# Bitcoin Re-entry

After 14 years

# About me

- Major in Cryptography
- Initiate Primitives Lane
- Write Smart Wallet Trend(paused)
- Currently doing research on bitcoin and non-profit organizations

# Most essential features

- Fixed supply and monetary policy
- UTXO model
- Minimized hardfork
- No “official” foundation
- Founder disappeared

# Fixed supply and monetary policy

- Total supply: no more than 21 million
- Halving: ~ every 4 years
- Dependent technologies: Proof of Work, Difficulty change

- Bitcoin is money

# UTXO model

- Structure: Multiple inputs and multiple outputs
- Different formats: P2PKH, P2SH, P2WPKH, P2TR
- Fee measurement: a block is limited to being 1 vMegabyte large, or 4 million weight units.

- Lightweight(Small state): Possible to run a full node
- Simple metering: Governance minimized

# Minimized hardfork

- Hardfork: A change to the protocol that is not compatible with older versions; that is, older client versions would not accept blocks created by newer client versions, considering them invalid.
- Bitcoin protocol has only implemented 1 practical permanent hard fork.
- You can fully sync any version of Bitcoin Core released after January 2013 with its default configuration.

# No “official” foundation

- Bitcoin Foundation? Est. in 2012, its 501(c)(6) tax status was revoked by the IRS on May 15, 2022.
- Who supports bitcoin development?
  - Developers: Brink, Independent, Square, Chaincode, Blockstream, MIT DCI, DG Lab, Trezor, BitMEX…
  - Donors: Craig Hammell, Samara Asset Group, Exodus, Coinbase, …
- Bitcoin is fully decentralized developed

# Founder disappeared

- Satoshi Nakamoto disappeared since Dec.12, 2020
- Bitcoin Core is a client for Bitcoin protocol

- No single person or entity controls Bitcoin

# Useful Resources

- BIP:
  - https://github.com/bitcoin/bips
- Contribute to Bitcoin Core:
  - https://bitcoin.org/en/bitcoin-core/contribute/
- Bitcoin Optech:
  - https://bitcoinops.org/
- bitcoin-dev mailing list:
  - https://lists.linuxfoundation.org/mailman/listinfo/bitcoin-dev
- BTC Study:
  - https://www.btcstudy.org/
- Bitcoin Core PR Review Club
  - https://bitcoincore.reviews/

# Directions to watch

- Fee bumping: RBF / CPFP
- Payment: Lightning Network
- Asset: RGB / Taro
- Scalability: Musig / Taproot / Miniscript / PSBT

# Experience of attending btc++

- https://btcplusplus.dev/

Thank you!