The Science of Digital Money

A Little About Me...

- Software Engineer @ Microsoft in Pittsburgh
- Run https://chaintuts.com creating Bitcoin & blockchain related tutorials
  - Articles, videos, and code projects
  - On YouTube, Twitter, Github
  - Support: Patreon, Crypto, Spreadshirt Apparel
- Strong believer in digital sovereignty with digital money!

What are Cryptocurrencies?

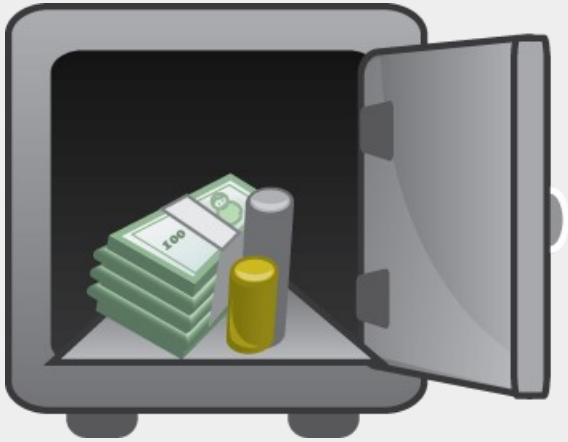
- Cryptocurrencies like Bitcoin Cash, Litecoin, etc. are *digital cash*
- Different form of money than what we are used to – money without central authorities or trust
- Have several key technical properties:
  - Decentralized
  - Peer-to-peer
  - Cryptographically secured

Key Properties of Cryptocurrencies

- Decentralized
  - No one single party controls issuance or transaction processing
- Peer-to-peer
  - Network of users running software, no central “servers”
- Cryptographically secured
  - Transaction validation is backed by math & consensus algorithms, not trust

How...does that work?

- Core computing/information systems concepts
  - The big buzzword – *Blockchains*
    - Hash functions
    - Proof-of-work
  - Public Key cryptography
    - Private keys – where the money is
    - Public keys & addresses
    - Digital signatures

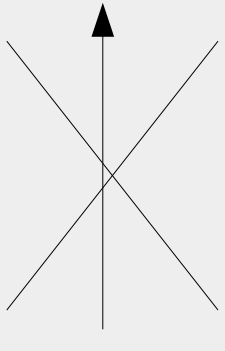


- *Don’t Panic* – we’re just going to get the basics :)

Understanding Blockchains

- First, cryptographic hashes
  - A *one-way* function that takes any data, gives a unique “fingerprint”
  - Ex:

“I love Bitcoin”



SHA-256

024A8A19F6D71E090E93602B64D0FE0D83F
D0E22841778E5D790E54D307B0104

Understanding Blockchains

- Hash properties are used for “Proof-of-Work” to secure the blockchain
- Every 10 minutes, transactions are pooled together and batch processed
- “Proof-of-work” nonce is added to tx data to get a verifiable *block hash*

Understanding Blockchains

Tx data +
“Nonce” - random number

“Block hash” ex:

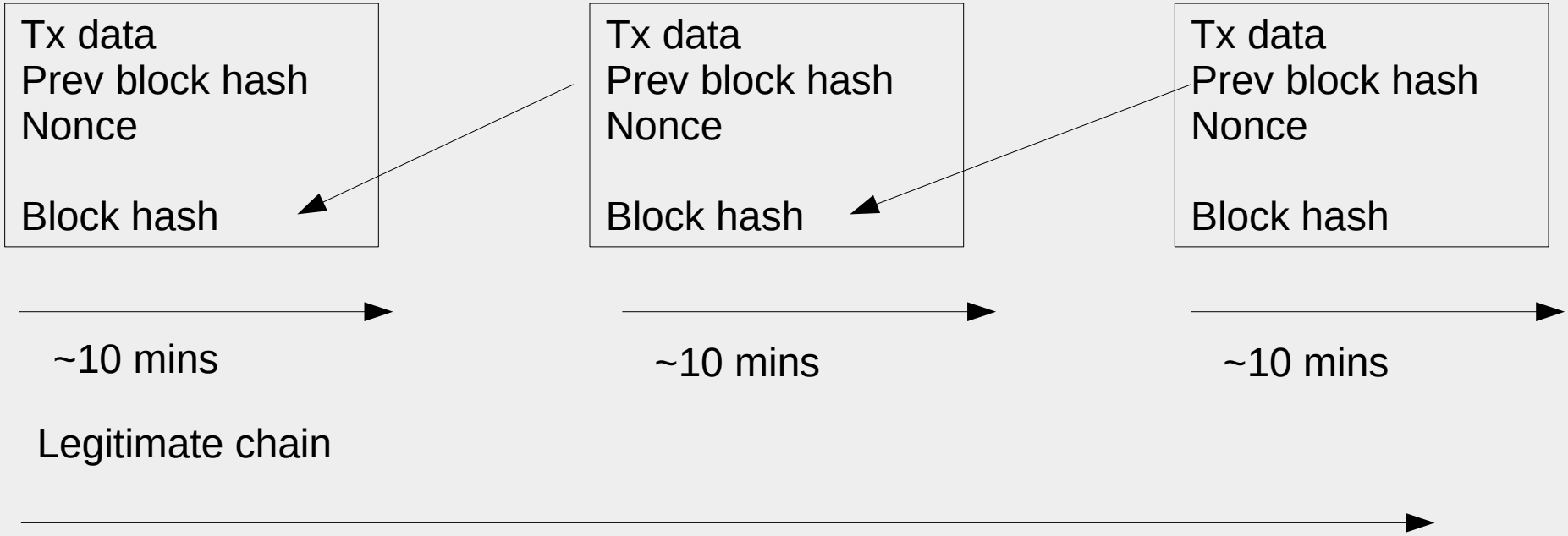
000000000000000059ddd45ec82331174a165f3322235d909ccf1ba3052f32

Goal is to find a nonce such that the *block hash* is less than the *difficulty target*

Understanding Blockchains

- How does that help secure the blockchain?
- Each block contains the hash of the *previous block*
- Remember – if any data changes, the hash changes
- It turns out – the further back you go in history, the more difficult it is to change

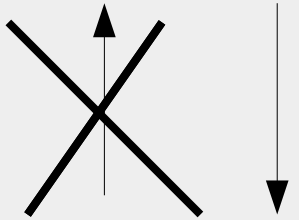
Understanding Blockchains



Attacker: Has to outcompute legitimate miners – 30 mins worth of mining in under 10 minutes...no way!

Understanding Public Key Crypto

0x12351bc143badf2348fe38e8f8b785b...

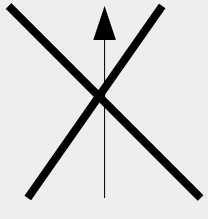


Elliptic Curve
(secp256k1)

PRIVATE KEY

0x04135981abcd7f7a7d7b7c720….

PUBLIC KEY



“Double hash” (SHA-256
and RIPEMD160)
And Base58check encoding

1MT3uNoFLP82j2aSD5Qtibm2kXJ7RWumAM

ADDRESS
(PUBLIC KEY
HASH)

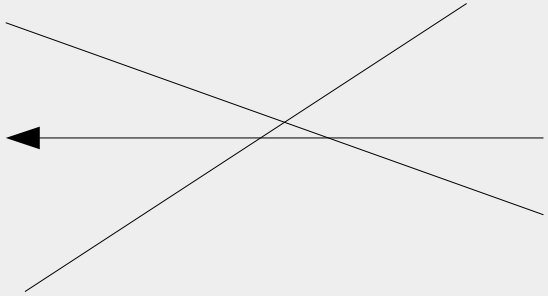
Understanding Public Key Crypto

Tx data (message)

User private key

signs

Public key
Digital signature



Cannot get private key from public key, but

CAN prove the user owns those funds via the signature!

Understanding Public Key Crypto

- To spend funds sent to you, sign a tx with key *without revealing it*
- User keeps private keys to prove they own funds sent to public address
- User does not have to reveal private keys, *ever*
- Address is completely public
- This is different than what we’re used to – push vs. pull transaction

Confused??? It’s Okay

- The important thing is not understanding every system detail – it’s understanding *why the implementation is important*
- This is a good lesson for computing in general
  - Understanding roughly why software does what it does allows you to use it safely & effectively

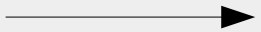
Confused??? It’s Okay

- Let’s discuss why the *technical properties* impact society and finance

Why Cryptocurrencies Matter

Because cryptocurrencies are:

- Decentralized
- Peer-to-peer
- Cryptographically secured



They are

- Trustless
- Global
- Censorship resistant

Why Cryptocurrencies Matter

- Bitcoin is Trustless
  - No need to trust corporations or goverments
  - Corruption and greed happen – people steal, bad decisions are made, etc.
  - Trustless systems operate without a central point of failure!

Why Cryptocurrencies Matter

- Bitcoin is Global
  - No borders on the blockchain!
  - International transactions are fast & cheap
  - Compare to traditional services – imagine being a migrant worker or a refugee
    - Western union will charge you 30% to send money back home
    - It takes days or weeks, not minutes
  - With Bitcoin Cash, etc. - send money anywhere, any time, for less than a penny

Why Cryptocurrencies Matter

- Bitcoin is Censorship resistant
  - No central authority, no censorship
  - Extremely valuable to dissidents, journalists, and the oppressed
    - Real world use case – the new Snowden book!
    - Make payments for services like VPNs, secure email
    - The list goes on
  - Allows civil disobedience and truly *free as in freedom* transacting

Final Thoughts

- My opinion – Bitcoin is the most fascinating applications of computer science to date
- The technical properties of cryptocurrencies give them some incredible social and economic properties
- What you're learning here matters – study how it applies to emerging technologies!

The Fun Part – Free Money!

- Go to app store of your choice
- Download the bitcoin.com wallet or Coinomi wallet
- Set up a *Bitcoin* ***Cash*** (Not Bitcoin BTC) or Litecoin wallet
- See me as time permits for some free currency of your choice!

Questions?