NERA
ECONOMIC CONSULTING

29 March 2018

Cryptocurrencies: Fundamentals, Developments, and Regulation

By **Dr. Airat Chanyshev***

This paper presents a review of theoretical foundations of blockchains and cryptocurrencies together with a discussion of recent market developments and regulatory responses. A simplified description of the cryptographic math is in the Appendix.

What Is a Currency?

A currency is usually associated with the following qualities: medium of exchange, store of value, and unit of account.

Primitive forms of money included sea shells, cattle, tobacco, and other goods. Tobacco leaves, for example, were used as currency as recently as the 17th century in Virginia and North Carolina. The actual tobacco was later substituted with tobacco warehouse receipts.[1]

Coins were invented independently in ancient China and ancient Greece. China later introduced paper currency, which was described by Marco Polo in the 13th century as a great invention:

> With these pieces of paper... [Kublai Khan] causes all payments on his own account to be made; and he makes them to pass current universally over all his kingdoms and provinces and territories, and whithersoever his power and sovereignty extends. And nobody, however important he may think himself, dares to refuse them on pain of death. And indeed everybody takes them readily, for wheresoever a person may go throughout the Great Kaan's dominions he shall find these pieces of paper current, and shall be able to transact all sales and purchases of goods by means of them just as well as if they were coins of pure gold. And all the while they are so light that ten bezants' worth does not weigh one golden bezant.[2]

**Dr. Airat Chanyshev has a PhD in mathematics from Moscow University and MBA in finance from the Wharton School.*

The US dollar (USD) went through several periods of convertibility, first to silver and then to gold, but has been a fiat currency since 1973.

Bitcoin (BTC), the first cryptocurrency to gain acceptance, is a private (no sovereign issuer) and decentralized (no issuing body) currency. It is similar to a fiat currency in that it is not convertible into any commodity.[3] It is similar to cash in that individuals can transact in bitcoins directly, without an intermediary. Bitcoin has advantages over paper currency: transactions can be done remotely, bitcoins cannot be counterfeited, and they cannot be stolen because Bitcoin addresses are protected by cryptographic protocols.

Similar to paper currency, electronic cash can still be lost; if you lose your password (your ”keys”), then there is no mechanism to retrieve your holdings. In fact, it is estimated that a large share of all bitcoins—between 17% and 23%—may have been lost already, mostly in the early days of the network when bitcoins had little value.[4]

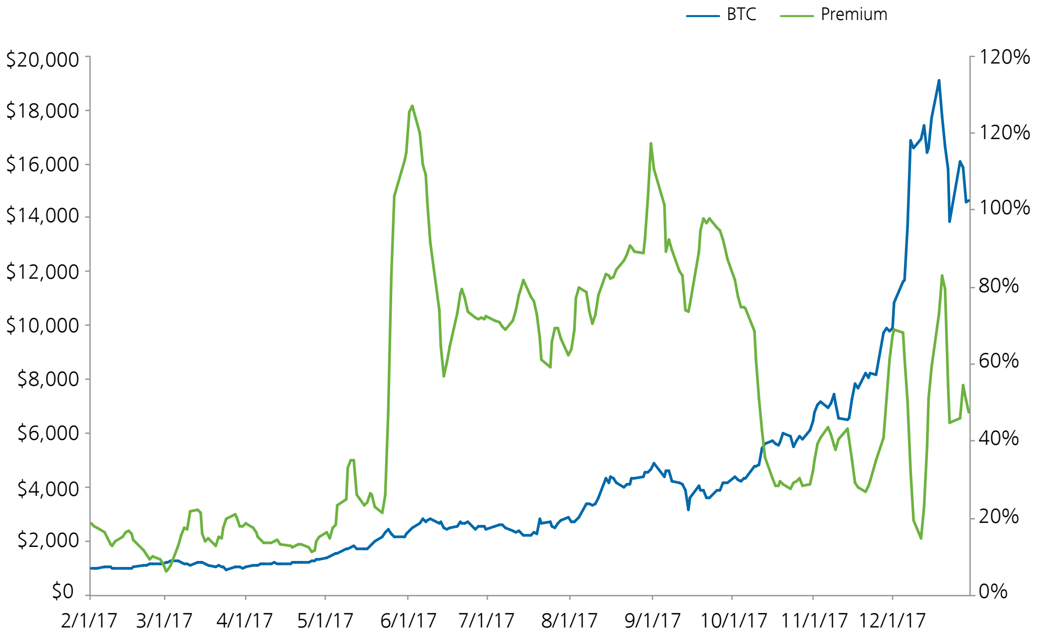
While cryptocurrencies have features of ordinary currencies to some extent, and some retailers accept bitcoins as a form of payment, much of the current demand for cryptocurrencies is not based on their use as a medium of exchange or store of value.

The figure below is an illustration of the extraordinary demand for bitcoins. It shows the price of bitcoins and the premium over bitcoins charged for the right to hold it through Bitcoin Investment Trust (GBTC). GBTC’s bitcoin holdings are the only asset of the Trust, and each share of the Trust is supported by 0.092 bitcoins. If, say, the price of a bitcoin is $1,000, the value of bitcoins in one share of the Trust would be $92. However, GBTC has been valued significantly higher than the value implied by its bitcoin holdings.

As stated on GBTC’s website:

> [GBTC] enables investors to gain exposure to the price movement of bitcoin through a traditional investment vehicle, without the challenges of buying, storing, and safekeeping bitcoins.[5]

Figure 1. **BTC Price and GBTC Premium over BTC (2017)**



Source: Polymath, "Cryptocurrency Market Capitalizations," https://coinmarketcap.com; Nasdaq, "Bitcoin Investment Trust Historical Stock Prices," Nasdaq, http://www.nasdaq.com/symbol/gbtc/historical.

If Bitcoin is overvalued, as many believe it is, then GBTC is even more overvalued. The convenience of holding bitcoins indirectly through GBTC has a premium of up to 100% (plus the 2% annual management fee charged by the Trust).

What Is a Blockchain?

A "blockchain" is simply a list of every single transaction since the very first one. For example, as of December 2017, the Bitcoin blockchain was approximately 150 gigabytes in size and contained 280 million transactions.[6] It is public; anybody (theoretically) can see and check all the records. It is called a blockchain for the following reasons.

1. New transaction records are added not individually, but in blocks. New blocks are constantly being added. As of December 2017, the Bitcoin blockchain consisted of about 500,000 blocks.[7]

2. All blocks are consecutively numbered and inseparably "chained" together by a cryptographic algorithm.

The blockchain is supported by a decentralized peer-to-peer network of users. A "transaction" is a record informing the network that a certain amount of bitcoins (or another cryptocurrency) is being transferred from one "bitcoin address" to another. A bitcoin address is a unique identifier on the network (similar to a bank account, though there is no bank). The address is based on the user's "public key," which in turn is generated from the "private key." The pair of private-public keys is kept offline and is used to establish ownership of bitcoins. The private key is simply a random number smaller than $2^{256} \approx 10^{77}$; the public key is calculated from the private key. The keys are generated not by the network, but on the end user's computer using the Elliptic Curve Digital Signature Algorithm (see the Appendix for further discussion of elliptic curve cryptography). One can generate multiple bitcoin addresses, each with its own set of keys, and combine them into a "bitcoin wallet," which is simply a set of addresses and keys.

When a transaction is broadcast, everybody in the network knows that the indicated amount of bitcoins should be deducted from the sender's address and added to the receiver's address. The sender signs the transaction with his or her private key, so everybody knows that the transaction is authentic. Because all the previous transactions are public, everybody can also verify that the sender had enough bitcoins. As such, the transaction will be accepted by the network, included in one of the new blocks, and permanently added to the blockchain.

One of Bitcoin's security options is "multi-signature" ("multisig"), a process in which a transaction has to be signed by several accounts in order to be authorized. For example, three accounts can be designated as signatories, and at least two signatures are required for authorization.

Curiously, the idea of a public ledger appeared much earlier than Bitcoin, in connection with a primitive currency—stone money of the island of Yap in the Pacific. The "coins" were in the form of giant limestone wheels (called rai), which were quarried and shipped to Yap from another island, Palau, 250 miles away.[8] Rai could be up to 9,000 pounds and for centuries their quarrying and transportation was a big part of the local economy. Because they are heavy, rai were not moved once on the island; so while their locations did not change, the stones' ownership changed through transactions. The record of ownership—the ledger—was kept orally and was based on public consensus.

The following section introduces the theoretical issues underlying all cryptocurrencies.

The Byzantine Generals Problem (Consensus and Block Validation)

All cryptocurrencies—for example, Bitcoin or Ether (ETH)—are based on blockchains, which are public ledgers of transactions. The idea of creating a public ledger sounds simple, but it is surprisingly difficult to implement. The main problem to resolve in a decentralized structure is how to reach consensus on a particular state of the system (e.g., to agree on a given list of bitcoin transactions).[9]

On the island of Yap, the consensus regarding ownership of the stones was reached by direct interactions among the island's inhabitants. In the context of cryptocurrencies, the consensus is reached using the concept of "proof-of-work" (PoW) and the relevant model for reaching consensus can be illustrated by the so-called Byzantine Generals Problem. The problem describes a scenario in which several divisions of an army lay siege to a city. While each division is under the command of its own general, there is no one in charge of the military operation as a whole. The generals must decide on when to attack the city, but their only ability to communicate is through a messenger. Furthermore, they are not certain who of the other generals they can trust. There may be traitors who will try to foil their plan by preventing them from agreeing on a time of attack.

The generals must come up with a protocol ensuring that they will be able to attack the city within a reasonably short time and that their plan will not fail due to a lack of consent. A successful protocol will be one in which the loyal generals, following the protocol, are able to reach an agreement, regardless of what the traitors do. In other words:

- Generals who are NOT traitors will be able to agree on a reasonable time of attack.

- Generals who are traitors, as long as their number is small, will not be able to influence the decision.

It has been found that consensus is impossible to achieve if one-third or more of the generals are traitors.[10] Furthermore, under more restrictive, deterministic conditions, consensus is impossible if there is even a single traitor.[11]

While the particular scenario described above may seem artificial, the Byzantine Generals Problem has become extremely relevant for cryptocurrencies. Like the generals, Bitcoin users need to agree on the valid transactions that have been broadcast to the network (the equivalent of the suggested attack time), despite the fact that some users may be trying to add fraudulent transactions to the blockchain or reject valid transactions. Consensus in the Bitcoin setting takes a relatively long time to achieve—an hour or longer in practice. The longer the time, the more certain one can be that consensus has been reached regarding a given new transaction; the probability of error declines exponentially with time. Satoshi Nakamoto[12] explains how the Bitcoin algorithm can solve the generals' problem:[13]

> They don't particularly care when the attack will be, just that they all agree. They use a proof-of-work chain to solve the problem. Once each general receives whatever attack time he hears first, he sets his computer to solve an extremely difficult proof-of-work problem that includes the attack time in its hash. The proof-of-work is so difficult, it's expected to take 10 minutes of them all working at once before one of them finds a solution. Once one of the generals finds a proof-of-work, he broadcasts it to the network, and everyone changes their current proof-of-work computation to include that proof-of-work in the hash they're working on. If anyone was working on a different attack time, they switch to this one, because its proof-of-work chain is now longer.
>
> After two hours, one attack time should be hashed by a chain of 12 proofs-of-work. Every general, just by verifying the difficulty of the proof-of-work chain, can estimate how much parallel CPU power per hour was expended on it and see that it must have required the majority of the computers to produce that much proof-of-work in the allotted time. They had to all have seen it because the proof-of-work is proof that they worked on it. If the CPU power exhibited by the proof-of-work chain is sufficient to crack the password, they can safely attack at the agreed time.

Bitcoin introduces incentives for those who participate in reaching the consensus—be it generals or, in reality, bitcoin miners. Each new block that a miner adds to the chain (or each time another general broadcasts confirmation of the time of attack) the miner is rewarded with newly minted bitcoins.

Immutability

One of the ostensibly desirable features of blockchains is immutability; all accepted transactions are supposed to stay in the chain forever and cannot be altered.

In October 2017, the US Commodity Futures Trading Commission (CFTC) released "A CFTC Primer on Virtual Currencies," which asserted:

> Virtual currencies are relatively unproven and may not perform as expected (for example, some have questioned whether public distributed ledgers are in fact immutable).[14]

Indeed, in certain situations, publicly-distributed ledgers can be altered, provided there is general agreement in the user community.

The DAO Attack

The DAO (Decentralized Autonomous Organization) was a virtual organization that existed on the Ethereum Blockchain. Ethereum (ETH) was proposed in late 2013 by Vitalik Buterin, a 19-year-old programmer from Toronto, as a new open-source protocol for creating decentralized applications.[15] In Buterin's words, "whereas in bitcoin the protocol exists to maintain the currency, in ethereum, the viewpoint is much more that the currency exists to maintain the protocol."[16]

In May 2016, The DAO offered and sold approximately 1.15 billion DAO Tokens in exchange for approximately 12 million ETH, valued at $150 million at the time (see the SEC decision regarding the offering for the background on The DAO).[17] The DAO computer code had a flaw, and on 17 June 2016, an unknown attacker diverted about one-third of the ETH held by The DAO to an address controlled by the attacker.[18] The security feature of the code prevented the attacker from withdrawing the ETH for 27 days.

The majority of the Ethereum community decided to change the Ethereum protocol and update the blockchain to "undo" The DAO, so that ETH could be returned to The DAO Token investors before the funds were withdrawn by the attacker. The change was implemented on 20 July 2016.

Not everybody in the Ethereum community agreed with the change; about 20% of ETH holders opposed it. The minority insisted on immutability of the blockchain as a matter of principle and argued that the majority decision was a client bailout and set a bad precedent.

> We believe in decentralized, censorship-resistant, permissionless blockchains. We believe in the original vision of Ethereum as a world computer you can't shut down, running irreversible smart contracts. We believe in a strong separation of concerns, where system forks are only possible in order to correct actual platform bugs, not to bail out failed contracts and special interests.[19]

The minority refused to update the protocol and continued on the old blockchain, which became a different cryptocurrency called Ethereum Classic (ETC).

Hard Forks

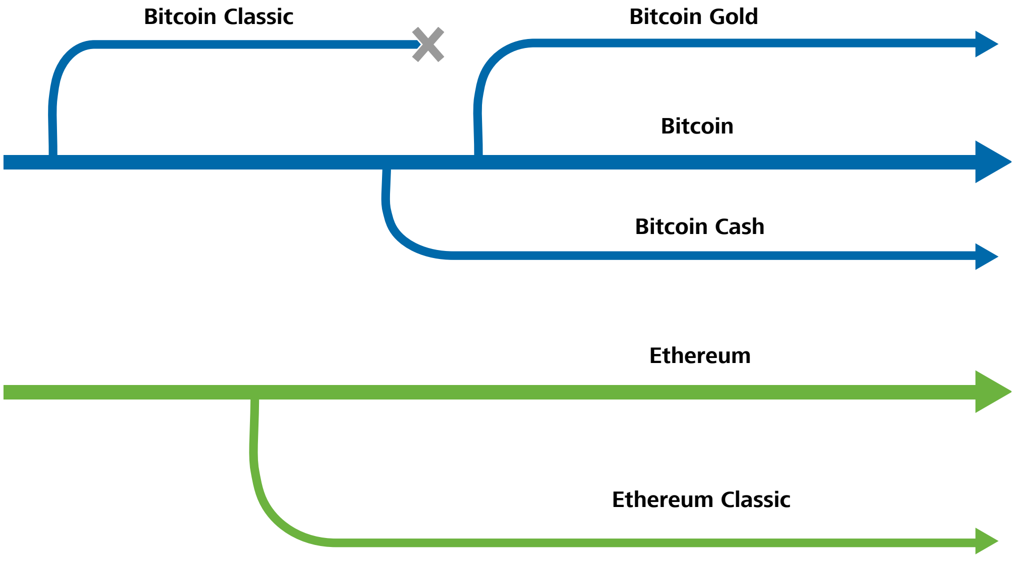
The Ethereum split after The DAO attack is an example of a "hard fork," in which a new protocol is adopted by the community. Accordingly, new transactions on the forked blockchain would be seen as invalid under the old rules.

Bitcoin has also experienced hard forks that resulted in the creation of new blockchains and related cryptocurrencies, as shown in the diagram below. Bitcoin Cash forked from Bitcoin in August 2017 as a change to the protocol that raised the limit on the block size (from 1MB to 8MB). Another fork was Bitcoin Gold, which sought to return to the original "one-CPU-one-vote" principle.

> Bitcoin Gold decentralizes mining by adopting a PoW algorithm, Equihash, which cannot be run faster on the specialty equipment used for Bitcoin mining (ASIC miners). This gives ordinary users a fair opportunity to mine with ubiquitous GPUs.[20]

Not all hard forks survive. For example, Bitcoin Classic, started in 2016, stopped operations by the end of 2017 as interest in the currency declined.

Figure 2. **Blockchain Hard Forks**



At the same time, Bitcoin Cash and Ethereum Classic proved to be reasonably successful.

The fork that created Ethereum Classic had an interesting side effect. By design, the attacker who stole four million ETH from The DAO would not have any ETH in the updated Ethereum blockchain (after the fork). However, the attacker would still have four million coins in the old blockchain (now called Ethereum Classic). Ethereum Classic (ETC) traded in the range of $2 to $20 in the months following the attack, which means the fork made the attack at least partially successful.

Smart Contracts and Errors in Computer Code

In the example of the DAO, the Ethereum fork was precipitated by a bug in the DAO computer code. The issue was not with the Ethereum blockchain itself, but with a "smart contract" built using the Ethereum platform.

Smart contracts were proposed by Nick Szabo in 1996.

> The basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a beginner's level problem in design with finite automata, dispense change and product fairly. Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means.[21]

A smart contract goes beyond defining the rules of the agreement among the parties in that they actually enforce those rules, validating contract conditions and controlling the transfer of assets. Such a contract can be correctly executed without mutual trust and without the need of an external trusted authority.

The DAO example demonstrated that smart contracts are not perfect and that there are no regulations to oversee disputes arising out of flawed smart contracts. If a problem arises with a traditional contract, the dispute could be resolved in court (e.g., the contract can be rescinded or damages can be paid). A problem (some would say a benefit) with a smart contract is that it executes no matter what and no one oversees the execution. An additional question is how the government should regulate and tax such contracts.

Considering the complexity of smart contracts, it is not surprising that coding errors can happen. However, blockchains are not well-suited to address such issues because their immutability means one cannot fix errors in the contract code after the contract starts executing.

Another example of an application glitch took place in November 2017 when approximately $150 million worth of ETH in a multisignature wallet created by the company Parity was frozen and rendered inaccessible to its owners. As described in the company release, on 6 November 2017, a flaw in the smart contract code was exploited by an anonymous user. The user was able to first make himself the sole "owner" of the wallet and, after that, destroyed access. This blocked funds in 587 wallets holding a total of 513,774 ETH.[22]

In response to the event, Parity pointed to the need for greater testing of smart contract applications, not only at the individual company, but also within the cryptocurrency system in which the contract exists.

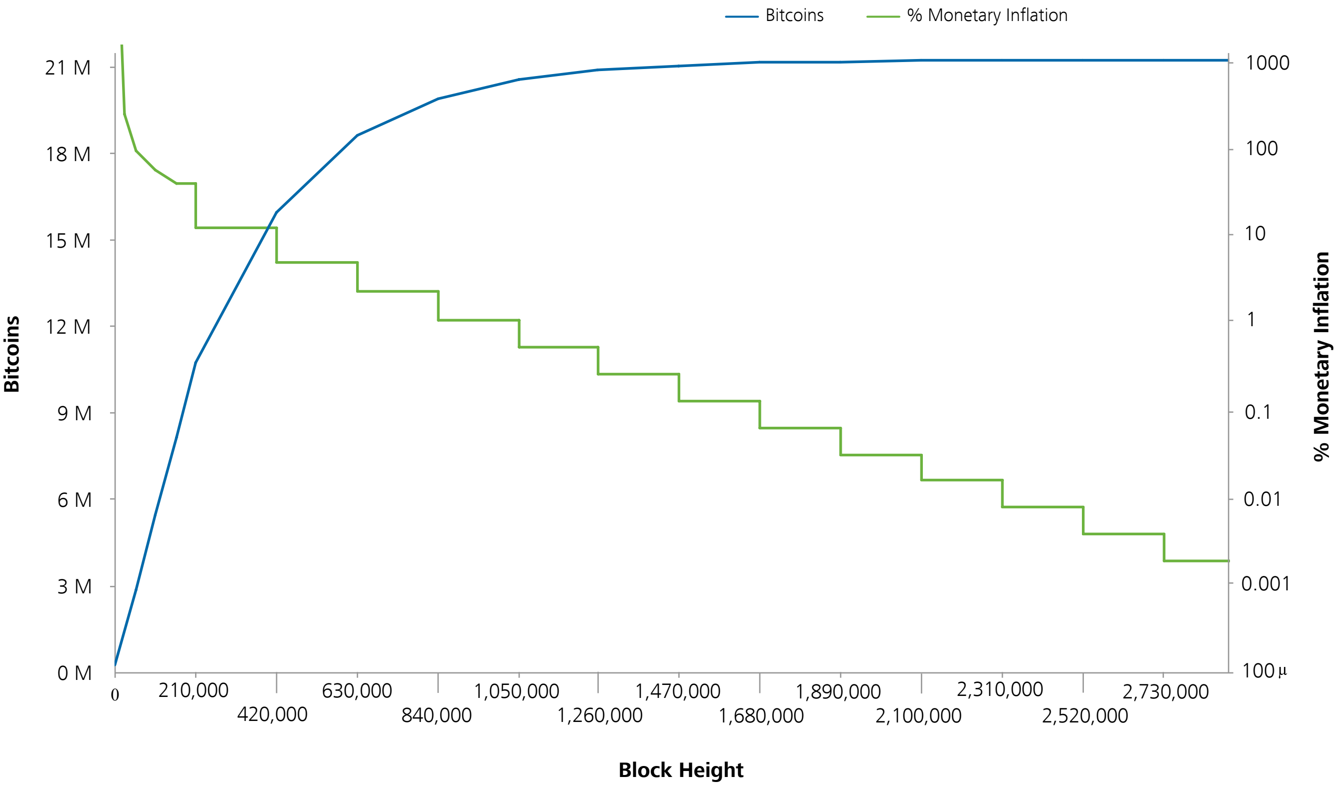
> However, rather than just having more audits, we strongly believe that more extensive and formal procedures and tooling around the deployment, monitoring and testing of contracts will be needed to achieve security. We believe that the entire ecosystem as a whole is in urgent need of such procedures and tooling to prevent similar issues from happening again, in particular if and when the number and complexity of live contracts grows.[23]

In this most recent event, there didn't seem to be any way to release the funds short of a system update and another fork.[24] Two days after the incident, Ethereum Foundation's head of security, Martin Swende, addressed the Parity freeze, saying: "I see it as an objective fact that these funds cannot be unlocked unless there is a hardfork involved."[25] These events highlight the challenges arising out of decentralized blockchain structures.

Supply of Bitcoin and Economic Issues

A particular design feature of Bitcoin (but not of other cryptocurrencies) is that the total potential supply of bitcoins is limited. There is also a set schedule of bitcoin issuances until around 2140 when the maximum number of bitcoins, 21 million, will be reached. The figure below shows the scheduled supply of bitcoins until the 2060s; while bitcoins will continue to be issued after that, the supply will be negligible.

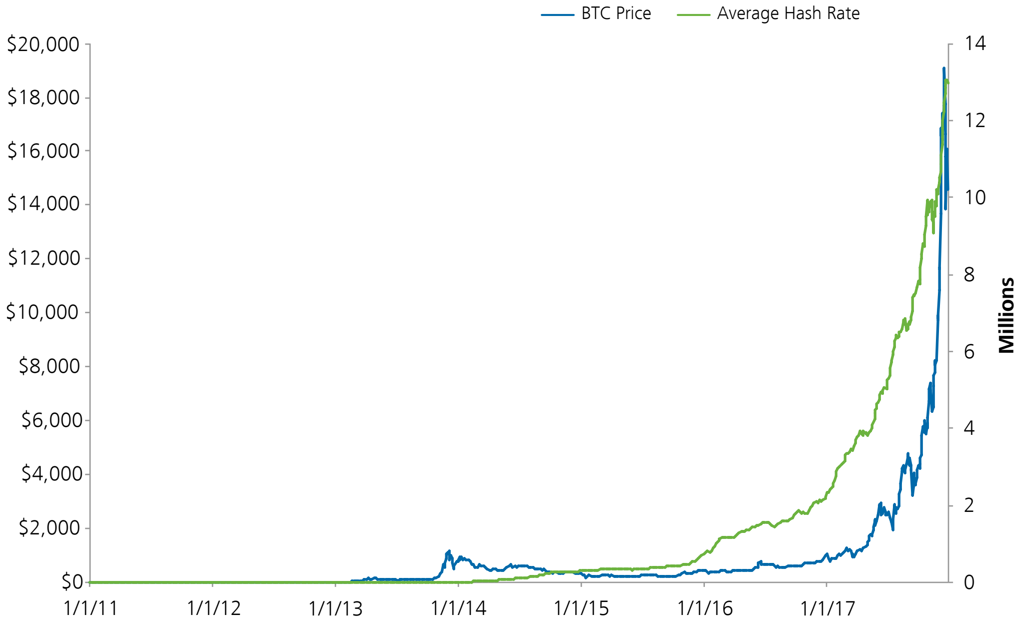
Figure 3. **Bitcoin Supply**



Notes and Sources:
Bitcoin supply is calculated based on the "halving" procedure specified in the following two sources:
https://en.bitcoin.it/wiki/Block
https://en.bitcoin.it/wiki/Controlled_supply.
Inflation = Coinbase * BlocksPerYear/existing Coins.

The figure below shows the price of bitcoins from January 2011 through December 2017 as the black line. It also shows the average total hash rate (i.e., the total computer speed dedicated to mining) in TH/s (one trillion hashes per second). The increase in the hash rate over time reflects the increase in resources allocated to mining new blocks. It also reflects hardware upgrades, as mining is now done by specialized hardware, and application-specific integrated circuits (ASIC), designed with the sole purpose of bitcoin mining (i.e., running the Bitcoin hash function).

Figure 4. **Bitcoin Price vs. Average Hash Rate (in TH/s)**
(2011–2017)



Source: Blockchain, available at https://blockchain.info/charts/hash-rate?timespan=all&daysAverageString=7; and Coindesk, available at https://www.coindesk.com/price/

As the price of bitcoins has gone up, more resources have been added to bitcoin mining. As suggested by Nakamoto (discussed in more detail below), mining involves solving intentionally difficult computational puzzles in order to add new blocks to the chain (and, thus, contribute to consensus) and get the reward. As the total hash rate goes up, the difficulty of finding the next block automatically adjusts so that it always takes about 10 minutes to mine a new block (14 seconds for a new Ethereum block).

This mining incentive has resulted in several undesirable effects:

- **Creation of Mining Pools and Concentration of Mining**
  Nakamoto's vision of Bitcoin (and mining) in 2008 was a decentralized, one-CPU-one-vote model.[26] The reality turned out to be very different, as economies of scale have arisen in mining. The figure below shows the concentration of mining power (by hash rate) of bitcoins by mining pool.

Table 1. **Concentration of Mining Power[1] by Mining Pool**

Mining Pool	
AntPool	20.7%
BTC.com	10.8%
BTC.TOP	10.6%
Bixin	7.6%
F2Pool	7.1%
BTCC Pool	7.1%
Bitfury	6.0%
ViaBTC	5.8%
BitClub Network	4.6%
BW.COM	4.0%
SlushPool	3.1%
GBMiners	2.5%
Unknown	2.3%
Bitcoin.com	2.0%
1Hash	1.5%
Waterhole	1.2%
KanoPool	0.8%
BATPOOL	0.8%
Telco 214	0.7%
CANOE	0.3%
Bitcoin India	0.2%
Total	**99.7%**

Source: blockchain.info

[1] By hash rate of Bitcoin.

Moreover, it is estimated that about 70% of mining is currently done in China.[27] This level of concentration goes against the original idea of Bitcoin as a decentralized network, as mining can become vulnerable to government regulation and abuse of power either in the form of a "51% attack," when a group of miners control a majority of the network's hash power,[28] or by preventing others from reaching a beneficial consensus.

- **Increased Economic Costs in the Form of Electricity and Mining Hardware**
  Similar to the stone money of Yap, creation and maintenance of cryptocurrencies is costly. The annual electricity consumption by bitcoin miners is about 30 TWh, and the electricity consumption per bitcoin transaction is approaching a staggering 300 kWh.[29] Additionally, significant resources are devoted to development and production of specialized mining equipment.

More on Proof-of-Work (PoW) and Mining

The means of reaching consensus in Bitcoin and other cryptocurrencies is, as described by Nakamoto, “an extremely difficult proof-of-work problem.” Note that on Yap, the difficult task was quarrying and transporting the currency to the island. With Bitcoin, in order to add a record (block of transactions) to the chain and be rewarded with bitcoins, one needs to find a number (x) such that when a special function (hash function) is applied to this number, together with the proposed block, the resulting hash value begins with a required number of zeros.

The status of the blockchain and current mining activity is reported in real time on multiple websites. A typical screen showing the status of the blockchain looks like this:

Table 2. **Blockchain Mining Status**

Latest Blocks					
Height	Relayed By	Size(B)	Reward	Time	Block Hash
499,297	AntPool	1,032,771	15.43178096 BTC	right now	000000000000000000610d1c27570458c765c13054e0636762255dce772bec4
499,296	unknown	1,041,949	16.25384352 BTC	2 min ago	0000000000000000003d967cc5ffc6f1ed8a4267c29770441ecee636f5bcc2a6
499,295	BTC.TOP	1,018,986	16.00554838 BTC	8 min ago	00000000000000000025db8b8fa6a7a760ed1275de5efc3b189c248c7d8f1cae
499,294	F2Pool	1,148,198	16.21159638 BTC	9 min ago	0000000000000000003e9f4f02f5d0059f6128b24c0e3461d0f48163bbdb275f
499,293	AntPool	1,049,485	16.70370005 BTC	10 min ago	0000000000000000008c3bdf208ceb075276a20541b42bc5cce3f2a23f881d65
499,292	BW.COM	998,287	16.35601044 BTC	23 min ago	00000000000000000018cdca7c4b82346c7ef41aa89935c334e1faf3a3798d
499,291	BTC.com	1,034,090	16.69298359 BTC	25 min ago	00000000000000000093e7bb9a65baeaeba64d69a0d9cf44lb7d1ec5e0774e75
499,290	BTC.TOP	1,066,326	16.68272025 BTC	36 min ago	00000000000000000023b12b9e46bffb32031434bd09e66b4a081c26f659e332
499,289	AntPool	1,048,725	15.89387699 BTC	47 min ago	00000000000000000041e9eacf766defe62703c508f9cad3834b10ef4597b3fb
499,288	BitClub	1,059,729	15.20911253 BTC	1 hr 9 min ago	00000000000000000062acc46bfb7cf77b729c835f48a8eb25956a9d11ef47cca

Source: https://btc.com

In the “Latest Blocks” section in the figure above, you can see the latest block being added (block number 499,297), the name of the miner adding the block (AntPool), block size, the miner’s reward in bitcoins, the time it took to mine the block, real-time hashrate, and other information. Note AntPool’s reward of 15.43178096 BTC in this figure. Each block currently results in 12.5 BTC issued. The rest, 2.93178096 BTC, are transaction fees, which operate as an additional form of compensation for miners.[30]

Note also the block hash that starts with 18 zeros, representing the number of zeros currently required for the block to be accepted and added to the chain.[31] This arrangement—that in order to add a record to the chain, one must perform a difficult but meaningless calculation—may look artificial. However, currently this is the only method of providing voting advantage to the loyal majority against the potentially maleficent minority. Under the PoW protocol, the majority literally overpowers the minority with greater computational resources.
These efforts still rely on the same cryptographic algorithms behind Bitcoin, and on additional research to support new consensus protocols. The fact that information can be encrypted relatively easily so that nobody can break it (even with the resources of the whole world) suggests that better systems can be developed for reaching consensus, which would not require voluminous competing calculations of PoW.

Proof-of-Stake

PoW consensus is achieved by miners performing the work of solving math puzzles that have no shortcut analytic solution and must be solved by brute force. Miners are paid for their work and anyone is free to become a miner and try to make money validating new blocks.

There is an alternative consensus algorithm that has been considered. It is called proof-of-stake (PoS). Under PoS, new blocks are validated by those who own the coins. Instead of competition among miners, with massive efforts and massive rewards, the right to validate the next block in the chain can be randomly assigned among existing coin holders.[32] The advantages include:

- **Low cost.** There is no need for intensive computations and, thus, no high hardware and electricity bills. Low cost also means there is less need to compensate miners with newly minted coins.

- **Better security from the introduction of penalties for attacks.** The block validators can be required to post the coins they own as security, making potential 51% attacks expensive for the attacker.

- **Lower cost of centralization.** A serious problem in blockchain operation is the potential emergence of large colluding groups of miners, which could engage in maleficent behavior (e.g., "selfish mining").[33]

PoS will mean there will be no need for the current mining industry.

Despite the potential advantages, the implementation of PoS has been delayed by the lack of a practical PoS consensus algorithm. Among other issues that need to be resolved is the so-called "nothing at stake" problem in which, in the event of a fork, a validator is motivated to validate every chain (as there are no mining costs), resulting in a failure of the consensus algorithm.[34]

Ethereum is currently planning to move to a trial hybrid PoW/PoS mode (which will be called the "Constantinople" hard fork) in which one in every 50 transactions will be validated using PoS. All other transactions will still be validated using PoW.[35]

Classification by the United States Government Regulatory Agencies

SEC

The US Securities and Exchange Commission (SEC) decision regarding The DAO concluded that DAO Tokens were securities and therefore subject to registration.

> All securities offered and sold in the United States must be registered with the Commission or must qualify for an exemption from the registration requirements....

> This Report reiterates these fundamental principles of the US federal securities laws and describes their applicability to a new paradigm—virtual organizations or capital raising entities that use distributed ledger or blockchain technology to facilitate capital raising and/or investment and the related offer and sale of securities. The automation of certain functions through this technology, “smart contracts,” or computer code, does not remove conduct from the purview of the US federal securities laws.[36]

Although the SEC made a determination for DAO Tokens, it is not clear what the classification of Ether is under SEC rules. It is the digital asset used on the Ethereum blockchain, and can be used as a token, which would give ETH some features of a security.

CFTC

On 17 September 2015, the Commodity Futures Trading Commission (CFTC) issued a guidance that classified Bitcoin and other virtual currencies as commodities covered by the Commodity Exchange Act.[37]

On 17 October 2017, after questions about the SEC DAO decision and the CFTC 2015 guidance, the CFTC issued further guidance that referred to the SEC analysis of the DAO tokens:

- There is no inconsistency between the SEC’s analysis and the CFTC’s determination that virtual currencies are commodities and that virtual tokens may be commodities or derivatives contracts depending on the particular facts and circumstances.

  - The CFTC looks beyond form and considers the actual substance and purpose of an activity when applying the federal commodities laws and CFTC regulations.[38]

IRS

The Internal Revenue Service (IRS) regards Bitcoin as property for federal tax purposes.[39]

Recent Developments

ICOs

Initial Coin Offerings (ICOs) are a way of crowdfunding by selling tokens or cryptocoins. ICOs generally raise money in other cryptocurrencies, with Ethereum’s smart contract platform being the most popular. If there is investor demand, ICOs are an efficient way of starting crypto projects.

The DAO is an example of an ICO that was launched through the Ethereum platform. The DAO ICO raised $150 million and is notable because it resulted in an 18-page letter from the SEC concluding that token sales are subject to securities laws.[40] So far, according to the Coindesk ICO Tracker,[41] ICOs have raised $3.5 billion, with the largest ICO, that of blockchain data storage network Filecoin, raising $250 million in August 2017.

Interactive Coin Offering

In a November 2017 paper, Teutsch, Buterin, and Brown proposed modifications to the current protocol, so that future ICOs can be interactive.[42] The proposed modifications include the following:

- ICOs are "token crowdsales" and should have no limit on the money raised, as is currently common. "Capped sales can reach tens of millions of dollars and sell out in a matter of minutes, leaving buyers unable to participate, disappointed, and frustrated. Uncapped sales, which run without such maximums, provide buyers little clue as to the fraction of total tokens their contribution will ultimately purchase."

- ICOs should be "interactive," (i.e., investors should be able to cancel the purchase). "Potential buyers may enter and exit the crowdsale based on behaviors of other buyers, and in doing so tend the valuation towards a market equilibrium."

Availability of Futures

In a surprise move, on 24 July 2017, the CFTC granted approval to be a derivatives clearing organization for LedgerX.

> Under the order, LedgerX will be authorized to provide clearing services for fully-collateralized digital currency swaps. LedgerX, which was also granted an order of registration as a Swap Execution Facility on July 6, 2017, initially plans to clear bitcoin options.[43]

The CTFC clarified that it was not endorsing Bitcoin itself.

> This authorization to provide clearing services for fully-collateralized digital currency swaps does not constitute or imply a Commission endorsement of the use of digital currency generally, or Bitcoin specifically.[44]

Many investors expressed concern about bitcoin futures. For example, on 15 November 2017, in a full-page ad in the *Wall Street Journal*, Interactive Brokers founder Thomas Peterffy published an open letter to CFTC Chairman J. Christopher Giancarlo, stating the following:

> There is no fundamental basis for valuation of Bitcoin and other cryptocurrencies, and they may assume any price from one day to the next.... Margining such a product in a reasonable manner is impossible. While the buyer (the long side) of a cryptocurrency futures contract or call option could be required to put up 100% of the value to ensure safety, determining the margin requirement for the seller (the short side) is impossible.[45]

On 10 December 2017, Bitcoin futures contracts started trading on the Cboe Futures Exchange under the ticker "XBT". Bitcoin futures are cash-settled based on the Gemini Exchange bitcoin prices.[46] The futures have no price limits. However, there are limits on price volatility in that trading will be halted for two or five minutes respectively, if prices move more than 10% or 20% from the previous day's settlement price.[47]

Additionally, the Chicago Mercantile Exchange (CME) Group plans to launch bitcoin futures on 17 December 2017.[48]

The margin requirements for Bitcoin futures have been set at 44% by the Chicago Board Options Exchange (CBOE), and at 47% by CME.[49] Usually, margins on futures are around 5% to 15%.[50]

ETF Denials

On 10 March 2017, the SEC denied an application for the first exchange-traded fund (ETF) that would trade like a stock and track the price of bitcoins.[51] The SEC issued a similar order on 28 March 2017, regarding another ETF proposal.[52]

The reasoning presented by the SEC had two parts. First, the markets for Bitcoin are unregulated and, therefore, rules to prevent fraud and market manipulation cannot be effectively enforced.

> …the Commission believes that the significant markets for bitcoin are unregulated and that, therefore, the Exchange has not entered into, and would currently be unable to enter into, the type of surveillance-sharing agreement that helps address concerns about the potential for fraudulent or manipulative acts and practices in the market for the Shares.[53]

Second, the SEC reasons that there were no futures markets for Bitcoin.

> When the spot market is unregulated, there must be significant, regulated derivatives markets related to the underlying asset with which the Exchange can enter into a surveillance-sharing agreement.[54]
>
> …for the commodity-trust ETPs approved to date for listing and trading, there have been in every case well-established, significant, regulated markets for trading futures on the underlying commodity—gold, silver, platinum, palladium, and copper—and the ETP-listing exchange has entered into surveillance-sharing agreements with, or held Intermarket Surveillance Group membership in common with, those markets.[55]

Since the introduction of bitcoin futures, new bitcoin ETF applications were filed in December 2017.[56]

Potential Regulatory Investigations

The introduction of bitcoin futures means potential future claims of price manipulation, fraudulent sales practices, or other disruptions to market integrity that will be the subject of CFTC investigations. Further regulatory investigations can be brought by possible approval of bitcoin ETFs. In September 2017, the SEC announced the creation of the Cyber Unit, which will target cyber-related misconduct, including violations involving blockchains and initial coin offerings. The SEC also created the Retail Strategy Task Force, which will watch for misconduct impacting retail investors.[57]

On 4 December 2017, the Cyber Unit brought its first charges against a company known as PlexCorps and obtained an emergency asset freeze to stop a fraudulent ICO that raised around $15 million from investors.[58] The Unit also stopped another ICO, by the company called Munchee, arguing that the ICO constituted unregistered securities offers and sales.[59]

On 11 December 2017, the Chairman of the SEC issued a "Statement on Cryptocurrencies and Initial Coin Offerings."[60] The statement gives a warning to broker-dealers, securities lawyers, accountants, and consultants, and reminds market participants of their responsibility to comply with regulations.

> I believe that gatekeepers and others, including securities lawyers, accountants and consultants, need to focus on their responsibilities. I urge you to be guided by the principal motivation for our registration, offering process and disclosure requirements: investor protection and, in particular, the protection of our Main Street investors....
>
> I also caution those who operate systems and platforms that effect (sic) or facilitate transactions in these products that they may be operating unregistered exchanges or broker-dealers that are in violation of the Securities Exchange Act of 1934.

Regarding ICOs, the statement warned about potential fraud and manipulation, as well as limited investor protection.

> A number of concerns have been raised regarding the cryptocurrency and ICO markets, including that, as they are currently operating, there is substantially less investor protection than in our traditional securities markets, with correspondingly greater opportunities for fraud and manipulation…
>
> Selling securities generally requires a license, and experience shows that excessive touting in thinly traded and volatile markets can be an indicator of "scalping," "pump and dump" and other manipulations and frauds.

The statement also said that whether a particular digital asset is a security will be evaluated on a case by case basis.

> A key question for all ICO market participants: "Is the coin or token a security?" As securities law practitioners know well, the answer depends on the facts.… It is especially troubling when the promoters of these offerings emphasize the secondary market trading potential of these tokens. Prospective purchasers are being sold on the potential for tokens to increase in value—with the ability to lock in those increases by reselling the tokens on a secondary market—or to otherwise profit from the tokens based on the efforts of others. These are key hallmarks of a security and a securities offering.

Conclusion

Cryptocurrencies are still in the development stage and government actions can influence their adoption, use, and price. The effect of any single government action may be difficult to predict. One of the reasons for cryptocurrency development was precisely to avoid government regulation and, as such, significant demand for cryptocurrencies will always be present and some of the negative effect of government regulation is already priced in. Additionally, cryptocurrencies like Ethereum provide a platform for all sorts of applications like self-executing contracts. Some of these applications will be successful and, in turn, will support the underlying cryptocurrency.

As cryptocurrencies and related digital assets become more widely accepted, there will be a higher level of scrutiny on the part of regulators, as well as inevitable investor disputes.

On the more technical side, a potential threat to cryptocurrencies may come from advances in quantum computing. Some researchers suggest that a breakthrough in quantum computing might come within the next 10 years.[61] This threat, however, is common to most communications that use public key cryptography, including online banking. Currently, the creation of a commercially available quantum computer appears remote. In any event, cryptocurrency protocols can be enhanced in the future if the possibility becomes real.

In 2010, when discussing the future of Bitcoin, Satoshi Nakamoto wrote, "I'm sure that in 20 years there will either be very large transaction volume or no volume."[62] At least some cryptocurrencies will have large volume by 2030, even if Nakamoto's Bitcoin will not be one of them.

Appendix: Cryptographic Math

This section provides a glimpse at the math behind cryptocurrencies.

Hash Function

A hash function is a mathematical formula that converts input data to a string of numbers and letters of a predetermined fixed length. Hash functions are impossible to invert; that is, the input data cannot be derived by knowing the output string. Any modification of the data, however slight, either by accident or intentional, will change the hash value.
The hash function used in Bitcoin is SHA-256. Here are examples of the SHA-256 values calculated on an empty word and on two slightly different sentences (the second sentence has a period at the end).[63]

sha256(‘’) =

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

sha256(‘The quick brown fox jumps over the lazy dog’) =

d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592

sha256(‘The quick brown fox jumps over the lazy dog.’) =

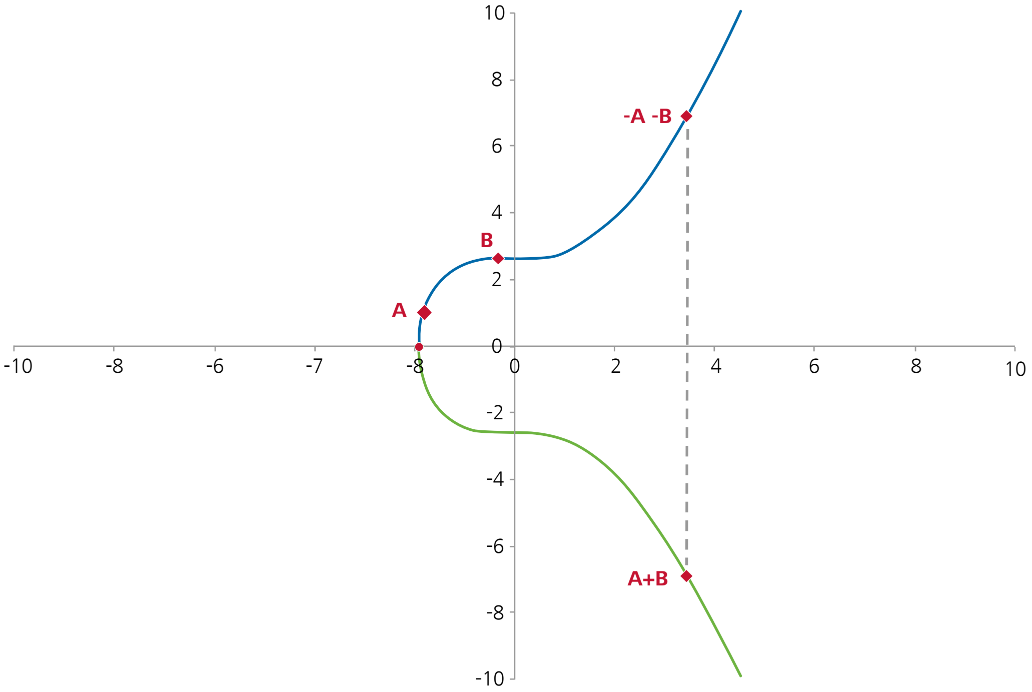
ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c

If the difficulty requirement is that the hash should begin with a certain number (k) of zeros, then the miner needs to find a number (x) such that SHA-256 (block; x) starts with k zeros.64 As the difficulty requirement k goes up, the difficulty of finding x increases exponentially. There are many possible x values that satisfy this requirement, but they are all difficult to find, as there is no way to predict what the output of the hash function will be. The only way to find such a number is by brute force. Therefore, every block suggested by a miner serves as a proof of the amount of work performed by the miner. It is unlikely that there is a way to circumvent brute force calculations. In any event, it will be possible to replace SHA-256 with another hash function.[65]

Encryption

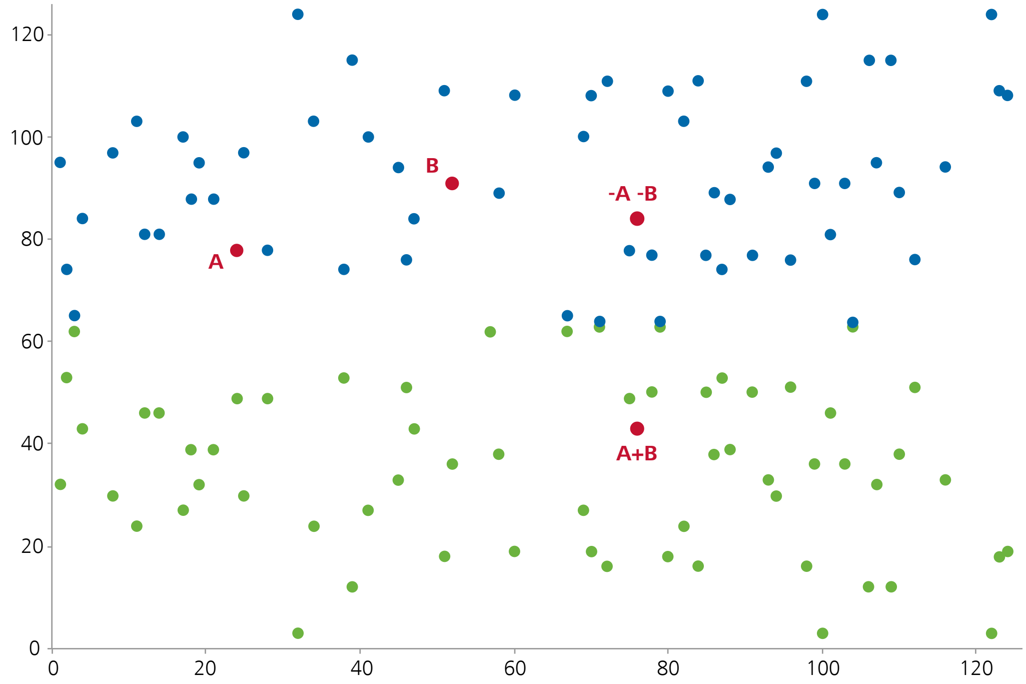
The security of Bitcoin and other cryptocurrency signatures is based on certain properties of the so-called elliptic curves, namely that for any two points A and B on the curve, one can define their "sum" A+B.[66] The particular curve used in Bitcoin (and also Ethereum) is $y^2=x^3+7$.[67] The figure below demonstrates the shape of the curve using real numbers, and how A+B is defined for a given A and B.

Figure 5. **Elliptic Curve of Bitcoin Security Signature: $y^2=x^3+7$**



Note that the curve is symmetric because for every point (x,y) on the curve, point (x,-y) will also lie on the curve.

Figure 6. **Encrypted "Curve" of Bitcoin Security Signature: $y^2=x^3+7$**



For encryption purposes, instead of real numbers, a large prime number *p* is selected and all calculations are done mod(*p*), using remainders when dividing numbers by *p*.[68] For example, if *p* equals 127, the above picture will look like this:
The "curve" now looks like a collection of random points. However, the chart is not random, as the "curve" retains the underlying algebraic structure (i.e., it is still symmetric and it is still possible to uniquely define point A+B, given points A and B).
Having defined addition, one can calculate multiples of a given point: 2*A, 3*A, 4*A, etc. The cryptographic trick is that, if p is large, then given A and n, one can easily calculate n*A. However, if given A and n*A instead, it turns out that finding n is extremely difficult. This is called the elliptic curve discrete logarithm problem (ECDLP).

The *private key* (n) of a Bitcoin address is simply a random number (smaller than *p*). The *public key* is then calculated from the private key as n*G, where G is a special point on the elliptic curve called the generator point (the same for all Bitcoin keys).

This way, a public key can be shared with anyone and, although the relationship between the two keys is known (i.e., public key = private key*G), it is not possible to find the private key.

The *p* value used in Bitcoin is very large (i.e., $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \approx 10^{77}$), and computers are not expected to be able to perform such a calculation (finding n) in the foreseeable future.

Notes

[1] Sharon Ann Murphy, "Early American Colonists Had a Cash Problem. Here's How They Solved It," *Time Magazine*, 27 February 2017, available at http://time.com/4675303/money-colonial-america-currency-history/.

[2] Marco Polo, "The Travels of Marco Polo," Translated by Henry Yule, Book II, Chapter 24, available at https://en.wikisource.org/wiki/The_Travels_of_Marco_Polo/Book_2/Chapter_24.

[3] Note that CFTC classifies Bitcoin itself as a commodity.

[4] Jeff John Roberts and Nicolas Rapp, "Nearly 4 million bitcoins have been lost forever, study says," *Business Insider*, 27 November 2017, available at http://uk.businessinsider.com/nearly-4-million-bitcoins-have-been-lost-forever-study-says-2017-11?IR=T.

[5] See Grayscale at https://grayscale.co/bitcoin-investment-trust/.

[6] See Blockchain at https://blockchain.info.

[7] See Bitaps at https://bitaps.com.

[8] Michael F. Bryan, "Island Money," Federal Reserve Bank of Cleveland, 2004, available at https://www.clevelandfed.org/newsroom-and-events/publications/economic-commentary/economic-commentary-archives/2004-economic-commentaries/ec-20040201-island-money.aspx.

[9] Many of the ideas used in Bitcoin had been suggested before: Hashcash (1997), B-Money (1998), and Bit Gold (1998). Bitcoin was the first cryptocurrency project detailed and practical enough to be implemented and gain acceptance.

[10] Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, July 1982, pp. 382-401, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.126.9525&rep=rep1&type=pdf.

[11] Michael J. Fischer, Nancy A. Lynch, and Michael S. Paterson, "Impossibility of Distributed Consensus with One Faulty Process," *Journal of the ACM*, Vol. 32, no. 2, pp. 374–382, 1985, available at https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf.

[12] The anonymous creator of Bitcoin. Bitcoin was suggested in 2008 in a white paper by Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," available at https://bitcoin.org/bitcoin.pdf.

[13] Satoshi Nakamoto Institute, "Bitcoin P2P e-cash paper," 13 November 2008, available at http://satoshi.nakamotoinstitute.org/emails/cryptography/11/#selection-39.0-103.42.

[14] LabCFTC, "A CFTC Primer on Virtual Currencies," Commodity Futures Trading Commission, 17 October 2017, available at http://www.cftc.gov/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf.

[15] "Who Created Ethereum?" *Bitcoin Magazine*, available at https://bitcoinmagazine.com/guides/who-created-ethereum/.

[16] Joon Ian Wong, "Ethereum's inventor on how 'initial coin offerings' are a new way of funding the internet," Quartz, 14 September 2017, available at https://qz.com/1075124/ethereum-founder-vitalik-buterin-discusses-initial-coin-offerings-the-consensus-algorithm-and-the-most-interesting-apps/.

[17] "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO," *SEC Release No. 81207*, 25 July 2017, available at https://www.sec.gov/litigation/investreport/34-81207.pdf.

[18] The flaw in the code allowed withdrawal of funds to be executed multiple times before the account balance was updated in the code. As a result, more ETH could be withdrawn from The DAO than was due to the attacker's DAO account balance.

[19] Arvicco, "Let's keep the original censorship-resistant Ethereum going!" Ethereum Classic Blog, 14 July 2016, available at https://ethereumclassic.github.io/blog/2016-07-15-start-project/.

[20] See BitcoinGold at https://bitcoingold.org/.

[21] Nick Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1996, available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[22] "A Postmortem on the Parity Multi-Sig Library Self-Destruct," Parity Technologies, 15 November 2017, available at http://paritytech.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/.

[23] Ibid.

[24] "On Classes of Stuck Ether and Potential Solutions," Parity Technologies, 11 December 2017, available at http://paritytech.io/on-classes-of-stuck-ether-and-potential-solutions/.

[25] Adam Reese, "Ethereum Foundation's Martin Swende Addresses Parity Freeze," ETHNews, 8 November 2017, available at https://www.ethnews.com/ethereum-foundations-martin-swende-addresses-parity-freeze.

[26] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."

[27] Willie Tan, "Brief Overview of China's Cryptocurrency Mining: Capital, Costs, Earnings," The CoinTelegraph, 16 August 2017, available at https://cointelegraph.com/news/brief-overview-of-chinas-cryptocurrency-mining-capital-costs-earnings.

[28] A 51% attack can happen when a group of miners control the majority (51% or greater) of the network's hash power and can create new forks and take control of the network.

[29] "Bitcoin Energy Consumption Index," Digiconomist, available at https://digiconomist.net/bitcoin-energy-consumption. 300kWh is approximately 10 days of electricity for the average US residential utility customer in 2016; see https://www.eia.gov.

[30] Transaction fees are not mandatory, but are added to most bitcoin transactions. Transaction fees are collected by the miner who mines the block that includes the transaction. Higher transaction fees make the transaction more attractive for the miners to include in the currently mined block, meaning that a transaction with relatively high fees is likely to be included in the next block, while transactions with low or no fees may be ignored and therefore take longer to process.

[31] The length of the hash string is 256 bits. By convention, the presentation is in the hexadecimal format, making the length of the hash string 64 digits. The hexadecimal format uses 16 digits instead of 10: 0, 1, 2, … 9, a, b, c, d, e, f.

[32] The actual PoS algorithms are highly complex.

[33] Ittay Eyal and Emin Gun Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," Cornell University, available at https://www.cs.cornell.edu/%7Eie53/publications/btcProcFC.pdf.

[34] "What exactly is the Nothing-At-Stake problem?" StackExchange, available at https://ethereum.stackexchange.com/questions/2402/what-exactly-is-the-nothing-at-stake-problem.

[35] Jordan Daniell, "Ethereum Stepping Stones: Constantinople and Casper," ETHNews, 27 October 2017, https://www.ethnews.com/ethereum-stepping-stones-constantinople-and-casper.

[36] "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO," *SEC Release No. 81207*, 25 July 2017.

[37] "CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering," Commodity Futures Trading Commission Press Release, 17 September 2015, available at http://www.cftc.gov/PressRoom/PressReleases/pr7231-15.

[38] LabCFTC, "A CFTC Primer on Virtual Currencies," Commodity Futures Trading Commission, 17 October 2017.

[39] "IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for US Federal Fax Purposes; General Rules for Property Transactions Apply,"https://www.irs.gov/newsroom/irs-virtual-currency-guidance.

[40] ""Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO," *SEC Release No. 81207*, 25 July 2017.

[41] "All-Time Cumulative ICO Funding," Coindesk, available at https://www.coindesk.com/ico-tracker.

[42] Jason Teutsch, Vitalik Buterin, and Christopher Brown, "Interactive coin offerings," 11 December 2017, available at https://people.cs.uchicago.edu/~teutsch/papers/ico.pdf.

[43] "CFTC Grants DCO Registration to LedgerX LLC," Commodity Futures Trading Commission, 24 July 2017, available at http://www.cftc.gov/PressRoom/PressReleases/pr7592-17.

[44] Ibid.

[45] *The Wall Street Journal*, 15 November 2017. See also Matthew de Silva, "Bitcoin Futures Threaten Destabilization, Warns Interactive Brokers Group CEO," ETHNews, 16 November 2017, available at https://www.ethnews.com/bitcoin-futures-threaten-destabilization-warns-interactive-brokers-group-ceo.

[46] See Gemini at https://gemini.com.

[47] "Cboe XBT Bitcoin Futures," Cboe, available at http://cfe.cboe.com/products/bitcoin-qrg.pdf.

[48] "CME Bitcoin Futures Frequently Asked Questions," CME Group, 15 December 2017, available at http://www.cmegroup.com/education/cme-bitcoin-futures-frequently-asked-questions.html.

[49] Annie Massa, "Higher Margins Set for CME's Soon-to-Launch Bitcoin Futures," Bloomberg Markets, 12 December 2017, available at https://www.bloomberg.com/news/articles/2017-12-12/higher-margins-set-for-cme-s-soon-to-launch-bitcoin-futures.

[50] "Bitcoin-futures contracts create as many risks as they mitigate," *The Economist*, 14 December 2017, available at https://www.economist.com/news/finance-and-economics/21732541-and-dont-mention-tulip-bulb-futures-bitcoin-futures-contracts-create-many-risks.

[51] *Release No. 34-80206*, Securities and Exchange Commission, 10 March 2017, available at https://www.sec.gov/rules/sro/batsbzx/2017/34-80206.pdf.

[52] *Release No. 34-80319*, Securities and Exchange Commission, 28 March 2017, available at https://www.sec.gov/rules/sro/nysearca/2017/34-80319.pdf.

[53] Ibid.

[54] *Release No. 34-80206*, Securities and Exchange Commission, 10 March 2017.

[55] *Release No. 34-80319*, Securities and Exchange Commission, 28 March 2017. "ETP" means exchange-traded product.

[56] Helen Partz, "Bitcoin ETFs Seek Approval Following Launch of Futures," The CoinTelegraph, 14 December 2017, available at https://cointelegraph.com/news/bitcoin-etfs-seek-approval-following-launch-of-futures.

[57] "SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors," Securities and Exchange Commission, 25 September 2017, available at https://www.sec.gov/news/press-release/2017-176.

[58] "SEC Emergency Action Halts ICO Scam," Securities and Exchange Commission, 4 December 2017, available at https://www.sec.gov/news/press-release/2017-219.

[59] "Company Halts ICO After SEC Raises Registration Concerns," Securities and Exchange Commission, 11 December 2017, available at https://www.sec.gov/news/press-release/2017-227.

[60] Jay Clayton, "Statement on Cryptocurrencies and Initial Coin Offerings," Securities and Exchange Commission, 11 December 2017, available at https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

[61] "We find that the proof-of-work used by Bitcoin is relatively resistant to substantial speedup by quantum computers in the next 10 years, mainly because specialized ASIC miners are extremely fast compared to the estimated clock speed of near-term quantum computers. On the other hand, the elliptic curve signature scheme used by Bitcoin is much more at risk, and could be completely broken by a quantum computer as early as 2027, by the most optimistic estimates." Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel, "Quantum attacks on Bitcoin, and how to protect against them," October 2017, available at https://arxiv.org/abs/1710.10377.

[62] "What's with this odd generation?" Satoshi Nakamoto Institute, 14 February 2010, available at http://satoshi.nakamotoinstitute.org/posts/bitcointalk/57/.

[63] See https://www.npmjs.com/package/js-sha256.

[64] This description is a simplification of the actual algorithm.

[65] "SHA-256 is very strong.... It can last several decades unless there's some massive breakthrough attack." "If SHA-256 became completely broken, I think we could come to some agreement about what the honest block chain was before the trouble started, lock that in and continue from there with a new hash function." See "The Quotable Satoshi," Satoshi Nakamoto Institute, available at http://satoshi.nakamotoinstitute.org/quotes/encryption/.

[66] See Neal Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, Vol. 48, N. 177, January 1987, pp. 201-209, available at http://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf.

[67] This is curve "Secp256k1" per Standards for Efficient Cryptography classification. See Daniel R. L. Brown, "SEC 2: Recommended Elliptic Curve Domain Parameters," *Standards for Efficient Cryptography*, 27 January 2010, available at http://www.secg.org/sec2-v2.pdf.

[68] This means that only p numbers are used {0, 1, 2, … p-1}, and any number greater than p-1 is considered equal to one of those. For example, p is equal to 0, 3p+5 is equal to 5, etc.

About NERA

NERA Economic Consulting (**www.nera.com**) is a global firm of experts dedicated to applying economic, finance, and quantitative principles to complex business and legal challenges. For over half a century, NERA's economists have been creating strategies, studies, reports, expert testimony, and policy recommendations for government authorities and the world's leading law firms and corporations. We bring academic rigor, objectivity, and real world industry experience to bear on issues arising from competition, regulation, public policy, strategy, finance, and litigation.

NERA's clients value our ability to apply and communicate state-of-the-art approaches clearly and convincingly, our commitment to deliver unbiased findings, and our reputation for quality and independence. Our clients rely on the integrity and skills of our unparalleled team of economists and other experts backed by the resources and reliability of one of the world's largest economic consultancies. With its main office in New York City, NERA serves clients from more than 25 offices across North America, Europe, and Asia Pacific.

Contact

For further information and questions, please contact the author:

Dr. Airat Chanyshev
Senior Consultant
New York City: +1 212 345 7336
airat.chanyshev@nera.com

The opinions expressed herein do not necessarily represent the views of NERA Economic Consulting or any other NERA consultant. Please do not cite without explicit permission from the author.