Bitcoin

Trevor Gallen

Introduction

- In December 2018, market cap of cryptocurrencies reached nearly 400 billion U.S. dollars ($141 billion now)
- Equivalent to 11% of value of printed U.S. currency near peak
- What is Bitcoin, and why could it possibly have value?

Bitcoin

- Invented anonymously in 2009
- Idea: create a "bitcoin" (like me printing a TrevorDollar with a unique serial number)
- Problem: unlike a TrevorDollar, how do we know you're the one that owns it?
- Solution: shared public ledger, a list of who owns which blockchain (change ledger when someone transfers the digital TrevorDollar)
- Problem: who gets to change ledger?
- Solution: make it super hard to fake blocks and change blockchain, have every user have a publicly verifiable password for their bitcoins to confirm their identity
- Problem: but then why would anyone put in effort?
- Solution: reward them with bitcoins

Bitcoin-specific

- Allows for anonymous transactions
- Total number of Bitcoins are capped
- Bitcoins don't require a central server ("peer-to-peer")/are decentralized

How does an economist see it?

- Bitcoin is one of many intrinsically worthless, storable, non-dividend-paying objects in "limited" quantity

- We know how to value assets: the asset pricing formula!

- Value of an asset p_t is discounted (R) return from appreciation $p_{t+1} - p_t$ and dividend d_t:

$$p_t = \frac{p_{t+1} + d_{t+1}}{R}$$

- Or can plug in repeatedly:

$$p_t = \sum_{i=1}^{\infty} \frac{d_{t+i}}{R^i}$$

- Price should be equal to discounted net present value of future dividends!

Asset Pricing

$$p_t = \sum_{i=1}^{\infty} \frac{d_{t+i}}{R^i}$$

- In other words, for price to be correct, I must be indifferent between selling today and holding and selling tomorrow
- But that's true of tomorrow's price as well!
- So I should be indifferent between selling today and holding and selling two periods, three periods, infinite periods from now
- By assumption we rule out bubbles

But...

- But there's a problem! Bitcoin doesn't pay any dividends! How could it possibly have value?

$$p_t = \sum_{i=1}^{\infty} \frac{0}{R^i} = 0$$

- Is it just a bubble?

- Not so fast! "Dividends" come in many forms

Enter 3Com, Palm and Convenience Yield (Cochrane 2002)

- Company 3Com owned Company Palm, and then sold 5% of shares
- At end of year, would give the rest to 3Com stockholders (spin-off company)
- So two ways of owning same company
- Buy one share of Palm via buying 3Com stock, can buy it at \$54.54
- Buy one share of Palm via buying Palm stock, can buy it at \$81.81
- Is this insanity?

More Insanity

- One year treasury bill paying off $100 one year from now sells for $94.17
- But another asset prices one year paying off $100 one year from now at $100! (what asset?)

More Insanity

- One year treasury bill paying off $100 one year from now sells for $94.17
- But another asset prices one year paying off $100 one year from now at $100! (what asset?)
- Cash!

More Insanity

- One year treasury bill paying off $100 one year from now sells for $94.17
- But another asset prices one year paying off $100 one year from now at $100! (what asset?)
- Cash!
- Why hold the worse asset?
- Liquidity!
- But note that Palm *far* more liquid (traded) than 3Com
- "Convenience" yields real?

Bitcoin provides a convenience yield

- Bitcoin has tons of potential convenience yields
- Allow people to dodge taxes, launder money
- Allow people to dodge government regulation
- Allow people to transact anonymously
- Allow people to transact without a fee or for a low fee
- Irreversible (maybe good?)
- So maybe it can have value

Bitcoin provides a convenience yield

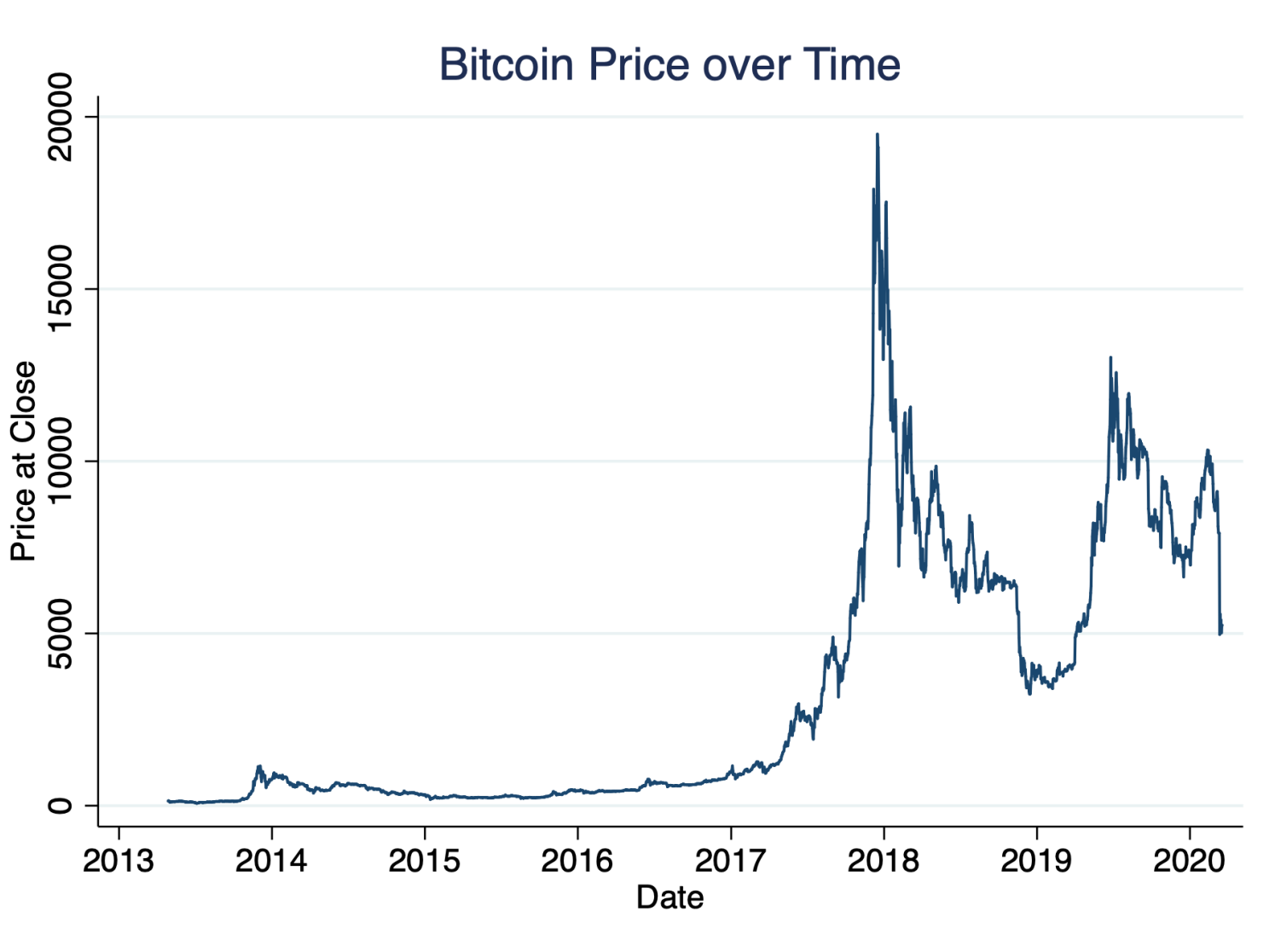
- Bitcoin has tons of potential convenience yields
  - Allow people to dodge taxes, launder money
  - Allow people to dodge government regulation
  - Allow people to transact anonymously
  - Allow people to transact without a fee or for a low fee
  - Irreversible (maybe good?)
- So maybe it can have value

Simple Bitcoin Economics

- Schilling and Uhlig (2019) develop a theory of Bitcoin speculation and pricing when competing against the dollar

- Beyond our scope, but a few possibilities from asset pricing equation:
  - If people holding/speculating in bitcoin (not spending) then must have real return (otherwise hold better asset)

  - On the other hand, Bitcoin/dollar should follow a random walk w/o drift (otherwise invest in one and sell other)
- Extreme volatility possible even if the second (no speculation)
- Other: if Bitcoin/dollar a Martingale but bitcoins fixed and dollars not, then eventually as Medium of exchange Bitcoin falls in importance in long run
- Is Bitcoin/dollar a Martingale?



Statistical test of random walk at daily frequency says no.
(Incidental: fell in value during crisis)

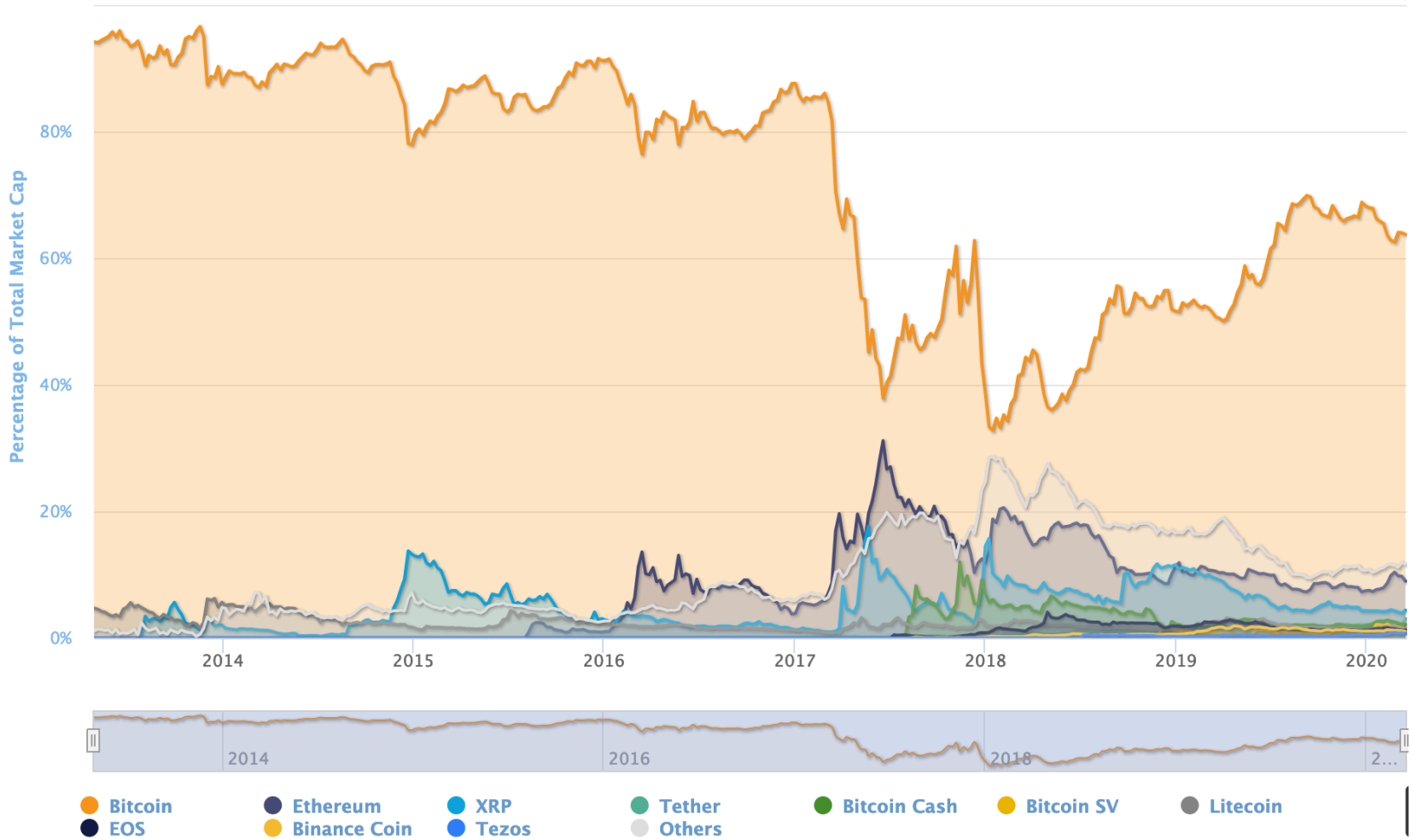
Some issues

- Note if bitcoin's value comes from convenience yield, then it shouldn't see continuous price appreciation unless convenience yield increasing
- Quantity of cryptocurrency not limited in long run
- Economic limits of blockchain
- Lets expand on these last two

Inflation with Bitcoin

- Even if total Bitcoins are capped, Bitcoin-like things aren't!
- Example: Bitcoin Cash, but also all other coins
- I am free to create TrevorCoins, parallel to Bitcoins with same initial ledger (chain) that everyone can trade
- Bitcoin market cap?

Bitcoin Market Cap



Economic Limits of Blockchain

- If you ever have a significant share of network, can try to "fake" transactions
- Merchant can wait for multiple confirmations back, but if you own many transaction-confirming computers, could fake confirmation for all
- This is a "majority attack"
- What economic principles must be true to protect from attack?

Economic Limits of Blockchain

- Two things must be true:
  - Miners at the margin must be indifferent between mining or not (otherwise entry or exit), so reward sets mining power
  - Computational costs of a majority attack must exceed benefits
- This means that recurring payments to miners (flow) must *always* exceed payoffs from a one-off attack *stock!*
- E.g. to steal just 10% of Bitcoin's peak $400 billion market cap I should be willing to spend $40 billion on computing power. Right now only rewards miners 5 billion/year so should be able to rent them out!

Fixes

- It's possible to fix these vulnerabilities
- Digital currency issued by government with central ledger run by govt and fixed to dollar (for instance)
- Or just a StableCoin: much of what bitcoin is, but backed by currency (or anything)
- Other possible mitigation mechanisms: need to have costs, but proof of work (work cost) or proof of stake (cost of illiquid reserves)

My own take

- I am not invested in Bitcoin or any digital currency to my knowledge
- I can't see much difference between Bitcoin and rocks
  - But! anonymous, decentralized may be good
- On the other hand, enormous energy consumption: 0.25% of total world energy, or 1.6% of U.S.'s energy consumption
- Boon to criminals (is that "bad"? "good"? depends on why they're criminals)
- In general I think elastic currency is good, rigid currencies set up for bank runs.
- I expect Bitcoin qua Bitcoin to be run down/limited by a combination of:
  - Speculative attack (Budish)
  - Fixed asset + Martingale (Schilling/Uhlig)
  - "Inflation" via other Cryptocurrencies
  - Loss of competitive edge in liquidity via Stablecoin