BITCOIN—An Introduction

Feb 2021

Digital Economics

Advantages: Lower

- Search Costs
- Replication Costs
- Transaction Costs
- Tracking Costs
- Verification Costs

Disadvantages: Higher chances for

- Hacking
- Losing Privacy

Origin of Bitcoin

- Financial crisis of 2008
- Fiat currency, Quantitative Easing and Satoshi Nakamoto
- Key: Decentralization via peer-peer network, open-ledger
- Bitcoin – Digital currency? Cashless Eco System?
- Is it Anonymous? Not really; Public vs Private ledgers
  Keep the wallet address new or secret or third party sources!
- Not fungible
- Decentralized Digital Currency
- hut8mining.com

Table 1: Bitcoin Activity to Date

	2015	2018	2021
Total bitcoins minted	$\approx$ 14 million	$\approx$ 17 million	$\approx$ 18.625 million
US dollar equivalent at market price	$\approx$ 3.5 billion	$\approx$ 100 billion	$\approx$ 868 billion
Total number of reachable Bitcoin nodes	$\approx$ 6,500	$\approx$ 9800	
Total (cumulative) number of transactions	62.5 million	$\approx$ 350 M	$\approx$ 615 M
Total number of accounts ever used	$\approx$ 109 million		$\approx$ 861 M
Block chain size	$\approx$ 30.3 GB	$\approx$ 173 GB	$\approx$ 327 GB
Number of blocks to date	$\approx$ 350,000		
Estimated daily transaction volume	$\approx$ 200,000 BTC ($\approx$ \$50 million)	$\approx$ 250,000 BTC ($\approx$ 1.56 billion)	$\approx$ 3 billion
Average transaction value	$\approx$ 2 BTC ($\approx$ \$500)	$\approx$ 2.56 BTC ($\approx$ \$16K)	
Computation invested in puzzle solutions	$\approx$ 4,254 exaflops		
Power consumption	$>$173 MW (continuously)		

Bohme et al. (2015)
Maximum $\sim$ 21 million – to be reached by 2140

Bitcoin Design Principles

- Scarcity
- No Counterfeiting
- Price Stability
- Correct Bookkeeping

Underlying Technology (bitcoin.org/en/choose-your-wallet)

- Bitcoins are recorded as transactions.
- All transactions can be traced.
- Cryptography: Public-Private key to store/spend money, validate transactions.
- New transactions are periodically grouped in a block; compared to a recently published block yielding sequence of blocks; hence, 'block chain.'

Buying/Storing Bitcoins

- Wallet Software: bitcoin.org/en/choose-your-wallet
- Bitcoin Exchanges similar to currency exchanges; coindesk.com
- How do exchanges operate? Fees, Limit order book.
- Peer to Peer Networks: gemini.com ; kraken.com etc

Mining

- Blockchain Foundation—keeping the transactional record operational and updated as a public good; users assistance is sought.
- Miners are awarded with new bitcoins; they solve a mathematical puzzle—computationally intensive/Random component — Pre-existing conditions of the block remain in fact; publishes a 'block' with proof-of-work—others verify—Entire process is called mining.
- Consensus reached by voting—May take six rounds/one hour.
- Computationally intensive.

Other Facts

- Ceiling of 21m bitcoins
- Miners can earn through transaction fee (0.0001 bitcoin)
- "One computational cycle, one vote" vs "one person, one vote;" cannot game the system with fake, multiple identities.
- No governance structure as in the conventional payment systems; no verification of transactors' credibility; no prohibition of items; no reversal of transactions.

Bitcoin Ecosystem

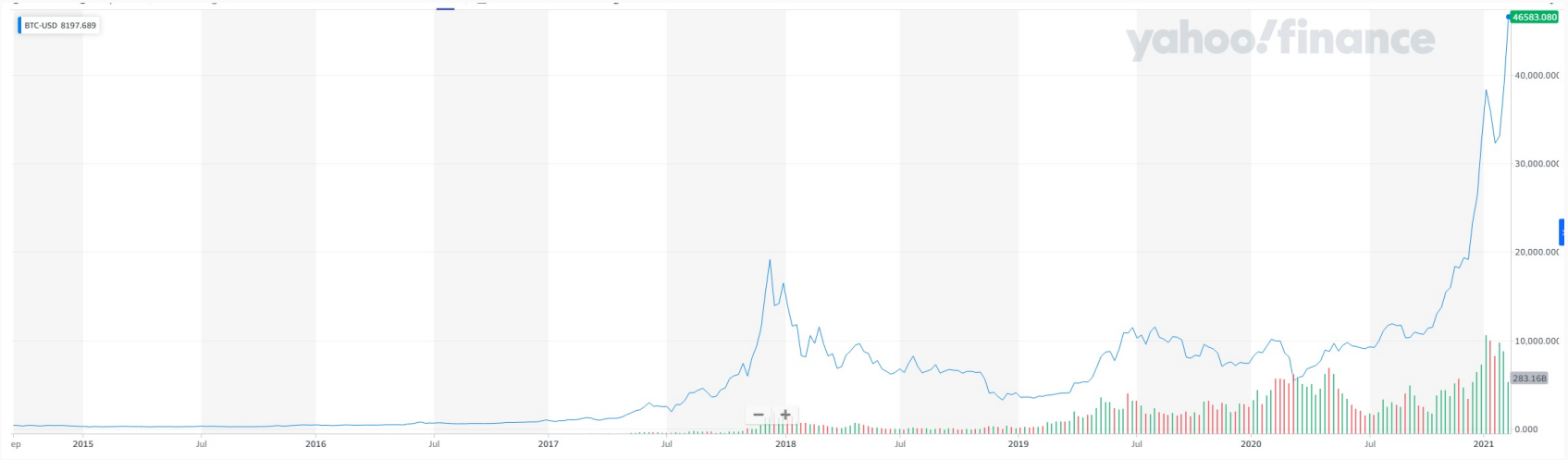
- Key Innovation: Decentralization of Core technologies, Privacy
- Intermediaries
  Currency Exchanges
  - BitForex, BitMEX, bitFlyer, etc.
  - Double Auctions (0.2 to 2% fee)
  - Bitcoin still a 'payment' system
- Digital Wallet Services
  - Holds account information
  - Imposes onerous technicality
  - Shared server vs own computer; private key is the key.
- Mixers
  - Promote Anonymity (Cost 1 to 3%.)
- Mining Pools

Uses of Bitcoin

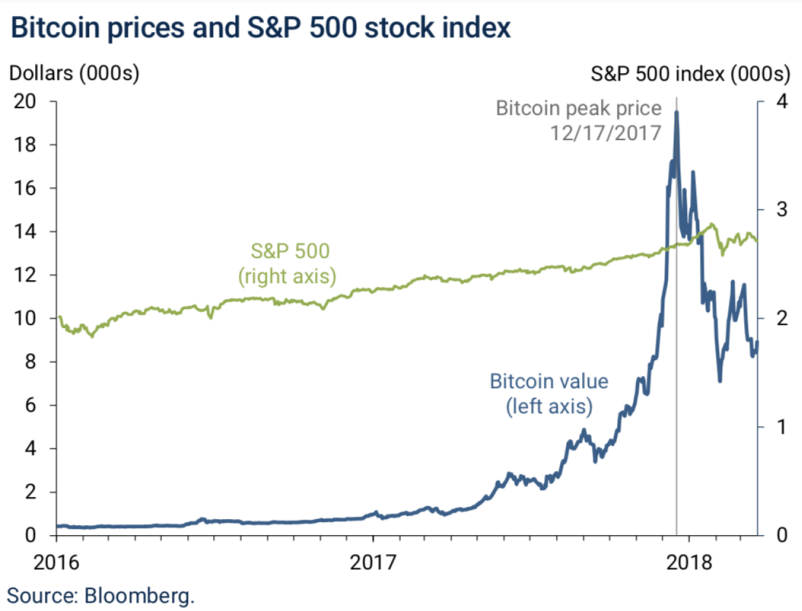
- Silk Road (Past)
  - Illicit Activities
  - High transaction cost (8%)
- Consumer Payments, Buy and Hold: (Current)
  - Low Cost, but no rebates
  - Strict book-keeping has costs
- Possibilites (Future)$\rightarrow$ Could be used for all-purpose payments (overstock.com accepts bitcoins)
  $\rightarrow$ can replace Western Union

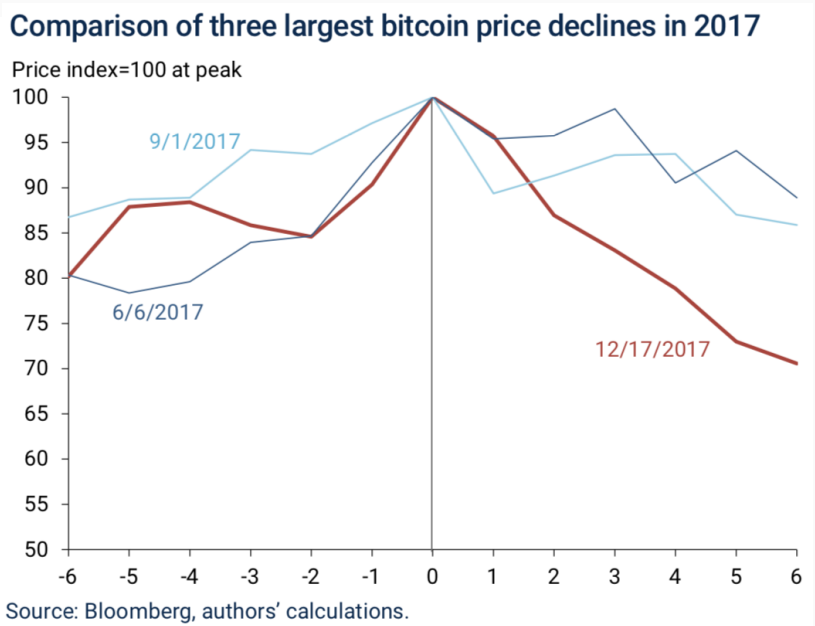
Risks in Bitcoin

- Market Risk—fluctuates with exchange rate.
- Shallow Market
- Counterparty risk (several exchanges have disappeared!)
- Transaction Risk (Irreversibility) (some can double spend as it takes time to update a block chain)
- Operational Risk (Infrastructure/security risk: Hacking)
- Privacy Risk (Pseudonymous)



US Dollar-Bitcoin Exchange Rate along with daily Bitcoin Trade Volume





(Effect of Starting Futures)

Key References:

R. Böhme, N. Christin, B. Edelman, and T. Moore (2015): *BitCoin: Technology and Governance*, Journal of Economic Perspectives, Vol 2, p 213–238.

A. Berentsen and F. Schar (2018): *A Short Introduction to the World of Cryptocurrencies*, Rserve Bank of St. Louis Review, Vol 100, p 1–16.

G. Hale, A. Krishnamurthy, M. Kudlyak, and P. Shultz (2018): *How Future Trading Changed Bitcoin Prices*, FRBSF Economics Letter, 12, May 7.