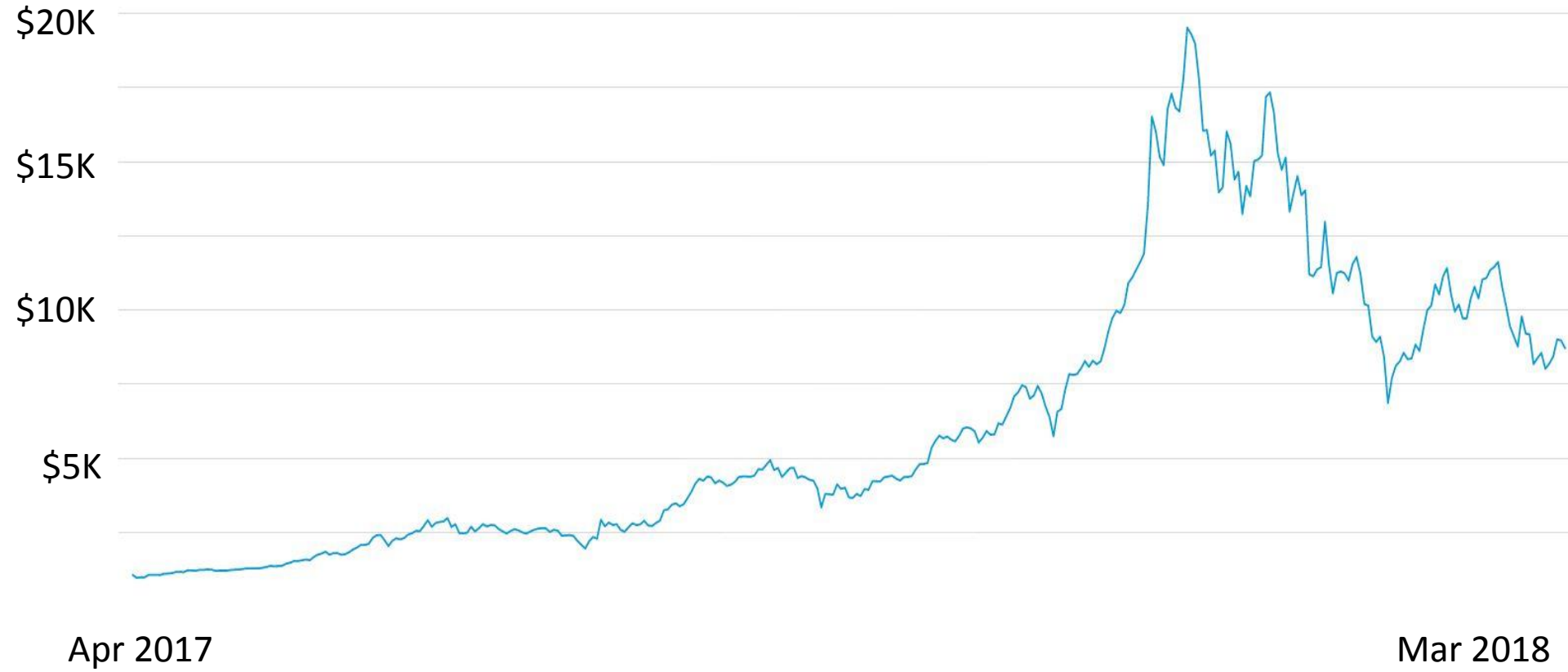
What is Bitcoin?
What is Blockchain?

A closer look

Bitcoin Market Price in USD
1 year history



www.blockchain.info March 23, 2018

What is Bitcoin

- Bitcoin has been called a fraud and Ponzi scheme by some.
- It’s been promoted as a sure-fire get-rich quick scheme or silver bullet for many things by others.
- It is neither.
- But it continues to work as designed; creating a new block of transactions every 10 minutes or so, regardless of the rhetoric surrounding it.

What is Bitcoin

- The Bitcoin network is a decentralized network of nodes, enabling direct peer-to-peer transactions anywhere in the world, with no intermediaries.
- **Transactions between individuals anywhere with no intermediaries**
- These transactions are denominated in “Bitcoin” (or actually small fractions of a Bitcoin)

- There are no master nodes: no one is in charge, anyone can join

- All participating full nodes have a complete transaction history from the beginning of Bitcoin.

- Transactions are stored in a data structure called a **Blockchain**.

Bitcoin Nodes

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Fri Mar 23 2018 13:26:00 GMT-0400 (Eastern Daylight Time).

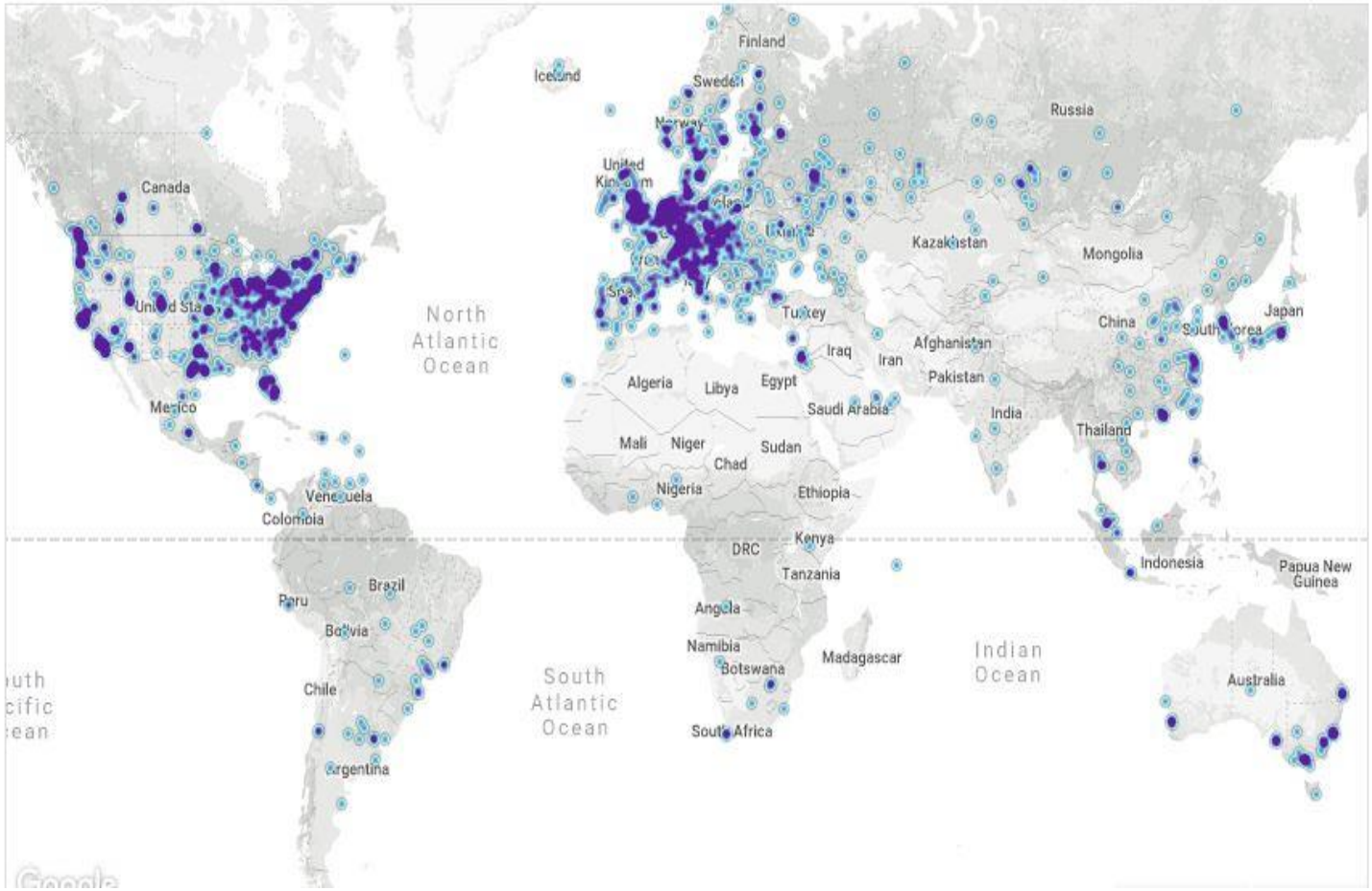
12123 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2719 (22.43%)
2	China	2035 (16.79%)
3	Germany	1966 (16.22%)
4	France	698 (5.76%)
5	Netherlands	516 (4.26%)
6	United Kingdom	414 (3.41%)
7	Canada	397 (3.27%)
8	Russian Federation	385 (3.18%)
9	n/a	313 (2.58%)
10	Singapore	219 (1.81%)

More (104) »

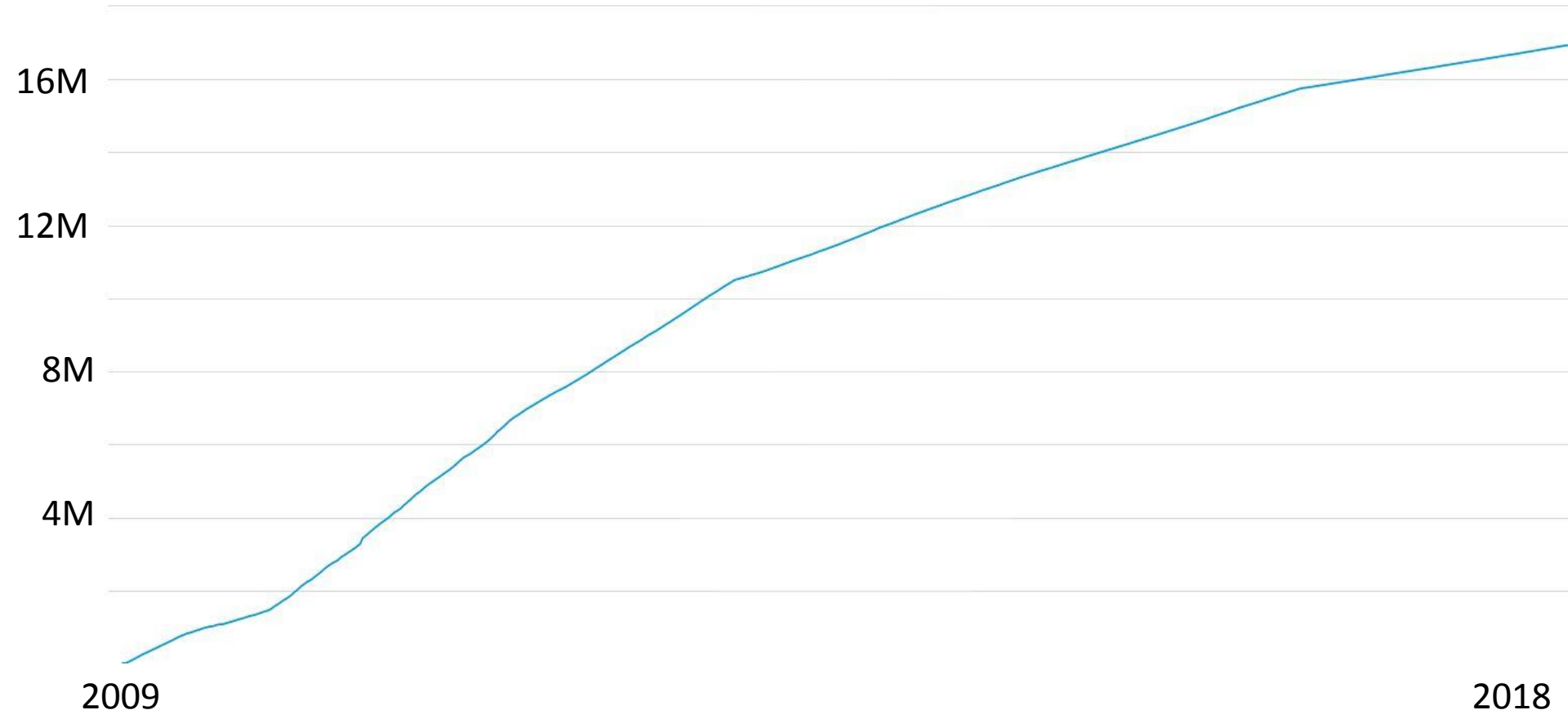


https://bitnodes.21.co/ March 23, 2018

Bitcoin Intro

- All nodes run effectively the same open source software (The Bitcoin core client) to validate transactions and forward new transactions.
- Some nodes, called miners, also put new transactions into new blocks and add them to the blockchain history.
- Miners that find a new block that meets the requirements are rewarded with Bitcoin.
- The difficulty of the requirements is automatically adjusted so that a new block of transactions is added approximately every 10 minutes.
- So the supply of Bitcoin is known and limited.

Bitcoin Supply



The supply is increasing, but at a decreasing rate; every 4 years the rate is halved. The total number of Bitcoin will top out at approx 21M.

Chart from www.blockchain.info March 23, 2018

Bitcoin Origin

- So how did it start?

- In November 2008 a paper by Satoshi Nakamoto (pseudonymous, believed by some to be Australian Craig Wright, believed by others to be Nick Szabo, or others to be neither), “Bitcoin: A Peer-to-Peer Electronic Cash System”, was posted to a cryptography mailing list site on the internet

- The original paper can now be found at various sites, including
  - http://nakamotoinstitute.org/bitcoin
  - https://bitcoin.org/bitcoin.pdf

- January 2009 the first **open source** client was released and the first bitcoins created

Bitcoin Predecessors

- The concept of electronic cash had been around for decades
- David Chaum and his company DigiCash developed eCash in the 1980s
- In the 1990s several schemes were also tried by banks, some with cards (Mondex, later acquired by MasterCard), some using browsers and certificates (SET)
- One company involved with SET, CyberCash, also developed a CyberCoin used for micropayments. CyberCash eventually went bankrupt in 2001. Their technology was purchased by Verisign and then sold to PayPal.

Bitcoin Predecessors

- eGold, run by a company called Gold & Silver Reserve, Inc. backed by gold held right here in Melbourne Florida, enabled users to own and spend increments based on whatever fiat currency they chose.
- They achieved substantial volume of trading between 2000 and 2008

- With the changing regulatory environment post-9/11, they found themselves in violations of many money-transmitting laws, even though they had been previously trying to comply.
- Their system was found, or at least alleged, to be used for various types of criminal activity.
- The system was used for several types of hacks that affected partners including banks.

- They were eventually shut-down and prosecuted, notwithstanding their previous attempts to comply with regulations


Bank of America
175
EAST NASA BLVD.
OMNIPAY
.com
the primary source of e-gold

Bitcoin Predecessors

- The immediate predecessors to Bitcoin were;
  - B-money, proposed by Wei Dai in 1998
  - Bitgold, proposed by Nick Szabo. Blog posts were published in 2005, but he said he had been working on it since 1998

- Though b-money and BitGold were similar, neither was fully developed or even fully specified with a white paper such as the original tract for Bitcoin.

- Bitcoin brought together these and several other cryptographic concepts, and most importantly added the idea of decentralization. This is notable because in posts and messages Satoshi noted that centralization was the reason that many of the previous electronic cash schemes had failed.

Enter Bitcoin

- So as we've seen, many electronic cash systems had been proposed prior to Bitcoin, and a number of them had been implemented.

- But various problems hampered the efforts, even of those that had some traction and success
  - Centralization
  - Security issues

- The financial crises of 2008 sparked substantial additional interest in alternatives to currencies managed by central banks

- Enter Bitcoin

Bitcoin Design

- So how does it work?

- Bitcoin makes extensive use of two important cryptographic techniques:
  - public/private key cryptography
  - “hashing”, or one-way encryption

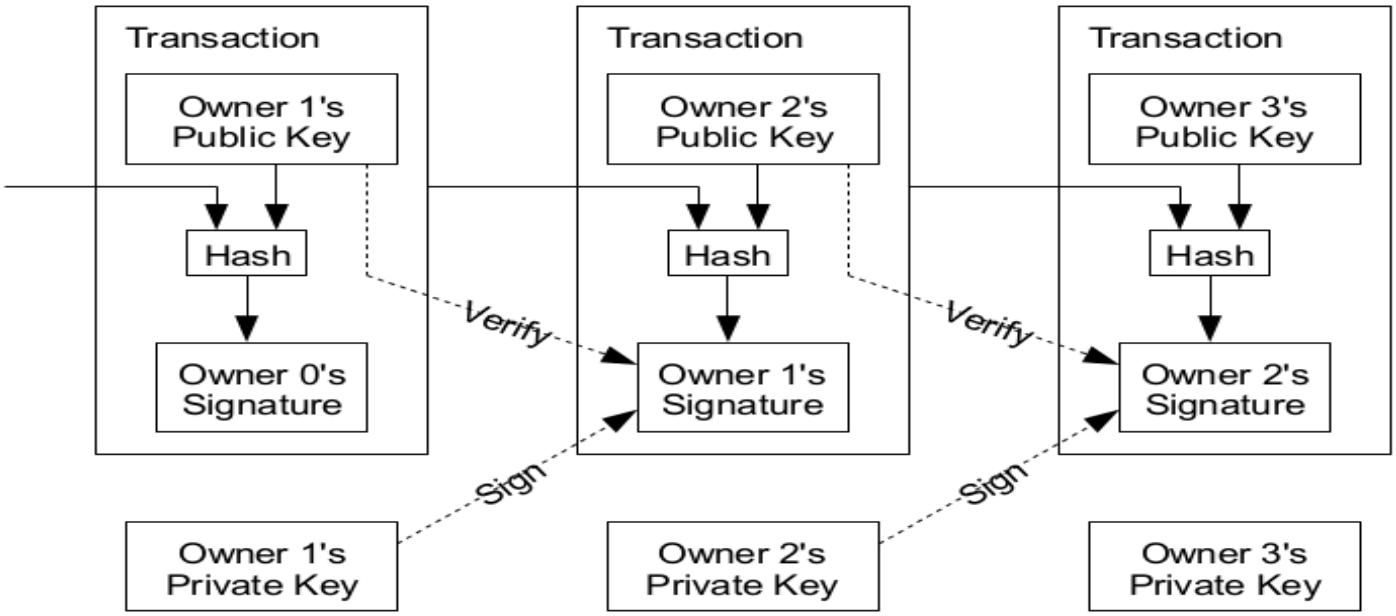
Public/Private Keys

- Public / Private key cryptography is used by Bitcoin to authenticate that a transaction that spends Bitcoin was actually sent by the previous owner.

- Public / private key cryptography:
  - Public and Private keys are logically in mathematically related pairs
  - A message can be encrypted with one and only decrypted with the other
  - The public key is publicly available for anyone to use to verify that a “signed” message is from the holder of the corresponding private key
  - In other words, a message whose signature can be decrypted with someone’s public key, must have been signed with their private key.
  - So in Bitcoin, if the signature of a transaction message that spends bitcoin can be decrypted by the public key that held the bitcoin, then it’s valid; that message must be from the owner.

Bitcoin Design

- From Satoshi Nakamoto's original paper:



How is Bitcoin “Held”

- Anyone can download and use a program called a software wallet, which holds the keys (codes) used to generate Bitcoin addresses, and send or receive Bitcoin.

- So Bitcoin wallets, whether on an individual computer or in an exchange, hold keys to addresses.

- Bitcoin transactions are typically sent to an address that is derived from the keys.

- No information about the owner of an address is kept anywhere. Possession of the keys is all that is required to control the Bitcoin in an address.
- If the keys are lost, the Bitcoin becomes forever unspendable.

How is Bitcoin “Held”: Wallets

- If someone has the keys to an address that has received Bitcoin, they can then spend that Bitcoin by sending it to someone else, provided is hasn’t previously been spent.

- So Bitcoin wallets do not actually hold Bitcoin, but they hold keys that effectively control the Bitcoin sent to the associated addresses.

- The addresses that have received Bitcoin and have not spent it, are the effective owners of the Bitcoin.

- All Bitcoin transaction history is accounted for in the Bitcoin blockchain history that all full nodes have, so it is effectively public information.

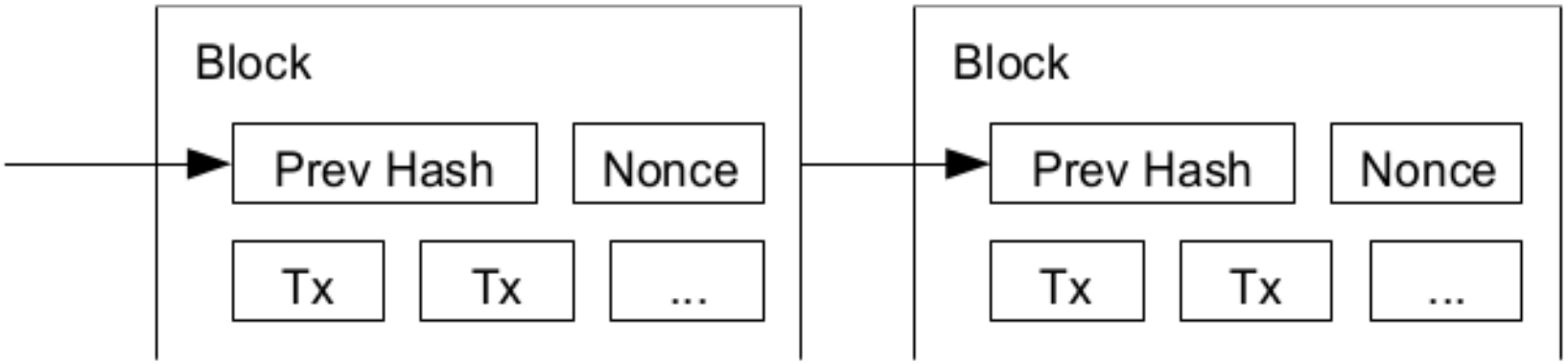
Hashing

- Hashing is the other cryptographic technique that is central to Bitcoin, and is used to prove that history has not been tampered with.

- Hashing is one-way encryption
  - A message or block of any length can be “hashed” to produce a relatively small fixed length byte string
  - The original string cannot be determined from the hashed value
  - So a long message can be reduced to a small hash, and that hash can be efficiently signed by a private key.
  - And the hash of a prior transaction block can be (and is) incorporated a subsequent block, making it easy to verify that the prior block has not been tampered with.

Bitcoin Transaction Blocks

- Transaction blocks are sequential.
- Each transaction block contains a hash. That hash is of the previous block's hash and the current block's transactions, so any attempts at changing transaction history could immediately be detected.
- The block header also include a nonce, which is determined by the miner (more on that later)
- The diagram below is also from Satoshi Nakamoto's original paper.



Bitcoin: What's the big deal

- So the Bitcoin blockchain replaces a trusted third party financial intermediary.

- Bitcoin was the first decentralized digital currency using peer-to-peer technology to function without an intermediary, such as a central server or a financial institution.

- This system enables the network to reach consensus without the need of information on user identities and without trust relationships.

The Bitcoin Blockchain

- The Bitcoin blockchain contains the payment history of every bitcoin in circulation and provides “proof” of who (or what public key / address) owns what at any given juncture.

- It is essentially a **distributed state transition ledger** that is replicated on thousands of computers, Bitcoin’s “nodes”, around the world and is publicly available.

- Many other similar blockchains or distributed ledgers have since been implemented.

Buying Bitcoin: Exchanges

- So how do you buy Bitcoin?

- Though Bitcoin was designed for individuals to hold their own wallets and transfer directly to other individuals, now the vast majority of most users' Bitcoin and other cryptocurrency transactions with local currency go through Centralized exchanges

- And there are actually several types of exchanges
  - Centralized v Decentralized
  - Crypto-Fiat v Crypto-only
    - "Fiat" means a currency (e.g. USD, EUR, …) that has value because of a government decree.
    - Crypto means cryptocurrency, a digital currency secured by cryptography. Other terms are alt-coin, alt-tokens, tokens, digital assets, … . BTC is usually the symbol for Bitcoin.
  - Other Exchanges: Futures (CME, CBOE as of Dec 2017), CFD, …

Exchanges

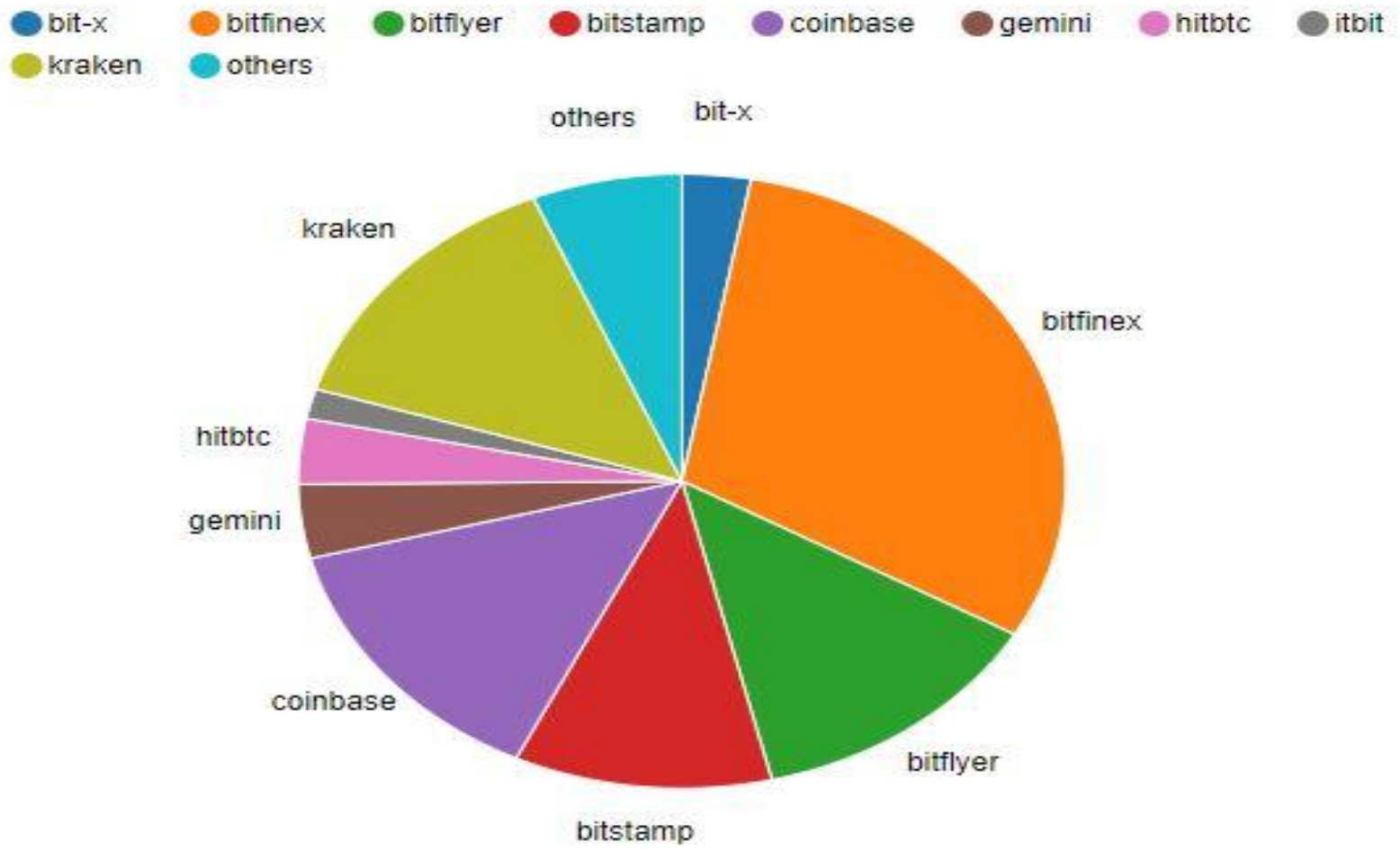
- Centralized exchanges settle trades similar to stock exchanges, with bids and asks, “market” prices, …
- Decentralized exchanges allow users to deal directly with other users, possibly with a procedure for holding currency like USD in escrow during the transaction
- Crypto-Fiat exchanges allow users to purchase cryptocurrencies like BTC with local currency (“fiat”) like USD.
- Most of these follow KYC/AML and require documentation to open an account.
- Crypto-Only exchanges only quote cryptocurrencies in relation to each other. Fiat (USD, EUR, …) is not used. They typically carry an extensive list of crypto-currencies, some carry many hundreds.
- By dealing only with cryptocurrencies, many of these exchanges hope to be free of money-transmitter and securities rules.

Exchanges

- The largest exchanges that accept local currency (“fiat”) like USD only offer a few different cryptocurrencies.

- So to buy any other crypto-currencies, requires several steps:
  1. Establish an account and purchase BTC at a major exchange. This will involve documentation like any other financial account.
  2. Deposit funds, usually with a wire transfer to buy BTC (CC purchases have been largely disallowed by the CC companies as of last month).
  3. Establish an account at a crypto-only exchange that carries the alt-coin you are interested in.
  4. Transfer BTC from the first exchange to the crypto-only exchange: to transfer typically you first get a receiving address from the target exchange, then copy and paste that to the transfer function on the sending exchange. The transfer may take many minutes to be confirmed.
  5. When the BTC has reached the crypto-only exchange, you can buy the other desired cryptocurrency with the BTC

Exchange shares



Centralized Crypto-Fiat

- The largest and most well-known exchanges in the US include:
- **Coinbase**
  - Coinbase is the UI geared toward ease-of-use for novice or average retail investors, and has relatively high fees.
  - One of largest in US; $50B traded, over 10M customers, $1B revenue 2017
  - BTC, ETH, LTC, BCH
  - Based in San Francisco
- **Gemini**
  - New York based, licensed exchange and custodian
  - US$ deposits are FDIC insured
  - Founded and run by Winklevoss twins (Harvard / Facebook)
  - BTC, ETH
- Others in the US; Bitflyer (started in Japan, locally in SF), Kraken, Bittrex
- Other European; Bitstamp, …

Centralized Crypto-Fiat
Bitfinex: Tether

- Bitfinex is of interest in that the ownership is the same as that of cryptocurrency Tether (USDT) which is meant to be the crypto equivalent of $1 USD, and enables trading on crypto-only platforms.

- There has been, and continues to be much speculation as to whether Tether is properly backed by USD as it has claimed. Some critics believe Tether is unsupported by USD and rather has been used to inflate the price of BTC.

- In January 2018 Tether dissolved the relationship with its auditor, prominent crypto firm Friedman LLC. Friedman had issued preliminary report in Fall 2017 that Tether was fully-backed by USD, but the report contained caveats.

- Recent research (Feb 18, 2018) from BitMEX does not draw conclusions as to whether it is fully backed, but expects that it would be supported.
- Ownership group of Bitfinex is opaque; led by JL Van de Velde (Dutch from Hong Kong/Taiwan)

Asian Exchanges

- China prohibited domestic exchanges in September 2017. There is some speculation that they may be allowed and regulated in the future. Up to early 2017 the Chinese market was by far the largest market, and the exchanges were the largest by volume. Most of these have migrated to other jurisdictions, some have closed.

- Korean exchanges: Korea prohibited anonymous accounts in January 2018, and was rumored to be considering closing exchanges, but later stated it was would regulate rather than ban.

- Japanese exchanges; Japan recognized cryptocurrencies as legal in early 2017 and began regulating exchanges later in 2017

Centralized Crypto Only

- The largest and most well-known of the Crypto-only exchanges include:
- **Poloniex**
  - Based in Delaware
  - One of oldest pure crypto exchanges
  - **Recently purchased by Circle (which itself is partially funded by Goldman Sachs)**
- **Binance**
  - Hong Kong based, with multiple offices
  - One of largest by trading volume
- **Bittrex**
  - Founded 2013, opened 2014, based in Seattle and Las Vegas
  - Historically Crypto only, low fees
  - Announced coming USD trading; full KYC/AML
  - Suspended some new accounts in late 2017 for compliance reviews and temporarily halted new user registrations, though still accepting new corporate accounts
  - Extensive list of crypto-pairs, considered good security
  - Geared more towards institutional and sophisticated traders, account minimums to be introduced

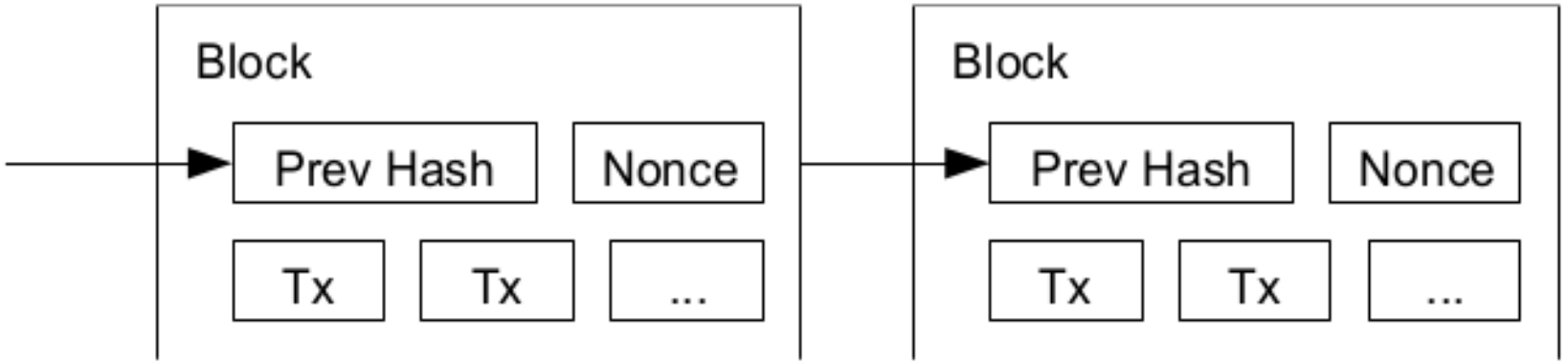
Exchange Issues

- Mt. Gox
  - Japan; largest BTC exchange in 2013. In 2014 lost over 600,000 BTC in biggest Bitcoin breach, due to poor record-keeping and alleged hacking
- EtherDelta
  - One of first decentralized exchanges, hacked and likely unable to come back
- Coincheck (Japanese exchange)
  - Lost NEM tokens worth $533 million in a major breach in Jan 2018
  - Had not passed Japanese regulatory requirements but had been allowed to operate while its application was pending
- Bitfinex / Tether
  - Questions

- New Decentralized exchanges:
  - Network effects; need substantial user base

What are Miners

- Recall the block diagram



- Miners have to find an arbitrary number, a “nonce”, that when included in the hash of the block, will result in a value in a specific value range.
- A property of the hash function is that there is no way to determine such a number other than just trying random numbers until finding one whose result matches the desired result.

- This is the work that miners do.

What are Miners

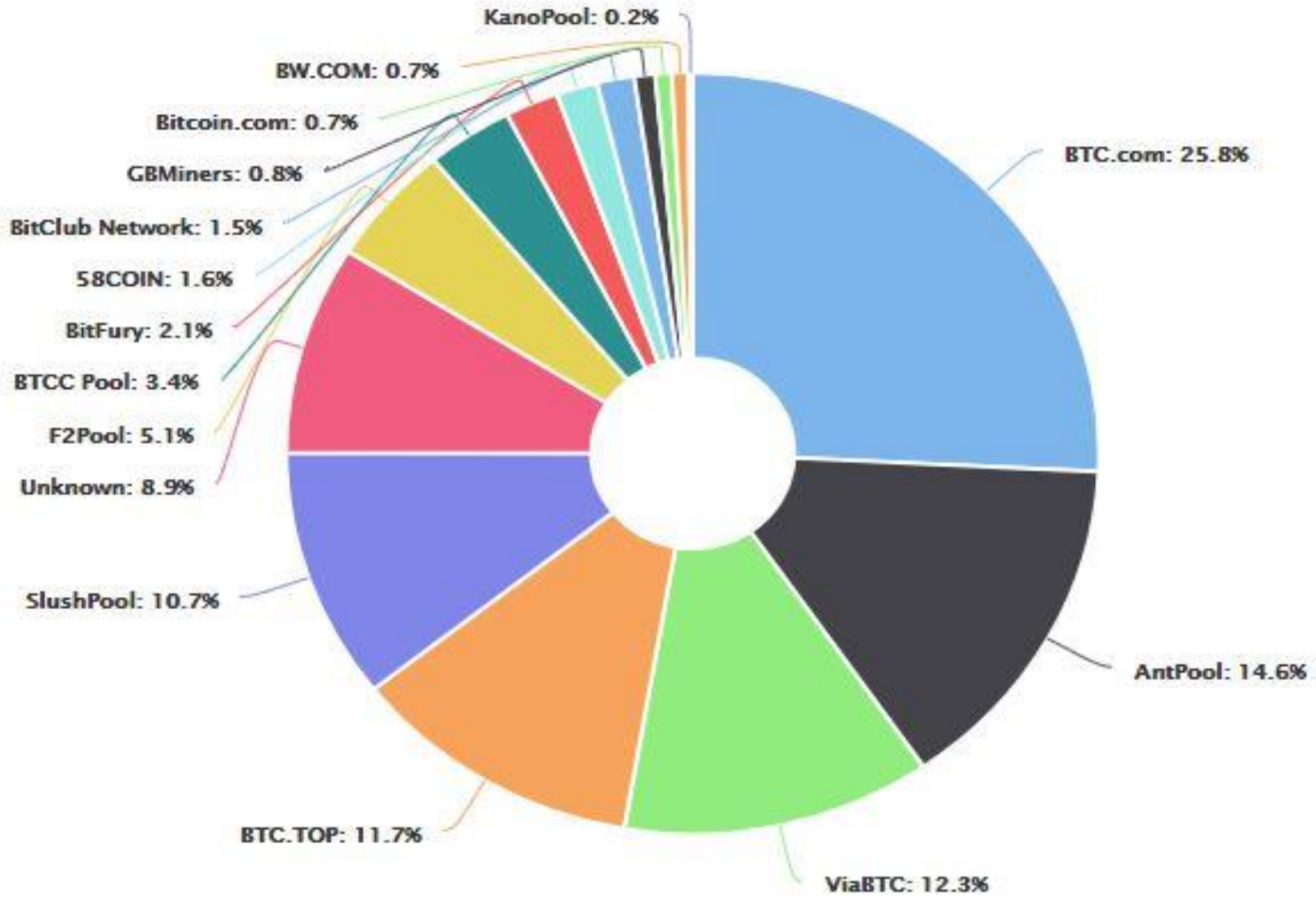
- So Bitcoin Miners are nodes that work to solve the nonce hash problem for a new block
- The node that first solves (“mines”) the nonce hash problem for the block receives compensation in BTC in the form of a “genesis” transaction on that block.
- That amount started at 50 BTC and has been halving every 4 years or so and is now 12.5 BTC
- This is how Miners are compensated for the work that they do in building and maintaining the blockchain.

Miners

- Anyone can be a miner
- Their compensation will be in relation to the speed of the processing power relative to that of all other miners

- In the last few years ASIC (Application Specific Integrated Circuits) systems designed specifically for mining have been developed and now represent the vast majority of Bitcoin mining power
- Most mining is now done by or through large mining pools. A number of these pools allow individual miners to join.

- Ethereum and some other coins purposely use a mining algorithm that lends itself to GPUs rather than ASICs, so as to avoid mining power concentration.



https://blockchain.info/pools 2/25/2018, see also https://btc.com/stats/pool

Mining Countries

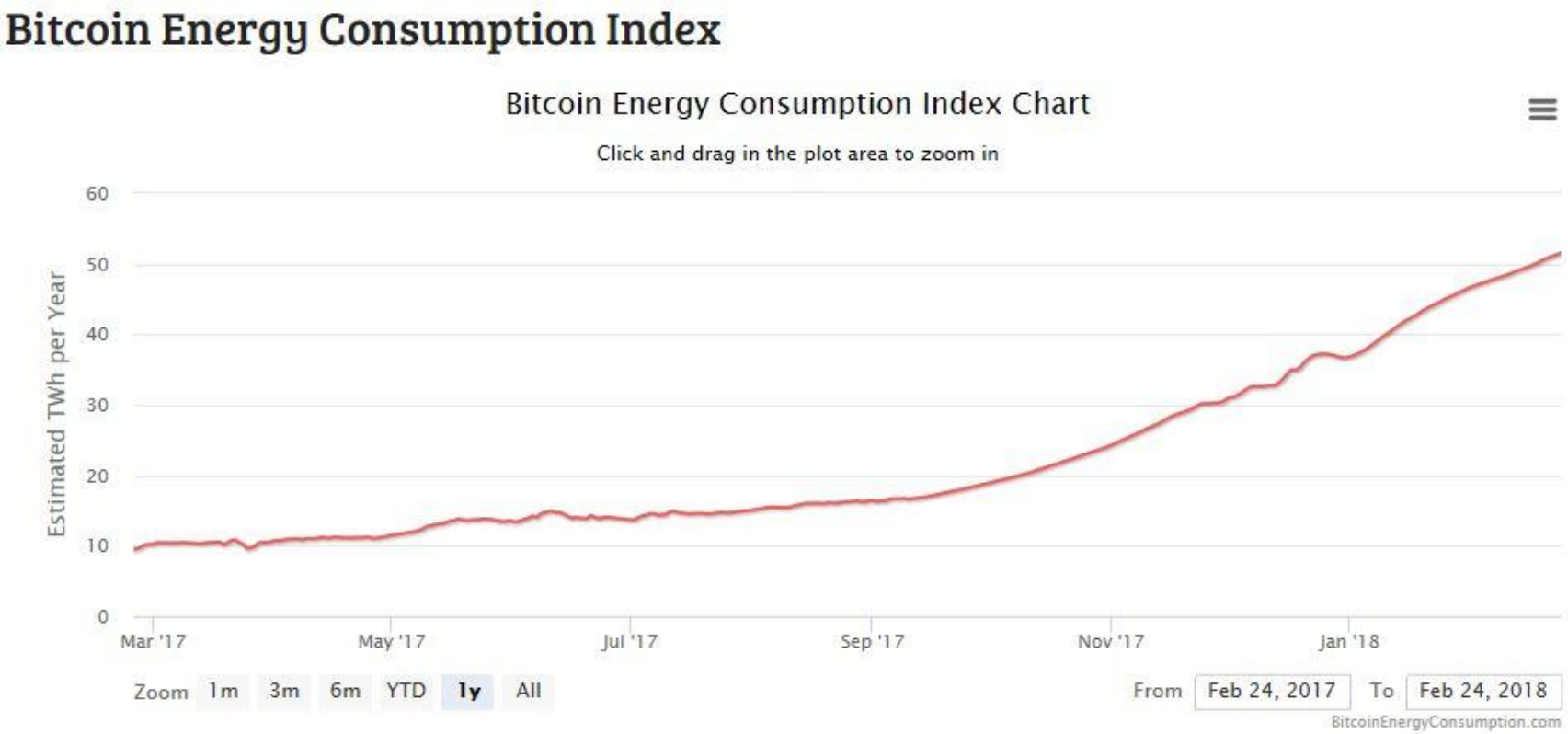
- The crack down on cryptocurrency exchanges in China, as well as talks of power regulations applying to miners, has prompted Chinese miners to consider new sites to operate from.

- Canada has become a desirable mining location with relatively low electricity costs in some provinces, and relatively low cooling costs due to its climate
- Canada's Hydro Quebec has been overwhelmed with requests from cryptocurrency miners looking to setup operations in Quebec, due to its low cost electricity and large potential energy supply.

- Iceland has also become a major mining center, with mining power demands likely to exceed those of all residential customers

- US Cities with cheap electricity, like Plattsburgh NY and Wenatchee WA, have also become mining centers, with the issues and growing power demands that result

Bitcoin Mining Energy Consumption



https://digiconomist.net/bitcoin-energy-consumption

Bitcoin Mining Energy Consumption

- Digiconomist: constant alarmist about Bitcoin power consumption, probably overstated.

Description	Value
Bitcoin's current estimated annual electricity consumption* (TWh)	51.51
Annualized global mining revenues	$8,158,168,150
Annualized estimated global mining costs	$2,575,467,717
Country closest to Bitcoin in terms of electricity consumption	Uzbekistan
Estimated electricity used over the previous day (KWh)	141,121,519
Implied Watts per GH/s	0.233
Total Network Hashrate in PH/s (1,000,000 GH/s)	25,531
Electricity consumed per transaction (KWh)	768.00
Number of U.S. households that could be powered by Bitcoin	4,769,385
Number of U.S. households powered for 1 day by the electricity consumed for a single transaction	25.97
Bitcoin's electricity consumption as a percentage of the world's electricity consumption	0.23%
Annual carbon footprint (kt of CO2)	25,240
Carbon footprint per transaction (kg of CO2)	376.49

https://digiconomist.net/bitcoin-energy-consumption

Bitcoin Mining Energy Consumption

- Alternative estimates, more realistic;

As of **11 January 2018** (average hash rate of 16200 PH/s):

	Lower bound	Best guess	Upper bound
Power consumption (MW)	1620	2100	3136
Energy consumption (TWh/yr)	14.19	18.40	27.47
Energy consumption (Mtoe/yr)	1.220	1.582	2.362
Energy consumption (quad Btu/yr)	0.048	0.063	0.094
Percentage of world's energy consumption[5]	0.01295%	0.01678%	0.02506%
Percentage of world's electricity consumption[5]	0.0715%	0.0927%	0.1385%
Electricity cost (million USD/yr)[6]	$710	$920	$1374
Energy efficiency (J/GH)	0.100	0.130	0.194

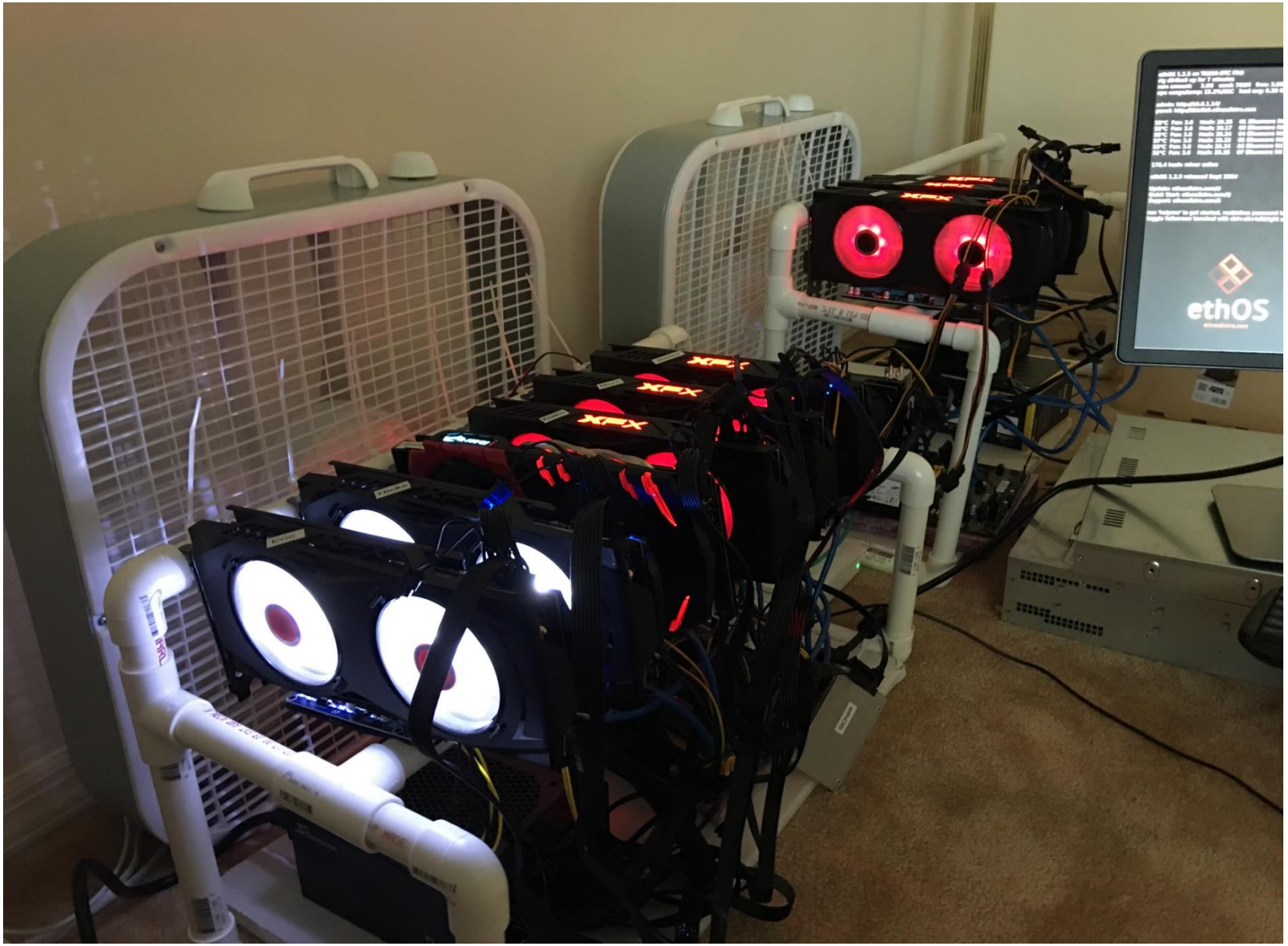
blog.zorinaq.com/bitcoin-electricity-consumption/

Ethereum

- Ethereum is the second most widely held crypto-currency, behind only Bitcoin
- It is a Scriptable Blockchain environment, designed to enable Smart Contracts in addition to just transfers between accounts.
- Ethereum has its own blockchain; it does not use the Bitcoin blockchain
- ETH (“ether”) is Ethereum’s cryptocurrency. It’s meant to pay for work on the Ethereum platform rather than to be a general purpose currency. However it trades like any other virtual currency.
- It was first described in a paper in late 2013 by Vitalek Buterin, and developed in
- Most ICOs are released on the Ethereum blockchain and funded by ETH.

Ethereum Mining

- Ethereum uses a different mining algorithm than Bitcoin.
- It designed its own algorithm specifically so that it would lend itself to general purpose CPUs or GPUs, making it difficult to design an ASIC that would have any processing advantages.
- This is to make it so that individual miners would be competitive and avoid a concentration of mining power
- So it has become a popular cryptocurrency to mine by hobbyists, building home-made systems of a potentially large number of GPUs, connected to processors, supported by PVC


XFX
ethOS

Other Virtual Currencies / ICOs

- There have been hundreds of virtual coins introduced recently, most using the Ethereum blockchain and most introduced in 2017
- An ICO is an “Initial Coin Offering”. It is when an investor can buy coins directly from the organization issuing them, before they trade on any exchanges.
- It is similar to an IPO for stocks.
- There is some ambiguity as to whether the SEC will consider them to be securities, and enforce securities law.

Other Virtual Currencies / ICOs

- The SEC has not issued definitive guidance, but has asked a number of participants for more information, and appears to be leaning towards classifying them all as securities.

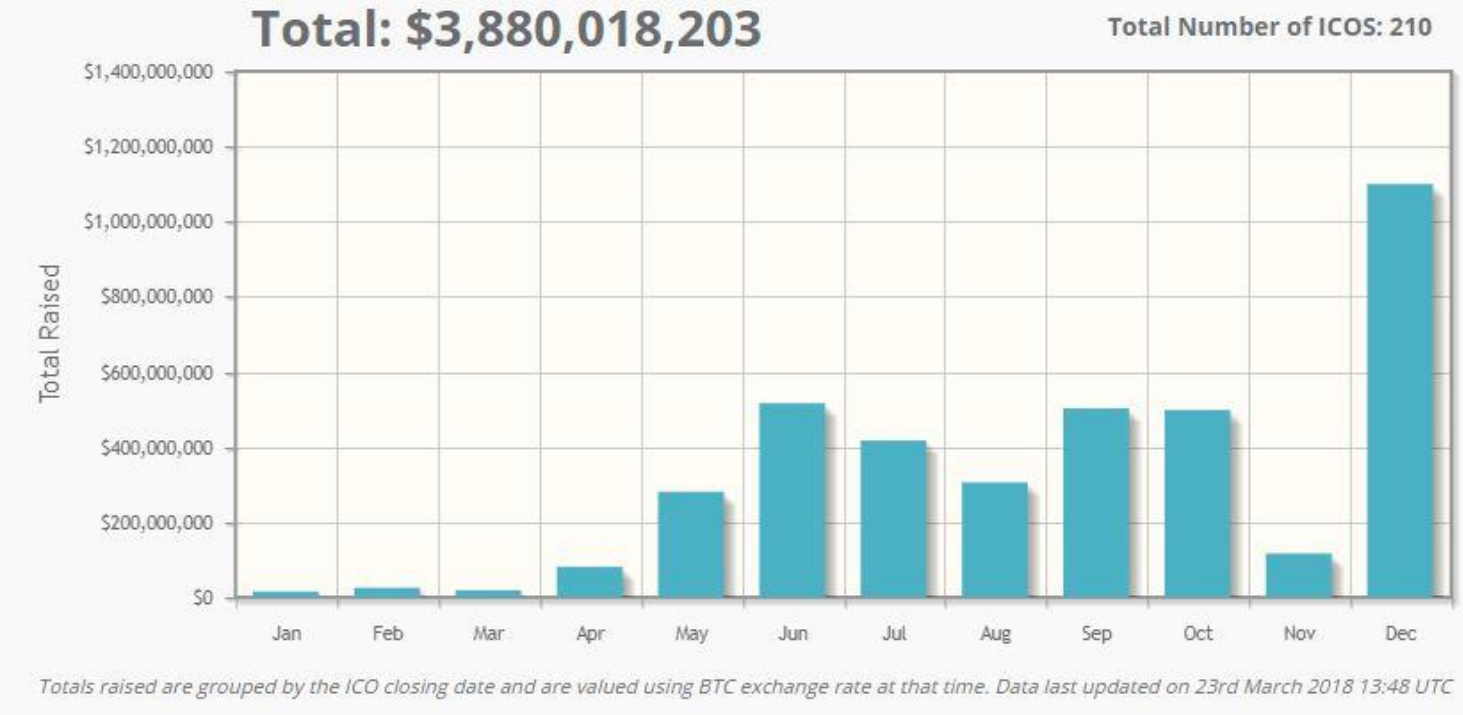
- Some tokens are designed as “utility tokens”, and hope to avoid regulation by being used as a utility rather than an investment. It is not yet clear if the SEC recognizes this distinction.

- There is also ambiguity as to whether tokens and token trading should be regulated by the SEC or the CFTC.

- The CFTC seems much more receptive, and has allowed Bitcoin futures trading on the exchanges that it regulates.

Other Virtual Currencies / ICOs

- There have been hundreds of virtual coins introduced recently, most using the Ethereum blockchain and most introduced since mid 2017



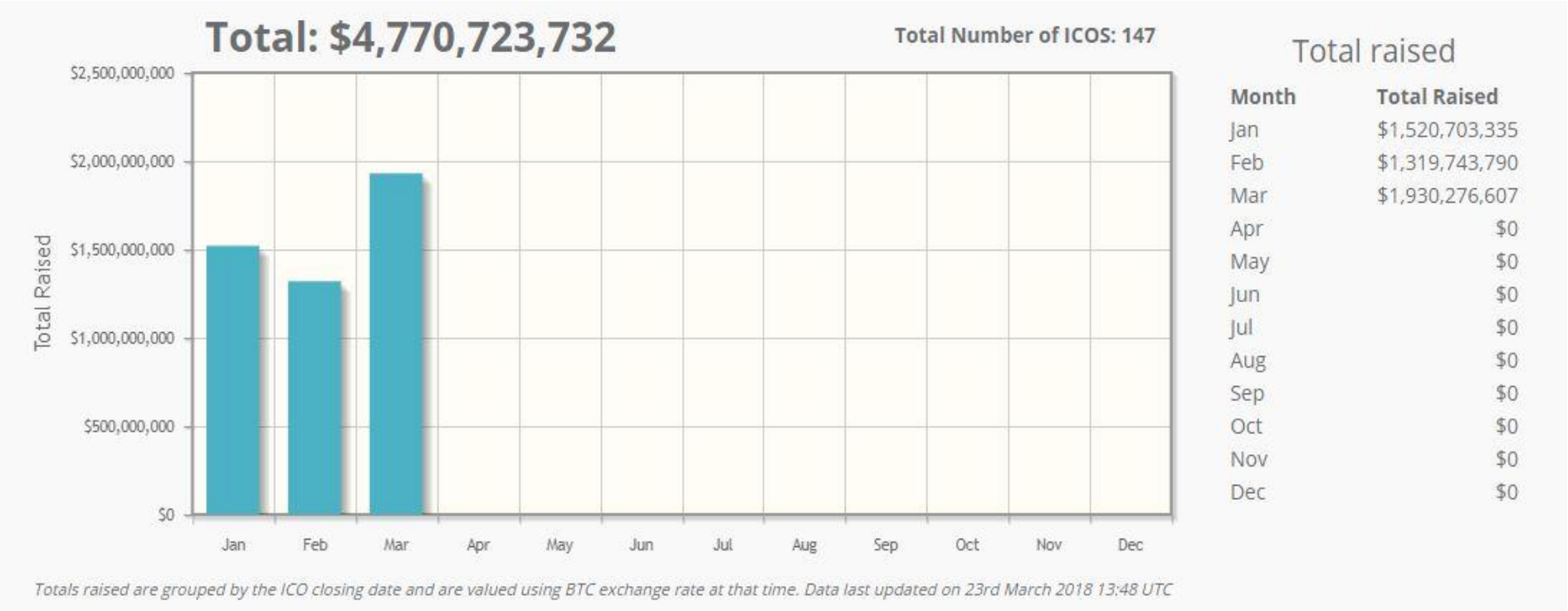
Total raised

Month	Total Raised
Jan	$15,358,278
Feb	$25,460,157
Mar	$18,660,713
Apr	$81,427,029
May	$281,012,458
Jun	$516,537,695
Jul	$417,281,712
Aug	$305,986,446
Sep	$502,951,511
Oct	$498,713,046
Nov	$116,706,256
Dec	$1,099,922,902

https://www.coinschedule.com/stats.php March 23 2018

Other Virtual Currencies / ICOs

- The pace has even increased in 2018.

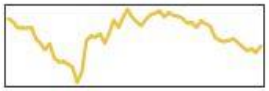
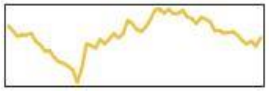


Total raised

Month	Total Raised
Jan	$1,520,703,335
Feb	$1,319,743,790
Mar	$1,930,276,607
Apr	$0
May	$0
Jun	$0
Jul	$0
Aug	$0
Sep	$0
Oct	$0
Nov	$0
Dec	$0

https://www.coinschedule.com/stats.php March 23 2018

Top Crypto-currencies

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$146,263,883,988	$8,636.66	$5,314,230,000	16,935,237 BTC	-0.19%	
2	Ethereum	$51,669,531,223	$525.26	$1,520,900,000	98,368,689 ETH	-1.50%	
3	Ripple	$25,040,399,904	$0.640514	$359,757,000	39,094,227,299 XRP *	-1.96%	
4	Bitcoin Cash	$17,114,414,620	$1,004.74	$309,431,000	17,033,675 BCH	-0.37%	
5	Litecoin	$9,037,713,147	$162.09	$361,056,000	55,758,064 LTC	-1.18%	
6	EOS	$5,172,907,831	$6.93	$898,708,000	746,603,253 EOS *	2.30%	
7	Cardano	$4,831,924,428	$0.186366	$135,299,000	25,927,070,538 ADA *	-6.38%	
8	NEO	$4,368,916,500	$67.21	$137,213,000	65,000,000 NEO *	-2.92%	
9	Stellar	$4,330,083,342	$0.233441	$49,336,500	18,548,941,024 XLM *	-1.47%	
10	IOTA	$3,622,256,070	$1.30	$31,058,900	2,779,530,283 MIOTA *	-0.85%	

As of midday ET March 23, 2018 as per coinmarketcap.com

Other Blockchains

- The technology is open-source, so any set of nodes could start their own blockchain
- There are several companies that develop and support blockchains
- Multichain (multichain.com) is an open platform for building public and private blockchains
- OpenChain (openchain.org) is an open source blockchain that companies can implement. Each company implements its own blockchain and specifies a single node as the authority to validate transactions.

Other Blockchains

- IBM has a made a major investment in blockchain with their HyperLedger product and related technology, and with several development centers around the country (and world).

- Microsoft, working with Ethereum and other partners, has been offering Blockchain as a Service (BAAS) through Azure since late 2015.

- There are many bank-related blockchain tests and trial runs going on.
- It is particularly suited for keeping track of ownership, which could be applied to things like asset tracking, securities settlement, etc.

- The financial industry has become very interested, and had even “coined” their own term for it “Distributed Ledger Technology”

Recent Events; Markets and Regulations

- The Chicago Board Options Exchange (CBOE), the largest U.S. options exchange, began offering Bitcoin futures in December 2017.
- The Chicago Mercantile Exchange also began offering Bitcoin futures in December 2017
- In December 2017 Bloomberg added quotes for ETH, LTC, and XRP in addition to BTC on its Bloomberg trading terminal
- Several brokerages, including TD Ameritrade now allow client trading in Bitcoin futures.
- Nikkei Asian Review reported today that Yahoo Japan would start a cryptocurrency exchange in 2018
- Canadian stock market operator TMX announced yesterday that they would open a crypto-currency brokerage, initially focused on BTC and ETH, in the second quarter of this year.
- This month, the Financial Stability Board of the G20 began asking for information regarding potential regulation of Bitcoin.

Resources

- Cointelegraph.com
- Coindesk.com

Economics

- Is BTC money?
  - Freedom of transactions
  - Unit of account?
  - Accepted as payment: Network effect
  - Particularly valuable if local currency unstable?
- Threats:
  - Volatility
  - Government action
  - Technical vulnerability?
- Value/FX Rates?
  - Usually driven by relative I (Inflation) or i (interest rates)
  - Impacted by monetary authorities

Contacts

Bernard Parenteau

- bparente@fit.edu
- bern@floridalogic.com

- Local Meetup Group:
  - Melbourne Bitcoin/Crypto currency/Blockchain
  - https://www.meetup.com/Melbourne-Bitcoin-Crypto-Currency-Blockchain-Forum/