent to hash cracking
- *N* increased by group consensus
  - Maintains constant block time (10 minutes)
- To exchange any bitcoin, must get transaction inserted in to blockchain
- Person that mines a new block earns 25 BTC
  - Often split among a “mining pool”

LIMITED CIRCULATION

- Increasing *n* means fixed maximum blocks
  - Reward for mining halves every 210,000 blocks (started at 50 BTC)
- Therefore a fixed maximum number of bitcoins (~21 Million)
- 16 million currently in circulation
- Once all coins mined, no further transactions possible
- Estimated last coin: 2140
- Worthless mining: 2036-2048



ALT-COINS

MEGACOIN
COINYE
RON PAUL COIN
IN RON WE TRUST
PRESIDENT 2014

NAMECOIN (2011)

- “Facts” aren’t just monetary transactions:
  - Email addresses
  - PGP keys
  - Domain names
- Decentralized data store can replace:
  - DNS
  - Address Books
  - Key servers
- Value no longer fiat
- Otherwise identical (1st fork)
- Total value: 38.6 million USD

ETHEREUM (2013)

- “Facts” can also be *smart contracts*
- Embedded scripting language in blockchain
- Programmatically-enforceable agreements for
  - Security deposits
  - Provably fair gambling
  - Generic distributed computing
  - Much more if IoT integration takes off
- Total value: 22.5 billion USD

GREATEST CYBER-HEIST IN HISTORY

- The Decentralized Autonomous Organization (DAO) was an automated venture capitalism fund
  - Pay in to the fund and vote on what should be funded
  - No administration, 100% automated and wild
- Biggest crowdfunding campaign in history
  - 100+ million USD as of May 2016
- Everything went terribly wrong

THE DAO HACK

- All Ethereum code publicly visible and immutable
- Attacker found a bug in the DAO trading code, siphoned 3.6 million ether ($50 million USD)
- DAO developers became the “Robin Hood group”
- Cornell hosts Ethereum boot camp at same time
  - Majority of all Ethereum node operators present at camp
  - Agree to a “hard fork”
  - Patch the DAO code, reverse all thief transactions

ETHEREUM CLASSIC (2015)

- People kept using the original (hacked) Ethereum branch
- Becomes its own currency
- "Moral High Ground" of not rewriting history
- Total value: 1.5 billion USD
  - 5th largest cryptocurrency by market value
- Creates two parallel universes:
  - One where the hack never happened
  - One where thief got 67.4 million USD in coins

QUESTIONS?

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