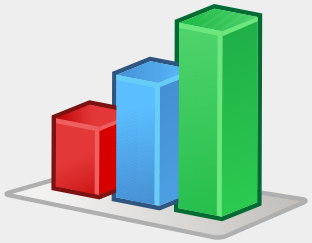
The McKenna School Guide to Cryptocurrencies

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!

A Poll...

- How many of you have heard of?
  - Bitcoin
  - Bitcoin Cash
  - Litecoin
  - Ethereum



- How many of you have owned some?
- How many of you have bought something with it?

What are Cryptocurrencies?

- Cryptocurrencies are a form of *Digital Cash*
- But they’re not like a credit card, or Venmo, or Paypal
- They truly behave like digital dollar bills, thanks to several key properties

What Cryptos Offer

- **A *decentralized* model** – No corporations or governments control Bitcoin Cash, Litecoin, etc.
- **Censorship resistance –** No one can stop your payments to anyone
- **Global payments –** Send money to anyone, anywhere!
- **Sound money –** A limited supply that can’t be changed

Decentralization

- Bitcoin & others are built on peer-to-peer software – it's a *protocol* not a *product*
- The broader community of users, developers, and miners make decisions on protocol
- No corporate, regulatory, or political concerns govern cryptocurrencies
- **Compare to:** Credit cards – built to make CC companies money/shareholder interests

Censorship Resistance

- Because Bitcoin is decentralized, it’s also built to be *censorship resistant*
- No one can decide that you’re not allowed to make a transaction for any reason
- **Compare to:** Venmo, Paypal – censor industries like legal cannabis, adult industry, political figures.
- **Compare to:** Credit/Debit – US Gov trying to seize profits from Edward Snowden book

Global Commerce

- Because Bitcoin is decentralized and censorship resistant, it's also *global*
- Send money to anyone, anywhere – support an international cause, send money to family, etc.
- No limits on amounts, no high fees, no sanctions lists
- **Compare to:** Western Union – 8% or more fee, won't serve some areas

Sound Money

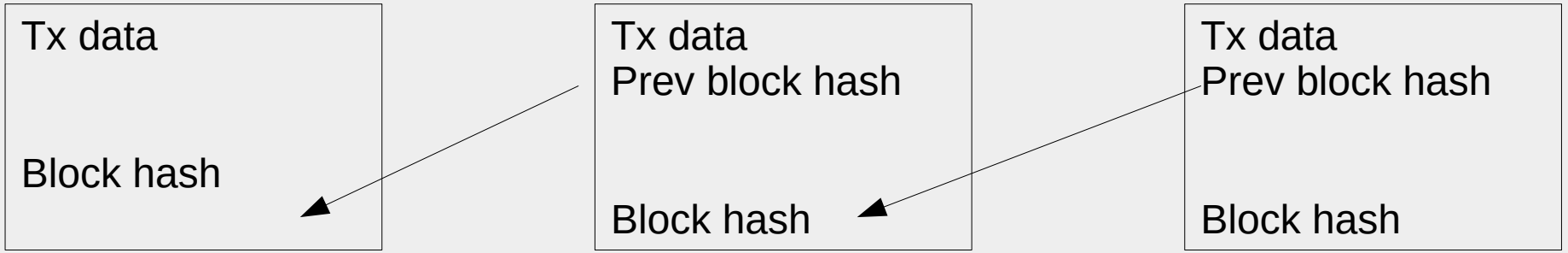
- Most major cryptos have a *limited supply* set by the protocol. 21 million Bitcoin Cash, 84 million Litecoin
- Some don’t have a cap (Ethereum), but supply is *predictable*
- **Compare to:** USD – inflating every time the Fed arbitrarily decides to print more

How Are Properties Achieved?

- The Blockchain – a distributed database of transactions, cryptographically secured by digital signatures and proof-of-work
- Proof-of-Work – Algorithms that require extensive computing to solve
- Digital Signatures – cryptography for proving ownership of funds without trust

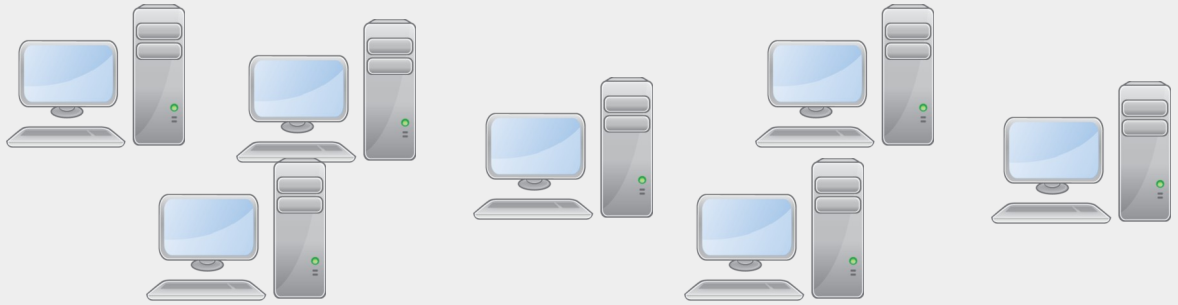
Blockchain

- A public ledger of all transactions (transfers) that have occurred
- A new “block” of transactions are batch processed every *N* minutes
- Each block is linked cryptographically to the last one



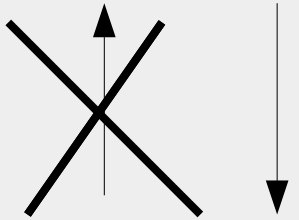
Proof-of-Work

- For a new block to be “mined” (added to the chain), miners must compute a very hard problem
- Uses a *lot* of electricity and computing power
- Once the problem is solved, anyone can verify the answer instantly (hence: “Proof-of-work”)
- Because each block is linked, older blocks become *impossible* to change (6+ confirmations)



Digital Signatures

0x12351bc143badf2348fe38e8f8b785b...

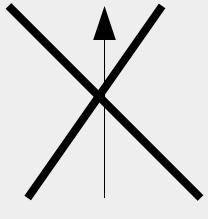


Elliptic Curve
(secp256k1)

PRIVATE KEY

0x04135981abcd7f7a7d7b7c720….

PUBLIC KEY



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

1MT3uNoFLP82j2aSD5Qtibm2kXJ7RWumAM

ADDRESS
(PUBLIC KEY
HASH)

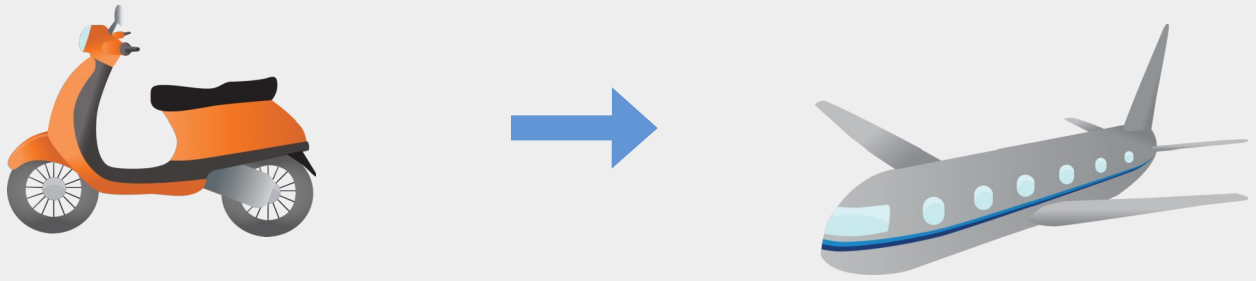
Confused? Don’t Panic

- You don’t have to be a tech nerd to understand these properties…
- A little bit of knowledge goes a long way to understanding *why this is important*

:)

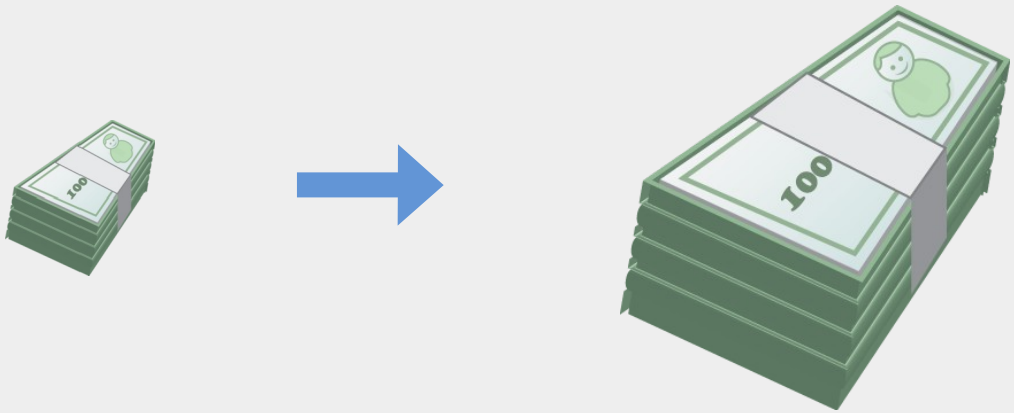
Why Should Finance Pros Care?

- Improved interoperability between institutions
  - ACH takes *days* to clear
  - Cryptocurrencies take minutes
  - This could vastly improve efficiency of transfers/clearing
  - More efficient transfer is more efficient business



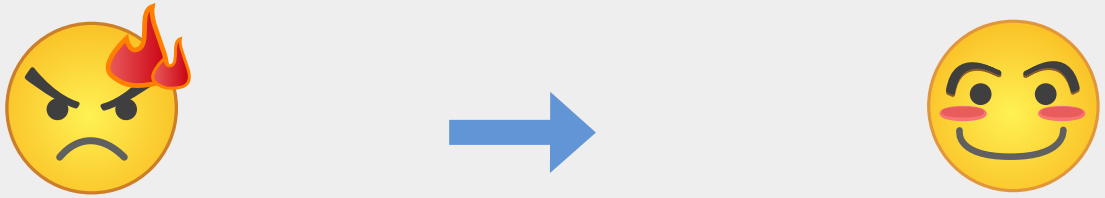
Why Should Finance Pros Care?

- A sound money future
  - Imagine your currency holdings in *cash* (not investments) growing in value over time
  - No more needing to just keep up with inflation (2-3%)
  - Increased *predictability* in currency markets



Why Should Finance Pros Care?

- *Dramatically* more secure payments
  - *Billions* per year are spent on fraud prevention and losses associated with ID theft
  - Every time you use a credit card, you're revealing *private information* you *trust* the merchant with
  - With cryptocurrencies, the protocol is *inherently* more secure thanks to public key cryptography



Lastly – Should I Invest?

- My opinion – No! Cryptocurrencies are highly speculative to treat as a “set and forget” investment

  HOWEVER!

- “Invest in Education” - Andreas Antonopoulos
- You *should* get some crypto and USE IT!
  - Learn how it works
  - Understand its valuable properties
  - **Be a part of this bright future of money!**

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) Wallet
- See me as time permits for some free BCH

Questions?