Nicholas Weaver Talk
2018-04-20 (School of Information)
Notes by Frank Lin

Result of five+ years of observing and researching the cryptocurrency space

Cryptocurrencies don't work as currencies
Public blockchains are grossly inefficient and don't provide "trustless trust"
Private blockchains are ploys for money
Things that can be done: education, blackhats, government intervention, moderately funded adversaries

Cryptocurrency: a tradable cryptographic token, goal is to create irreversible electronic cash with no centralized trust
Based on the notion of a public ledger, the "blockchain", which is append-only

(Public) Blockchain: everyone gathers bundles of loose checks, validates there are sufficient funds, and staples them together into a "block", with a pointer to the previous pile

Bitcoin: first widespread development of this idea; Bitcoin wallet is simply a collection of cryptographic keys; Bitcoin blockchain is implementation of the shared ledger

Bitcoin mining: particular instance used to protect the transaction history for Bitcoin based on a cryptographic hash function; every miner takes all the unconfirmed transactions and puts them in a block

- Block has fixed capacity, limiting the global rate to ~3 transactions per second
- Attaches to the front and hash of previous block
- Performs the proof of work calculation: hashes the block, changing it trivially until the hash starts with enough 0s
- On success it broadcasts the new block

The Blockchain Size problem

- To verify, potentially check every transaction since beginning of chain
- Amazingly inefficient storage

The Blockchain Power problem

- Bitcoin system consumes at minimum 10 GW of power (as much as NYC)
- Proof of work creates a Red Queen's race
- No way to reduce Bitcoin's power consumption without reducing Bitcoin's price or the block reward
- Bitcoin is secured by the burning of Chinese coal

Irreversibility Problem

- Everything electronic in modern banking is by design reversible except for cryptocurrencies

True value of cryptocurrency: censorship resistance
If you believe there should be no central authorities, cryptocurrencies are the only solution for electronic payments
But this enables drug dealing, money laundering, crim2crim payments, gambling, attempts to hire hitmen, etc.
Ease of theft of the cryptocurrencies themselves
Ransomware and extortion
Ransomware only exists because of cryptocurrencies
Some good uses: payments to Wikileaks and Backpage when they were under financial restrictions

Otherwise, cryptocurrencies do not work unless you need censorship resistance

- Any volatile cryptocurrency transaction for real-world payments requires two currency-conversion steps
- It is the only way to remove the volatility risk
- But if you believe in the cryptocurrency, you must “hodl”!
- Result is that promised financial applications (cheap remittances, etc.) can never apply in volatile currencies like Bitcoin

“Stablecoins” are no better

- Removing the two currency-conversion steps requires eliminating volatility
- Requires an entity to convert dollars to tokens and vice versa at par
- This is a bank

No significant cryptocurrency/public blockchain is decentralized
Proof of work is provably wasteful
“Articulated trust” is vastly cheaper

Non-currency blockchain
“Private” or “Permissioned” Blockchain; simply a cryptographically signed hashchain (techniques known for 20+ years) — dumb version of Git
Purpose is just to get money from people

The rest is speedrunning 500 years of bad economics
Almost every cryptocurrency exchange is full of frauds banned in the 1930s
Many stablecoins are just wildcat banks
Every tradable ICO is really an unlicensed, unregulated security (South Sea Bubble)

Prescription is fire 🔥

Takeaways

- Knowledge can immunize you from the field
- Blackhats can make a fortune from massive theft
- Governments can destroy the utility using existing regulation
- Anyone can spam a cryptocurrency to death

The SEC, IRS are finally warming up