An Introduction to Bitcoin and Blockchain Technology

February 2016

KAYE | SCHOLER

An Introduction to Bitcoin and Blockchain Technology

Bitcoin technology began to enter the public discourse in 2011, largely through its association as an anonymous payment system used on illicit and underground websites. As with most innovations that are first described in tabloid format, the story mischaracterized the technology and failed to identify the most important and varied potentials of what Bitcoin and its associated "Blockchain" technology promise. This primer will attempt to reboot your introduction to Bitcoin and convey some of the reasons why many in the financial and technology sectors are excited about its promise. A glossary of common terms appears at the end of this primer.

Bitcoin Overview

Trying to explain Bitcoin in short form is no easy task; however, it helps when one understands what it is and is not. Bitcoin is an information technology breakthrough that facilitates both a secure, decentralized payment system and a tool for the storage, verification and auditing of information, including digital representations of value. A bitcoin is also the intangible unit of account that facilitates the decentralized computer network of Bitcoin users. Bitcoin is not a company or a company product. Contrary to many news reports, it is not anonymous and was not built for bad actors, though bad actors have, at times, brought Bitcoin into the headlines.

Bitcoin is important because it represents a new means of forming consensus reliably and promptly across time and geography. As currently designed, Bitcoin is an open and transparent system that allows all users to easily come to an agreement on the authenticity of transactions and information stored on the network, all without the need to involve a trusted third party and without the concern of censorship of information or value transmitted across the network.[1] Adaptations of the Bitcoin technology allow for different controls and access, but the basic premise of reliable and prompt network agreement regarding information (including value) is at the heart of this technology.

Unlike traditional computer networks and payment systems, Bitcoin is not administered by any centralized authority or controlled by any rights holder. Instead, it was introduced to the world as an open source project. It may be utilized by any person, without fee, by downloading Bitcoin software and accessing the peer-to-peer network. These users collectively provide the infrastructure and computing power that processes and verifies transactions and information posted through that network and recorded on its decentralized ledger. A group of computer scientists and programmers volunteer their time toward

1. The consensus forming mechanism of Bitcoin allows users to verify that a transaction that was sent was authorized by a user having control over a particular private key. As a payment system, Bitcoin also verifies that the value attached to a transaction (denominated in bitcoins) is both genuine and controlled by the holder of the private key. Information may be included in transactions as part of a memo field. Bitcoin typically only verifies the authenticity of a transaction and the bitcoins sent in such transaction; information included in a memo field is only confirmed to be a part of the transaction (i.e., the content is not verified). At the same time, Bitcoin transaction memo fields may be used to establish a verifiable timestamp or proof of existence through unique hashing of document data.

upgrading and improving the Bitcoin software code, primarily through an open repository on the GitHub website.

A significant economy has grown, and continues to grow, around Bitcoin, both as a payment network and as a potential information technology tool. There has also been substantial investment in bitcoins as a digital asset. The economy is driven on the one hand by direct participants and venture capitalists seeking to disrupt existing systems and on the other hand by financial institutions seeking to appropriate the innovation to improve those same existing systems. Understanding the diversity of the economy begins with understanding Bitcoin itself. Broken down at its most basic level, Bitcoin is comprised of three separate innovations, as outlined below.

The Big "B", the "Blockchain" and the Little "b"

The first of these is Big "B" Bitcoin. When using the capitalized term, one is referring to the Bitcoin software and the decentralized computer network (Bitcoin Network) of users running that software. The Bitcoin software and protocols (the source code) were first described in a white paper released in November 2008 by an author using the pen name Satoshi Nakamoto[2] and Bitcoin itelf was released in a proof–of–concept software client in January 2009.[3] Nakamoto's innovation spawned from an online community of computer scientists who studied cryptography and the application of the technology toward the creation of an efficient and verifiable digital asset (or virtual currency) system. Upon the launch of the Bitcoin Network in January 2009, users were largely limited to hobbyists and the computer scientists testing the software in an attempt to verify Bitcoin's working parts, which were largely drawn from public-private key cryptography,[4] the "Hashcash" proof-of-work algorithm[5] and peer-to-peer network connections using a "gossip protocol."[6] Early users also were attracted to the political and economic message that could be drawn from a digital asset not tied to a central bank's money supply policy or easily subject to government censorship of transfer.

Unlike prior attempts to develop a digital asset, the technology proposed by Nakamoto did not rely on a

2. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," November 1, 2008, available at bitcoin.org/bitcoin.pdf (retrieved August 7, 2015).
3. The original proof-of-concept software client has been periodically updated and serves as the reference software for individuals seeking to develop Bitcoin-related software. The reference client incorporates all improvements or adjustments made to the Bitcoin protocol, and any developer creating software adaptations can know that, to the extent their software is compatible with systems running the reference client, it will be compatible with the Bitcoin Network as a whole. The reference client is now commonly known as "Bitcoin Core."
4. Public-private key cryptography or asymmetric encryption is a system of encryption first described by Stanford University researchers in the 1970s that, at its core, relies on the ability to generate a function that is easy to perform in one direction, but difficult or impossible to reverse engineer without a particular key. See Whitfield Diffie and Martin E. Hellman, "New Directions In Cryptography," IEEE Transactions on Information Theory, Vol IT-22 No. 6, November 1976, available at www-ee.stanford.edu/~hellman/publications/24.pdf (retrieved October 9, 2015). Public-private key cryptography relies on an algorithmic relationship between two keys (a mathematically linked pair of numeric or alphanumeric characters), of which a user makes one public and keeps the other private. A user may then use a public key to encrypt a message that may only be decrypted with its private key. In another example employed in Bitcoin, a user may verify the authenticity of a message or transaction by "signing" a digital signature with its private key in a way that may be verified with the associated public key. In either case, the private key used in combination with the public key provides a secure methodology to verify information. For a non-technical explanation of public-private key cryptography, see Panayotis Vryonis, "Explaining Public-Key Cryptography to Non-Geeks," Medium, August 27, 2013, available at medium.com/@vrypan/explaining-public-key-cryptography-to-non-geeks-f0994b3c2d5 (retrieved October 9, 2015).
5. Hashcash is a proof-of-work algorithm developed by Adam Back in the late 1990s as a means of limiting the systematic abuse of un-metered internet resources (e.g., spam email or denial of service attacks on web resources). See Adam Back, "Hashcash – A Denial of Service Counter-Measure," August 1, 2002, available at www.hashcash.org/papers/hashcash.pdf (retrieved October 9, 2015). The mechanism operates through the generation of a code or "hash" that proves the generator of the hash has expended a certain amount of computational power. In Bitcoin, a proof-of-work system similar to Hashcash has been employed whereby a "block" may be added to the Blockchain only if the "miner" proposing the block solution has included a particular proof-of-work hash. In the case of Bitcoin, this involves the inclusion of a "nonce" that has at least a certain number of zeroes at its beginning, which number increases to adjust for increased levels of work that are sought to be proven. See Nakamoto, Footnote 2.
6. A gossip protocol is a system whereby information is shared on a peer-to-peer basis. In the Bitcoin implementation, each user represents a "node" that directly connects with several other nodes that share transactions and block data amongst each other. Information regarding transactions and blocks spreads rapidly through the Bitcoin Network because each node connects to multiple other nodes and is constantly listening for new information, which it passes along to the nodes it is connected to. For a more complete explanation of the gossip protocol implementation in Bitcoin, see Christian Decker and Roger Wattenhofer, "Information Propagation in the Bitcoin Network," 13th IEEE International Conference on Peer-to-Peer Computing, 2013, available at www.cs.ucsb.edu/~rich/class/cs290-cloud/papers/bitcoin-delay.pdf (retrieved October 9, 2015).

Blockchain Size

The Bitcoin Blockchain is stored locally on all computers running a full implementation of the Bitcoin software client. As of February 23, 2016, the Blockchain was approaching 57 GB in size. As time progresses and as the use of Bitcoin increases, users' ability to handle and manage the size of the Blockchain will rely on reduced costs associated with computer storage and internet bandwidth access.

Additionally, there are Bitcoin improvement proposals geared toward increasing the scalability of Bitcoin. While some of these proposals increase the maximum size of each block added to the Blockchain (from the current maximum of 1 MB per block), others seek to reduce the required storage capacity for the Blockchain. One such proposal involves the selective pruning of old Bitcoin transaction data.

The debate relating to scaling Bitcoin has provoked controversy both within and without the Core Development community, in large part because many proposals involve a "hard fork" of the Bitcoin software. Proposals including Bitcoin XT and Bitcoin Classic will not be fully reverse compatible with the existing Bitcoin Core reference client.

centralized clearing house (a trusted third party) to verify money supply and transactions.[7] Instead, the Bitcoin community progressively built out a decentralized network of computers that exert a tremendous amount of computing power toward the singular purpose of validating and clearing transactions on the Bitcoin Network. The distributed and decentralized network allows each individual user to verify the validity of individual transactions and the system, as a whole, through the cryptographic protocols and the transaction history of the Bitcoin Network, which is stored by each user on a distributed ledger known as the Blockchain. The technology, then, is a solution to the Byzantine General's Problem, which ponders how a system can generate consensus and, more specifically, a recipient can verify that a digital asset or transaction (or any information) is valid both at the time sent and received.[8]

The "Blockchain" represents the second great innovation from Nakamoto. As a distributed ledger, the Blockchain is stored locally on the computer hard drive of every user running a full version of the Bitcoin software. The ledger records the history of every transaction sent and confirmed on the Bitcoin Network, including information included as a part of those transactions. As of February 23, 2016, the size of the Blockchain was approaching 57 GB of data. Information is added to the Blockchain through the proof-of-work "mining" process. Users running a special mining variant of the Bitcoin software expend great amounts of computing power in order to win the right to add another block to the Blockchain, which is accompanied by a reward of 25 bitcoins.[9] The concept of proof-of-work mining ensures that an adjusted amount of work and computing power must be expended to solve a block, with the block reward providing an economic incentive for honest mining. The expenditure of computing power serves to secure the integrity of the Blockchain, while the miners themselves verify through public-private key cryptography the validity of each transaction they include in a block. When a transaction is included in a block, the transaction has been validated and "cleared" by the miner.[10]

Although it has been often reported that Bitcoin is an anonymous payment system, the Blockchain is a transparent record of all transactions between users on the Bitcoin Network. Users on the Bitcoin Network are identified by the digital addresses (i.e., hashes of their public keys) that they control, and such digital addresses serve as their pseudonyms on the Blockchain. The identity of users on the Blockchain can often be determined through a combination of either voluntary identification of users with their digital addresses (e.g., through identity verification with Bitcoin exchanges or custodians), accidental identification by users or by statistical analysis.[11]

Distributed ledger technology can be applied to a variety of purposes other than the transfer of digitally stored value. The same principles that allow the Blockchain to be a functional means of creating, verifying and transferring value can be applied to information or even to exercisable rights (e.g., smart contracts or voting systems). The first core use case of Blockchain technology has, however, been as a payment system.

The underpinning of the Bitcoin Network payment system is in the third innovation: the little "b" bitcoin. The lowercase version of bitcoin references the core unit of value on the Bitcoin Network. A bitcoin can be

7. The prior generation of digital money included Liberty Reserve and E-Gold, which were centralized services with non-public transaction histories that relied on the central issuer to verify transactions and reserves.
8. See Leslie Lamport, Robert Shostak and Marshall Pease, "The Byzantine Generals Problem," Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, Pages 382-401, available at research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf (retrieved October 13, 2015). See also Marc Andreessen, "Why Bitcoin Matters," New York Times, January 21, 2014, available at dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_r=0 (retrieved October 13, 2015).
9. The block reward or "coinbase" received by a miner who has earned the right to add a block to the Blockchain was initially set at 50 bitcoins. After every 210,000th block is added to the Blockchain, the size of the block reward is halved. As the Bitcoin source code adjusts the difficulty of the mining process in an effort to ensure that blocks are solved, on average, about every 10 minutes, there is approximately four years between halvings. The first halving of the block reward (to 25 bitcoins) occurred on October 28, 2012. The second halving (to 12.5 bitcoins) is projected to occur in the middle of July 2016. See Bitcoin Block Reward Halving Counting, available at bitcoinblockhalf.com/ (retrieved February 23, 2016).
10. Although a bitcoin transaction is deemed clear upon its inclusion in a block on the Blockchain, best practices dictate that a user considers a transaction confirmed after its inclusion in a block and the addition of five subsequent blocks to the Blockchain. See, e.g., Confirmation, available at en.bitcoin.it/wiki/Confirmation (retrieved October 20, 2015).
11. See, e.g., Sarah Meiklejohn, et al, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," IMC'13, October 23–25, 2013, Barcelona, Spain, available at cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf (retrieved October 20, 2015). See also Dorit Ron and Adi Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," Financial Cryptography and Data Security, Lecture Notes in Computer Science, Volume 7859, 2013, available at eprint.iacr.org/2012/584.pdf (retrieved October 20, 2015).

subdivided to eight decimal places, with the smallest unit – a satoshi – having a value of 1/100,000,000th of a bitcoin. In sum, under the Bitcoin source code, a total of 21 million bitcoins will be created as mining rewards, distributed as compensation to miners in the process that adds blocks to the Blockchain. Approximately 72 percent (15.2 million of 21 million) of all bitcoins have been mined to date. By 2026, approximately 90 percent of all bitcoins will have been mined. The innovation of bitcoins as digital assets lies in the ability to verify the authenticity and ownership of a bitcoin and the ability to transfer possession nearly instantaneously for little or no cost, all without the reliance on a trusted third party or central clearinghouse. The Bitcoin Network makes such verification possible through its use of cryptographic proof of control and the transparent and distributed Blockchain.[12] By examining the transaction data and the Blockchain, a user can simply and quickly determine whether the transaction was authorized by the holder of the applicable private key, the bitcoins are controlled by that private key, and the bitcoins sent are valid (i.e., not counterfeit).

In general, one must spend some bitcoins to broadcast a transaction onto the Bitcoin Network and for inclusion in and clearing on the Blockchain. Transactions will propagate across the Bitcoin Network and be visible in an unconfirmed state within seconds.[13] Transactions typically are cleared and included on the Blockchain in the next solved block, but it may take longer than the average block solution time of just under 10 minutes for clearance.[14] For payments, this means the delivery of value; however, one can also embed information in Bitcoin transactions. Information can be included in Bitcoin transaction data through a "memo field" or by implementing advanced systems such as "colored coins," which assign additional meaning, rules or rights to specific bitcoin outputs. Bitcoin itself becomes "programmable money."

Beyond Bitcoin 1.0

While much of the funding and developments relating to Bitcoin have been directly tied to the Big "B," "Blockchain" and little "b," Bitcoin has already moved beyond its initial use case as a peer-to-peer payment system. The testing ground for that further innovation is in the development of altcoins, programming platforms and additional blockchains.

As an open source project, the Bitcoin Network and the Blockchain technology at its root are subject to "forking," which is the process of altering the Bitcoin source code to create a new project that is different and has limited backward compatibility with Bitcoin itself. From 2010 to 2014, this largely meant the creation of alternative payment systems or "altcoins" that were substantially similar to Bitcoin, with most having no material impact.[15] In most cases, the differences between altcoins and Bitcoin are limited in scope (e.g., Litecoin offers faster block confirmation times and Dogecoin features an inflationary

12. In this circumstance, we refer to cryptographic proof of control as the ability to establish, through a digital signature, that the holder of a private key has signed a transaction relating to bitcoins that are held in a previously unspent output (i.e., bitcoins previously received and not spent by the sender) assigned to the user's public key (or the digital address that is a unique hash of that public key). All transactions sent over the Bitcoin Network must include a digital signature signed by the private key controlling the bitcoins transmitted. A user can validate the transaction by (i) checking the digital signature against the applicable public key and (ii) checking the Blockchain to ensure that the bitcoins transmitted are from an unspent output assigned to the applicable public key. This authentication is typically automated by a user's software client.
An important distinction is that proof of control over a private key does not imply exclusive control over that private key or the bitcoins it has access to transfer. Private keys function somewhat like a secret – to the extent that the secret is revealed, you are not aware that the secret has been shared unless and until another party has exercised the secret. Once a Bitcoin transaction has been confirmed in the Blockchain, the transaction cannot be reversed. As such, procedures and policies regarding the safeguarding and management of private keys are very important for both retail and institutional holders of bitcoins.
13. See Decker and Wattenhofer, Footnote 6.
14. Transactions typically include the payment of a de minimis amount of bitcoins as a "miners fee." This amount is usually approximately 0.0001 (about 4 cents), but is optional. Payment of a miners fee will prioritize a transaction for inclusion in the next solved block. A transaction may not be included in the next available block if (i) the transaction has not yet been received by the miner that solves the block, (ii) the block has already been filled with other, higher priority unconfirmed transactions or (iii) the miner elects not to include the unconfirmed transaction. Although the average block solution time is just under ten minutes, it may take as little as seconds or in excess of an hour for any individual block to be solved.
15. As of the date of this primer, nearly 700 altcoins were tracked as having been quoted on an exchange market, although nearly all were not currently being traded or lacked a liquid market. See CoinMarketCap, available at coinmarketcap.com/all/views/all (retrieved February 21, 2016). A majority of these altcoins used substantially similar software and mining mechanisms as Bitcoin. As of February 21,2016, only three (Ethereum, Ripple and Litecoin) had a market capitalization in excess of $30 million and had a trading volume in excess of $200 thousand during the prior 24-hour period. By comparison, Bitcoin had a market capitalization of $6.8 billion and a daily volume of more than $93 million.

Bitcoin Network Computational Power

The Bitcoin Network infrastructure is provided by miners, who exert large amounts of computational power in finding a block solution that will allow them to add a new block to the Blockchain, thereby validating and clearing all the transactions that are included in that block. A block solution includes a proof-of-work hash that must meet specified criteria. The Bitcoin proof-of-work algorithm uses the SHA-256 variant of Secure Hash Algorithm 2 and requires a specific set of randomly generated zeroes in the solution.

Miners operate computer chips known as application specific integrated circuits (ASICs), which are designed for the specific purpose of running SHA-256 hashes on a continuous basis. The growth in the computational power of the Bitcoin Network was nearly parabolic from 2013 to early 2015, due to the increase in price of bitcoins (and, therefore, the block reward earned by miners) and improvements in bitcoin mining technology. Prior to 2014, Bitcoin miners relied on central processing unit (CPU) and graphical processing unit (GPU) technology found in standard computers. CPU and GPU processors were significantly less powerful and efficient at running SHA-256 hashes, resulting in a significant boom in computing power on the Bitcoin Network upon the introduction of ASIC units. Although the purpose of the ASICs is limited to running SHA-256 hashes, it is often cited that the Bitcoin Network is the most powerful computer network in the world.

money); however, certain altcoins such as Namecoin offered more purpose-backed forks.[16] From adoption and market size metrics, no altcoin has yet emerged as a true peer to Bitcoin. In theory, a new altcoin could overcome the network effect advantages held by Bitcoin through either the offering of superior features not easily incorporated into Bitcoin or through a failure or shortcoming being identified in the Bitcoin Network or source code. Even absent significant market share, altcoins do serve as a testing ground for new concepts in this emerging technological field, and may result in Bitcoin improvement proposals to incorporate useful concepts. Altcoins may become more impactful when generated in connection with programming platforms or Blockchain projects developed by financial institutions.

Projects organized around combining Bitcoin technology with advanced programming platforms have become a hot topic over the past two years. These projects seek to make Bitcoin and Blockchain technology more scalable for advanced use cases, and they are often referred to under the name Bitcoin 2.0 or Blockchain 2.0. Such programs include Ethereum,[17] which seeks to create a Turing-complete programming framework supported by an independent altcoin platform; Counterparty,[18] which seeks to do the same using a programming layer built on top of the Bitcoin Blockchain; and Blockstream,[19] which seeks to make Bitcoin interoperable with alternate blockchains (known as "sidechains") and their respective altcoins by allowing pegged transactions of assets and/or information. Numerous other projects, both utilizing Bitcoin and altcoins, are in development and have begun to receive more substantial public attention and funding.

Additionally, financial institutions including Barclays, UBS Bank of New York Mellon and Citibank are experimenting with Blockchain technology. This experimentation includes leveraging the above-referenced implementations and developing private, white-label test cases of blockchains. Private or "permissioned" blockchains differ from implementations such as the Bitcoin Blockchain in that they often are not (i) fully open-source in code, (ii) open-access for use and (iii) decentralized and transparent.[20] Instead, a private, permissioned blockchain leverages Blockchain technology within a more limited company or consortium ecosystem. Although much of the perceived benefits of Bitcoin are driven by its open-source, transparent, decentralized and open-access format, a private, permissioned blockchain may still have benefits as against a standard, centralized server system.

More advanced applications of Bitcoin and Blockchain technology have the ability to transform or impact any industry or product line that relies on the storage and verification of information or value. Bitcoin and Blockchain technology's programmable aspects may also facilitate the development of autonomous governance systems, contracts and legal constructs (e.g., "smart contract") or the ability of interconnected devices to interact with and even pay each other in the "Internet of Things." While many of the potential applications of this technology are grand in scope, it is entirely possible that the most impactful short-term results will be making existing payment, settlement and accounting products and services either more efficient or transparent.

16. The first altcoin to be forked from Bitcoin, Namecoin is substantially similar to its predecessor, but permits greater storage of information on its blockchain. Its primary use is as a decentralized domain name registry for .bit domains. See Namecoin, available at namecoin.info (retrieved October 12, 2015).
17. See Ethereum, available at ethereum.org (retrieved October 12, 2015); white paper available at github.com/ethereum/wiki/wiki/White-Paper (retrieved October 14, 2015).
18. See Counterparty, available at counterparty.io/docs/about_counterparty/ (retrieved October 12, 2015).
19. The "sidechain" concept seeks to allow the security and liquidity of the Bitcoin Network infrastructure to be leveraged by alternate blockchains that allow for different functionality. See Blockstream, available at blockstream.com (retrieved October 12, 2015); white paper available at blockstream.com/sidechains.pdf (retrieved October 14, 2015).
20. A Blockchain project can be categorized based on its openness in source code (i.e., open-source or closed-source development of the programming), data (i.e., private and opaque blockchain or public and transparent blockchain) and user access (i.e., private and permissioned access, or public and permissionless access). The use case for the Blockchain project will determine the best options for openness in each category.

Benefits and Weaknesses of Bitcoin and the Blockchain

As a payment system, Bitcoin has certain benefits over existing electronic systems. These benefits largely accrue to the recipient of a Bitcoin transaction, but certain benefits may be realized by senders of transactions (i.e., consumers or spenders) as well.

- Transparency. All Bitcoin Network transactions are cleared in the Blockchain, meaning a complete, auditable and immutable record of all activity exists.[21]
- No risk of chargeback fraud. Once sent and cleared, a Bitcoin transaction cannot be reversed by the sender.
- Low or no transaction costs. Bitcoin Network infrastructure is subsidized by the money supply's creation process.[22] As a result, transactions on the Bitcoin Network can be sent with the inclusion of minimal or no transaction fees. Furthermore, there is no cost to accessing the Bitcoin Network.
- Nearly instantaneous transactions. Bitcoin Network transactions register nearly instantaneously.[23] Confirmation and clearing of those transactions can occur within minutes to over an hour. For many other payment systems, clearance can take far longer.
- Network security. The Bitcoin Network itself is highly secure due to the use of cryptographic and decentralized Blockchain protocols. The public-private key pairs used provide ample security against the risk of a brute force hack or an accidental instance of two users generating the same private key.[24] Additionally, there is no single, centralized point of failure, which limits the susceptibility of the Bitcoin Network to downtime and hacking.[25]
- Protection of financial information. Bitcoin transactions can be performed without having to reveal sensitive personal and financial information to the recipient, limiting the potential exposure of such information to database hacks.
- Financial access. Although it cannot provide all of the services of banking institutions and its technical complexity may be too high for many users, Bitcoin can provide value storage and electronic payment services for users who lack access to traditional financial services.

Relative to these advantages, there are significant weaknesses relating to Bitcoin as a payment system and bitcoin as an asset.

- Difficult to use. Bitcoin is not consumer friendly. Most software to control, custody or transact in bitcoins is complex or difficult to use. Often, third-party software and solutions that can simplify this use involve entrusting bitcoins to such third party.
- Difficult to access. Although the Bitcoin Network is open access and liquid markets (relative to current

21. Some services, such as Bitcoin exchanges, pool user assets and track transactions between users using a ledger system. Transactions on an exchange's internal ledger (known as "off-blockchain transactions") are not actual Bitcoin transactions in that they are not broadcast to the Bitcoin Network and cleared on the Blockchain. Nevertheless, transaction data on the Blockchain is complete, leading one industry participant to note that "a blockchain is the only place where absence of evidence is evidence of absence." See twitter.com/buchmanster/status/554367408618500096 (retrieved October 12, 2015).
22. The subsidization of the Bitcoin mining process is funded by money supply creation, meaning that new bitcoins (and transaction fees optionally included by transaction senders) are awarded to the miners that clear transactions. As the mining reward is halved after every 210,000 blocks, the subsidization is reduced over time (although the value of the bitcoins paid as subsidy may increase or decrease due to market demand). If the mining reward subsidy, together with transaction fees paid by Bitcoin transaction senders, is not a sufficient incentive to exert computational power to mine, miners may begin to require the payment of minimum transaction fees that would reduce the cost benefits of transactions on the Bitcoin Network, relative to legacy payment systems. Additionally, to the extent that miners cease to exert computational power to verify and clear transactions, the Bitcoin Network will become relatively less secure (i.e., to the extent that honest miners are not incentivized to verify and clear transactions, it will become less expensive for dishonest participants to successfully mine blocks without including and clearing such transactions or broadcasting block solutions).
23. See Decker and Wattenhofer, Footnote 6.
24. The number of possible Bitcoin addresses (slightly less than 2^{160}) means that, for there to be a 0.1 percent likelihood of a collision between any two addresses, there must be 5.4x1022 addresses in existence. See, e.g., "Bitcoin and the Birthday Paradox," available at diyhpl.us/~bryan/papers2/bitcoin/bitcoin-birthday.pdf (retrieved October 12, 2015). Although future developments in computing technology may make current cryptographic standards obsolete, Bitcoin's open source code may be altered to employ more state of the art standards.
25. According to one website, the Bitcoin Network has been available (i.e., a user connecting to the network will find available nodes with which to connect) for 99.989 percent of the time since its launch on January 3, 2009. See bitcoinuptime.com (retrieved October 12, 2015).

demand and use) exist in the United States and certain other economies, few of the exchanges and services that allow the purchase of bitcoins are regulated and have a significant operational history. Furthermore, the opening of accounts with regulated exchanges requires anti-money laundering and "know your client" verification and account funding that makes it difficult for new users to acquire bitcoins quickly.

- Difficult to secure. Although the Blockchain and the cryptographic protocols that underlie Bitcoin are secure, users must safely store and use their private keys in order to safeguard their bitcoins. Securing private keys either on a computer or other medium requires proper personal computing and/or home security that relies on individual user sophistication.
- Lacks protections against mistakes. Unlike traditional electronic payments, Bitcoin transactions cannot be reversed and no administrator can restore access. As a result, a mistaken Bitcoin transaction or a lost private key will result in a user's loss of funds.
- Limited retail and institutional adoption. Although it far outpaces any altcoin in adoption and enjoys network effects relative to other digital assets, the use of Bitcoin remains somewhat limited relative to existing payment systems or financial technology.

As a technological innovation, the benefits of Bitcoin and the Blockchain are just beginning to be understood. The ability to leverage Blockchain technology to secure, verify and audit information in a scalable manner is one of many exciting elements of the innovation. Additionally, the ability to build out voting or rights ecosystems, programmable money or autonomous entities through "smart contracts" permits new decentralized applications that may hold value for the presently practical or the same type of future innovations that the Internet made possible for the pre-connected world.[26] Currently, institutions are using Blockchain technology to build proofs of concept relating to the settlement and recording of property rights and financial instruments.[27]

Understanding Bitcoins as Assets

Each bitcoin is a digital representation of a unit that can be transferred from one user to another without the involvement of intermediaries or third parties, thus facilitating direct end-user-to-end-user transactions with little or no transaction costs. Bitcoins have no physical existence beyond the record of transactions that are "stored" or reflected on the Blockchain. The current value of bitcoins is determined by the supply of, and demand for, bitcoins in the open market, as well as by the number of merchants and other users that accept them. Global trade in bitcoins currently consists of individual end-user-to-end-user transactions, together with OTC and facilitated exchange-based bitcoin trading. A small United States derivative market for bitcoin trading has also emerged, with some recent entrants seeking U.S. Commodity Futures Trading Commission (CFTC) regulation and oversight of their activities.[28] Bitcoins are also spent by consumers for goods and services.

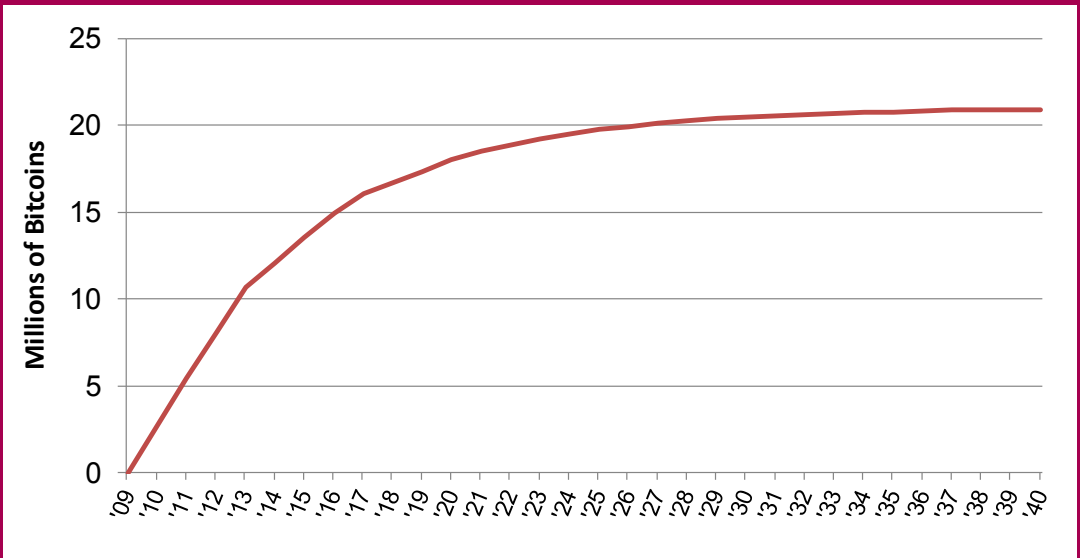
Trading markets for bitcoins are volatile and have limited liquidity. The risk profile of bitcoins appears to be very high, with many commentators expressing the opinion that an investment in bitcoin has a binary potential return (i.e., that bitcoins will eventually command either a high value or almost no value at all).[29] Part of the uncertainty regarding bitcoins is drawn from the lack of a consensus regarding their intrinsic value. In contrast to fiat currencies (the value of which is driven by the backing of the applicable government) and precious metals (the value of which are linked to historic industrial and commercial applications and cultural investment traditions), critics argue that

26. For a discussion of how some of the potential new Blockchain applications intersect with emerging law, see Aaron Wright and Primavera De Fillippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," March 10, 2015, available at papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (retrieved October 12, 2015). See also Joshua Fairfield, "Smart Contracts, Bitcoin Bots, and Consumer Protection," 71 Wash. & Lee L. Rev. Online 36 (2014), available at scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3 (retrieved October 12, 2015).
27. Examples of current projects include the ventures of Overstock and NASDAQ in developing systems for the settlement and lending of equities and bonds on private blockchains. See, e.g., Cade Metz, "Hedge Fund Borrows $10M in Stock Via The Bitcoin Blockchain," Wired, October 14, 2015, available at www.wired.com/2015/10/hedge-fund-borrows-10m-in-stock-via-the-bitcoin-blockchain (retrieved October 14, 2015).
28. Derivatives on bitcoins are more readily available in overseas markets, although platforms for such derivatives also have limited liquidity and generally lack regulatory oversight.
29. The lack of a clear risk profile and asset classification for bitcoins, as well as issues relating to the custody of bitcoins, may limit institutional investment in bitcoin and the ability of fiduciaries to advise retail clients to directly acquire bitcoins. Investment vehicles have been launched or proposed that provide direct or indirect exposure to the price of bitcoins. Such vehicles may, over time, increase investment exposure to bitcoin and advance the understanding of its asset classification and risk profile.

Bitcoin Money Supply

Bitcoin's money supply is rules-based and involves a projectable and known growth. New bitcoins are introduced into the money supply through a block reward or "coinbase" (currently 25 bitcoins) paid to Bitcoin miners who successfully validate and clear Bitcoin transactions by adding a block to the Blockchain. After every 210,000 blocks have been added, the size of the block reward is halved. As of February 23, 2016, 15,244,000 bitcoins had been mined, representing just under 72.6 percent of the eventual total of 21,000,000 bitcoins.

The below chart reflects the growth of the bitcoin money supply, from the initiation of the Bitcoin Network on January 9, 2009 to January 1, 2040, at which point approximately 99.5% of all bitcoins will have been mined. The data set used for the chart assumes that the next halving will occur on July 17, 2016 and that, thereafter, block solution times will average approximately every 10 minutes.



The money supply of bitcoins can only be changed by a "fork" of the Bitcoin source code, which would only become effective if and when adopted by a vast consensus of users and miners. Although many believe such a decision would be counter to the interests of Bitcoin users, a small handful of commentators have argued that an adjustment to the money supply may be beneficial if transaction fees appended to Bitcoin transactions are insufficient as an incentive for miner participation in the clearing and settlement process. Discussion of substantial changes to the core Bitcoin protocols have been controversial and will have difficulty in reaching the consensus required for adoption.

bitcoins have limited or no inherent or objective value. Bitcoin proponents often counter that bitcoins have value based on their ability to provide access to the Bitcoin Network and their use as a store of value and medium of exchange.[30]

Although the holding of bitcoins does not have the history and millennia-old traditions tied to precious metals, bitcoins are easily divisible, transferrable and fungible and appear to command a positive value relative to their cost of production (i.e., the cost of mining). [31] The four year history of trading in bitcoins indicates that perceived value of bitcoins may draw largely from speculation and momentum pricing in markets with limited liquidity. To date, a consensus does not exist and limited market analysis has been performed on the true intrinsic value of bitcoins, or that of the Bitcoin Network itself.

Due to the peer-to-peer structure of the Bitcoin Network, transferors and recipients of bitcoins can determine the value of bitcoins transferred by mutual agreement or barter. These participants generally assess the current value of bitcoins by reference to the price discovery occurring on one or more Bitcoin exchanges, usually by surveying the daily trading values and closing prices or the current value of a bitcoin price index. Bitcoins are traded on exchanges throughout the world, typically with publicly disclosed valuations for each transaction, measured by one or more fiat currencies such as the U.S. Dollar, the Euro or the Chinese Yuan.

Since the inception of trading in bitcoins, prices on Bitcoin exchanges have fluctuated greatly, and frequently, during certain time periods. Since the initial online quotation of a bitcoin-to-dollar exchange rate in 2009, the price of bitcoin experienced a low of $0.00 to a high of $1,242. Both the amount and rate of change in bitcoin prices have been significant from time to time, and their price is characterized as "volatile" by most market participants and observers. Despite its digital, rather than physical, existence, bitcoins share several characteristics with gold bullion: (i) both can act as a store of value, (ii) there is a limited quantity of each available and, therefore, an infinite supply will never be created, (iii) they are difficult and expensive to "mine" (i.e., generate) and (iv) their market prices are volatile.

In some ways, bitcoins represent a hybrid of existing asset classes, and this may be best understood as similar to other asset classes under specific circumstances. Bitcoin asset classification is defined by the specific use case at question. For example, when used to transmit value to another person,[32]

30. Commentators argue that the three principal characteristics of money are its use as (i) a medium of exchange, (ii) a store of value and (iii) a unit of account. While Bitcoin technology makes bitcoins an efficient medium of exchange, it is limited by the scope of its use (i.e., although relatively easy to use and accept, Bitcoin technology has not emerged as a standard form of payment in either developed or emerging economies). As a store of value, critics argue that the volatility of prices makes bitcoin a poor store of value. While this was particularly true in the period from 2011 to early 2015, proponents argue that in certain economies subject to high inflation and capital controls, bitcoin may be an effective suitable store of value. As a unit of account, the volatility of bitcoin prices also prevents common use of bitcoin to set prices for other goods or commodities. As a young asset class, bitcoin may eventually mature into an asset that better resembles money, although it appears to fail at least two of the principal characteristics of money at this time. See George Selgin, "Synthetic Commodity Money," University of Georgia, April 10, 2013, available at papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118 (retrieved October 12, 2015).
31. One researcher characterizes bitcoins as "synthetic commodity money," in that the characteristics aligning bitcoins with commodities such as precious metals (in particular, their scarcity) were derived based on the protocols of Bitcoin – the hard limits were not natural, but were drawn from difficult-to-change rules built into the source code. Selgin, Footnote 30.
32. For the purposes of applying federal regulation of money transmission, the Financial Crimes Enforcement Network (FinCEN), a bureau of the US Department of the Treasury, has determined that bitcoins and other "convertible virtual currencies" are distinguishable from real currencies in that they are a "medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency" and is not legal tender. FinCEN, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013, available at fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html (retrieved October 12, 2015). On the state level, regulators have differed in the application of state money transmission and money service business laws, as well as on the applicability of other regulatory requirements. Generally speaking, states have found that bitcoins fall outside of the statutory definition of "money," although they often have applied existing money service business regulations for similar reasons to how FinCEN has applied them on the federal level (i.e., although bitcoins are not money, they allow the transmission of value that may be converted into money). See, e.g., State of Washington Department of Financial Institutions, "Interim Regulatory Guidance on Virtual Currency Activities," December 8, 2014, available at www.dfi.wa.gov/documents/money-transmitters/virtual-currency-interim-guidance.pdf (retrieved October 12, 2015) (applying the Washington Uniform Money Services Act to specified activities and finding bitcoins to be a medium of value).

make an investment[33] or to make a political donation,[34] bitcoins are understood to fall into the category of a "thing of value" that is a substitute for true money. Despite this, bitcoins themselves generally do not meet a legal definition of money under federal or state regulation or statute.[35] From a tax perspective, the Internal Revenue Service and most states that have taken a position that bitcoins should be treated like property when spent and may be eligible to be treated as a capital asset when held as an investment.[36] In the area of derivative markets, the CFTC has affirmatively stated that bitcoins fall within the broad definition of a commodity under the Commodity Exchange Act, and that the offering of bitcoin derivatives and manipulation of markets used to price bitcoin derivatives are subject to their regulatory authority.[37] The Securities and Exchange Commission (SEC) has declined to opine on whether a bitcoin is a security, although standard issue bitcoins appear to lack the characteristics of a security, particularly as set forth in the *Howey* test.[38] Nevertheless, because of the programmable nature of Bitcoin, it is possible that bitcoins or altcoins can be structured to function as a security under specific circumstances.[39]

Bitcoins appear to best fit into the definition of commodity money when held as an investment or spent as a medium of exchange. "Commodity money" is money whose value stems directly from the asset or commodity of which it is made, and consists of objects that have an "inherent"

33. While not necessarily money, itself, bitcoins are deemed to fall within a broader definition of money when considered in respect of the Howey test of whether an investment of money has been made. See Footnote 38. See also U.S. v. Faiella, in which U.S. District Judge Rakoff rejected an argument that bitcoins were not money:

    > Money in ordinary parlance means 'something generally accepted as a medium of exchange, a measure of value, or a means of payment'.... Bitcoin clearly qualifies as 'money' or 'funds' under these plain meaning definitions.

    U.S. v. Faiella, U.S. District Court, Southern District of New York, No. 14-cr-00243, Memorandum Order at page 2, August 19, 2014, available at www.manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/BankingLaw@manatt/Faiella%20et%20al.%20v.%20United%20States.pdf (retrieved October 12, 2015). SEC v. Trendon T. Shavers and Bitcoin Savings and Trust, U.S. District Court, Eastern District of Texas, No. 4:13-cv-00416, Memorandum Opinion at page 3, August 6, 2013, available at ia600904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf (retrieved October 12, 2015) (holding that bitcoins "can be used as money").
34. In an advisory opinion, the Federal Election Commission (FEC) staff found that bitcoins would be included under the Federal Election Campaign Act definition of "anything of value" and would be treated as an in-kind contribution, rather than as money. FEC, "AO 2014-02 Political Committee May Accept Bitcoins as Contributions," May 8, 2014, available at www.fec.gov/pages/fecrecord/2014/june/ao2014-02.shtml (retrieved October 12, 2015).
35. For example, FinCEN regulations define "currency" as

    > the coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance. Currency includes U.S. silver certificates, U.S. notes and Federal Reserve notes. Currency also includes official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country.

    31 CFR Chapter X, Section 1010.100(m), available at www.law.cornell.edu/cfr/text/31/1010.100 (retrieved August 11, 2015). For a state perspective, see Washington Department of Financial Institutions guidance in Footnote 32 (finding that bitcoins are not "money" under the Washington Uniform Money Services Act) and Texas Department of Banking, "Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act," April 3, 2014, available at www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf (retrieved October 13, 2015) (finding that bitcoins are not "currency" under the Texas Finance Code).
36. See Internal Revenue Service, "IRS Virtual Currency Guidance," Notice 2014-21, March 25, 2014 available at www.irs.gov/irb/2014-16_IRB/ar12.html (retrieved October 12, 2015). See also, e.g., California State Board of Equalization, "Special Notice: Accepting Virtual Currency as a Payment Method," June 2014, available at www.boe.ca.gov/news/2014/l382.pdf (retrieved October 12, 2015).
37. See In the Matter of Coinflip, Inc. and Francisco Riordan, CFTC Docket No. 15-29, Order Instituting Proceedings, Making Findings and Imposing Remedial Sanctions, September 17, 2015, available at cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf (retrieved October 12, 2015)(memorializing a settlement relating to an unregistered bitcoin options trading operation). See also "Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition & Forestry," December 10, 2014, available at cftc.gov/PressRoom/SpeechesTestimony/opamassad-6 (retrieved October 12, 2015) (noting that the CFTC has broad regulatory authority over instruments that track commodities, including virtual currencies).
38. In S.E.C. v. W.J. Howey Co., 328 U.S. 293 (1946), an investment contract (a type of security enumerated in Section 2(a)(1) of the Securities Act of 1933) would be found where a transaction involved persons investing money in a common enterprise with the expectation of profits to come solely from the efforts of others. In subsequent case law, a multi-factor test has emerged for the Howey test: the asset, interest, enterprise, instrument or arrangement must involve: (i) an investment of money; (ii) in a common enterprise; and (iii) with the expectation of profits coming solely from efforts of others. While the acquisition of bitcoins may involve an investment of money, it appears to fail both the second and third factors of the Howey test.
39. For example, bitcoins or altcoins may be "colored" in a manner that the person having control over a colored coin can exercise voting rights in a governance system or equity rights over an interest tied to such a colored coin.

value, beauty or utility in addition to the value of their use as money. "Commodity money" has various industrial and commercial applications and uses, and exhibits some of the important features of true or "fiat" currency, such as durability, divisibility, portability and relative ease of storage. Bitcoins embody all four of these characteristics: (i) the Blockchain is remarkably durable, stored digitally on the local computers of all users operating a full version of the Bitcoin software; (ii) bitcoins are currently divisible down to one one-hundred millionth; (iii) bitcoins are portable in that they may be transferred easily through a Bitcoin transaction or through the delivery of control over a private key; and (iv) bitcoins are easily and permanently stored on the Blockchain, with users capable of easily storing their private keys on computers, mobile devices or other media. Bitcoins' characteristics of a finite supply and difficulty in mining are characteristics that mimic precious and base metals that comprise some of the more longstanding forms of commodity money.

As a form of commodity money, bitcoins are analogous to precious metals from an asset classification standpoint; however, they lack the longstanding history of precious metals as an investible asset and have been subject to significantly higher price volatility. As more liquid, regulated means of acquiring bitcoin exposure – both directly and indirectly – develop, it is possible that bitcoins will become a more trusted store of value, unit of account and medium of exchange. The risk profile of an investment in bitcoins may similarly adjust as markets begin to settle and price volatility has a more established history in liquid markets.

Regulation of Bitcoin

As an emerging technology, Bitcoin has been the subject of intrigue among government agencies, industry participants and advocacy groups seeking to determine whether this new technology (and its underlying asset) can be addressed under current regulatory regimes, or whether new regulation is required to address Bitcoin's unique characteristics. Many have argued for a hands-off or light approach to regulation of the Bitcoin industry; however, the financial nature of much of what Bitcoin can facilitate has led to a push for regulation that appears familiar, in part.

Bitcoins are not illegal in the U.S., as has been recognized by the Department of Justice. In *U.S. v. Ulbricht,*[40] the Assistant U.S. Attorney, in the criminal complaint against Ross William Ulbricht, noted that "Bitcoins are not illegal in and of themselves."[41] In a 2013 letter, the Department of Justice noted the "recognition that online payment systems, both centralized and decentralized, offer legitimate financial services."[42] However, users and service providers participating in the nascent technology of digital assets continue to operate with limited regulatory guidance. Furthermore, existing regulations, adopted before the invention of digital assets, are often ill-suited to address their hybrid features as a technology and an asset class, as discussed by the Mercatus Center in "Bitcoin: A Primer for Policymakers."[43]

Beginning with the 2013 guidance released by the Financial Crimes Enforcement Network (FinCEN), U.S. regulation on both the federal and state level has focused on what are commonly referred to as the "choke points" of the Bitcoin ecosystem. These choke points include Bitcoin exchanges, custodians and related financial services-oriented operators. Regulators have placed their focus on that area principally because they represent the onramp where consumers and users exchange and store traditional or fiat value into or from bitcoins. Furthermore, businesses operating at those chokepoints most clearly resemble the traditional financial services operations with which regulators are familiar and have existing protocols in addressing.

Together with the focus on choke points, U.S. regulators, lawmakers and enforcement agencies have identified consumer protection, fraud and money laundering as priorities in the more general Bitcoin ecosystem. These concerns deal less with the regulation of the Bitcoin Network or bitcoins as assets, and more with the monitoring of actions using bitcoins in lieu of traditional money. Bitcoin-related activities are currently addressed on a use-case by use-case basis.

40. U.S. v. Ulbricht, U.S. District Court, Southern District of New York, NO. 14-CR-68 (KBF).
41. See Sealed Complaint at page 7, Southern District of New York, available at www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Benthall,%20Blake%20Complaint.pdf (retrieved October 14, 2015).
42. See Peter J. Kadzik, Letter to Honorable Thomas R. Carper and Honorable Tom Coburn, October 23, 2013, available at online.wsj.com/public/resources/documents/VCurrenty111813.pdf (retrieved October 14, 2015).
43. See Jerry Brito et al., "Bitcoin: A Primer for Policymakers," Mercatus Center, August 19, 2013 at pages 27 to 38, available at mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf (retrieved October 14, 2015).

Regulation

U.S. regulation in the Bitcoin ecosystem focuses on the choke points where bitcoins are converted from fiat currency to digital value (e.g., Bitcoin exchanges and retail platforms). Both federal and state regulators are focused on issues including consumer protection, cybersecurity and adherence to anti-money laundering and Office of Foreign Assets Control requirements.

Technological Regulation

Bitcoin as a technology and network – and bitcoins as a unit – are strictly regulated by the Bitcoin source code and protocols that are adopted, on a consensus basis, by participants in the Bitcoin ecosystem. The Bitcoin Network, the Blockchain, Bitcoin transactions and bitcoins all operate strictly in accordance with the rules set forth in the source code, which are periodically updated and patched by a volunteer cadre of programmers working on the open source project. These volunteer programmers are commonly referred to as the "Core Developers."[44] The proposals and results of that work are auditable in both the reference Bitcoin Core software client and the open GitHub resource page. To date, no government agency has sought to exert control over the process of development of Bitcoin software, and no domestic agency has sought to limit internet access or connections to the Bitcoin Network.

U.S. Federal Regulation

The U.S. government has been a leading force in developing a regulatory framework for Bitcoin. On March 18, 2013, FinCEN became the first major governmental agency to directly provide guidance on Bitcoin and other digital asset networks when it released guidance on money transmission and money service business regulation with respect to digital assets.[45] FinCEN's guidance called for broad registration of participants in the Bitcoin marketplace as money transmitters, excepting users acquiring bitcoins for use "to purchase real or virtual goods or services." This pronouncement applied FinCEN's current regulatory structure and did not require the adoption of new rules.

Similarly, on March 25, 2014, the Internal Revenue Service (IRS) released guidance on the treatment of convertible digital assets (such as bitcoins) for U.S. federal income tax purposes.[46] This guidance did not require adoption of new regulations but instead classified bitcoins as "property" that is not currency for U.S. federal income tax purposes. The guidance also clarified that bitcoins could be held as capital assets.

The Federal Reserve Board also issued a statement clarifying that bitcoins, Bitcoin and other digital payment systems are generally outside the scope of its jurisdiction.[47] However, Chair Janet Yellen confirmed that they fall within the purview of FinCEN and the Justice Department.[48]

More recently, the CFTC took the formal regulatory position that bitcoins are commodities within the definition of the Commodity Exchange Act.[49] The CFTC held hearings on the regulation of bitcoins as commodities in 2014 and has entertained applications for swap and derivative platforms from TeraExchange and LedgerX.[50]

The SEC also has been examining with interest the purchase and sale of digital assets. Although the SEC has not articulated a regulatory position with respect to

44. Prior to 2014, core development was in part driven and financed by the Bitcoin Foundation, a non-profit advocacy group whose mission was the promotion of Bitcoin adoption. In the past two years, private concerns including Blockstream, BitPay and MIT have financed the activities of several Core Developers.
45. See Footnote 32.
46. See Footnote 36.
47. In a letter to the leadership of the Committee on Homeland Security and Government Affairs, then-Chairman Ben Bernanke of the Board of Governors of the Federal Reserve System wrote:

    > Although the Federal Reserve generally monitors developments in virtual currencies and other payments system innovations, it does not necessarily have authority to directly supervise or regulate these innovations or the entities that provide them to the market. In general, the Federal Reserve would only have authority to regulate a virtual currency product if it is issued by, or cleared or settled through, a banking organization that we supervise.

    Ben S. Bernanke, Letter to Honorable Thomas R. Carper and Honorable Tom Coburn, September 6, 2013, available at online.wsj.com/public/resources/documents/VCurrenty111813.pdf (retrieved October 14, 2015).
48. Daniel Wilson, "Yellen Says Fed Has No Authority Over Bitcoin," Law360, February 27, 2014, available at law360.com/articles/513990/yellen-says-fed-has-no-authority-over-bitcoin (retrieved October 14, 2015).
49. See Footnote 37.
50. Douwe Miedema, "TeraExchange Announces First Bitcoin Derivative," Reuters, March 24, 2014, available at www.reuters.com/article/2014/03/24/us-bitcoin-derivatives-idUSBREA2N1CX20140324 (retrieved October 14, 2015). The first bitcoin swap transaction was executed on TeraExchange's swap execution facility in October 2015. "TeraExchange Completes First Bitcoin Derivatives Trade on Regulated Exchange," MarketWatch, October 9, 2014, available at www.marketwatch.com/story/teraexchange-completes-first-bitcoin-derivatives-trade-on-regulated-exchange-2014-10-09 (retrieved October 14, 2015). See also Letter to Phyllis Dietz, Acting Director, Division of Clearing and Risk, CFTC, dated March 6, 2015 from Kari Larsen, General Counsel and Chief Regulatory Officer of LedgerX, requesting an extension of the review period until June 30, 2015, available at www.cftc.gov/ucm/groups/public/@otherif/documents/ifdocs/ledgerxreviewextension3-6-2015.pdf (retrieved October 14, 2015).

the legal characterization of bitcoins (e.g., whether or not bitcoins are securities), it has taken various actions against persons or entities misusing bitcoins in connection with fraudulent schemes such as the Ponzi scheme in the *Shavers* case,[51] inaccurate and misleading disclosures[52] and the offering of unregistered securities.[53] Both the SEC and the Financial Industry Regulatory Authority have issued investor alerts about the possible risks of investments in bitcoins and other digital assets.[54]

Other federal agencies including the Consumer Financial Protection Bureau, Department of Justice and Department of Homeland Security have studied the regulation of Bitcoin and its impact on their existing mandates. The legislative arm of the government has also investigated bitcoin, with hearings hosted by Senate and House committees in 2013 and 2014, and reports issued by the U.S. Government Accountability Office and the Congressional Research Service.[55]

U.S. State Regulation

The states are taking a variety of approaches with respect to Bitcoin, with most driven by state banking, finance or securities agencies focused on consumer protection and anti-money laundering mandates. Some states are considering the regulation and licensing of activities involving bitcoins and other digital assets in accordance with their existing money transmitter and money service business laws. Others are considering amending their existing regulatory structure to better accommodate the use of digital assets.

Still other states have decided to implement a new regulatory regime, rather than apply existing money transmitter laws and regulations to bitcoins and other digital assets. New York adopted final regulations in June 2015, which are intended to regulate the conduct of businesses that are involved with digital assets, and to prohibit any person or entity involved in such activity to conduct activities without a license (BitLicense).[56] The regulations adopted by the New York State Department of Financial Services, among other things, require that

51. See SEC v. Trendon T. Shavers and Bitcoin Savings and Trust, U.S. District Court, Eastern District of Texas, No. 4:13-cv-00416. The initial civil complaint brought against Trendon T. Shavers for his operation of the Bitcoin Savings and Trust was filed in July 23, 2013. See "SEC Charges Texas Man With Running Bitcoin-Denominated Ponzi Scheme," SEC, July 23, 2013, available at sec.gov/News/PressRelease/Detail/PressRelease/1370539730583 (retrieved October 14, 2015). A judgment was entered against Shavers, subsequent to which criminal charges were filed on November 3, 2014. See "Manhattan U.S. Attorney and FBI Assistant Director Announce Securities and Wire Fraud Charges Against Texas Man For Running Bitcoin Ponzi Scheme," Department of Justice, November 6, 2014, available at www.justice.gov/usao-sdny/pr/manhattanus-attorney-and-fbi-assistant-director-announce-securities-and-wire-fraud (retrieved October 14, 2015).
52. In February 2014, the SEC halted trading in Imogo Mobile Technologies due to a lack of disclosure regarding the Bitcoin-related technology company's operations. See Angel Gonzalez, "SEC Suspends Trading in Murky Bellevue Tech Firm," Seattle Times, February 19, 2014, available at www.seattletimes.com/business/sec-suspends-trading-in-murky-bellevue-tech-firm/ (retrieved October 14, 2015). See also "Investor Alert: Bitcoin and Other Virtual Currency-Related Investments," SEC, May 7, 2014, available at sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html (retrieved October 14, 2015).
53. See, e.g., In the Matter of Erik T. Voorhees, Release No.9592, SEC, June 3, 2014, Administrative Proceeding File No. 3-15902, available at sec.gov/litigation/admin/2014/33-9592.pdf (retrieved October 14, 2015) and In the Matter of BTC Trading Corp and Ethan Burnside, Release No 9685, SEC, December 8, 2014, available at sec.gov/litigation/admin/2014/33-9685.pdf (retrieved October 14, 2015). In each case, the SEC settled with the subjects of investigations into the sale of unregistered securities that were offered on platforms that permitted the investment of bitcoins or litecoins for the purchase of such unregistered securities. The SEC actions did not consider the question of whether bitcoins, as the consideration for unregistered security sales, were themselves a security.
54. See "Investor Alert: Bitcoin and Other Virtual Currency-Related Investments," SEC, May 7, 2014, available at investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments (retrieved October 14, 2015) and "Investor Alerts – Bitcoin: More than a Bit Risky," Financial Industry Regulatory Authority, March 11, 2014, available at finra.org/investors/alerts/bitcoin-more-bit-risky (retrieved October 14, 2015).
55. See General Accountability Office, "Virtual Economies and Currencies," May 15, 2013, available at gao.gov/products/GAO-13-516 (retrieved October 20, 2015); General Accountability Office, "Virtual Currencies: Emerging Regulatory, Law Enforcement and Consumer Protection Challenges," May 29, 2014, available at gao.gov/products/GAO-14-496 (May 2014) (retrieved October 20, 2015); and Congressional Research Service, "Bitcoin: Questions, Answers, and Analysis of Legal Issues," October 13, 2015, available at fas.org/sgp/crs/misc/R43339.pdf (retrieved October 20, 2015).
56. "NYDFS Announces Final BitLicense Framework for Regulating Digital Currency Firms," New York Department of Financial Services, June 3, 2015, available at dfs.ny.gov/about/speeches/sp1506031.htm (retrieved October 14, 2015). The BitLicense regulations appear at New York Codes, Rules and Regulations, Title 23, Chapter I, Part 200 – Virtual Currencies, available at dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf (retrieved October 14, 2015).

licensees are adequately capitalized, maintain detailed books and records, adopt anti-money laundering policies that comply with the Bank Secrecy Act of 1979, ensure they have robust cybersecurity policies and incorporate a variety of other compliance policies.

Certain states may use the BitLicense as a template for new digital asset legislation or regulation, while others are designing their own regulatory regimes.[57] For example, the State Assembly of California is considering AB-1336, a virtual currency act that, among other things, will require annual renewable licensing from the Department of Business Oversight (absent an exemption).[58] Other states have examined the introduction of new, digital asset-focused frameworks or the amendment of current money transmission regulations to address digital assets.[59]

International Regulation

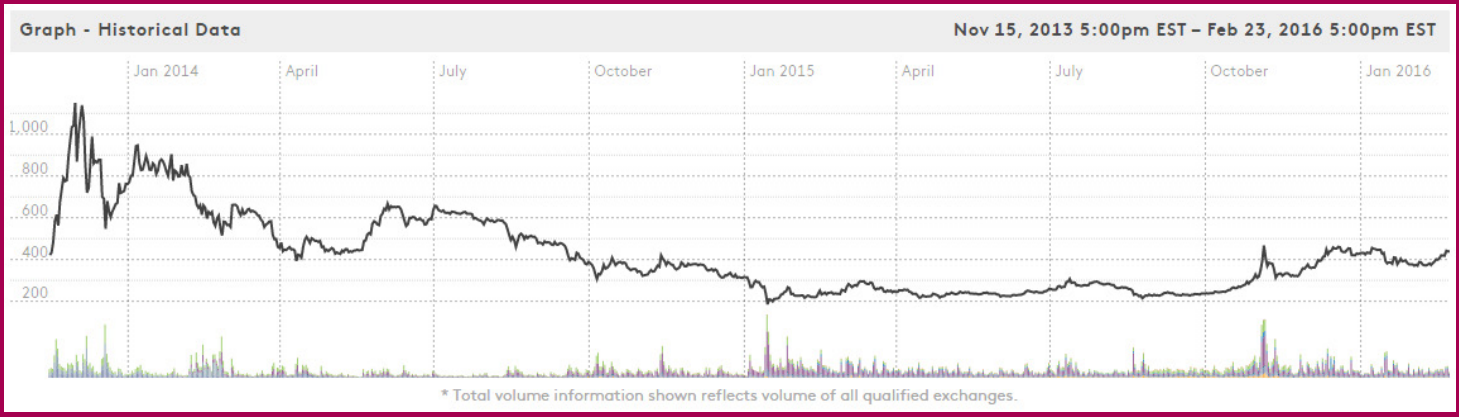
International regulation of Bitcoin is an even more diverse and fractured situation. While some governments such as the Isle of Man have been welcoming of the new technology, others such as Russia have been contentious, in no small part due to the threat Bitcoin may pose toward capital controls. A proper survey of international regulation is beyond the scope of this primer; however, many Eurozone and Commonwealth economies appear to be moving toward a regulatory stance similar to those taken in the United States.

Conclusion

Bitcoin and Blockchain technology are an important development in the FinTech economy. The Bitcoin Network has resulted in an important ecosystem with varied projects that have raised more than $1 billion in venture capital financings since 2013. Such investments will allow entrepreneurs and financial institutions to experiment with each of the Big "B" Bitcoin and the Blockchain, as well as, little "b" bitcoin in an effort to transform the way international finance and information technology operate.

Bitcoin has evolved past the historical difficulty and unsavory public association with bad actors. The promise that is provided is something which all participants in finance or FinTech must be keenly aware. Additionally, navigating and understanding the complex and evolving regulatory constructs around Bitcoin and Blockchain ventures is imperative for businesses seeking to participate in this exciting new ecosystem.

57. The Conference of State Bank Supervisors has released for comment a model regulatory framework for state level regulation of virtual currency businesses. See Draft Model Regulatory Framework, Conference of State Bank Supervisors, available at csbs.org/regulatory/ep/pages/framework.aspx (retrieved October 14, 2015).
58. California Legislature, Assembly Bill No 1326 – Virtual Currency, available at leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1326 (retrieved October 14, 2015).
59. See, e.g., Matt Friedman, "Regulation and Tax Breaks for Bitcoin Proposed by N.J. Lawmakers," NJ Advance Media, May 27, 2015, available at nj.com/politics/index.ssf/2015/05/regulation_and_tax_breaks_for_bitcoin_proposed_by.html (retrieved October 14, 2015) (discussing proposed new legislation for digital asset businesses) and North Carolina General Assembly House Bill 289, available at ncleg.net/gascripts/BillLookUp/BillLookUp.pl?BillID=H289&Session=2015 (retrieved October 14, 2015) (proposing the amendment of the North Carolina Money Transmitters Act to apply to digital assets such as bitcoins).



Bitcoin Price

The above chart shows the price of one bitcoin based on an exponential, volume-weighted average of the trading price on certain of the most liquid US dollar exchanges. The chart ranges from November 2013 to February 2016. (Source: WinkDex at winkdex.com)

The price of bitcoin experienced periods of extreme volatility, particularly during late 2013 to early 2014, when bitcoin trading prominently emerged in market headlines. The February 2014 collapse of early Bitcoin exchange giant Mt. Gox resulted in greater regulatory focus and consumer protection, and eventually in the establishment of regulated Bitcoin exchanges in the United States. In the 20 months since Mt. Gox, the professionalism and level of capitalization of prominent operators in the Bitcoin ecosystem has increased, although the majority of bitcoin trading continues to be conducted on overseas exchanges that are not currently fully compliant with U.S. federal and state regulatory registration and licensing requirements.

Bitcoin and Blockchain Glossary

Bitcoin – With a capitalized "B", Bitcoin refers to i) the Bitcoin Network, ii) the Source Code or software based on the Source Code, or iii) the general technology relating to Bitcoin and the Blockchain.

bitcoin – When a lowercase "b", bitcoin refers to a unit of account that may be transferred on the Bitcoin Network. There will be a maximum of 21 million bitcoins.

Blockchain – The distributed, public ledger containing the history of all transactions on the Bitcoin Network which is stored locally on the computer hard drive of each user running a full version of the Bitcoin Network software (some users, typically on smartphones, run a "lite" version of the software client that does not store the Blockchain).

The Blockchain includes the full list of blocks (which include all confirmed transaction data) that have been mined since the beginning of the Bitcoin Network. The Blockchain is designed so that each block contains a cryptographic reference to the block that came before it, thereby linking each block into a verifiable and tamperproof chain.

Address – A bitcoin address is used to receive and send transactions on the bitcoin network. It contains a string of alphanumeric characters, but can also be represented as a scannable QR code. A bitcoin address is also the public key in the pair of keys used by bitcoin holders to digitally sign transactions (see Public key).

Altcoin – The collective name for virtual currencies or digital assets offered as alternatives to Bitcoin. Litecoin, Feathercoin and Peercoin are all Altcoins.

ASIC – An Application Specific Integrated Circuit is a silicon chip specifically designed to do a single task. In the case of bitcoin, they are designed to process SHA-256 hashing problems, the proof-of-work algorithm used to mine new bitcoins.

Bitcoin 2.0 – A reference word for applications of Bitcoin or Blockchain technology that is more advanced or complicated than the basic payment system application proposed by the Bitcoin white paper. Examples of Bitcoin 2.0 projects include Counterparty, Ethereum, Blockstream, Swarm, Domus and Hedgy.

Bitcoin Network – The peer-to-peer computer network operating on the Source Code and supported by an infrastructure of user nodes and miners.

Block reward – The reward of bitcoins granted to a miner automatically when that miner solves for a "block". The block reward currently is 25 bitcoins per block, but the number will be halved in July 2016. A transaction granting a block reward to a miner is known as a "coinbase" (the base transaction for the new bitcoins).

Cold Storage – A term for various security measures used for keeping bitcoins offline to reduce the risk of remote access to a wallet's private key.

Confirmation – The inclusion of a transaction in a block added to the Blockchain, along with each subsequent block being added. Industry standard is that a transaction has fully cleared with six confirmations (i.e., inclusion in a block and the subsequent addition of five additional blocks).

Core Developers – Programmers working on the open-source Source Code for Bitcoin. They are not formally employed by or paid by, and are not in control of, the Bitcoin Network; however, they have elevated access on the GitHub resource page for the Bitcoin Network where the main "reference" version of the Source Code is developed.

Halving – Refers to reducing reward every 210,000 blocks (approximately every 4 years). Since the genesis block on January 9, 2009 to block 209,999 on November 28, 2012, the reward was 50 BTC. The reward will be 25 BTC (until approximately July 17, 2016), then 12.5 BTC and so on till 1 satoshi around 2140, after which point no more bitcoins will ever be created. Due to reward halving, the total supply of bitcoins is limited: only about 2,100 trillion satoshis (21 million bitcoins) will ever be created.

Hash or Hashing – A mathematical process that takes a variable amount of data and produces a shorter, fixed-length output. A hashing function has two important characteristics. Firstly, it is mathematically difficult to work out what the original input was by looking at the output. Secondly, changing even the tiniest part of the input will produce an entirely different output. Hashing is used in cryptography.

Hashrate – A measure of computing power, it is equal to the number of "hashes" that can be run in one second. The Hashrate is also sometimes referred to in PetaFlops (a measure of a computer's processing speed and can be expressed as a quadrillion (thousand trillion) floating point operations per second (FLOPS)).

Miners – The users on the Bitcoin Network that run specific Bitcoin software that allows them to validate, clear and record transactions on the Blockchain, all in exchange for a reward of newly created bitcoins.

Node – A computer connected to the Bitcoin Network using a Bitcoin software program that relays transactions to others. Each user actively on the Bitcoin Network is a node.

P2P or peer-to-peer – Decentralized interactions that happen between at least two parties in a highly interconnected network. An alternative system to a 'hub-and-spoke' arrangement, in which all participants in a transaction deal with each other through a single mediation point.

Private key – An alphanumeric string kept secret by the user, and designed to sign a digital communication when hashed with a public key. In the case of Bitcoin, this string is a private key designed to be mathematically linked to a ***public key*** (which can be publicly distributed). The public-private key pair form of cryptography is standard and accepted security practice. A third party can verify that a digital signature was issued by a private key by comparing the digital signature with the public key, all without having to know the actual private key.

Satoshi – The smallest unit that may be sent on the Bitcoin Network, it is equivalent to 1/100,000,000th of one bitcoin.

Source Code – The open-source software which includes protocols governing rules for movement and ownership of bitcoins and the cryptography system that secures and verifies Bitcoin transactions.

Transaction – A chunk of binary data that describes how bitcoins are moved from one owner to another. Transactions are stored in the Blockchain. Every transaction (except for coinbase transactions) has a reference to one or more previous transactions (inputs) and one or more rules on how to spend these bitcoins further (outputs).

Transaction fee or miner fee – A small fee imposed on some transactions sent across the Bitcoin Network. The transaction fee is awarded to the miner that successfully hashes the block containing the relevant transaction.

Wallet - A method of storing bitcoins for later use. A wallet holds the private keys associated with Bitcoin addresses. The Blockchain is the record of the bitcoin amounts associated with those addresses. Because a wallet's address and public key are not secret and are associated with the wallet, a wallet and address are sometimes used interchangeably.

About Kaye Scholer's FinTech Practice

Financial Technology is driving rapid change in the Financial Services industry and in the way we spend, save, transfer and invest our money. Our deep experience with emerging growth and expanding companies extends to all industries in the global economy where novel technologies and business models are reshaping the market. Kaye Scholer is committed to advising all the players in this evolving area, including public and venture-backed FinTech businesses, financial institutions, venture capital firms, funds and card associations, in order to help them mitigate risks and identify and take advantage of opportunities. We offer sophisticated counsel in a broad range of areas, including:

- Virtual Currency: counsel companies that are developing fundamental financial businesses for the virtual currency ecosystem, specifically advising on the creation of the first bitcoin ETF and one of the first US regulated bitcoin exchanges; routinely advises funds and banks on "virtual currency" related matters.
- Exchange-Traded Funds: assist clients with regulatory, structural, operational, trading, listing and compliance issues related to ETFs, open-end investment companies and UITs registered under the 1940 Act, liquid alternatives, derivative securities and the licensing of financial indexes and services for use with those products.
- Corporate, Venture, IPOs & M&A: represent FinTech companies in the negotiation of venture rounds, initial public offerings, mergers, stock, asset and whole-business acquisitions, and other transactions involving changes in corporate control, as well as advise on general corporate advice, SEC reporting and compliance, and the issuances of registered and exempt securities.
- State and federal regulatory matters: advise clients on financial and payment system regulation, consumer and commercial lending regulation, start-up regulations in connection to state lender licensing laws and money transmitter laws, and CFPB, FTC, FinCEN, SEC, CFTC, OFAC and bank regulatory laws and regulations.
- Marketplace Lending: represent major financial institutions acting as lenders, structuring agents and initial purchasers in warehouse lending facilities to fund purchases of marketplace loans and in securitization transactions backed by marketplace loans.
- Emerging Growth: represent and partner with next generation financial technology and payments companies across the FinTech industries, including lending exchanges, payments, point of sale, personal financial management, virtual currency and SaaS.
- Technology and Digital Transactions: help market leaders and innovators in the FinTech, Mobile, eCommerce, and SaaS sectors, among many others, execute transactions related to the development, acquisition, licensing, sourcing and integration of complex technologies, systems and software.
- Cybersecurity and privacy: ensure that payment systems and technologies are both inherently secure and that they provide security and privacy for customers; provide strategic advice to resolve complex cybersecurity issues at the intersection of law, security, policy, technology, innovation and economics.
- Antitrust and other litigation matters: perform antitrust reviews of mergers and anticompetitive conduct in these markets, as well as labor and employee benefits matters.
- International: advise on potential FinTech structures to raise debt and equity and international structuring of financial technology.

Contacts

Gregory E. Xethalis
Counsel, Kaye Scholer LLP
+1 212 836 7730
gregory.xethalis@kayescholer.com

Kathleen H. Moriarty
Partner, Kaye Scholer LLP
+1 212 836 8276
kathleen.moriarty@kayescholer.com

Jenna B. Levy
Associate, Kaye Scholer LLP
+1 212 836 7729
jenna.levy@kayescholer.com

Chicago
Frankfurt
London
Los Angeles
New York
Shanghai
Silicon Valley
Washington, DC
West Palm Beach

www.kayescholer.com