Cryptocurrency

Trevor Gallen

Introduction

- Crypto is obviously a pretty new topic!
- I'll give a broad overview
- Note: I'm not an expert on the crypto aspect
- Disclaimer: I have $\approx$\$40 worth of cryptocurrency (discounted transactions)

What is crypto?

- Digital currency
- Start with a public ledger: you have X, I have Y everybody knows what wallet has what
- I want to pay you Z: submit transaction to ledger
- To submit, I give my. password (hard to guess, easy to verify, can be anonymous)
- A bunch of people see the transaction and compete to solve a puzzle and add it to the ledger (blockchain). If win, get rewarded (proof-of-work). Verify ledger against all others, if agree with 51%, then win.
- Alternatively, lock up coins, distribute based on stake: verify with others, reward validators

Features of Crypto

- Note: not all of these are true for every coin
- Irreversible
- Anonymous
- Instantaneous (compared to ACH)
- Limited in quantity (good and bad(??))
- No centralized authority

Values of Assets

- What's the value of any asset? Take interest rate of r

$$P_t = D_t + \frac{P_{t+1}}{1+r}$$

$$P_t = D_t + \frac{D_{t+1} + \frac{P_{t+2}}{1+r}}{1+r}$$

$$P_t = D_t + \frac{D_{t+1}}{1+r} + \frac{P_{t+2}}{(1+r)^2}$$

$$P_t = \sum_{\tau=0}^{\infty} \frac{D_{t+\tau}}{(1+r)^{\tau}}$$

- The no-arbitrage price of an asset is the net present value of its dividends

- What are the dividends of Crypto? (what are dividends of cash(?))

Convenience yield (and issue)

- Bitcoin pays no dividends
- But it does have a "convenience yield"
- Ability to easily, anonymously transact
- But:
$$MV = PY$$
- Issue is if you want to stay in crypto all the time, or quickly convert V plays an important role!
- Also M plays an important role: even if Bitcoin limited, Bitcoin derivatives, Ethereum, etc. are not
- Let's talk flavors of coin

Coin flavors

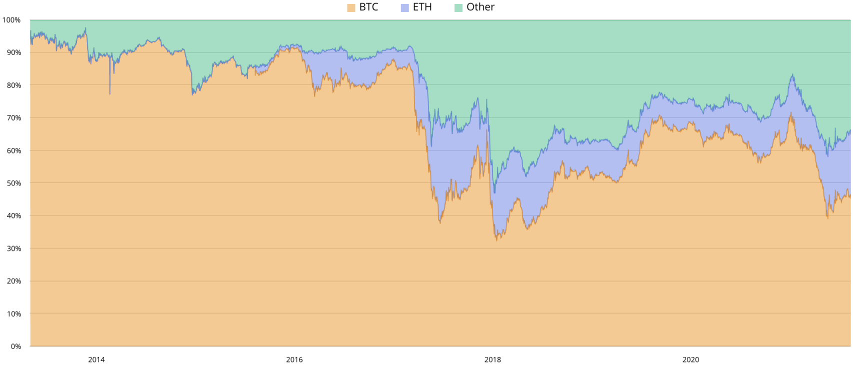
- Bitcoin pays no dividends
- But it does have a "convenience yield"
- Ability to easily, anonymously transact
- But:

  $$MV = PY$$

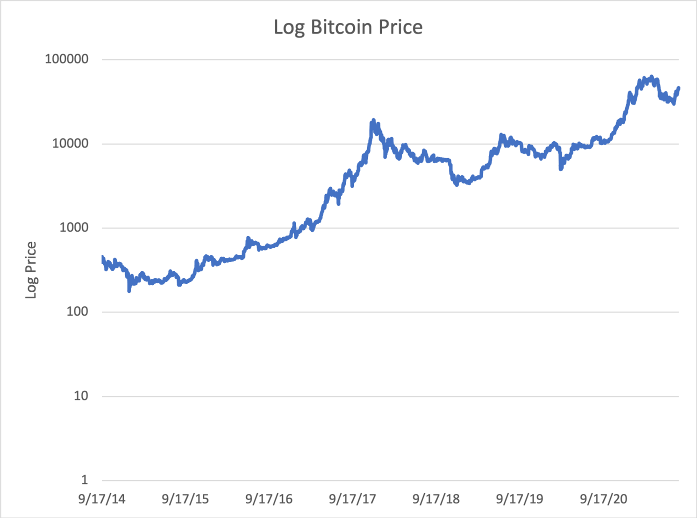
  or:

  $$P_B = \frac{Y}{MV}$$
- M and V are dangerous for BTC.
  - $V \uparrow$ if people able to switch in and out for transactions (not hold). Relevant when not speculative (stability could be dangerous for value!)
  - $M \uparrow$ if other cryptocurrencies enter, hard forks, etc.
- Cochrane: "Long history of unbacked money suggests the long term value of any unbacked cryptocurrency must be zero"

Bitcoin dominance

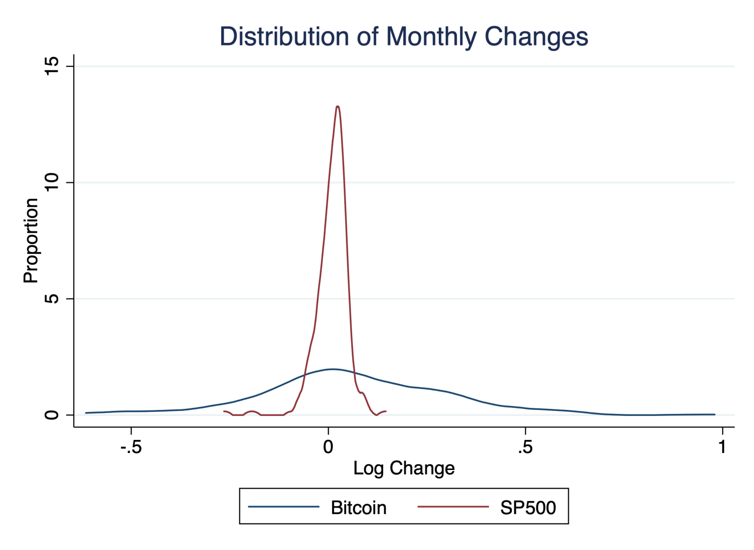


Bitcoin Price



Very volatile! Month-to-month variance is high

Bitcoin Log Price Change Distribution



Very volatile! Year-to-year variance is high

Other coins

- Ethereum: like Bitcoin, move toward proof-of-stake, “smart” contracts
- Bitcoin Cash: “hard fork” of Bitcoin
- Tether: “stablecoin” theoretically backed by dollar assets
- Ripple: bank-owned servers (“centralized”)
- Binance Coin: Ethereum-like, created by an exchange as private currency (create value via fee discount)
- Monero: “privacy coin,” obscures public ledger, great for illegal transactions

Economic limits of blockchain

- Budish (2018)
- Two things are true in proof-of-work
  1. Free entry means zero-profit condition for miners
  2. Must incentivize enough miners to make a "majority attack" impossible *at all times*
- Together, **flow** payments to miners big compared to **stock** value of bitcoin
- This is tricky! If all Bitcoin worth \$1 trillion, and could steal \$1 billion with attack, then need to always be paying miners enough that the computational cost is >\$1 billion
- Natural limit to how valuable the stock can be in proof-of-work
- Splitting currencies makes attacks easier

Future of Crypto

- History of unbacked currencies suggests extreme caution
- Near-instantaneous, irreversible, anonymous technology offers real convenience yield
- But economic limits to value, $V \uparrow$ and $M \uparrow$ makes hard to see why value shouldn't go to zero in the long run
- My ideal: security-backed proof-of-stake (anonymity may suffer). "Stocks as money"
- Coin proliferation, government coins, stablecoins, etc. threaten anonymous coins (Y is split!)