Introduction to Bitcoin & Ethereum

A Little About Me...

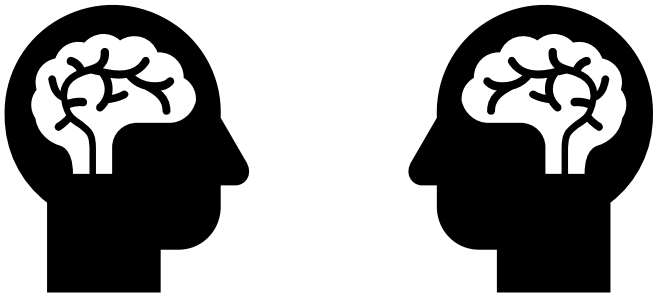
- Software Engineer @ Microsoft in Pittsburgh
- Run https://chaintuts.com creating cryptocurrency & blockchain related tutorials
- Articles, videos, and code projects
- On YouTube, Twitter, Github
- Support: Patreon, Crypto, Spreadshirt Apparel
- Focus is on understanding & teaching core concepts

Why Cryptocurrencies?

- Technology exists to solve problems…it generally doesn't appear for no reason
- Bitcoin and Ethereum emerged after years of trying to solve a specific set of problems
- These problems are problems of *trust*

Why Cryptocurrencies?

- Our traditional financial system relies entirely on *trust* and *centralized* institutions
  - Central banks issue currency as desired, based on their chosen economic policy
  - Credit card companies and banks control the flow of transactions between people
  - Fraud prevention and security requires monitoring by these companies

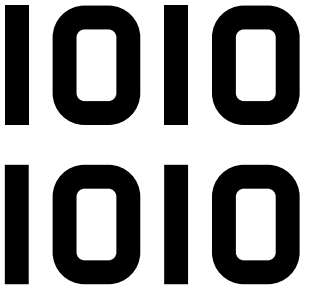


Why Cryptocurrencies?

- The centralized model works…until it doesn't
  - Inflation & national debt hurts savers
  - Censorship is real – think industries like legal cannabis, adult industries, or even "normal" businesses that make mistakes
  - Fraud is rampant and *inherent* in the credit card system

Early Attempts…

- Digicash, etc.
- Used digital signatures for transactions, so senders could cryptographically prove their identities
- Problem – still required a central institution to process transactions and prevent *double-spends*



In Comes Bitcoin!

- The first to combine ideas such as digital signatures and Proof-of-Work to create a truly *trustless, decentralized money*
- Bitcoin operates in a way that is peer-to-peer – no central institutions are required to process transactions

How Does It Work…Roughly?

- Each user has a Bitcoin wallet consisting of *private keys*
- *Private keys* used to derive public *addresses* – money is sent to an address, which has a balance
- Send money to another user by creating a transaction, *signing* that transaction with your key (thus proving ownership), and broadcasting to the network

How Does It Work…Roughly?

- *Miners* race to solve a computationally difficult problem called *proof-of-work* – The winner gets a reward of new coins and validates a “block” of transactions
- Every node on the network can validate blocks/transactions to ensure others are following the rules!

NO TRUST NEEDED, thanks to cryptography!

Critical Properties of Bitcoin

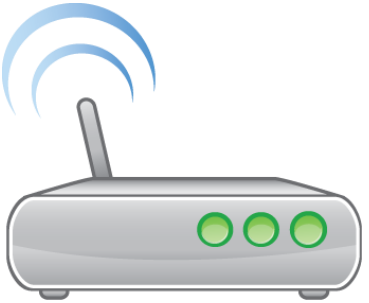
- Decentralized & Peer to Peer – no trusted institutions needed
- Censorship resistant – because it's decentralized, no authority can stop/censor transactions
- Global – because of the above, Bitcoin is the first truly borderless currency

What Bitcoin Doesn’t Do Well

- *No one chain solves every applicable problem*
- Bitcoin doesn’t scale well – high tx fees make it less accessible for folks in developing areas
  - **Yes, I am aware of lighting – it’s a UX mess at the moment**
- Energy consumption??
- Bitcoin isn’t as programmable as other chains…

What is Ethereum?

- Ethereum goes beyond decentralized *currency* to decentralized *computing*
- Ethereum can host *smart contracts* for *decentralized applications*
- Features turing-complete scripting via the Ethereum Virtual Machine with robust capabilities



Why Ethereum?

- Ethereum smart contract use cases:
  - Creating new “sub currencies” such as tokens – useful for new applications like Brave’s ad-replacement system
  - Non-fungible tokens – potential to exchange assets such as cars in the future with simple crypto transactions instead of the DMV
  - Decentralized voting
  - Many, many more possibilities…

What Ethereum Doesn't Do Well

- Not for performant computing
  - Gas limits
  - Use where decentralization and trustlessness matters most
- Dapp bugs can be *catastrophic*
  - Millions of $ of value can be lost in an instant, with no recourse

In My Humble Opinion

- These technologies are a **tremendous** benefit to society
- The first time we have the option to transact with each other without trust
- Not perfect for every use case, but offers us a *choice* we have never had before

Choice in Technology Matters!