THE BITCOIN INDUSTRY AND MARKET

Bitcoin is a decentralized digital currency that enables instant transfers to anyone, anywhere in the world. Managing transactions in bitcoins occurs via an open source, cryptographic protocol platform known as the Bitcoin Network, which uses peer-to-peer technology to operate with no central authority. The Bitcoin Network is an online, end-user-to-end-user network that hosts the public transaction ledger, known as the Blockchain, and the source code that comprises the basis for the cryptographic and algorithmic protocols governing the Bitcoin Network.

No single entity owns or operates the Bitcoin Network, the infrastructure of which is collectively maintained by a decentralized user base. As the Bitcoin Network is decentralized, it does not rely on either governmental authorities or financial institutions to create, transmit or determine the value of bitcoins.

Rather, the value of bitcoins is determined by the supply of and demand for bitcoins in the Bitcoin Exchange Market, the prices set in transfers by mutual agreement or barter as well as the number of merchants that accept bitcoins.

Because bitcoins are digital files that can be transferred without the involvement of intermediaries or third parties, there are little or no transaction costs in direct end-user-to-end-user transactions.

Bitcoins can be used to pay for goods and services or can be converted to fiat currencies, such as the USD, at rates determined by the Bitcoin Exchanges. Additionally, third party service providers such as Bitcoin Exchanges are also used for transfers but they may charge significant fees for processing transactions. On November 1, 2008 an individual (or possibly a group of individuals) published a research paper under the name of Satoshi Nakamoto describing the design for a new virtual currency called bitcoin. Shortly thereafter, on January 3, 2009, Mr. Nakamoto mined the first 50 bitcoins, known as the genesis block, and with this, he set off a new era of digital currency. While Mr. Nakamoto is considered to be the creator of bitcoins and the Bitcoin Network, no individual with that name has been reliably identified as the Bitcoin Network's creator. Satoshi Nakamoto is apparently a pseudonym for the inventor or the group of inventors responsible for the creation of bitcoins.

After the creation of the genesis block, the Bitcoin Network was initially formed mostly by a small group of early adopters. It started to gain traction approximately a year later and was quickly adopted by a vast peer-to-peer network. Mr. Nakamoto, or the individual or group which used the pseudonym, disappeared shortly after the creation of the Bitcoin Network, however, despite his anonymity and eventual disappearance from the web, the use of the Bitcoin Network among early adopters continued to grow, highlighting the strengths of the Bitcoin Network he created – a decentralized network with no single representative body. Today the Bitcoin Network is sustained by a significant number of miners, programmers, bitcoin account holders and service providers that collectively provide the Bitcoin Network with more computer processing

strength than the most powerful supercomputer in the world. The Bitcoin Network is now, and for a while has been, under active, unofficial development by a group of engineers headed by Gavin Andresen, Chief Scientist at the Bitcoin Foundation, and Wladimir J. van der Laan, who was appointed to the role of lead developer in April 2014. As an open source project, bitcoin is not represented by an official organization or authority, although groups including, most prominently, the Bitcoin Foundation work to organize the bitcoin community and to develop and protect the Bitcoin Network's code. 16

The Bitcoin Network's Operations

In order to own, transfer or use bitcoins, a person generally must have Internet access to connect to the Bitcoin Network. Bitcoin transactions between parties occur very rapidly (within several seconds) and may be made directly between end-users without the need for a third-party intermediary, although there are entities that provide third-party intermediary services. To prevent the possibility of double-spending a single bitcoin, each transaction is recorded, time stamped and publicly displayed in a "block" in the publicly available Blockchain.

Thus, the Bitcoin Network provides confirmation against double-spending by memorializing every transaction in the Blockchain, which is publicly accessible and downloaded in part or in whole by all users' Bitcoin Network software programs (described below). This memorialization and verification against double-spending is accomplished through the bitcoin mining process, which adds "blocks" of data, including recent transaction information, to the Blockchain.

Bitcoin Transfers

Prior to engaging in bitcoin transactions, a user must first obtain a digital bitcoin "wallet" (analogous to a bitcoin account) in which to store bitcoins. A "wallet" is an open-source software program that generates bitcoin addresses and enables users to engage in the transfer of bitcoins with other users. A user may install a bitcoin software program on its computer or mobile device that will generate a bitcoin wallet or, alternatively, a user may retain a third party to create a digital wallet to be used for the same purpose.

There is no limit on the number of digital wallets a user can have, and each such wallet includes one or more unique addresses and a verification system for each address consisting of a "public key" and a "private key," which are mathematically related. In a typical bitcoin transaction, the bitcoin recipient creates a new bitcoin address and directs the payor to send the payment to the address by providing the address, or public key, which encodes the payment and serves as an address for the digital wallet, to the payor who will initiate the transfer. This activity is analogous to a recipient providing an address in wire instructions to the payor so that cash may be wired to the recipient's account.

The payor approves the transfer to the address provided by the recipient by “signing” the transaction request from the recipient with the private key of the address from where the payor is transferring the bitcoins. The recipient does not make public its related private key or provide it to the payor, because the private key authorizes access to, and transfer of, the funds from the recipient’s digital wallet to other users. The process of signing the transaction is typically automated by the software that runs the payor and recipients digital wallet.

The transfer is made from the payor to the recipient’s wallet and this transaction is validated by the Bitcoin Network.

“Off-Blockchain transactions” involve the transfer of control over or ownership of a specific digital wallet holding bitcoins or of the reallocation of ownership of certain bitcoins in a pooled-ownership digital wallet, such as a digital wallet owned by a Bitcoin Exchange. Information and data regarding Off-Blockchain transactions is generally not publicly available in contrast to true bitcoin transactions, which are publicly recorded on the Blockchain. Off-Blockchain transactions are not truly bitcoin transactions in that they do not involve the transfer of transaction data on the Bitcoin Network and do not reflect a movement of bitcoins between addresses recorded in the Blockchain. Off-Blockchain transactions are subject to risks as 17 any such transfer of bitcoin ownership is not protected by the protocol behind the Bitcoin Network or recorded in and validated through the Blockchain mechanism.

Cryptographic Security Used in the Bitcoin Network

Public and Private Keys

All transactions on the Bitcoin Network are secured using public-key cryptography, a technique which underpins many online transactions. Public-key cryptography works by generating two mathematically related keys (one a public key and the other a private key) in such a way that the encrypting key cannot be used to decrypt a message and vice versa. One of these, the private key, is retained in the individual’s wallet and the other key is made public and serves as the address to which a bitcoin can be transferred and from which money can be transferred by the owner of the bitcoin wallet. In the case of bitcoin transactions the public key generates an address (a string of letters and numbers) that is used to encode payments, which can then only be retrieved with the associated private key that is used to authorize the transaction. In other words, the payer, uses his private key to approve any transfers to a recipient's account. Users on the Bitcoin Network can confirm that the user signed the transaction with the appropriate private key, but cannot reverse engineer the private key from the signature.

Double-Spending and the Bitcoin Network Confirmation System

To ensure the integrity of bitcoin transactions from the recipient’s side (i.e., to prevent double-spending by a payor), every bitcoin transaction is broadcast to the Bitcoin

Network and recorded in the Blockchain through the “mining” process (defined below), which time-stamps the transaction and memorializes the change in the ownership of the bitcoin(s) transferred. Adding a block to the Blockchain requires bitcoin “miners” (defined below) to exert significant computational effort to verify it is a valid transaction. Requiring this computational effort, or “proof of work,” prevents a malicious actor from either adding fraudulent blocks to generate bitcoins (i.e., counterfeit bitcoins) or overwriting existing valid blocks to reverse its prior transactions. A transaction in bitcoins between two parties is recorded in the Blockchain in a block only if that block is accepted as valid by a majority of the nodes on the Bitcoin Network. Validation of a block is achieved by confirming the cryptographic hash value included in the block’s solution and by the block’s addition to the longest confirmed Blockchain on the Bitcoin Network. For a transaction, inclusion in a block on the Blockchain constitutes a “confirmation” of the bitcoin transaction. As each block contains a reference to the immediately preceding block, additional blocks appended to and incorporated into the Blockchain constitute additional confirmations of the transactions in such prior blocks, and a transaction included in a block for the first time is confirmed once against double-spending. The layered confirmation process makes changing historical blocks (and reversing transactions) exponentially more difficult the further back one goes in the Blockchain. Bitcoin Exchanges and users can set their own threshold as to how many confirmations are required until funds from the transferor are considered valid. However, statistically speaking, a transaction is virtually final after six confirmations as it would be extremely difficult to challenge the validity of the transaction at that point. 18 At this point in the evolution of the Bitcoin Network, bitcoin transactions are considered irreversible. Once a transaction appears in the Blockchain, no one has the authority to reverse it. If someone were to attempt to undo a past transaction in a block recorded on the Blockchain, such individual would have to exert tremendous processing power in a series of complicated transactions that may not be achieved at this point in the Bitcoin Network’s development.

Bitcoin Mining – Creation of New Bitcoins

Mining Process

The process by which bitcoins are created and bitcoin transactions are verified is called mining. To begin mining, a user, or “miner,” can download and run a mining client, which, like regular Bitcoin Network software programs, turns the user’s computer into a “node” on the Bitcoin Network that validates blocks. Each bitcoin transaction results in new blocks being added to the Blockchain and new bitcoins being issued to the miners. Miners, through the use of the bitcoin software program, engage in a set of prescribed complex mathematical calculations in order to add a block to the Blockchain and thereby confirm bitcoin transactions included in that block’s data. All bitcoin transactions are recorded in blocks added to the Blockchain. Each block contains the details of some or all of the most recent transactions that are not memorialized in prior blocks, as well as a record of the award of bitcoins to the miner who added the new block. In order to add blocks to the Blockchain, a miner must map an input data set (i.e., the Blockchain, plus a block of the most recent

Bitcoin Network transactions and an arbitrary number called a “nonce”) to a desired output data set of a predetermined length (the “hash value”) using the SHA-256 cryptographic hash algorithm. Each unique block can only be solved and added to the Blockchain by one miner; therefore, all individual miners and mining pools on the Bitcoin Network are engaged in a competitive process of constantly increasing their computing power to improve their likelihood of solving for new blocks. As more miners join the Bitcoin Network and its processing power increases, the Bitcoin Network adjusts the complexity of the block-solving equation to maintained a predetermined pace of adding a new block to the Blockchain approximately every ten minutes. A miner’s proposed block is added to the Blockchain once a majority of the nodes on the Bitcoin Network confirms the miner’s work. Miners that are successful in adding a block to the Blockchain are automatically awarded a fixed number of bitcoins for their effort plus any transaction fees paid by transferors whose transactions are recorded in the block. This reward system is the method by which new bitcoins enter into circulation to the public. Incentives for Mining As noted above, miners that are successful in adding a block to the Blockchain are automatically awarded a fixed number of bitcoins for their effort. Given the increasing difficulty of the target established by the Bitcoin Network, current miners are required to invest in expensive mining devices with adequate processing power to hash at a competitive rate. The first wave of mining devices used central processing units (CPUs) used in standard home computers. Miners soon discovered that graphic processing units (GPUs) provided them with more processing power and the second wave of miners entered the Bitcoin Network. Today, the Bitcoin Network is well into a 19 third wave of mining devices which consist of mining computers that are designed solely for mining purposes. Such devices include ASIC (application-specific integrated circuit) machines built specifically for bitcoin mining by specialized companies like Cointera and HashFast. These new computers are significantly more expensive than standard home computers. Miners also incur substantial electricity costs in order to continuously power and cool their devices while solving for a new block. Blockchain decreases over time and the production (and reward) of bitcoins will eventually cease. Once such incentive mechanism ceases to be profitable, miners will only have transaction fees to incentivize them and as a result, it is expected that miners will need to be better compensated with higher transaction fees to ensure that there is adequate incentive for them to continue mining.

Mining Pools

The significant increase in the number of miners and the increasing in mining capacity have radically increased the difficulty of finding a valid hash since the first block was mined. In some respects, hashing is akin to a mathematical lottery, and miners that have devices with greater processing power (i.e., the ability to make more hash calculations per second) are more likely to be successful miners.

Currently, the likelihood that an individual acting alone will be able to be awarded a bitcoin is extremely low. As a result, mining “pools” have developed in which multiple miners act cohesively and combine their processing power to solve blocks. When a

pool solves a new block, the pool operator receives the bitcoin and, after taking a nominal fee, splits the resulting reward among the pool participants based on the processing power they each contributed to solve for such block. Mining pools provide participants with access to smaller, but steadier and more frequent, bitcoin payouts.

According to blockchain.info, as of October 15, 2014, the largest three identifiable mining pools were Discus Fish, Ghash.io, and KnCMiner, which, when aggregated, represented approximately 55% of the processing power on the Bitcoin Network (as calculated by determining the percentage of blocks mined by each such pool over the prior four days). Also according to blockchain.info, on such date, the eight largest identifiable pools (Discus Fish, GHash.io, KnCMiner, Elgius, BTC Guild, two unnamed pools, and Slush) accounted for 74% of the mining processing power on the Bitcoin Network. In late May and early June 2014, reports indicated that GHash.io approached and, during a 24- to 48-hour period in early June, may have exceeded one-half of the processing power on the Bitcoin network, as measured by the self-reported processing power of the pool and by measuring the percentage of blocks mined by the pool.

It has not been confirmed whether GHash.io exceeded one-half of the processing power on the Bitcoin Network for any period of time, and its percentage of the processing power on the Bitcoin Network has since fallen below 40 percent. As of October 16, 2014, GHash.io was determined to have found 22 percent of blocks over the prior four days by blockchain.info.

Mathematically Controlled Supply

The supply of new bitcoins is mathematically controlled in a manner so that the number of bitcoins grows at a limited rate pursuant to a pre-set pace. To achieve this, the bitcoin source code is designed to automatically halve the number of bitcoins awarded for solving a new block after every 210,000 blocks are added to the Blockchain. Currently, the fixed reward for solving a new block is 25 bitcoins per block and this is expected to decrease by half to become 12.5 bitcoins after the next 210,000 blocks have entered the Bitcoin Network.

This deliberately controlled rate of 20 bitcoin creation means that the number of bitcoins in existence will increase at a controlled rate until the number of bitcoins in existence reaches the pre-determined 21 million bitcoins. As of December 31, 2014, over 13.67 million bitcoins have been mined and estimates of when the 21 million bitcoin limitation will be reached range from 2022 to 2140.

Modifications to the Bitcoin Protocol Bitcoin is an open source project (i.e., a product whose source code is freely available to the public and that utilizes crowdsourcing to identify possible issues, problems and defects) with no official developer or group of developers that controls the Bitcoin Network.

However, the Bitcoin Network’s development is overseen by a core group of

developers at the Bitcoin Foundation (the “Core Developers”). The Core Developers are able to access and can alter the Bitcoin Network source code and, as a result, they are responsible for quasi-official releases of updates and other changes to the Bitcoin Network’s source code. The release of updates to the Bitcoin Network’s source code does not guarantee that the updated will be automatically adopted. Users and miners must accept any changes made to the bitcoin source code by downloading the proposed modification of the Bitcoin Network’s source code.

A modification of the Bitcoin Network’s source code is only effective with respect to the bitcoin users and miners that download it. If a modification is accepted only by a percentage of users and miners, a division in the Bitcoin Network will occur such that one network will run the pre-modification source code and the other network will run the modified source code; such a division is known as a “fork” in the Bitcoin Network. Consequently, as a practical matter, a modification to the source code (e.g., a proposal to increase the 21 million total limit on bitcoins or to reduce the average confirmation time target from 10 minutes per block) only becomes part of the Bitcoin Network if accepted by participants collectively having a majority of the processing power on the Bitcoin Network. Bitcoin Value Bitcoins are not a fiat currency (i.e., a currency that is backed by a central bank or a national, supra-national or quasi-national organization) and are not backed by hard assets or other credit.

As a result, the value of bitcoins is currently determined by the value that various market participants place on bitcoins through their transactions. Exchange Valuation Due to the peer-to-peer framework of the Bitcoin Network and the protocols thereunder, transferors and recipients of bitcoins are able to determine the value of the bitcoins transferred by mutual agreement or barter with respect to their transactions.

As a result, the most common means of determining the value of a bitcoin is by surveying one or more Bitcoin Exchanges where bitcoins are bought, sold and traded. On each Bitcoin Exchange, bitcoins are traded with publicly disclosed valuations for each transaction, measured by one or more fiat currencies such as the USD or the Chinese Yuan.

Bitcoin price indexes have also been developed by a number of service providers in the bitcoin space. For example, Coindesk, a digital currency content provider, launched a proprietary bitcoin price index in September 2013 and bitcoinaverage.com provides an average of all bitcoin prices on several Bitcoin Exchanges. The Sponsor uses the Index calculated by TradeBlock to determine the Bitcoin Market Price, as described under “Description of the 21 Trust– Bitcoin Market Price”. Additionally, the XBT designation as bitcoin’s ISO 4217 currency code is already accepted by some providers for data feeds and a number of data feeds and other trading platforms are contemplating adopting XBT for their trading platforms. As the bitcoin price discovery and the adoption of XBT become main stream, the valuation of bitcoins will be more akin to the valuation of a fiat currency. Forms of Attack Against the Bitcoin Network Exploitation of Flaws in the Bitcoin Network’s Source Code As with any other computer code, flaws in the Bitcoin Network source code have been exposed by certain

malicious actors. Several errors and defects have been found and corrected, including those that disabled some functionality for users, exposed users' information, or allowed users to create multiple views of the Bitcoin Network. Discovery of flaws in or exploitations of the source code that allow malicious actors to take or create money in contravention of known Bitcoin Network rules have been relatively rare.

For example, in 2010, a hacker or group of hackers exploited a flaw in the Bitcoin Network source code that allowed them to generate 184 billion bitcoins in a transaction and send them to two digital wallet addresses. However, the bitcoin community and developers identified and reversed the manipulated transactions within approximately three hours, and the flaw was corrected with an updated version of the bitcoin protocol.

The Core Developers, in conjunction with other developers and miners, work continuously in an attempt to ensure that flaws are quickly fixed or removed. Because open source codes rely on transparency to promote community-sourced identification and solution of problems within the code, such flaws have been discovered and quickly corrected by the Core Developers or the bitcoin community.

Greater than Fifty Percent of Network Computational Power

A malicious actor can structure an attack whereby such actor gains control of more than half of the Bitcoin Network's processing power or "hashrate." During May and June 2014, mining pool GHash.io's hashing power approached 50 percent of the processing power on the Bitcoin Network. During a brief period in early June, the mining pool may have controlled in excess of one-half of the Bitcoin Network's processing power. Although no malicious activity or abnormal transaction recording was observed, the incident establishes that it is possible that a substantial mining pool may accumulate close to or more than a majority of the processing power on the Bitcoin Network.

If a malicious actor acquired sufficient computational power necessary to control the Bitcoin Network, among other things, it would be able to reverse transactions and possibly engage in double-spending, or prevent some or all transactions from being confirmed, and prevent some or all other miners from mining any valid new blocks. A number of computer scientists and cryptographers believe that the immense collective processing power of the Bitcoin Network makes it impracticable for an actor to gain control of computers representing a majority of the processing power on the Bitcoin Network. Some estimates indicate that it may currently require an investment of approximately $400 million dollars to be able to purchase the necessary hardware to control 51% of the Bitcoin Network. 22

Cancer Nodes

Cancer nodes are fake internet protocols (IPs), which a malicious actor sets up to either place the user on a separate network or disconnect them from all networks. This

form of attack involves a malicious actor propagating “cancer nodes” to isolate certain users from the legitimate Bitcoin Network. A target user who is surrounded by such cancer nodes would be placed on a separate “network,” allowing the malicious actor to relay only blocks created by the separate network and thus opening the target user to double-spending attacks. By using cancer nodes, a malicious actor also can disconnect the target user from the bitcoin economy entirely by refusing to relay any blocks or transactions. Bitcoin software programs make these attacks more difficult by limiting the number of outbound connections through which users are connected to the Bitcoin Network.

Double Spending Risks

A malicious actor may attempt to double-spend bitcoins by manipulating the formation of the Blockchain rather than through control of the Bitcoin Network. Variations of this form of attack include the “Finney attack,” “race attack,” and “vector76 attack.” In this type of attack, a miner creates a valid new block containing a double-spend transaction and schedules the release of such attack block so that it is added to the Blockchain before a target user’s legitimate transaction can be included in a block. All double-spend attacks require that the miner sequence and execute the steps of its attack with sufficient speed and accuracy.

Typically, transactions that allow for a zero-confirmation acceptance tend to be prone to these types of attacks. Users and merchants can reduce the risk of a double-spend attack by waiting for multiple confirmations from the Bitcoin Network before settling a transaction.

These attacks require extensive coordination and are very expensive. Accordingly, traders and merchants may still execute instantaneous, low-value transactions without confirmation, because it is generally agreed that a malicious miner would be unwilling to carry out a double-spend attack for low-value transactions. Users and merchants can take additional precautions by adjusting their Bitcoin Network software programs to connect only to other well-connected nodes and to disable incoming connections.

These precautions reduce the risk of double-spend attacks involving manipulation of a target’s connectivity to the Bitcoin Network (as is the case with vector76 and race attacks). Uses of Bitcoins Global Bitcoin Market Global trade in bitcoins consists of individual end-user-to-end-user transactions, together with facilitated exchange-based bitcoin trading. A limited market currently exists for bitcoin-based derivatives. There is currently no reliable data on the total number or demographic composition of users or miners on the Bitcoin Network.

Bitcoin Exchange Market

Online Bitcoin Exchanges represent a substantial percentage of bitcoin buying and selling activity and provide the most data with respect to prevailing valuations of bitcoins. Currently, there are several Bitcoin Exchanges servicing approximately 200

countries.

These exchanges include 23 established exchanges such as Bitstamp, BTC-e, and Bitfinex, which provide a number of options for buying and selling bitcoins. In addition to open online Bitcoin Exchanges, there are “dark pools” where market participants have the ability to execute large block trades without adversely impacting the price of bitcoins. Tradehill, which is no longer operating, was an example of one such dark pool. Goods and Services Bitcoins increasingly can be used to purchase goods and services, either online or at physical locations.

While reliable data is not readily available on the retail and commercial market penetration of the Bitcoin Network, there are numerous indications of its increasing acceptance. For example, the bitcoin payment processors Bitpay and Coinbase publicly represent that over 88,000 businesses and organizations (in approximately 200 countries) are now using those processors’ services to accept bitcoin payments. Additionally, PayPal recently announced that it would allow merchants that use its payment processing services to accept bitcoin.

A wide range of industries now accept bitcoins as a form of payment, from newspapers such as The Chicago Sun-Times to national sports franchises such as the Sacramento Kings. There are also many real-world locations that accept bitcoin, several of which are located in New York City. Additionally, for-profit internet-based companies such as Microsoft, WordPress, Reddit, Zynga, Expedia, Dell, TigerDirect.com and Overstock.com, as well as non-profit institutions such as Khan Academy have received attention for accepting donations in bitcoins.

End-User-to-End-User

The bitcoin end-user-to-end-user ecosystem operates on a continuous, 24-hour per day basis. This is accomplished through decentralized peer-to-peer transactions between parties on a principal-to-principal basis. All risks and issues of credit are between the parties directly involved in the transaction.

Liquidity can change from time to time during the course of a 24-hour trading day. The Bitcoin Network rules that require transaction fees are generally not enforced, therefore transaction costs, if any, are negotiable between the parties and may vary widely, although, where transaction fees are included, they are paid by the sending party in a bitcoin transaction.

These transactions occur remotely through the Internet, in-person through forums such as localbitcoins.com (which offers both online and in-person opportunities to buy and sell bitcoins), Satoshi Squares (an open-air bitcoin trading market held in cities throughout the U.S. and overseas), or the Bitcoin Center NYC and physically through bulletin boards.

There are currently no official designated market makers for bitcoins and hence no

standard transaction sizes, bid-offer spreads or typical known cost per transaction. Marketplaces like localbitcoins.com and Satoshi Square are intended to create a market by bringing together counterparties trading in bitcoins but they do not provide any clearing or intermediary function.

Anonymity and Illicit

Use Bitcoins have a reputation for providing privacy to its users, but the Bitcoin Network was not designed to ensure the anonymity of users. While the Blockchain records the unique addresses of individual bitcoin “wallets,” it does not contain anything about the people using them.

However, an analysis of the public log of all bitcoin transactions suggests that it may be easy for a law enforcement agency to identify a number of bitcoin users. (Off-Blockchain transactions occurring 24 off the Bitcoin Network are not recorded and do not represent actual bitcoin transactions or the transfer of bitcoins from one digital wallet address to another, though information regarding participants in an Off-Blockchain transaction may be recorded by the parties facilitating such Off-Blockchain transactions). Nevertheless, users determined to maintain anonymity may take certain precautions to enhance the likelihood that they and their transactions remain anonymous.

For instance, a user may send its bitcoins to different addresses multiple times to make tracking the bitcoins through the Blockchain more difficult or, more simply, engage a so-called “mixing” service to switch its bitcoins with those of other users. As with any other asset or medium of exchange, bitcoins can be used to purchase illegal goods, fund illicit activities or to launder money. Bitcoins have been used for illicit gambling and making purchases of illegal goods.

For example, Silk Road, an anonymous online marketplace that sold illegal substances prior to its seizure and the arrest of its founder and operator in October 2013, accepted only bitcoins. In November 2014, a number of U.S. and foreign law enforcement agencies seized Silk Road 2.0, Hydra and Cloud 9, among others, which were allegedly similar online marketplaces, although other similar websites remain operational.

Additionally, Charlie Shrem, the founder of Bitinstant and a former vice chairman of the Bitcoin Foundation, was charged with money laundering and operating an unlicensed money transmitting business, and pleaded guilty in September 2014 to aiding and abetting an unlicensed money transmitting business. The use of bitcoins for illicit purposes, however, is not promoted by the Bitcoin Network or the user community as a whole.

Competition

Bitcoins are not the only type of digital currencies founded on cryptography, although

as of the date of this Disclosure Statement it is considered the most prominent. Other cryptographic digital currencies have developed since the Bitcoin Network's inception: Litecoin, Ripple, PPCoin and Terracoin are just a few examples of bitcoin alternatives. The Bitcoin Network, however, possesses the "first-to-market" advantage and has captured the majority of the industry's market share.

Government Oversight

Digital currencies, such as bitcoin, are a recent technological innovation and the regulatory schemes to which bitcoins and the Bitcoin Network may be subject have not been fully explored or developed. For example, the SEC and CFTC are exploring ways to regulate bitcoins but have yet to issue official statements describing how each will treat bitcoins for a variety of regulatory purposes.

On March 25, 2014, the IRS issued Notice 2014-21 containing guidance and frequently asked questions relating to virtual currencies such as bitcoins. The Notice concludes that, for U.S. federal tax purposes, virtual currency should be treated as property, and general tax principles applicable to property transactions should also apply to transactions using virtual currency. FinCEN has also released official guidance concerning bitcoins and the Bitcoin Network. On March 18, 2013, FinCEN issued interpretive guidance relating to the application of the Bank Secrecy Act to distributing, exchanging and transmitting "virtual currencies." More specifically, it 25 determined that a user of bitcoins will not be considered a money services business or be required to register, report and perform recordkeeping; however, an administrator or exchanger of bitcoins must be a registered money services business under FinCEN's money transmitter regulations. As a result, Bitcoin Exchanges that deal with U.S. residents or otherwise fall under U.S. jurisdiction are required to register with FinCEN and comply with FinCEN regulations.

On January 30, 2014, FinCEN published two interpretive letters elaborating on the original guidance. One addresses bitcoin mining operations and confirms, among other things, that "so long as the user is undertaking the transaction solely for the user's own purposes and not as a business service performed for the benefit of another," the miner is not engaged in money transmission services through the sale of its own mined bitcoins and dividend of profits to investors. The other interpretation addresses certain bitcoin investment activities and provides that the investment in bitcoin for the benefit of the investor itself is not, under the circumstances described in the interpretation, money transmission for purposes of the FinCEN regulations. However, the interpretation also notes that the provision of investment-related or brokerage services in connection with such investment activity would require additional analysis. The interpretation further provides that the provision of software for bitcoin services is not considered money transmission under the circumstances described in the interpretation.

On October 27, 2014, FinCEN published two more interpretive letters further elaborating on its March 2013 guidance. One letter indicated that a virtual currency

exchange, even where it buys from customers for the exchange's inventory and sells to customers out of its own inventory, acting as a dealer rather than a broker, is nevertheless engaged in money transmission, under the circumstances described in the interpretation. The other letter indicated that a company that provides payment processing services by taking legal tender payments from customers of merchants and providing those merchants with payments in bitcoin is engaged in money transmission, under the circumstances described in the interpretation.

Similarly, U.S. states have begun to examine whether bitcoin activities require licensing under applicable state money services business, money transmitter, prepaid or stored value, or virtual currency business laws.

A number of states, such as California, Idaho, New York, Virginia and Washington, are actively requiring bitcoin businesses to register on a state level as money transmitters or money service businesses.

However, certain other state regulators, such as the Texas Department of Banking and the Kansas Office of the State Bank Commissioner, have found that bitcoins do not constitute money, and that transmission of bitcoin does not constitute money transmission requiring licensure.

On June 28, 2014, the Governor of the State of California signed into law a bill that removed state-level prohibitions on the use of alternative forms of currency or value (including bitcoins).

The New York Department of Financial Services ("NYDFS") also held hearings on January 28, 2014 and January 29, 2014 as part of an ongoing inquiry into the appropriate regulatory guidelines for virtual currencies. On March 14, 2014, NYDFS issued a public order that the department would consider formal proposals and applications in connection with the establishment of regulated virtual currency exchanges operating in New York. On July 17, 2014, the NYDFS published its proposed comprehensive regulatory scheme for virtual currency businesses, called the "BitLicense." Prompted by concerns about the use of virtual currency in money laundering, consumer fraud and other criminal activity, the proposal represents one of the first attempts to comprehensively regulate bitcoin and other virtual currency activities. Under the proposed 26 regulations, most businesses involved in virtual currency transactions in or involving New York, excluding merchants (as well as consumers), would be required to apply for licenses from the NYDFS.

The proposed regulations also have anti-money laundering, cyber security, consumer protection, and financial and reporting requirements, among others. Many commentators, including those who have published comment letters, have stated that if finalized as proposed, the regulations would profoundly impact the virtual currency industry, for example by creating significant compliance costs and high barriers to entry for new bitcoin and virtual currency businesses. Other states and countries are likely to look to the BitLicense regime when determining whether and how to regulate

bitcoin-related activities. The Superintendent of the NYDFS has stated that the NYDFS expects to repropose the regulations with certain changes, which the Superintendent of the NYDFS has indicated will include the clarification that mere software developers and miners will not be required to be licensed, and the introduction of a transitional license for startups and new businesses with tailored requirements and examinations, among other changes. The Superintendent of the NYDFS has stated that the BitLicense regime will likely have an effective date of early 2015. We cannot predict what changes the NYDFS will make to the proposal or when the BitLicense regime may become effective. The BitLicense framework when finalized and effective may adversely affect the ability of consumers or businesses in New York to use bitcoins and the ability of bitcoin businesses in New York and elsewhere to operate effectively, and therefore may adversely affect the price of bitcoins. T

he USD is currently one of the dominant currencies that are traded for bitcoins. Thus, the U.S. Federal, State and local government regulations may have the most significant impact on the Bitcoin Network and the price of bitcoins. In addition, various foreign jurisdictions may adopt laws, regulations or directives that affect bitcoin. While certain governments such as Germany – where the Ministry of Finance has declared bitcoins to be “Rechnungseinheiten” (a form of private money that is recognized as a unit of account, but not recognized in the same manner as fiat currency) – have issued guidance as to how to treat bitcoins, most regulatory bodies have not yet issued official statements regarding their intention to regulate or determinations on regulation of bitcoin, bitcoin users and the Bitcoin Network.

Among those for which preliminary guidance has been issued in some form, Canada, Taiwan and Spain have labeled bitcoin as a digital or virtual currency, distinct from fiat currency, while Sweden and Norway are among those to categorize bitcoin as a form of virtual asset or commodity. In July 2014, the European Court of Justice indicated it would determine what value-added tax treatment should be afforded to bitcoin transactions throughout the EU.

In China, a recent government notice classified bitcoins as legal and “virtual commodities;” however, the same notice restricted the banking and payment industries from using bitcoin, creating uncertainty and limiting the ability of bitcoin exchanges to operate in the then-second-largest bitcoin market.

On August 20, 2014, the Australian Taxation Office released guidance stating that bitcoin transactions will be “treated like barter transactions with similar taxation consequences” and that “[i]ndividuals who use bitcoin as an investment may be subject to capital gains tax rules when they dispose of it, as they would for shares of similar assets,” while the Australian Senate has also recently launched an inquiry into the country’s tax treatment and regulation of bitcoins.

The government of Israel and the Israel Tax Authority are reportedly looking into taxing the profits from bitcoin trading. Conversely, regulatory bodies in some countries such as India and Switzerland have declined to exercise regulatory authority when afforded

the opportunity.

In March 2014, after the collapse of Mt. Gox, Japan confirmed that under its laws bitcoin is not considered a currency and therefore not subject to regulation.

At the other extreme, Russia's Ministry of Finance has issued a draft bill, expected to pass in Spring 2015, that 27 would ban bitcoin and other "money surrogates" and impose monetary penalties for its use or even the advocacy of its use.

In July 2014, Ecuador banned the use of bitcoin and other digital currencies and announced a plan to create a state digital currency backed by assets of the Ecuadorian central bank. In May 2014, the Central Bank of Bolivia banned the use as currency of digital assets including bitcoins.