RBC Capital Markets

EQUITY RESEARCH

January 3, 2018

Crypto Currency & Blockchain Technology: A Decentralized Future

A Potential Multi-Trillion Dollar Opportunity

The $10tril Bull Case: While the Crypto-Currency space has many risks, the opportunity appears vast with constant technology updates. With a rapid rise in prices we outline the bull case for building a decentralized future: _1) A Secure World Computer:_ a decentralized world computer without a third-party intermediary. If there is one positive technology item that we can agree on, it is that the Blockchain has never been hacked. What happens if we build on top of this secure layer?; 2_) Store of Value:_ this is the most commonly cited use case for crypto currencies and the least interesting, in our view: offshore accounts valued at an estimated ~$21 trillion and gold at $8 trillion; _3) International Remittance:_ the sending of payments overseas estimated at half a trillion dollars per year; _4) "Fat Protocols":_ ability to own the protocol layer which increases in value as the applications grow – reverse model compared to today's environment; _5) Mining:_ computing power being used to secure the network through Proof-of-Work which is currently a multi-billion dollar market; and _6) Improved scaling:_ development efforts (including Lightning Network) appear on track to deliver scaling that accommodates higher transactions/second, ultimately driving higher utility and network value. _Net Net: by utilizing decentralized computing and opensource software, we see a multi-trillion dollar market emerging._

**RBC Will Host a Crypto-Currency Call On January 19 with Alex Rampell, General Partner at Andreessen Horowitz**

- **Central vs. Decentral:** While the store of value and payment use cases are well known, we think the underlying technology is misunderstood. We compare Filecoin and Box as tangible examples. With Box, your data is owned and controlled by a third party that has access to your information (a photo loaded can be retrieved by anyone with access to Box servers - employees). With Filecoin, your storage is distributed _**and**_ decentralized, making the holders unable to retrieve your photo (they would need to hack every computer on the decentralized network - Blockchain). Your information is now secure, and without your private keys, it cannot be accessed. This is the first example of building a "World Computer", as we could apply the same concept to a wide variety of decentralized applications (Dapps).

- **In Code We Trust:** The trust system from the original cypherpunks decades ago was intended to reallocate an old system of centralized markets towards open source, secure (encryption) and meritocratic markets. This would be governed by code (Blockchain, consensus) and valued on utility ("token-omics" vs. economics). The former is designed to become a virtuous cycle, whereby successful tokens drive more users, more miners, and higher network value.

- **Crypto Scaling is Underestimated:** As scaling and protocols mature, the value of a decentralized World Computer could potentially become a multi-trillion dollar industry. On the scaling front, Lightning Network (once deployed) could allow over a million transactions/sec on Bitcoin and Litecoin. On the protocol side, the introduction of IPFS (InterPlanetary File System) has helped scale Ethereum's network through its P2P distributed file system (similar to HTTP).

- **Many, Many Risks:** _1) Government Intervention:_ if crypto currencies are stolen, the government has no incentive to catch the criminal - not backed, _2) Wallet Hacking:_ computers are already being hacked to steal compute power, we think smartphone wallet hacking is the next major risk, _3) Scalability:_ processing transactions instantly without high mining fees is an issue, _4) Privacy:_ public display of transactions reduces privacy, making all transactions transparent, _5) 51% Attack:_ if a single central entity were to obtain over 50% of the compute power, the network could be attacked, and _6) Coordinated Attacks:_ there is risk of large scale manipulation to approve malicious forks or price manipulation of a coin.

Table of contents

#1 A World Computer

"Systems like Ethereum (and Bitcoin and NXT, and Bitshares, etc) are a fundamentally new class of cryptoeconomic organisms -- decentralized, jurisdictionless entities that exist entirely in cyberspace, maintained by a combination of cryptography, economics and social consensus" - Vitalik Buterin, co-founder of Ethereum

To avoid confusion, this section (Part 1) does not apply to Bitcoin. It relates to Ethereum and Ethereum competitors such as NEO, Cardano, EOS and a handful of separate crypto currencies. The world computer example is not related to Bitcoin. Instead, *we will use Bitcoin as an example of how the developing world computer is different from Bitcoin*.

Overview: In the traditional equity markets, a central authority primarily controls the network. These enterprises are now the most profitable. Rather than an ecosystem or network benefiting, the windfall is to the central provider. This model can be viewed as closed, but meritocratic. Entrepreneurship into these critical enterprises face higher barriers to entry, due to closed networks and high cash burn against growing R&D budgets of incumbents.

In the decentralized era, using Blockchain technology, networks are turned into open and meritocratic markets. Bitcoin was the first Blockchain, with the primary use case being peer-to-peer transport of digital currency. This represented the proof of concept. Under Blockchain technology, centralized proprietary services are being replaced with distributed and decentralized open ones; trusted entities replaced with verifiable computation; brittle location addresses replaced with resilient content addresses; inefficient monolithic services replaced with peer-to-peer algorithmic markets.

In Layman's Terms: While Bitcoin allows an individual to send digital money or code, it is limited in its ability to create "if then functions". A basic example is while an individual can send a Bitcoin from Person A to Person B, it does **Not** allow an individual to say "Send 1 Bitcoin to Person B if it rains in San Francisco tomorrow". This is a critical difference between a flexible Blockchain and the original blockchain used to simply send and receive data.

With a flexible Blockchain, we can now do *"if-then"* functions, which are also called Smart Contracts. Below is an example of several of these ideas:

Basic Example: John works at Company A. **If** John shows up to work on time and completes a task **then** release 1 Ethereum token to John's address from Company A's address. **If** John does not complete the task **then** no Ether is released.

More Complex: John and Mark want to place a bet on the weather in San Francisco tomorrow. If it rains in San Francisco, John wins; if there is no rain in San Francisco, Mark wins. **If** it rains in San Francisco **then** release 1 ether from Mark's address to John's address. **If** it does not rain in San Francisco **then** release 1 ether from John's address to Mark's address. We can now see how this additional functionality (something that Bitcoin lacks) could be applied to contracts.

Most Complex: This is likely the most difficult jump to explain, so we provide a deep dive into the implications by comparing Filecoin to a company such as Box. This should show the profound implications. With Box, your data is owned and controlled by a third party that has access to your information (a photo loaded can be retrieved by anyone with access to Box servers). With Filecoin, your storage is distributed and decentralized, making the holders unable to retrieve your photo (they would need to hack every computer on the decentralized network). Your information is now secure and without your private keys, they cannot be

accessed. This is the first example for building a *"World Computer"* as we could apply the same concept to borrowing and contributing compute power.

At its core this is still an "if-then function", it is simply applied to computing. *If John contributes storage capacity, he will receive tokens; if John uses storage capacity, he burns tokens.* With the basics out of the way, here is the detailed example:

BOX and Filecoin

To illustrate the difference, we examine the data and file storage market in both centralized and decentralized environments: using Box (centralized) and Filecoin (decentralized), respectively.

Exhibit 1: Box vs. Filecoin

	Box	Filecoin
Team	~1,500 employees	11 employees
Capital Raise	$733 million	$205M Coin Offering
Technology	Centralized data sharing	Decentralized Storage Network
Security	Not-Trustless	Cryptography: zk-SNARKS
Governance	Executives and BOD	Consensus Protocol
Valuation	Traditional Stock Metrics	Adoption Cycle
Value Dilution	Limitless Capital Raise	Controlled issuance

Source: RBC Capital Markets, Filecoin, and Box SEC filings.

Under our basic framework, we highlight the advantages of Filecoin including lower start-up costs (open networked community) while being more scalable (employees per users, proof of spacetime), secure (trustless, consensus protocol), and potential for limitless computing power (unlimited miners).

Exhibit 2: Traditional Box Storage

Source: Bitcoin Stack Exchange.

Box: Box provides a Software-as-a-Service (SaaS) cloud content management platform that enables organizations to securely manage cloud content while allowing easy, access and sharing of its content. Box customers can collaborate on content both internally and with

external parties, automate content-driven business processes, develop custom applications, and implement data protection, security and compliance features to comply with internal policies and industry regulations. _Team:_ Box has ~1500 employees, according to its last 10K, with 16 members on its executive team. _Capital raises:_ $733m, including 11 rounds of A-G of $558m + IPO of $175m. _Technology:_ Centralized data sharing to web and mobile applications for cloud content management and a platform for developing custom applications, and a series of industry-specific solutions. _Security:_ Not-trustless. Central and encryption based, vulnerable to hacks on multiple points of potential failure. _Governance:_ Executives/board of directors. _Valuation:_ Tied to traditional valuation metrics (P/S, EV/EBITDA, etc.), investor sentiment, consensus estimates, broader equity markets. _Value dilution:_ Limitless capital raises.

Filecoin: Filecoin is a decentralized storage network that turns cloud storage into an algorithmic market. This market is powered by Blockchain technology with a native protocol token (Filecoin), which miners earn by providing storage to clients. Conversely, clients spend Filecoin hiring miners to store or distribute data.

Team: Filecoin has 11 core employees, also a part of Protocol Labs, with additional support from its open source community.

Capital raises: $205m in total via token sale.

Technology: Filecoin uses Decentralized Storage Network (DSN) protocol, a construction built on a blockchain and with a native token. Clients spend tokens for storing and retrieving data and miners earn tokens by storing and serving data. The Filecoin DSN handles storage and retrieval requests respectively via two verifiable markets: the Storage Market and the Retrieval Market. Clients and miners set the prices for the services requested and offered and submit their orders to the markets. The markets are operated by the Filecoin network, which employs Proof-of-Spacetime and Proof-of-Replication, used within the protocol to cryptographically verify that data is continuously stored in accordance with deals made.

New Blocks: Miners can participate in the creations of new blocks for the underlying blockchain. The influence of a miner over the next block is proportional to the amount of its storage currently in use in the network.

Security: Cryptographic building blocks use a collision resistant hash function CRH: $\{0,1\}* \rightarrow \{0,1\}O(\lambda)$, meaning it's hard to find two inputs that hash to the same output. Filecoin uses the collision resistant hash function MerkleCRH, dividing a string in multiple parts; construct a binary tree and recursively apply CRH and outputs the root. In addition, the company also implements zk-SNARKs, which allows verification to the correctness of computations without having to execute them and not even learning what was executed (zero-knowledge proof).

Governance: Similar to other blockchain tokens, Filecoin is proposing a useful work consensus protocol, where the probability that the network elects a miner to create a new block (or the voting power of the miner) is proportional to its storage currently in use (relative to the rest of the network). The protocol is designed such that miners would rather invest in storage than in computing power (like Ethereum) to parallelize the mining computation. Miners offer storage and re-use the computation for proof that data is being stored to participate in the consensus.

Value: Utility tied to the token. The better the application, the more miners and the more users as token value rises, in a virtuous cycle.

Value dilution: Controlled token issuance.

Exhibit 3: Filecoin Storage Example
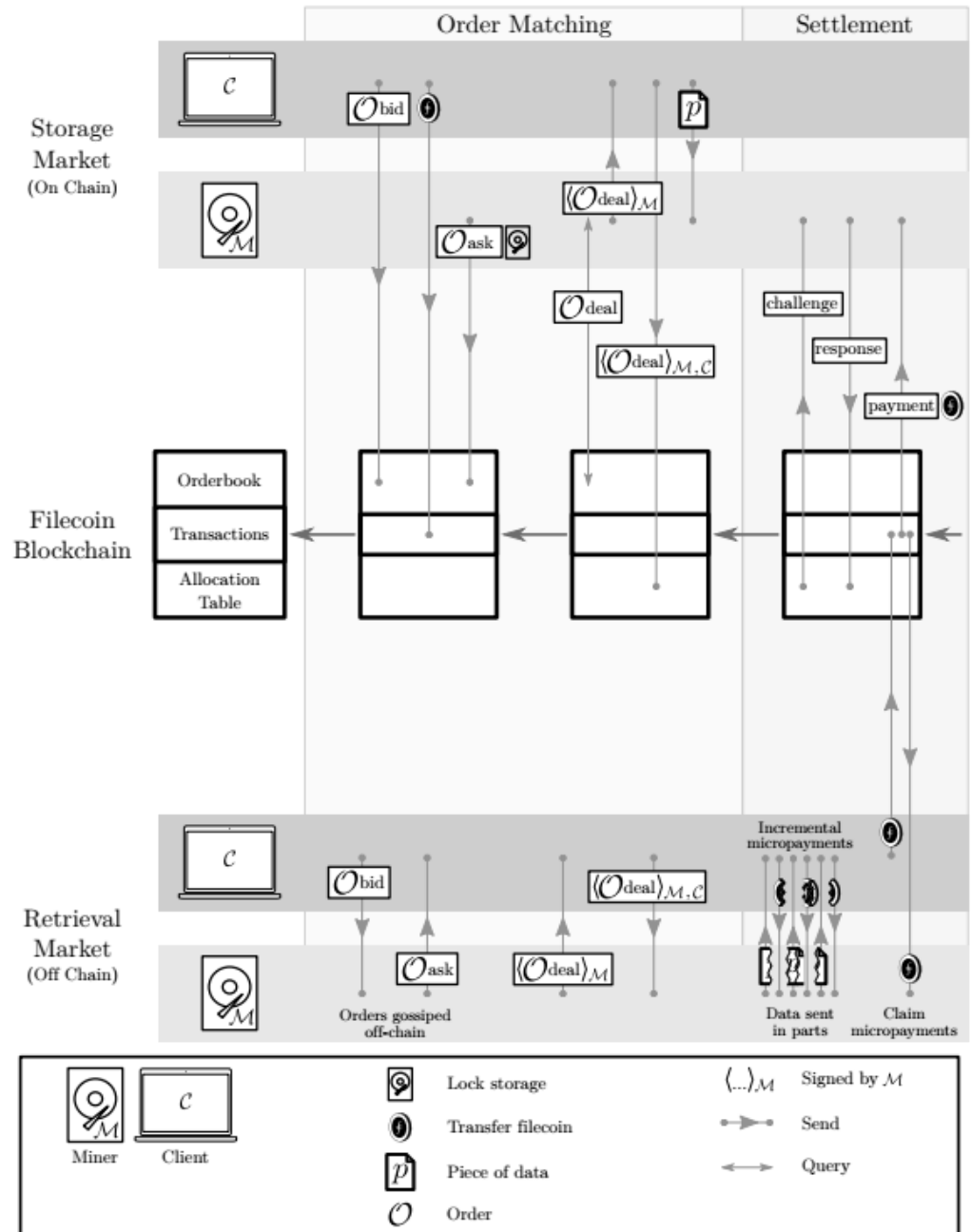
Source: Filecoin.

With the storage example explained, we could expand the use cases and imagine how individuals, companies and machines could rent processing power and communicate needs at significant speeds. A decentralized model would prevent access points for all of the data (photos as explained in the Filecoin example). While the technology is in nascent stages, IBM/Samsung have already built a washing machine that can order its own detergent using the Ethereum blockchain.

While there are several hundred Dapps being built on the Ethereum blockchain, we'll highlight a few. The vast majority of the 1,000+ crypto currencies are actually Dapps (start-ups) built on the Ethereum block chain. While it is unclear if any will succeed, below is a list of a few examples and clear use cases:

Golem – World Super Computer: This is a decentralized application for renting out your computing power. While many of us have multiple devices (desktops, laptops, phones, etc.), they are spending a large amount of time idling. This could be rented out using the Ethereum blockchain in a decentralized manner. In essence, Golem is a global, open sourced, decentralized supercomputer that anyone can access. It is made up of the combined power of a user's machines, from personal laptops to entire datacenters.

Basic Attention Token: This is another decentralized application to assign value to a user's attention. While we currently surf the internet using our IP addresses, TCP and finally viewing HTTP in the browser, if we go through the blockchain we can decentralize the platform and assign value to "attention". This would relate to the advertising space. Ad blockers would be enabled and an individual can then choose to see ads (click a switch) which then causes the company to pay out a small sum of tokens for each view. This would reverse the value chain compared to current advertising models.

Augur: This is a decentralized prediction market built on the Ethereum blockchain. It allows you to forecast events and be rewarded for predicting them correctly. When we think of the use of a fill function, online betting and prediction is one that comes to mind immediately. If two parties bet on the same event, the system can automatically push the reward to the winner.

Iconomi: ICONOMI Digital Assets Management Platform is a technical service that allows anyone from beginners to blockchain experts to invest in and manage digital assets. Given the complexity of managing digital assets, Iconomi intends to offer fast withdrawals and no contract lock-ins along with material amounts of liquidity.

How Does This Impact Compute: Recall, in mid-August an AI-infused computer beat a highly ranked professional gamer in Dota 2 (a complex video game). While the attention went to AI, we were most impressed by the amount of compute needed to succeed. This is significant for the future of blockchain/cryptography given that *the same amount of power could be garnered in a decentralized manner in the future*. A simple example would be GPU rentals needed to run AI or data sets when a large amount of information comes through the system (supply chain tracking for example). This is bullish for GPUs and computing in general as an individual or start-up company could access an enormous amount of compute power for a period of time without the need to build out a data center or rely on one central system.

Importantly, the speed of communication is critical for machine-to-machine communications. While 2-day clearing from accounts payable or 1-3 business day transactions are "good enough" for human communication, machines operate at much faster speeds where fractions of seconds can make a difference. By way of example, there is potential for Ethereum to clear 50,000-100,000 TPS in the next couple of years, which would already be on par with peak capacity of major credit card networks. If this type of speed continues to improve, machines could then communicate and trade resources at rapid speeds, improving efficiency in our everyday lives.

Microsoft Azure + AI Wins Dota 2: "*The bot's Artificial Intelligence (AI) learned the game from scratch through self-play. This is a feat of achievement for AI as Elon Musk states this is 'vastly more complex than traditional board games like chess & Go.' Shortly after it was announced that the AI bot won the tournament, Elon Musk also tweeted out his appreciation*

and thanks to Microsoft for using the Microsoft Azure cloud computing platform and its 'massive processing power' to win the tournament. This is a really great example of how the massive computing power of Microsoft Azure can be used; in addition to yet another stepping stone in the path towards much more advanced Artificial Intelligence (AI)." – BuildAzure.com - Chris Pietschmann

Security: The final key takeaway is if the outlined items occur, we could have a secure and private network that can be accessed worldwide - computing power, storage and communication at a materially faster speed without many security headaches. Overall, while we think Blockchain/cryptography is nascent, *we are bullish on the 10-year technology story*.

We are keeping this section a bit shorter as the key security feature is decentralization. Without a central entity to attack, the network (Bitcoin or other cryptocurrency networks) should remain secure (no point of entry).

With regard to Bitcoin, there are currently ~9,650 nodes in the world with ~27% located in the United States for the Bitcoin Network. Importantly, the cost of electricity is causing the process to be unprofitable in the United States and may increase issues in the future (centralization in China and other regions with lower electricity cost). While the number of nodes may be higher in the USA, the compute power due to the use of ASICs could centralize in certain areas if each node continues to add material amounts of compute power.

#2 Store of Value

The current market capitalization of gold is ~$8 billion and the total amount of capital held in offshore banking accounts was estimated to be around ~$21 trillion (according to 2013 study from the Guardian). Offshore tax havens include the Cayman Islands, Switzerland and several private banks. With a new digital store of value that cannot be seized, crypto currencies have unlocked a large market opportunity for the first viable use case: a store of value.

While technical details are provided later in this report, we can see the use case as material since the crypto currency now travels with you to any place with an internet connection: your phone to a laptop. This store of value cannot be seized without your private keys.

Using Bitcoin as an Example in Steps: 1) High net worth individual purchases Bitcoin. This Bitcoin is now loaded on the Blockchain and since he has opened his own digital wallet (without providing any of his personal information) he has the private keys; **2)** The address (or addresses) hold 1 Bitcoin as a basic example. That coin is now accessible in any part of the world with an internet connection; **3)** Since the coin is divisible into 1/100 millionth of a Bitcoin, the owner can send value in the form of fractions of pennies to the full coin ~$17,000 today; **4)** Since the information lives on the internet (blockchain), it is fully transportable. If the individual loses his phone and laptop, he can still access his funds with the use of his private key.

Finite Not Scarce: With the biggest item out of the way, store of value relative to offshore tax havens, the amount of bitcoin is finite at 21 million. Unlike gold, there will be less and less bitcoins issued until the supply cap of 21 million is hit in 2140. Gold, on the other hand, has actually seen an increase in supply on a year over year basis. This is important as gold is scarce but the amount of gold being pulled out of the ground has actually increased over time.

Exhibit 4: Over time, more gold is mined
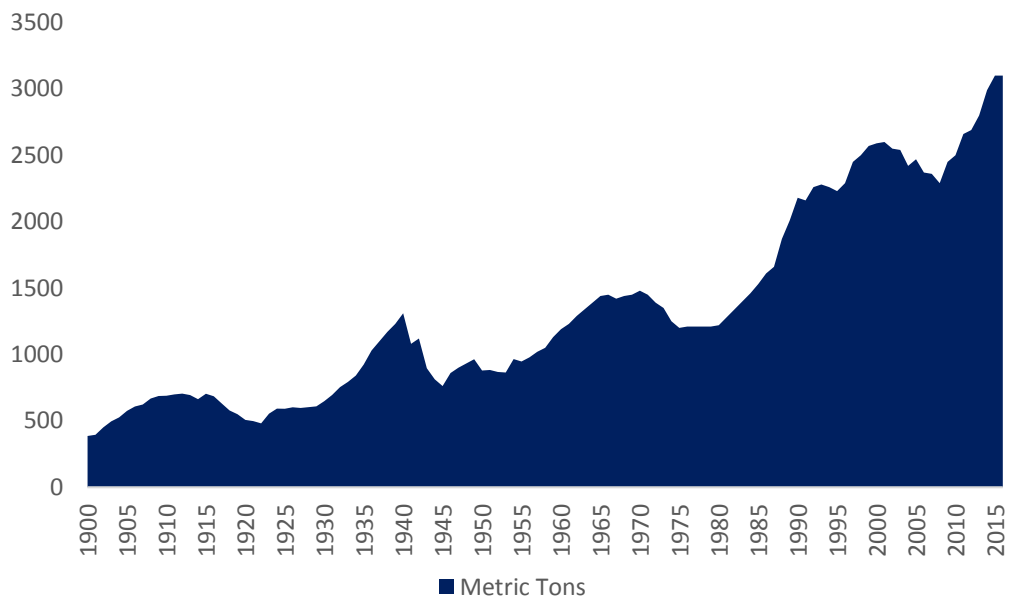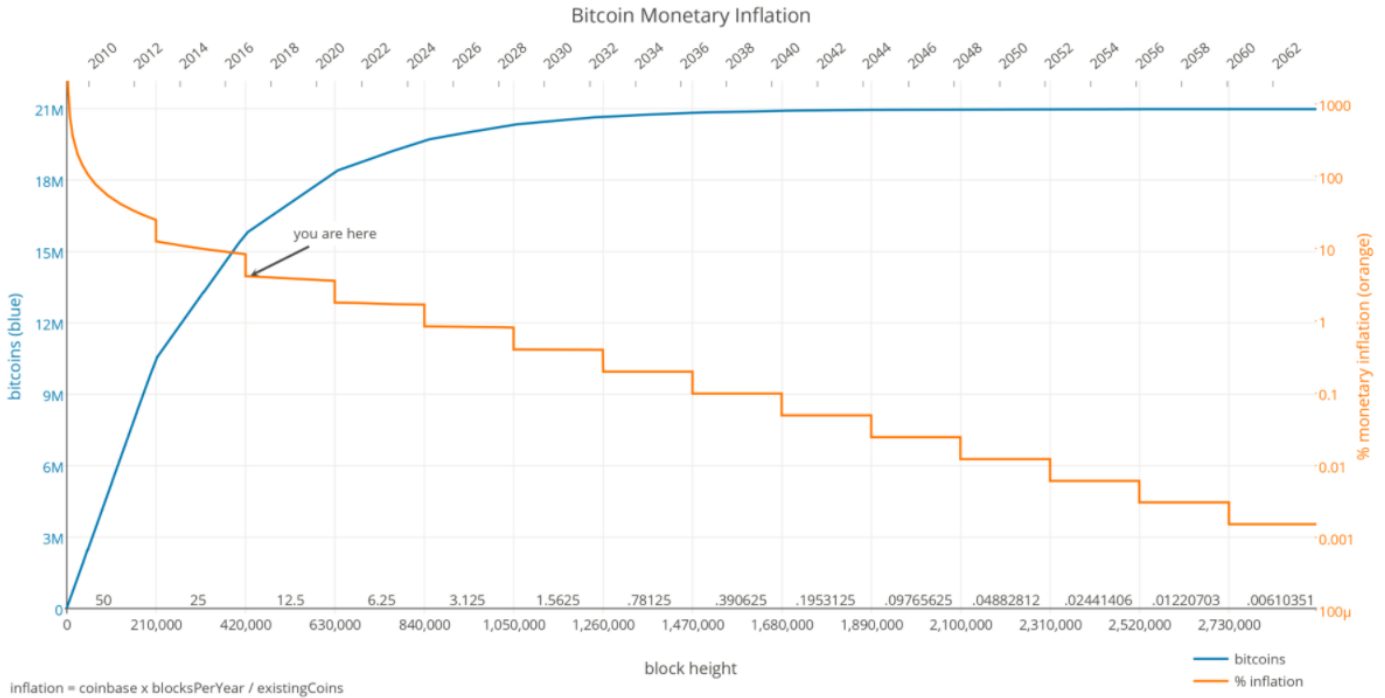

Source: Numbersleuth.org and Statistica.

We can compare this dynamic to the inflation rate of Bitcoin, which eventually reaches zero in the year 2140. This is an important distinction since there is a supply cap "finite" versus a scarce resource, which increases over time.

Exhibit 5: Over time less Bitcoin is issued until 21 million are released

Source: cointelegraph.com

#3 International Remittance

According to Pew Research Center, 582 billion US dollars were sent by relatives to family members in their home countries. While the exact number is difficult to track, the World Bank estimates the amount coming from each country.

With the use of crypto currencies, with an internet connection an individual, group or town can now have access to digital payments. This would not require a large ecosystem and could function with a smart phone or a dated laptop. Since Bitcoin is well known, we can use it again as an example in this case.

Example: A mother in Country A would like to send $100 to help her family in Country B. The typical transaction requires a middleman to convert the currencies from the fiat of Country A to the fiat of Country B. In the new crypto currency environment, the mother sends the crypto currency to the address of a family member in Country B. The crypto currency is received within a few seconds (or minutes) and can now be used by the family member.

In the first case, transaction fees and foreign exchange fees are applied. In the second case, using Bitcoin as an example, a small mining fee is used. While there are currently high mining fees as of today, this will likely be dramatically reduced with the lightning network deployment (covered later).

Beyond the Basics: With the layman's example out of the way, we can now extend this to supply chain management. If we were to take stock of all the items sitting around us (anyone reading this report in the US), we will likely find multiple items that were not manufactured in the United States (China, Mexico, etc.).

These companies that are creating the goods have to wait to receive payment for their work. This delay can last several days. Since crypto currencies can be sent rapidly and confirmed rapidly as well, it reduces the time from days to seconds.

We can then apply this logic to basic consulting services as well. If we would like to have a phone call, we can utilize the internet and have it done largely for free (cost of internet service); however, sending the person payment for their time would result in a time lag.
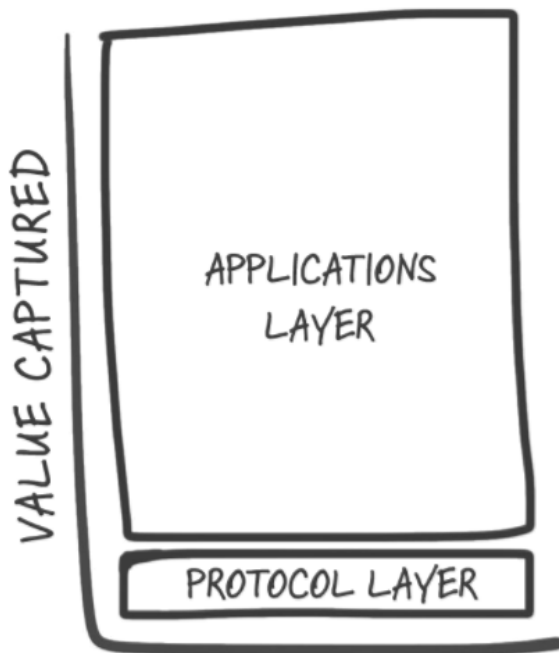
#4 Fat Protocols

With the real world example(s) out of the way, we see that the protocol layer will capture more value than the applications. As the application becomes successful, the protocol layer captures more value, which then creates more interest in additional Decentralized Application development. As an analogy, by owning the protocol layer, you are invested in "the network" versus a specific application on the network.

Centralized protocols such as TCP/IP (network/transport protocol), HTTP (application protocol), and SMTP (application/email protocol) have provided massive value to the applications that have emerged since. TCP/IP is an application of a complicated stack of network hardware while being a protocol for data transfer between computers. HTTP is a protocol for serving structured Web data and an application of TCP/IP. However, the protocols themselves are regarded as "thin", as monetization has occurred in a flourishing "fat" application layer built on the protocol. TCP/IP, HTTP, and SMTP have not gained value, but applications built on top such as leading internet companies have seen their value reach hundreds of billions of dollars.

Exhibit 6: Value Capture in Centralized Environment vs. Decentralized Environment

Current Centralized Environment   **Crypto Currency - Decentralized Environment**
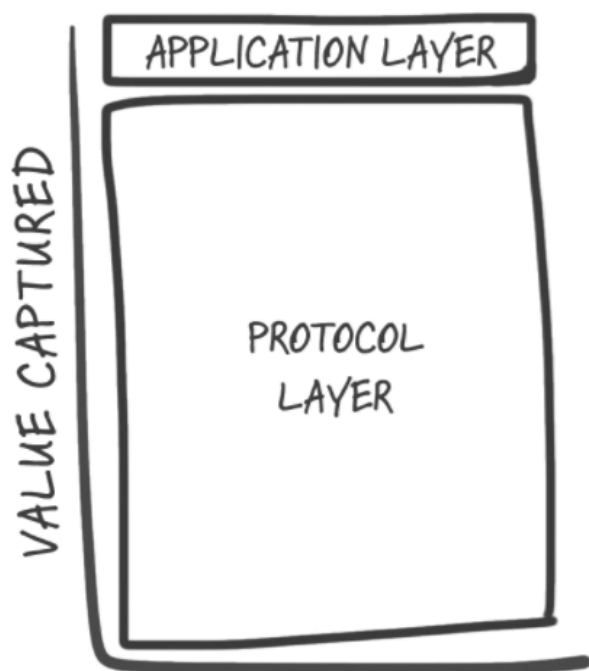
Source: Union Square Ventures.

In a Decentralized Web, "Fat" is a term for monetizable at the network level using "token-omics" as the application layer is "thin". In blockchain, you can own such valuable protocols. As an example, imagine any of these protocols being investable in the early 90's. In cryptography, investors can invest in protocol based tokens (potentially in favor of application based tokens), allowing for greater value capture on scalability.

One of the early successful examples are the DApps (Decentralized Applications) being built on top of the Ethereum protocol, which power smart contracts, as well as hyper-media/database protocols such as IPFS.

The Ethereum protocol was originally conceived as an upgraded version of a cryptocurrency, providing advanced features such as on-blockchain escrow, withdrawal limits, financial contracts, gambling markets and the like via a highly generalized programming language. The Ethereum protocol would not "support" any of the applications directly, but the existence of a Turing-complete programming language means that arbitrary contracts can theoretically be created for any transaction type or application.

According to stateoftheadpps, Ethereum has roughly 900 applications being built on top of it. Consequently, Ethereum has bootstrapped the smart contracts network. The illustration below shows the example that Ethereum and IPFS plays in the fat client stack.

Exhibit 7: Ethereum & IPFS

Source: BigChainDB.
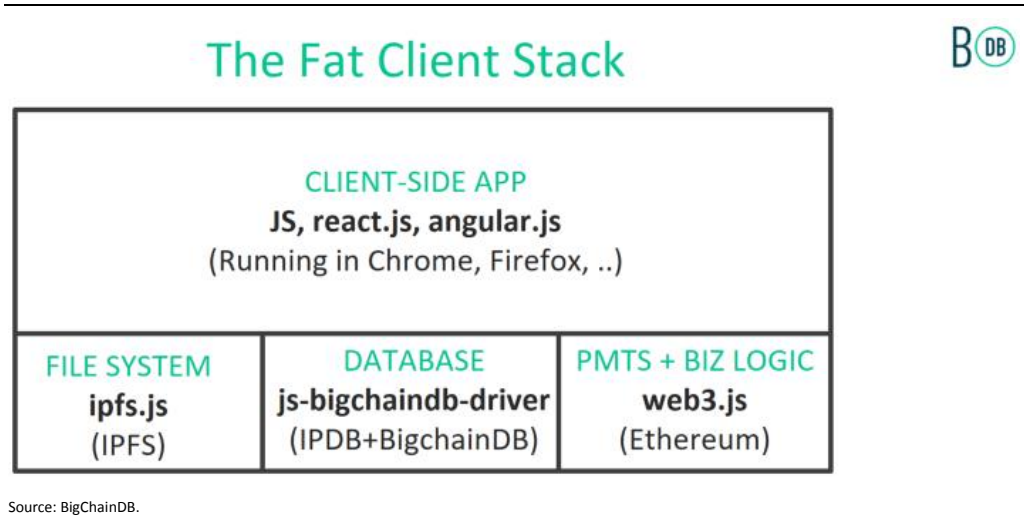
#5 Crypto Currency Mining

Crypto currencies use a process called "mining" which is essentially a reward system for confirming transactions. To keep the items high level, *miners use computing power to secure each crypto currency network and receive a reward (small amounts of the currency).* As a basic example: if person A buys a t-shirt from person B, this transaction needs to be confirmed and loaded to the Blockchain. To confirm this transaction a miner uses compute power to load the cryptographically secured transaction onto the ledger.

While this explanation is more than enough for high level understanding, a more complex answer is as follows: 1) Person A purchases an item from Person B using crypto currencies, 2) the transaction has a specific code attached to it that needs to be "guessed" through proof-of work to confirm the transaction, 3) the code is guessed correctly – the nonce, 4) the transaction is put onto the network and displayed to update the entire decentralized ledger on who owns which coins, and finally 5) block rewards are also given out by the system at a predetermined level to reward the miners in addition to their small fee for confirming transactions.

First Mining Process - Proof of Work

Notably, the process we have described above is called ***Proof-of-Work***. Proof-of-work requires large amounts of computing power. This type of algorithm is where the general population is building mining rigs to earn coins. We are starting here as it has the broadest public company implication and has been a notable piece of news/media over the past year.

Exhibit 8: Example of a cryptocurrency mining rig (GPU based) built by Mitch Steves

Source: RBC Capital Markets

To continue with the high-level section, another important item to be aware of is "what chips are used to mine the currency". In 2017, there was a significant amount of confusion in the industry as ASIC based coins (Bitcoin) were associated with Nvidia and AMD. To clarify this dynamic, below is a list of the major crypto currencies and how they are mined.

Notes: 1) for Coins that have the word ASIC, while you could use other chips (like a GPU), in most cases it could be significantly unprofitable – losing money to use anything besides an ASIC. This means the coins you receive would not cover electricity costs if you were to use a GPU instead of an ASIC; 2) for the Coins listed with the word GPU/CPU, the vast majority choose the GPU given that it is not profitable to use a CPU; and finally 3) the items with no chip/hardware associated with it use different algorithms to be covered towards the end of this section since it is less related to public technology companies.

Exhibit 9: List of currencies and their mining algorithms

Coin	Proof Type	Algo	Mining?	Max Hardware	Notes
Bitcoin	PoW	SHA256	Yes	ASIC	
Ethereum	PoW	Ethhash	Yes	GPU/CPU	
Bitcoin Cash	PoW	SHA256	Yes	ASIC	
Ripple	N/A		No		Proof of Correctness
DASH	PoW/PoS	X11	Yes	ASIC	
Litecoin	PoW	Scrypt	Yes	ASIC	
Open Trading Network	N/A		No		
Monero	PoW	Cryptonight	Yes	GPU/CPU	
Bitconnect	PoW/PoS	Scrypt	Yes	GPU/CPU	
NEO	N/A		No		Delegated BFT
NEM	PoI		No		Proof of Importance Vesting
IOTA	Tangle		No		
ETC	PoW	Ethhash	Yes	GPU/CPU	
EOS	DPoS		No		ERC-20Token
Omisego	PoS		No		ERC-20Token
Bitshares	PoS		No		
ZCash	PoW	Equihash	Yes	GPU/CPU	
LISK	DPoS		No		ERC-20Token
USDT	N/A	N/A	N/A	N/A	N/a
Gnonis	N/A	N/A	No		ERC-20Token
Stellar	PoS	N/A	No		
Waves	Leased PoS		No		
Stratis	PoW/PoS	X13	No		
Vertcoin	PoW	Lyra2RE	Yes	GPU/CPU	
Decred	PoW/PoS	BLAKE256	Yes	GPU/CPU	Hybrid PoW/PoS system
Bitcoin Gold	PoW	Equihash	Yes	GPU/CPU	

Source: Cryptocompare.

ASIC Based Coins: Bitcoin, Bitcoin Cash, Dash and Litecoin are mined with ASICs. This means the price upward should be a leading indicator for demand. If the price of these four currencies go up, we should see demand for ASICs increase. As an example, this would be a Bitmain S9 Antminer. The specific companies who should benefit include Xilinx and Cadence Design (chips made by Xilinx and tested by Cadence Design based on our research).

GPU Based Coins: Ethereum, Monero, Bitconnect, Ethereum Classic, zCash, Vertcoin, Decred and Bitcoin Gold are mined with GPUs. If the price of these eight crypto currencies increase in a material fashion, we should see an increase in the demand for AMD and Nvidia based GPUs. These algorithms require memory hard hashing which is why ASICs do not solve these mining dynamics in the future.

What is the ASIC TAM?

The ASIC TAM is significantly harder to calculate given that the market is rapidly evolving. New mining equipment is created every year. This "obsoletes" the value of the prior generation of miners. As an example, we'll use the S9 Antminer which has the following specifications:

1) **Hash Rate:** 12.93 TH/s ±5%
2) **Power Consumption:** 1275W ±7% (at the wall, with APW3, 93% efficiency, 25C ambient temp)
3) **Power Efficiency:** 0.098 W/GH ±7% (at the wall, with APW3, 93% efficiency, 25°C ambient temp)
4) **Rated Voltage:** 11.60 ~13.00V
5) **Chip quantity per unit:** 189x BM1387
6) **Dimensions:** 350mm(L)*135mm(W)*158mm(H)
7) **Cooling:** 2x 12038 fan
8) **Operating Temperature:** 0 °C to 40 °C
9) **Network Connection:** Ethernet
10) **Default Frequency:** 600M

With these metrics, we can create a minimum framework for the market opportunity at $*4.15 billion for mining equipment related to Bitcoin ASICs*. Importantly, we only looked at Bitcoin given that it is the largest crypto currency mined with ASICs (as a basic addition you could add ~$350-450M to the total if we wanted to include all ASIC based coins).

While we can compute these numbers, we think it is prudent to look at MGT Capital, a Bitcoin mining company run by John McAfee. On December 6, 2017, the company announced that it purchased 500 S9 Antmining rigs with shipment expected in 1Q2018. In total the company notes that it will have ~5,000 Bitmain S9s generating ~$4M in monthly revenue.

According to our rough math and pricing/Ebitda inputs provided in the company's press release, 5,000 Antmining rigs would result in ~$3.4M in monthly profit. We think this is largely in-line with the original press release given that the price appreciated by 20%. Back when it was released, the price of Bitcoin was around ~$13,000-14,000 per coin, which means the $14,500 price today is slightly higher, offset by a much larger network competing for the coins.

Exhibit 10: The Bitcoin Mining Market Opportunity from a High Level

Assumptions	
Bitcoin Price	$14,500
Block Reward	12.5
Network Rate (GH/s)	13,408,415,860
Block time (Divide)	600

Bitcoin Mining	S9 Ant Miner
GH/S Rate	12,930
Bitcoin Mined (day)	0.0017
Bitcoin Mined (year)	0.6336
Dollars (day)	$25.17
Dollars (year)	$9,186.59
Watts	1275
Cost KW/h	$0.10
Daily Cost	$3.06
Annual Cost	$1,116.90
Daily Profit	$22.11
Monthly Profit	$672.47
Annual Profit	$8,069.69

Mining Market	
Network Rate	13,408,415,860
Hash Rate of S9	12,930
Number of Miners	1,037,000
ASP of Miner	$4,000
Mining Revenue ($M)	**$4,148**
% Value to Chips	55%
Chip Opportunity ($M)	$2,281.40

Note: add 10-15% for all other ASIC coins.

Headline: The cost of the mining equipment creates a $3.5B opportuniy for ASIC miners (assuming all use high end equipment).

Additional Costs: This does not include: 1) cooling costs, 2) system/administration costs, 3) employees to ensure the data center is running and 4) cost of land/facilities and electrical costs.

Source: RBC Capital Markets, Bitmain Website and cryptocompare.

What is the GPU Cryptocurrency Mining TAM?

This is also a loaded question given the number of assumptions: 1) how many cryptocurrencies will be mined with GPUs in the future? - unknown, 2) will the value of cryptocurrencies sustain or grow allowing for a profitable mining rig? and 3) if the network rate increases dramatically, the economics could also diminish over time. As a quick example, we will use Cryptocurrency Ethereum to estimate a Total Addressable Market (the market could grow rapidly and the market could also go away).

Top Line:

- The current network hash rate is approximately 156,000 GH/s and the average hash rate of a 5 GPU mining rig is approximately 0.225 GH/S, meaning a total market so far of ~693K mining rigs. At an average price per rig of ~$2,700, this results in a total market of around $1.87B. Roughly a third is spent on GPUs alone, creating a ~$1.25 billion market.
- Finally, we note that this is only for Ethereum. If other crypto currencies become profitable (mining for Ethereum Classic or other currencies), the opportunity would be larger. This is a significant caveat given the run-up in prices of other GPU based coins mentioned earlier in this report
- To re-emphasize, the assumptions do not reflect the reality of Ethereum long-term. The amount to be mined will be flat and the algorithm is set to change (see follow up on page 18 "Could the TAM Go Away?")
- Notably, even if the algorithm changes, there are still many other large capitalization coins that require GPUs: Monero, Bitconnect, Ethereum Classic, zCash, Vertcoin, Decred and Bitcoin Gold are mined with GPUs.

Exhibit 11: Example of the opportunity

Assumptions	
Ether Price	$720.00
Block Reward	3
Network Rate (GH/s)	156,000
Block time (Divide)	15

	AMD Radeon Rx 580	GeForce GTX 1070	Difference
MH/S Rate (5 GPUs)	225	160	-28.9%
Ethers Mined (minute)	0.0000	0.0000	-28.9%
Ethers Mined (hour)	0.0010	0.0007	-28.9%
Ethers Mined (day)	0.0249	0.0177	-28.9%
Ethers Mined (year)	9.0969	6.4689	-28.9%
Dollars (minute)	$0.01	$0.01	-28.9%
Dollars (hour)	$0.75	$0.53	-28.9%
Dollars (day)	$17.94	$12.76	-28.9%
Dollars (year)	$6,549.78	$4,657.62	-28.9%
Watts	675	450	-33.3%
Cost KW/h	$0.15	$0.15	0.0%
Daily Cost	$2.430	$1.620	-33.3%
Annual Cost	$886.95	$591.30	-33.3%
Daily Profit	**$15.51**	**$11.14**	-28.2%
Annual Profit	**$5,662.83**	**$4,066.32**	-28.2%

Mining Rig Components	AMD Radeon Rx 580	GeForce GTX 1070
GPU ASP	$300	$400
# GPUs (5)	$1,500	$2,000
% of Cost	*68%*	*74%*
RAM	$20	$20
% of Cost	*1%*	*1%*
SSD	$50	$50
% of Cost	*2%*	*2%*
Power Supply	$200	$200
% of Cost	*9%*	*7%*
Motherboard/CPU	$300	$300
% of Cost	*14%*	*11%*
Mining Case + Cables	$100	$100
% of Cost	*5%*	*4%*
Cooling/Fan/Other	$25	$25
% of Cost	*1%*	*1%*
Total Cost	**$2,195**	**$2,695**
Break Even in Months	***4.7***	***8.0***

Source: RBC Capital Markets estimates and cryptocompare.com.

Could the TAM Go Away?

"This all sounds too good to be true… a breakeven in just four to six months? With pure profit following breakeven mark? What's the catch?"

The catch is that the entire opportunity could go to zero.

Potential Issues

- **Price:** If the price of Ethereum falls materially, the mining of ethers becomes unprofitable.
- **Block Reward or Block Time Change:** The block reward declines from 3 ether per 15 seconds. If the block reward were to change to 1 ether per 15 seconds (instead of 3), this would make the payback period 3x+ longer.
- **Higher Network Rate, Less Ethers for the Individual:** If the network rate increases, the same amount of Ethers needs to be split amongst a larger number of people. The number of Ethers received per GPU declines if the network rate goes up.
- **Built In Declines:** Ethereum is set up to move from "Proof of Work" to "Proof of Stake". To avoid technical terms, this means the algorithm will change (Casper). In the new algorithm, it is unclear if a GPU will be required. This transition is expected to happen by the end of the year (CY17). Finally, we note that there is potential for a "hybrid model" where GPUs would still be used and not see an immediate switch to Casper.
- **New Product for Mining:** Cryptocurrencies are not mined solely with GPUs. In the case of Bitcoin, a custom ASIC drives the mining process (GPU mining in your home would be unprofitable). If currencies require different chips/hardware, etc., the value of having a GPU miner declines. We think this is unlikely given that one of the primary concerns with bitcoin was the use of ASICs, which make it possible to take over more than 50% of the total hashing power (51% attack problem).

Exhibit 12: Example of the breakeven if the Block Reward goes to 1

Mining Rig Components	AMD Radeon Rx 580	GeForce GTX 1070
GPU ASP	$300	$400
# GPUs (5)	$1,500	$2,000
% of Cost	*68%*	*74%*
RAM	$20	$20
% of Cost	*1%*	*1%*
SSD	$50	$50
% of Cost	*2%*	*2%*
Power Supply	$200	$200
% of Cost	*9%*	*7%*
Motherboard/CPU	$300	$300
% of Cost	*14%*	*11%*
Mining Case + Cables	$100	$100
% of Cost	*5%*	*4%*
Cooling/Fan/Other	$25	$25
% of Cost	*1%*	*1%*
Total Cost	**$2,195**	**$2,695**
Break Even in Months	*20.3*	*33.6*

Source: RBC Capital Markets estimates and cryptocompare.com

What GPU is Best for Mining Ethereum?

"I've decided I want to build a miner and understand that I may lose the entire investment, what GPU offers the best potential return on investment?"

We think the quick answer is: AMD. If an individual can acquire an AMD GPU *at retail price,* the returns are the highest. The issue today is that AMD Rx 580s are being sold at a *premium* to retail prices today – out of stock. This creates a significant issue as 1) the longer a person must wait, the less likely the miner will be able to turn a profit (potential decline in block size, potential algorithm change etc.), and 2) a common mining rig requires ~4-6 GPUs multiplying the issue of both cost and time.

Potential Ramifications

- **Historical Issues:** Knowing that AMD GPUs offer the highest return for Ethereum miners, we think it is safe to assume that historical sales of GPUs for mining are skewed towards AMD. This implies that AMD would see a bigger impact from a sharp decline in the cryptocurrency mining market.
- This means that many of the GPUs sold by AMD are not being used for gaming given that they are the preferred GPU for mining.
- **Current Issues:** With AMD GPUs selling well above retail prices, this could temporarily drive up the demand for low-mid-end Nvidia GPUs such as the GTX 1070 (easier to get and prices are becoming more attractive).
- If the Market Grows: If GPU based cryptocurrency mining continues to be profitable (returns significantly higher than the cost), this could become a major long-term market.

In simple terms, if any cryptocurrency is profitable using a GPU based miner, the new OS will be downloaded and individuals will mine the new coin.

- **If the Market Collapses:** If the GPU mining market collapses, we could see an immediate oversupply scenario. Used GPUs could begin to flood the market.
- **Potential Long-term Ramification:** If the mining space continues to be lucrative, Nvidia and AMD could compete for market share within this segment (GPUs designed for mining). Given Nividia's history of offering lower power consumption products, we would not be surprised to see a new opportunity open for the company.

Can You Use an ASIC to Mine Ethereum?

Fake News! (hopefully you laughed). On a serious note, the algorithm is set up to prevent this from occurring. GPUs are used to mine Ethereum vs. ASICs (Bitcoin). Ethash is a "memory-hard algorithm", this means it is set up for GPU mining and is incompatible with an ASIC miner designed for Bitcoins. (Technical details can be found in the Ethereum White Paper, "A Next-Generation Smart Contract and Decentralized Application Platform".)

"The Bitcoin mining algorithm works by having miners compute SHA256 on slightly modified versions of the block header millions of times over and over again, until eventually one node comes up with a version whose hash is less than the target (currently around 2192). However, this mining algorithm is vulnerable to two forms of centralization. First, the mining ecosystem has come to be dominated by ASICs (application-specific integrated circuits), computer chips designed for, and therefore thousands of times more efficient at, the specific task of Bitcoin mining. This means that Bitcoin mining is no longer a highly decentralized and egalitarian pursuit, requiring millions of dollars of capital to effectively participate in. Second, most Bitcoin miners do not actually perform block validation locally; instead, they rely on a centralized mining pool to provide the block headers. This problem is arguably worse: as of the time of this writing, the top three mining pools indirectly control roughly 50% of processing power in the Bitcoin network, although this is mitigated by the fact that miners can switch to other mining pools if a pool or coalition attempts a 51% attack.

The current intent at Ethereum is to use a mining algorithm where miners are required to fetch random data from the state, compute some randomly selected transactions from the last N blocks in the blockchain, and return the hash of the result. This has two important benefits. First, Ethereum contracts can include any kind of computation, so an Ethereum ASIC would essentially be an ASIC for general computation - ie. a better CPU. Second, mining requires access to the entire blockchain, forcing miners to store the entire blockchain and at least be capable of verifying every transaction. This removes the need for centralized mining pools; although mining pools can still serve the legitimate role of evening out the randomness of reward distribution, this function can be served equally well by peer-to-peer pools with no central control" - A Next-Generation Smart Contract and Decentralized Application Platform (Ethereum White Paper)

Finally, given that the algorithm is expected to change "soon", with many anticipating sometime in 2018 we think the opportunity for Ethereum specifically will decline throughout the year. The first algorithm update will include a hybrid Proof-of-Work and Proof-of-Stake product and then switches (in theory) to Casper which is 100% Proof-of-Stake. At this time there is no major algorithm update expected for the other GPU based coins (continue with Proof-of-Stake and memory hard hashing).

What Are the Components of a GPU Miner?

While we provided the breakdown in the prior exhibits, the cost of a miner is approximately $2,000-3,000 with the bulk of the costs associated with the GPU (~66%). Importantly, if the market sees material growth, the mining equipment (not just the GPU) should see an increase in demand.

GPU (~66%) of Cost: This is relatively straight forward with Nvidia and AMD GPUs benefitting; **Mother Board/CPU (14%):** a standard Intel Mother board; **Power Supply (10%):** companies such as Corsair or EVGA power supply products; **RAM (1%):** Companies such as Kingston; **Solid State Drives (2%):** Companies such as Western Digital; **Other Costs (6%):** once all the equipment are in hand, the miner will need to connect all the products (cables) and create a basic case to keep all of the parts stable.

As a note, once the miner is complete, an operating system such as Windows is needed to login to the system. After logging into the new computer, GETH is installed (communication with the network) followed by 1) creating a wallet, 2) installing the mining software, and 3) officially starting the mining process.

Costs: The last component is costs. In order to run a miner, the user would need electricity and an internet connection. The primary cost of mining is ~$0.10-0.12 KW/h for electricity. Keeping it simple, as long as the revenue line (number of coins mined * price of coins mined) is larger than the total electrical costs, the miner should continue.

Now What is Proof of Stake?

One of the complaints of the Proof-of-Work model is the immense amount of computing power that is being used to secure the network. In the mainstream media we have seen multiple attacks on the electrical usage of the Bitcoin network in particular (with no mention of the electrical usage to find gold, diamonds and emeralds!).

Regardless of opinions, the electrical usage to secure the network is quite high and a new solution called "Proof-of-Stake" is attempting to secure the network without the use of immense computational power.

The concept of Proof-of-Stake is complex and the best way to understand it is through game theory. If we validate blocks based on the number of coins they have "at stake", this incentivizes the owner to only validate legitimate blocks. How are they incentivized? Well, if they validate an _incorrect block, their entire stake is removed instantly_. Since the nodes will be decentralized and distributed, it should prevent an individual from validating incorrect blocks.

This move to Proof-of-Stake from Proof-of-Work is topical in the Ethereum network given that the algorithm change is expected to occur at the end of 2018 (Casper). While we believe it will be delayed again, this is the current expectation given that it was originally set to launch in early 2018.

Delegated Byzantine Fault Tolerance

A Byzantine fault is any fault presenting different symptoms to different observers. This results in loss of service due to a system that requires consensus. This created the Byzantine Generals Problem highlighted in 1982.

"Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in

terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors." - The Byzantine Generals Problem by Leslie Lamport, Robert Shostak, and Marshall Pease, 1982.

Delegated Byzantine Fault Tolerance is the third idea for validating blocks.

In this environment, we have a Blockchain. Every single person using this Blockchain gets to choose their "delegate" leaders. If the delegate does a poor job, the users get to vote in a different delegate. At all times the delegate must publicly display each command and place it on the public ledger. Over time the commands lead to new rules and features that want to be added to the blockchain.

In order to decide if these rules or features are added, a delegate decides to "speak" to the community and message a proposal. This proposal is then spread across to all delegates and the new changes are passed if 66% of the delegates agree on the idea. If the number comes in at under 66%, it does not function and must be started all over again.

While this is a basic example, this type of mining already exists with a crypto currency called NEO.

Exhibit 13: NEO Delegated Byzantine Fault Tolerance
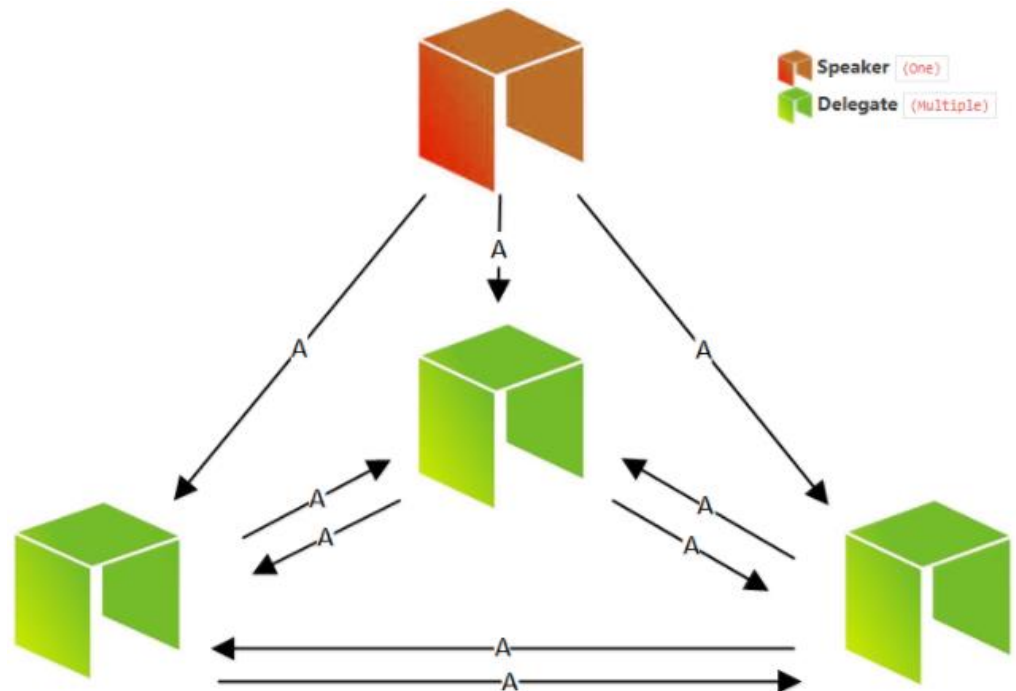
Source: NEO.org.

#6 Improved scaling

One of the largest issues with Blockchain protocols is lack of scalability. This addresses the *"when can I buy coffee with crypto currencies?"* problem. Scalability applies to the well-known crypto currencies at this time.

What the problem is - security and immutability at the cost of scalability: The ability to scale on-chain is limited as every fully run node in the network must process every transaction while maintaining a copy of every state. In traditional centralized database architectures, systems can scale with more computing power to accommodate higher throughput and lower latency (they grow at a more linear rate). However, in decentralized architecture, the number of transactions the blockchain can process is only equal to that of a single node that is participating in the network. Also, given that decentralized architecture operates from node to node, additional nodes that join the network is at risk to actually weaken and/or slow the network. Thus, while the decentralization has its many perks including security and immutability, it comes at the cost of scalability.

Exhibit 14: Average Block Size Over time (It's Getting Crowded!)
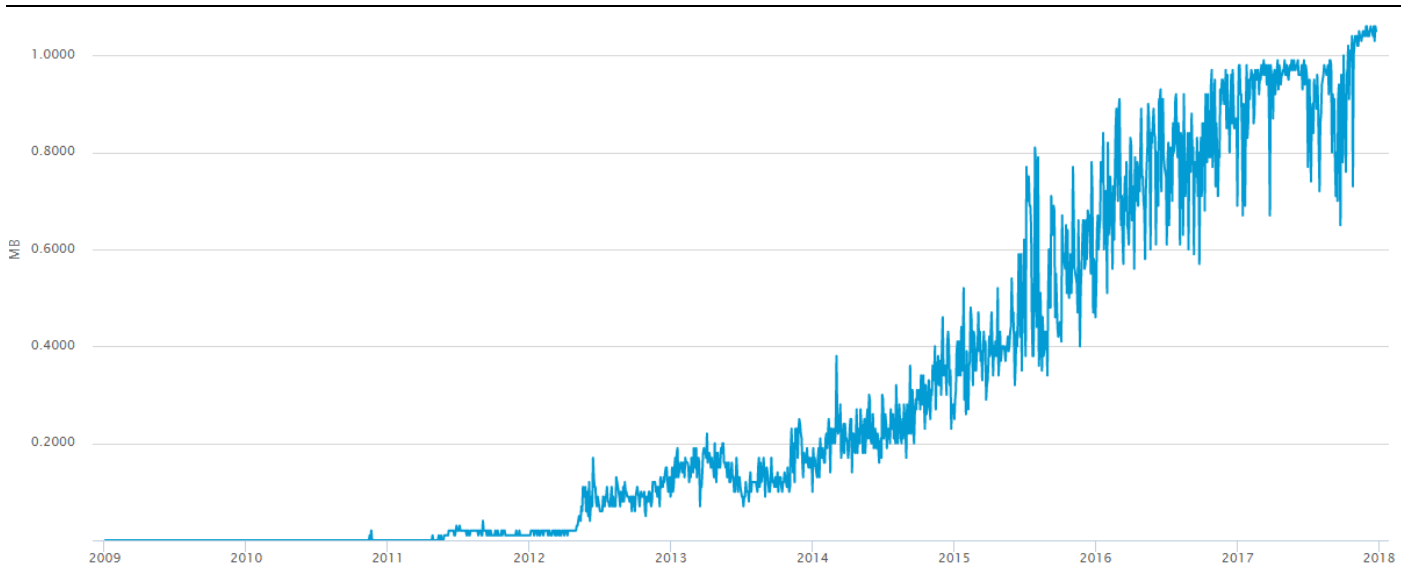
Source: Blockchain.info

Using Bitcoin as an Example: In examining Bitcoin's slow latency, recall that transactions are formed together into a block. This block is then chained to other blocks, and added to the network at the rate of 10 minutes per block. Each block is 1MB, and the average transaction is 250bytes; thus, each block can hold ~4200 transactions. At 10min rate per block, this works out to be ~7 Tx/sec. As Bitcoin has become more popular, block size has increased materially towards its full 1.0MB size. Due to the larger blocks, we have seen a material increase in the transaction cost as well.

Exhibit 15: Total Transaction Fees (It's Getting Expensive!)
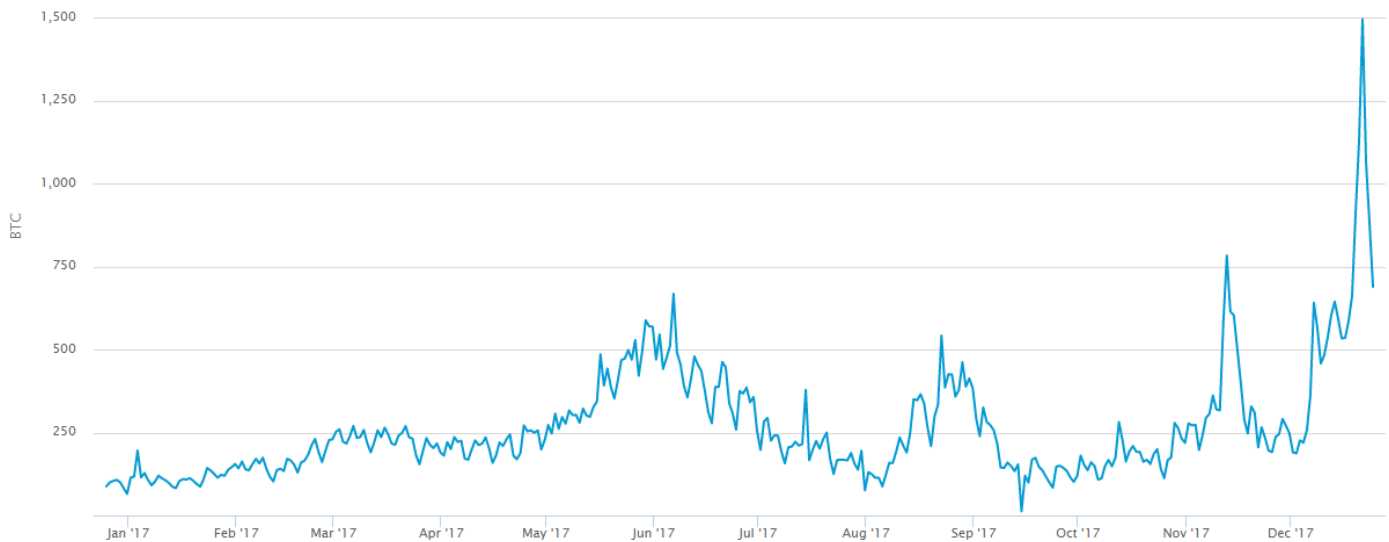
Source: Blockchain.info

On-chain scaling vs. Off-chain scaling: In the case of Bitcoin, the issue of scaling has produced two camps, those who were opposed to increased block size (Bitcoin) and those who were in favor of it (Bitcoin Cash). The debate has existed inside Bitcoin for years. During the New York Agreement in May 2017, there was an agreed upon upgrade option which ultimately led to Segregated Witness (SegWit). The solution was to segregate witness (signature) from the Tx to save space in the block. It was an upgrade that fixed many Bitcoin bugs and also opened the opportunity for future scaling via the Lightning Network. However, a group of miners did not agree to the solution, which resulted in a fork, or chain split, and Bitcoin Cash, which supported an 8MB block size.

Exhibit 16: Segregated Witness
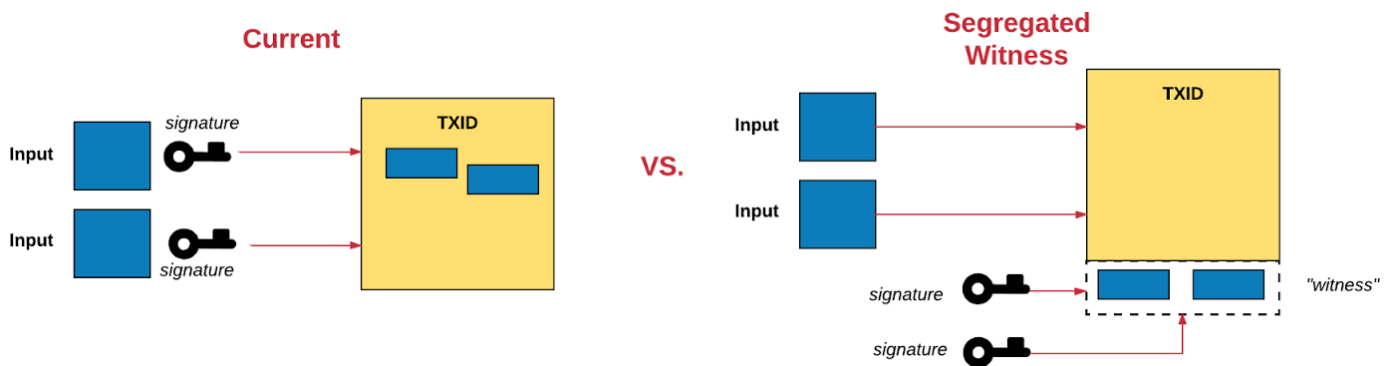
Source: Hackernoon.

Bitcoin could also increase its block size from 1MB to 2MB longer-term. Ultimately, however, we view on-chain scaling (including hard forks) as not a part of the larger solution as ongoing network congestion would still persist.

Off-chain with Lightning appears promising: There have been multiple solutions proposed to address scaling. The most promising appears to be with off-chain scaling at Lightning Labs, directed by Elizabeth Stark. In building a secondary network (or a Layer 2), in parallel to

blockchain, transaction congestion is kept off the corresponding on-chain network, allowing more transactions without stressing out the main chain.

Lightning Network transactions operate "off-chain" involving a small group of nodes (vs. all nodes in "on-chain") that link sender and receiver, think Alice and Bob in the illustration below. These nodes are linked through "payment channels" established on the underlying blockchain, which could be Bitcoin, Litecoin, etc. These channels are created when two participants assign funds on-chain into an entry, which requires both parties to sign off in order to move funds to/from the entry.

Exhibit 17: Example of lightning network

Source: lightning.engineering

This requires a single on-chain blockchain transaction. Opening and closing channels are the only Lightning Network actions which require broadcasting a transaction to the blockchain.

Exhibit 18: Channel Example

Source: lightning.engineering

These channels are to be considered virtual payment tubes that connect peers inside the network. Recall this is different vs. traditional on-chain scaling as when a typical on-chain Bitcoin transaction is transmitted and verified then stored by many thousands of nodes, this has resulted in significant fees and delays for users.

Lightning's implementation is thus far focused on Bitcoin (primary) and Litecoin (secondary). However, Lightning is also testing atomic swaps, which would allow cross-chain payment channels, think Bitcoin to Litecoin. Lightnings' latest development has been an alpha .3 release for the Bitcoin Testnet. The community is still working towards its mainnet release. *Lightning's core developers Thaddeus Dryja and Joseph Poon estimate that transactions could scale to many millions of Tx/sec.* As a basic explanation, other networks are scaling at a linear rate while the improved bitcoin network may grow at an exponential rate. If this is the case, we should see a material inflection rate (knee in the curve) where scalability is no longer an issue.

As we can see from the exhibit below, if a system can grow at an exponential rate versus a linear rate, the intersection results in material changes in growth. Even if we have a steep linear growth of 10x, 20x or even 40x, when the exponential growth intersects with the linear line we see a rapid divergence in scalability.

Exhibit 19: Knee in the Curve … Y-Axis represents transactions, X Axis represents unit of time
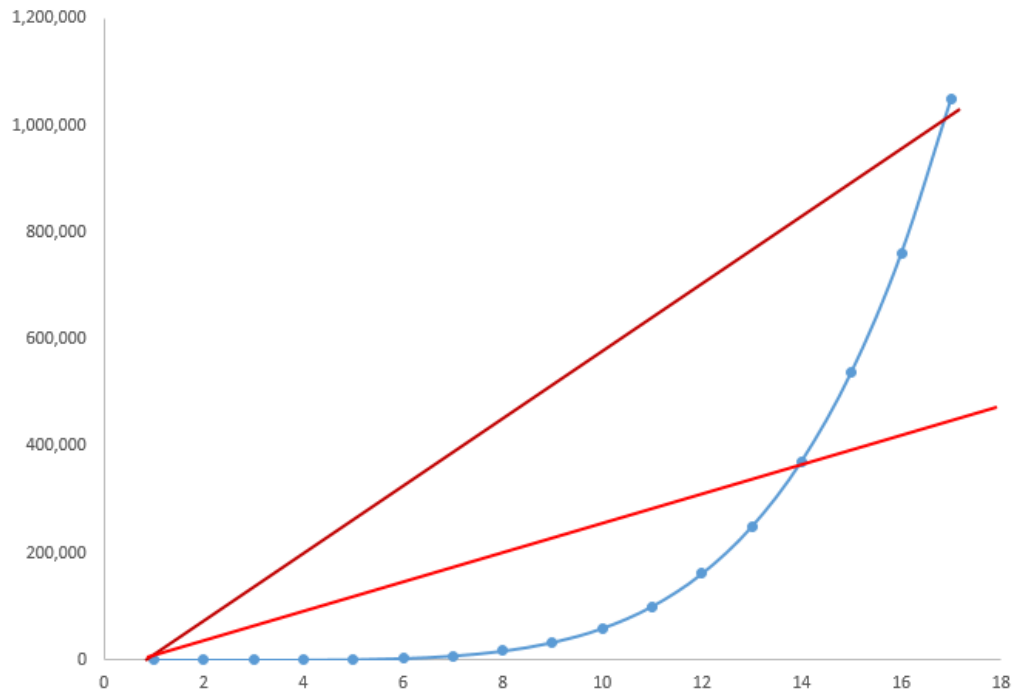
Source: RBC Capital Markets

Risks and Uncertainty

Many Risks: *1) Government Intervention:* if crypto currencies are stolen, the government has no incentive to catch the criminal - not backed, *2) Wallet Hacking:* computers are already being hacked to steal compute power, we think smartphone wallet hacking is the next major risk, *3) Scalability:* while the issues are being solved over time, processing transactions instantly without high mining fees is an issue and is still a debate point, *4) Privacy:* public display of transactions reduces privacy, making all transactions transparent, *5) 51% Attack:* if a single central entity were to obtain over 50% of the compute power, the network could be attacked, and *6) Coordinated Attacks:* there is risk of large scale manipulation to approve malicious forks or price manipulation of a coin.

1) Government Protection: If crypto currencies are stolen, the government has no incentive to catch the criminal, in our view, given that it is not protected or backed by a government or entity. If an individual wrote his private keys onto a piece of paper (which was subsequently stolen), a thief could then drain 100% of his account. It would then be up to the government to decide if the person should be prosecuted.

In addition, governments could decide that crypto currencies are illegal. While it would be incredibly difficult to stop a crypto currency from functioning (need to shut down the internet) by making it illegal, the acceptance could stall or stop entirely. In this scenario, making wallets and exchanges inaccessible would create a difficult and illegal environment where on and off ramps are removed (fiat/crypto changes).

2) Wallet Hacking: While the Blockchain has not been hacked, the third party providers of wallets (malware on smartphones), exchanges (Mt. Gox) have resulted in significant amounts of theft. We think this is a significant risk going forward as more and more hackers attempt to steal and unwind wallets that are not secure.

Example 1: If an individual decides to open his own wallet on his desktop or laptop and the private keys are displayed on his screen, he has already put himself in a compromised position. If the private keys are displayed on the screen, the malware could take a screen shot of these words and his account could be drained in the future.

Example 2: If an individual holds his crypto currencies on a smartphone, the entire value could also be drained if his phone is hacked. As an example, in a Copay wallet, the crypto currencies are held on an application on a user's phone. If someone unlocks and accesses the phone, all of the funds could then be sent instantly to another address … draining his or her account.

Example 3: Similar to Mt. Gox, there are exchanges that buy and sell crypto currencies. These exchanges are global and include: Bitfinex, GDAX, Coinbase, Bithumb, Bittrex, Binance and many more. With large amounts of money being held in these accounts, we think there is potential risk for yet another hack similar to Mt.Gox which could drain the value of thousands (or millions) of accounts.

3) Scalability: While the issues are being solved over time, processing transactions instantly without high mining fees is an issue. While we are bullish on the potential to scale due to lightning network (essentially IOUs) and Atomic Swaps (instant crypto to crypto exchange without an entity), the development is in early days and has several hurdles to jump over at this time.

Similar to when emails and storage devices came along, the debate was if it would be possible to send videos and pictures via the internet. Fast forward 15 years from the year

2001 and not only were we able to send the messages, but we were able to do so from a device that sits in the palm of our hands! To dampen our enthusiasm here, doing the same in a decentralized environment requires significant upgrades and changes to the ecosystem.

4) Privacy: The public display of transactions reduces privacy, making all transactions transparent. While this is not the case for all crypto currencies, knowing that the transactions cannot be edited and cannot be changed reduces privacy for any user of crypto currencies.

5) 51% Attack: If a single central entity were to obtain over 50% of the compute power, the network could be attacked. In this scenario, using a quantum computer for example, the blockchain could be unwound. While a hard fork could be issued to solve the problem, a 51% attack could result in severe damage to any blockchain based ecosystem.

6) Coordinated Attacks: Since the security of the network is based on Proof-of-Work, Proof-of-Stake or Delegated Byzantine Fault Tolerance, there is risk for collusion. Specifically, if a large number of nodes, computers or speakers decide to validate incorrect blocks, the system could devalue quickly.
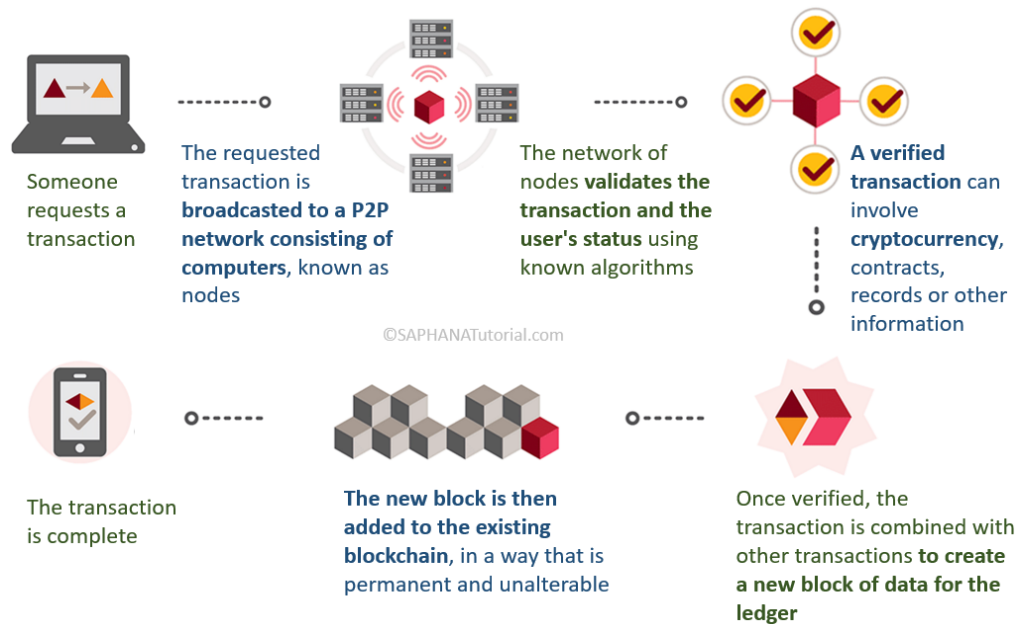
What is a Blockchain?

The blockchain is a cryptographically secured and shared distributed and decentralized ledger. A blockchain is a distributed and decentralized database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. This is significantly different from a centralized database given that it is open for all to see (public). In order to attack the network, one would have to attack all computers on a network that is spread around the world versus in a single data center or centralized a distributed ecosystem.

The value of a blockchain is that it enables a shared database without a central administrator (disintermediation). Rather than having some centralized application, blockchain transactions can have their own proof of validity and authorization to enforce the constraints.

A blockchain is a technology to efficiently record transactions, with key advantages being disintermediation, decentralized, distributed, programmable, verifiable, divisible, immutable, and with faster and lower cost to data.

Exhibit 20: Blockchain Technology Overview

Someone requests a transaction

The requested transaction is **broadcasted to a P2P network consisting of computers**, known as nodes

The network of nodes **validates the transaction and the user's status** using known algorithms

A verified transaction can involve **cryptocurrency**, contracts, records or other information

©SAPHANATutorial.com

The transaction is complete

The new block is then added to the existing blockchain, in a way that is permanent and unalterable

Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger**

Source: Seemit

Key advantages:

- **Decentralized model - no central point of failure, highly scalable:** A distributed model is used to move away from a single point of failure, as we currently have in centralized web 2.0 infrastructure. In centralized architecture, all the data is a unified body that is stored on one computer. In decentralized architecture, there is no central storage, and some servers provide information to the clients. The servers are connected with each other. In a distributed model, there are no data storages and all the nodes contain information. The clients are equal and have equal rights. Under this framework in blockchain, there are many replicas of the blockchain database and no one owns it. In fact, the more replicas there are, the more authentic and secure it becomes. A decentralized database is difficult to hack, to be manipulated, or otherwise disrupted as it requires the attacker to go after all of the computers on the decentralized network.

Exhibit 21: Centralized, Decentralized and Distributed
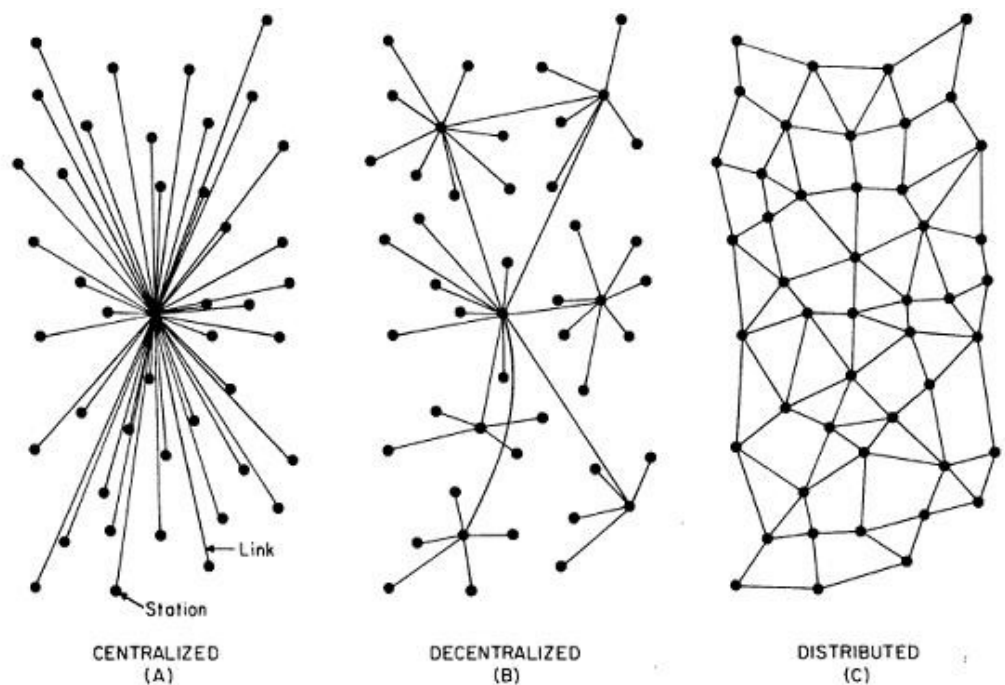
Source: Medium - Saurabh Goyal

- Blockchain networks are peer-to-peer without a single point of failure. The result is a highly scalable network. Since centralized systems follow a single framework, they do not have diversity, and evolve slowly.

- **Consensus - governance through code:** Blockchain security is built on consensus (and node participants). On a blockchain network, there is no centralized authority that determines the transaction order. Instead, many validating peers (nodes) implement the network consensus protocol. Consensus ensures that a quorum of nodes agree on the order in which the transactions are appended to the shared ledger. There are a few primary methods of finding consensus in a blockchain, and all distributed systems: the practical byzantine fault tolerance algorithm (PBFT), the proof-of-work algorithm (PoW), the proof-of-stake algorithm (PoS), and the delegated proof-of-stake algorithm (DPoS).

Exhibit 22: Examples of Consensus

Source: Cybercom Group.

- **Cryptographically authentic - use of hash to sign and validate:** Uses public/private signature technology that is the backbone of e-commerce and digital signatures. One analogy is similar to the username/e-mail and passwords for online accounts and portals; the username/e-mail will be public and passwords will be private. In the same way, in digital currencies, wallet address is your public key and the private key is the one that lets you authorize the transactions.

Exhibit 23: Cryptographically Authenticated
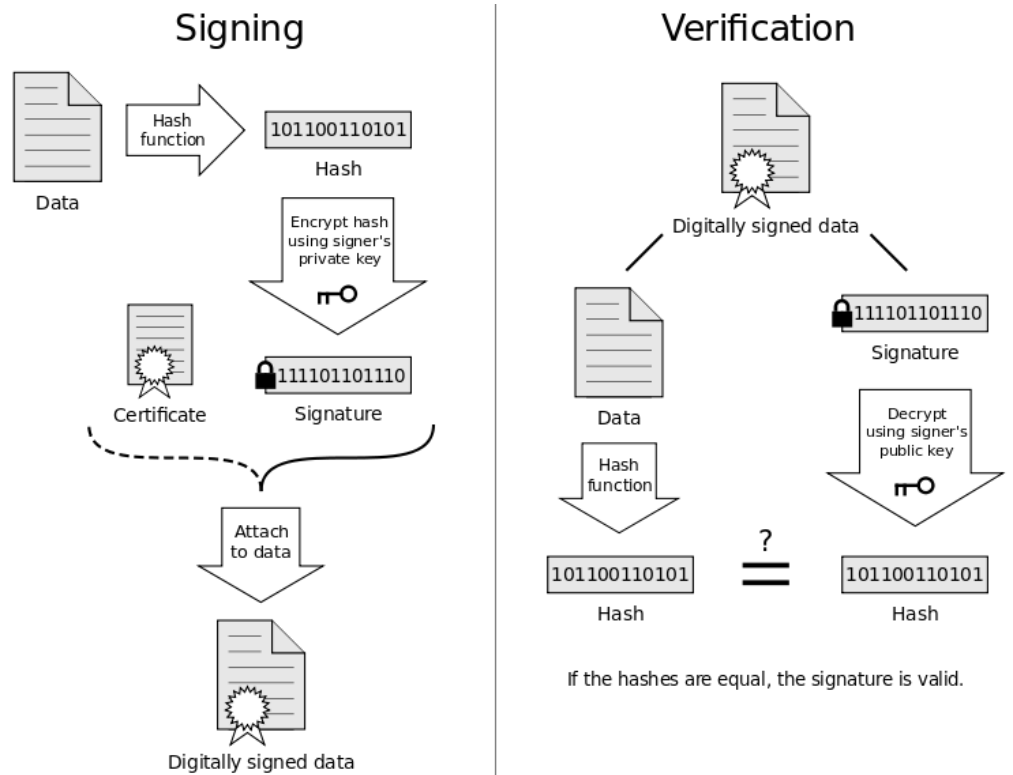
Source: Wikimedia

- **Ledger/Auditable - immutable:** The database is a write-once and read-many database, so it is an immutable record of every transaction that occurs. There is no update or delete like in a traditional database. Just as in accounting, if a mistake is made on the ledger, it cannot be erased. A compensating transaction must be posted to correct the

mistake. So there is nowhere to hide. The example below illustrates the move from the genesis block (green) to the current block. *"Blocks in the main chain (black) are the longest series of blocks that go from the genesis block (green) to the current block. Purple blocks are blocks that are not in the longest chain and therefore not used."* (Source: Bitcoin Wiki for color example).

Exhibit 24: Ledger Example

Source: Bitcoinwiki.

Bitcoin Was the First Blockchain Application: In 2008, an individual or group writing under the alias of Satoshi Nakamoto published an 8-page white paper entitled *"Bitcoin: A Peer-To-Peer Electronic Cash System".* This was the first blockchain application. The paper describes a peer-to-peer (P2P) version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution. The definition of a Bitcoin is a "chain of digital signatures". Bitcoin was the first proof of concept.

Satoshi's main argument addresses that buying and selling goods over the internet relies on financial institutions that act as 3rd parties to process financial transactions; or is dependent upon the 2 parties trusting a 3rd party to process their transaction (allowing for a transaction reversal). As the third party is delegated to facilitate the transaction, they spend time resolving disputes and dealing with fraud; this proves to be costly, in addition to time consuming.

The proposition was a P2P framework, or a set of interconnected computers, which work together, where an electronic cash system could be created. This P2P cash system, avoids the aforementioned problem of double spending (performing two transactions with one coin simultaneously) by using hashing and proof-of-work.

Abstract: *"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone."*

The paper was broken down into several key sections. We cover the premise of transactions, time stamp, proof of work, network and incentives:

- **Transactions - problem arises with double spending:** whereby each owner transfers the coin to the next owner by digitally signing a hash of the previous transaction and the public key of the next owner; and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership. However, this is problematic as it could lead to people "double spending" their digital currency.

Exhibit 25: Transaction Example
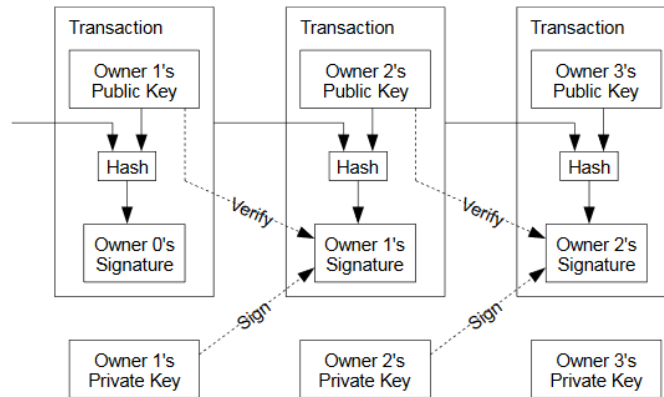
Source: "Bitcoin: A Peer-To-Peer Electronic Cash System" – Satoshi Nakamoto

- **Timestamp Server - the solution to double spending:** In order to solve the problem of double spending, the goal was to use a timestamp. The timestamp server is a piece of software that is used to digitally timestamp data. The server takes a small section of the transaction data (or a hash) and timestamps it. This time stamped hash is then made publicly available for everyone to see. The existence of this time stamped hash therefore proves that the transaction exists and is therefore valid.

Exhibit 26: TimeStamp Server
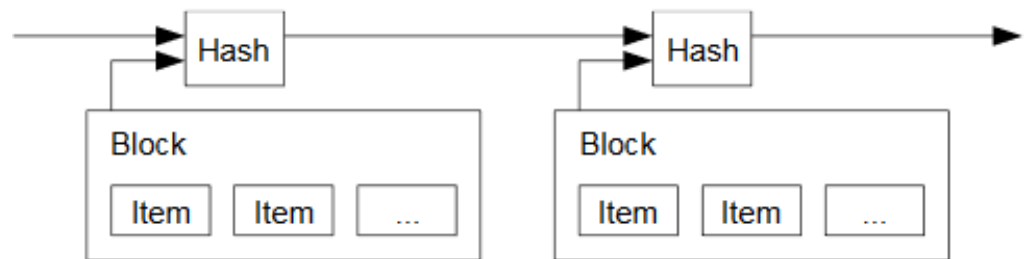
Source: "Bitcoin: A Peer-To-Peer Electronic Cash System" – Satoshi Nakamoto

- **Proof of work - validation of work through solving hash puzzles:** A proof-of-work system has to be used in order to implement the timestamp server across a network of computers (nodes). Proof-of-work is in a sense validation, and requires proof that a specified amount work has been done by the system. The completion of the work is rewards (or Bitcoins). This process of solving hash puzzles essentially locks the transactions (or resulting blocks) within the blockchain. At this point, it is nearly impossible to reverse a set of transactions (unlock a block), as the work done to solve the hash puzzle would have to be undone, meaning a miner would also have to do work on the whole chain to undo a single block.

Exhibit 27: Validation Example
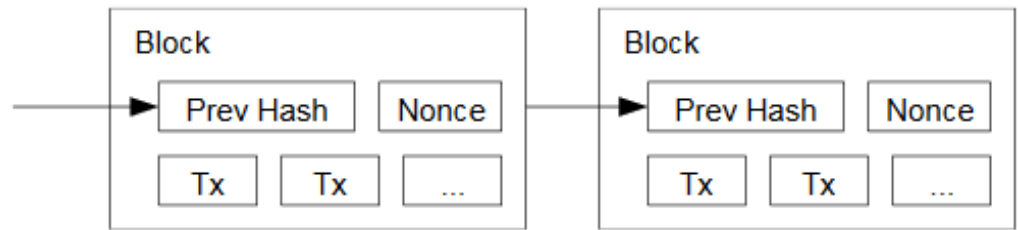
Source: "Bitcoin: A Peer-To-Peer Electronic Cash System" – Satoshi Nakamoto

- **Network - structure and process:** There were six primary rules including: 1) new transactions are broadcast to all nodes; 2) each node collects new transactions into a block; 3) each node works on finding a difficult proof-of-work for its block; 4) when a node finds a proof-of-work, it broadcasts the block to all nodes; 5) nodes accept the block only if all transactions in it are valid and not already spent; 6) nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

- **Incentives - Bitcoins and transaction fees:** Nodes, and their corresponding miners, are rewarded in bitcoins and transaction fees. The first transaction in a block creates a new coin, which is owned by the person (node) who created that particular block. This incentivizes people to use their computers (nodes) and connect to the Bitcoin network to help process Bitcoin transactions.

To complete the Bitcoin example, the following are high-level explanations of each level.

A Miner: A Bitcoin miner is essentially a banker/accountant updating the ledger. Computers are set up all over the world to update the ledger and process each transaction. The miner (computer) is constantly updating the Blockchain (ledger) by confirming each transaction.

Block Reward: Since the miners are contributing resources (computing power), they are given a reward. This reward currently stands at roughly 12.5BTC every 600 seconds. To keep it simple, assume that the amount of compute power contributed is equal to the amount of the reward. If two miners were on the network with the exact same compute power, they would win 50% of the block reward.

The amount of time for a new reward to be released is called the block time (600 seconds)

The amount of coins distributed is the block reward (12.5BTC) in this example

Network Hash Rate: This represents the number of miners on the network contributing resources. If the Network hash rate is 10 and goes to 20, this means the amount of compute power being used has doubled. Importantly, this does not mean that there are exactly "10 miners" or exactly "20 miners".

If one miner contributes half of the computing power (10) and 10 miners contribute the other half (1 each), there are 11 miners on the network creating a combined hash rate of 20.

Limited Supply: The last item to add is the built in limited supply. Since the number of coins released is fixed (and actually decreases over time), the maximum number of Bitcoins allowed to be mined is 21 million. This limit is written into the code and cannot be altered/changed at any time.

## Putting the Bitcoin and Blockchain Concept Together

The most common use case would be a long distance international transaction. If Person A lives in Canada and would like to send money to Person B in China, the currency would need to be converted. In the case of Bitcoin, a conversion is unnecessary.

A standard international transaction would require an intermediary. Person A sends Canadian dollars to Person B. When the money arrives, Person B now needs to convert the currency. When the currency is converted into Chinese Yuan, the exchange (bank for example) confirms the transaction happened.

Standard Currency Example: Canadian Dollar - > Centralized Exchange to Confirm -> Yuan Delivered

Bitcoin Example: Bitcoin -> Decentralized network confirms -> Bitcoin at new address

Exhibit 28: A Full Bitcoin Transaction
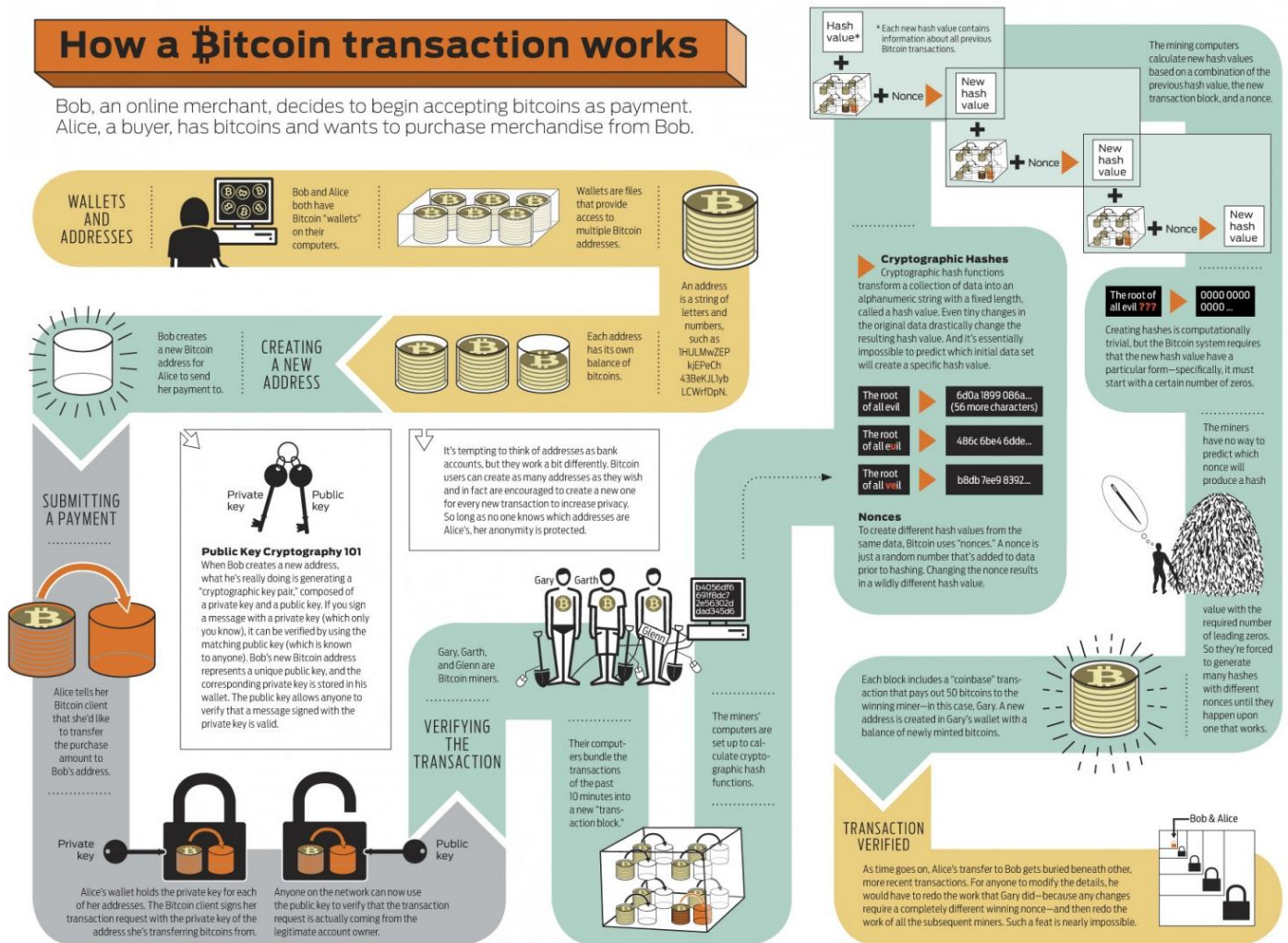
Source: IEEE Spectrum

Required disclosures

Conflicts disclosures

The analyst(s) responsible for preparing this research report received compensation that is based upon various factors, including total revenues of the member companies of RBC Capital Markets and its affiliates, a portion of which are or have been generated by investment banking activities of the member companies of RBC Capital Markets and its affiliates.

Distribution of ratings

For the purpose of ratings distributions, regulatory rules require member firms to assign ratings to one of three rating categories - Buy, Hold/Neutral, or Sell - regardless of a firm's own rating categories. Although RBC Capital Markets' ratings of Top Pick(TP)/ Outperform (O), Sector Perform (SP), and Underperform (U) most closely correspond to Buy, Hold/Neutral and Sell, respectively, the meanings are not the same because our ratings are determined on a relative basis (as described above).

			Investment Banking Serv./Past 12 Mos.	
Distribution of ratings				
RBC Capital Markets, Equity Research				
As of 31-Dec-2017				
Rating	Count	Percent	Count	Percent
BUY [Top Pick & Outperform]	868	52.42	281	32.37
HOLD [Sector Perform]	683	41.24	155	22.69
SELL [Underperform]	105	6.34	8	7.62

Conflicts policy

RBC Capital Markets Policy for Managing Conflicts of Interest in Relation to Investment Research is available from us on request. To access our current policy, clients should refer to
https://www.rbccm.com/global/file-414164.pdf
or send a request to RBC Capital Markets Research Publishing, P.O. Box 50, 200 Bay Street, Royal Bank Plaza, 29th Floor, South Tower, Toronto, Ontario M5J 2W7. We reserve the right to amend or supplement this policy at any time.

Dissemination of research and short-term trade ideas

RBC Capital Markets endeavors to make all reasonable efforts to provide research simultaneously to all eligible clients, having regard to local time zones in overseas jurisdictions. RBC Capital Markets' equity research is posted to our proprietary website to ensure eligible clients receive coverage initiations and changes in ratings, targets and opinions in a timely manner. Additional distribution may be done by the sales personnel via email, fax, or other electronic means, or regular mail. Clients may also receive our research via third party vendors. RBC Capital Markets also provides eligible clients with access to SPARC on the Firms proprietary INSIGHT website, via email and via third-party vendors. SPARC contains market color and commentary regarding subject companies on which the Firm currently provides equity research coverage. Research Analysts may, from time to time, include short-term trade ideas in research reports and / or in SPARC. A short-term trade idea offers a short-term view on how a security may trade, based on market and trading events, and the resulting trading opportunity that may be available. A short-term trade idea may differ from the price targets and recommendations in our published research reports reflecting the research analyst's views of the longer-term (one year) prospects of the subject company, as a result of the differing time horizons, methodologies and/or other factors. Thus, it is possible that a subject company's common equity that is considered a long-term 'Sector Perform' or even an 'Underperform' might present a short-term buying opportunity as a result of temporary selling pressure in the market; conversely, a subject company's common equity rated a long-term 'Outperform' could be considered susceptible to a short-term downward price correction. Short-term trade ideas are not ratings, nor are they part of any ratings system, and the firm generally does not intend, nor undertakes any obligation, to maintain or update short-term trade ideas. Short-term trade ideas may not be suitable for all investors and have not been tailored to individual investor circumstances and objectives, and investors should make their own independent decisions regarding any securities or strategies discussed herein. Please contact your investment advisor or institutional salesperson for more information regarding RBC Capital Markets' research.

For a list of all recommendations on the company that were disseminated during the prior 12-month period, please click on the following link: https://rbcnew.bluematrix.com/sellside/MAR.action

The 12 month history of SPARCs can be viewed at https://www.rbcinsightresearch.com.

Analyst certification

All of the views expressed in this report accurately reflect the personal views of the responsible analyst(s) about any and all of the subject securities or issuers. No part of the compensation of the responsible analyst(s) named herein is, or will be, directly or indirectly, related to the specific recommendations or views expressed by the responsible analyst(s) in this report.

Third-party-disclaimers

The Global Industry Classification Standard ("GICS") was developed by and is the exclusive property and a service mark of MSCI Inc. ("MSCI") and Standard & Poor's Financial Services LLC ("S&P") and is licensed for use by RBC. Neither MSCI, S&P, nor any other party involved in making or compiling the GICS or any GICS classifications makes any express or implied warranties or representations with respect to such standard or classification (or the results to be obtained by the use thereof), and all such parties hereby expressly disclaim all warranties of originality, accuracy, completeness, merchantability and fitness for a particular purpose with respect to any of such standard or classification. Without limiting any of the foregoing, in no event shall MSCI, S&P, any of their affiliates or any third party involved in making or compiling the GICS or any GICS classifications have any liability for any direct, indirect, special, punitive, consequential or any other damages (including lost profits) even if notified of the possibility of such damages.

References herein to "LIBOR", "LIBO Rate", "L" or other LIBOR abbreviations means the London interbank offered rate as administered by ICE Benchmark Administration (or any other person that takes over the administration of such rate).

Disclaimer

RBC Capital Markets is the business name used by certain branches and subsidiaries of the Royal Bank of Canada, including RBC Dominion Securities Inc., RBC Capital Markets, LLC, RBC Europe Limited, Royal Bank of Canada, Hong Kong Branch and Royal Bank of Canada, Sydney Branch. The information contained in this report has been compiled by RBC Capital Markets from sources believed to be reliable, but no representation or warranty, express or implied, is made by Royal Bank of Canada, RBC Capital Markets, its affiliates or any other person as to its accuracy, completeness or correctness. All opinions and estimates contained in this report constitute RBC Capital Markets' judgement as of the date of this report, are subject to change without notice and are provided in good faith but without legal responsibility. Nothing in this report constitutes legal, accounting or tax advice or individually tailored investment advice. This material is prepared for general circulation to clients and has been prepared without regard to the individual financial circumstances and objectives of persons who receive it. The investments or services contained in this report may not be suitable for you and it is recommended that you consult an independent investment advisor if you are in doubt about the suitability of such investments or services. This report is not an offer to sell or a solicitation of an offer to buy any securities. Past performance is not a guide to future performance, future returns are not guaranteed, and a loss of original capital may occur. RBC Capital Markets research analyst compensation is based in part on the overall profitability of RBC Capital Markets, which includes profits attributable to investment banking revenues. Every province in Canada, state in the U.S., and most countries throughout the world have their own laws regulating the types of securities and other investment products which may be offered to their residents, as well as the process for doing so. As a result, the securities discussed in this report may not be eligible for sale in some jurisdictions. RBC Capital Markets may be restricted from publishing research reports, from time to time, due to regulatory restrictions and/ or internal compliance policies. If this is the case, the latest published research reports available to clients may not reflect recent material changes in the applicable industry and/or applicable subject companies. RBC Capital Markets research reports are current only as of the date set forth on the research reports. This report is not, and under no circumstances should be construed as, a solicitation to act as securities broker or dealer in any jurisdiction by any person or company that is not legally permitted to carry on the business of a securities broker or dealer in that jurisdiction. To the full extent permitted by law neither RBC Capital Markets nor any of its affiliates, nor any other person, accepts any liability whatsoever for any direct or consequential loss arising from any use of this report or the information contained herein. No matter contained in this document may be reproduced or copied by any means without the prior consent of RBC Capital Markets.

Additional information is available on request.

To U.S. Residents:
This publication has been approved by RBC Capital Markets, LLC (member FINRA, NYSE, SIPC), which is a U.S. registered broker-dealer and which accepts responsibility for this report and its dissemination in the United States. Any U.S. recipient of this report that is not a registered broker-dealer or a bank acting in a broker or dealer capacity and that wishes further information regarding, or to effect any transaction in, any of the securities discussed in this report, should contact and place orders with RBC Capital Markets, LLC.

To Canadian Residents:
This publication has been approved by RBC Dominion Securities Inc.(member IIROC). Any Canadian recipient of this report that is not a Designated Institution in Ontario, an Accredited Investor in British Columbia or Alberta or a Sophisticated Purchaser in Quebec (or similar permitted purchaser in any other province) and that wishes further information regarding, or to effect any transaction in, any of the securities discussed in this report should contact and place orders with RBC Dominion Securities Inc., which, without in any way limiting the foregoing, accepts responsibility for this report and its dissemination in Canada.

To U.K. Residents:
This publication has been approved by RBC Europe Limited ('RBCEL') which is authorized by the Prudential Regulation Authority and regulated by the Financial Conduct Authority ('FCA') and the Prudential Regulation Authority, in connection with its distribution in the United Kingdom. This material is not for general distribution in the United Kingdom to retail clients, as defined under the rules of the FCA. RBCEL accepts responsibility for this report and its dissemination in the United Kingdom.

To German Residents:
This material is distributed in Germany by RBC Europe Limited, Frankfurt Branch which is regulated by the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

To Persons Receiving This Advice in Australia:
This material has been distributed in Australia by Royal Bank of Canada - Sydney Branch (ABN 86 076 940 880, AFSL No. 246521). This material has been prepared for general circulation and does not take into account the objectives, financial situation or needs of any recipient. Accordingly, any recipient should, before acting on this material, consider the appropriateness of this material having regard to their objectives, financial situation and needs. If this material relates to the acquisition or possible acquisition of a particular financial product, a recipient in Australia should obtain any relevant disclosure document prepared in respect of that product

and consider that document before making any decision about whether to acquire the product. This research report is not for retail investors as defined in section 761G of the Corporations Act.

To Hong Kong Residents:

This publication is distributed in Hong Kong by Royal Bank of Canada, Hong Kong Branch, which is regulated by the Hong Kong Monetary Authority and the Securities and Futures Commission ('SFC'), RBC Investment Services (Asia) Limited and RBC Investment Management (Asia) Limited, both entities are regulated by the SFC. Financial Services provided to Australia: Financial services may be provided in Australia in accordance with applicable law. Financial services provided by the Royal Bank of Canada, Hong Kong Branch are provided pursuant to the Royal Bank of Canada's Australian Financial Services Licence ('AFSL') (No. 246521.)

To Singapore Residents:

This publication is distributed in Singapore by the Royal Bank of Canada, Singapore Branch, a registered entity granted offshore bank licence by the Monetary Authority of Singapore. This material has been prepared for general circulation and does not take into account the objectives, financial situation, or needs of any recipient. You are advised to seek independent advice from a financial adviser before purchasing any product. If you do not obtain independent advice, you should consider whether the product is suitable for you. Past performance is not indicative of future performance. If you have any questions related to this publication, please contact the Royal Bank of Canada, Singapore Branch. Royal Bank of Canada, Singapore Branch accepts responsibility for this report and its dissemination in Singapore.

To Japanese Residents:

Unless otherwise exempted by Japanese law, this publication is distributed in Japan by or through RBC Capital Markets (Japan) Ltd. which is a Financial Instruments Firm registered with the Kanto Local Financial Bureau (Registered number 203) and a member of the Japan Securities Dealers Association ("JSDA").