BITCOINS: WHERE THEY CAME FROM
AND WHERE THEY ARE HEADED

Presentation to the Committee on Cyberspace Law
at the 2013 Annual Meeting of the
American Bar Association
San Francisco
August 9, 2013
by Denis T. Rice and Robert P. Taylor
Arnold & Porter LLP

BITCOINS: WHERE THEY CAME FROM AND WHERE THEY ARE HEADED

I. Introduction.

Essentially, a bitcoin is just a snippet of code, based on an algorithm. In the larger context, it is a new open-source digital currency that is available for use by any business or individual.[1] Bitcoin allows money to be sent by email at anytime, anywhere, at little or no cost. Some believe that bitcoin is "the next great step in Internet and global currency."[2] Others say it's just a "gimmick."[3] In any case, lawyers practicing in the cyberspace arena need at least a working knowledge of this relatively new digital currency (some would say "virtual currency") without borders, unregulated by any governmental authority or a central bank. This paper offers a brief overview of the origins and development of bitcoin and the various regulatory and practical issues that will ultimately determine its future.

II. Origins of Bitcoin.

In 2008, one "Satoshi Nakamoto" self-published a white paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*.[4] While "Nakamoto" is generally viewed as a fictitious name for group of computer geeks, the system introduced is real. The algorithm that generates a bitcoin was first described in Nakamoto.

Some of the significant moments in bitcoin history since the Nakamoto paper was published include:

- 2009—The Bitcoin Network came into existence with release of the first open source bitcoin client and issuance of the first bitcoins.

- August 2010—Bitcoin had its vulnerability to its protocol exploited when over 184 billion bitcoins were generated in one transaction and sent to two addresses on the Bitcoin Network. At that time, transactions which were not properly verified could become included in the Blockchain (described below), thereby allowing users to bypass the economic restrictions in the bitcoin system and create an unlimited amount of bitcoins. This transaction was quickly spotted and erased from the transaction log.

[1] Http://bitcoin.org. Bitcoin.org on its site refers to bitcoin as "a digital currency, a protocol and a software that enables instant peer-to-peer transactions, world-wide payments, almost no processing fees . . ." and says the "issuance of bitcoins is carried out collectively by the network."

[2] Chuck Jaffe, *Don't Laugh off Winklevoss Twins' Bitcoin ETF*, MARKETWATCH (July 8, 2013; online at www.marketwatch.com/Story/Story?guid=23229524-F7C6-11E2-834-002128040CF6 ["Jaffe"].

[3] Liz Hoffman, *Winklevoss Twins Tap Katten Team for Bitcoin ETF*, LAW360 (July 2, 2013) online at www.law_360.com/articles/454684/print?section+banking.

[4] Hereafter "Nakamoto," available at http://bitcoin.org/bitcoin.pdf.

- October 2011—exchange rate between the dollar and the bitcoin crashed from over $30 per bitcoin to below $2.00.

- February 2013—Coinbase, a bitcoin payment processor, reported selling one million dollars in bitcoins in one month at more than $22 each.

- March 2013—The U.S. Financial Crimes Enforcement Network ("FinCEN") issued regulatory "guidelines" for "decentralized virtual currencies." Bitcoin miners were classified as "money service businesses," potentially subject to registration. (*See* discussion of "Regulatory Issues" at Section IX, *infra*.)

- July 31, 2013—"Inside Bitcoins," a one-day conference in Manhattan, draws several hundred "entrepreneurs, dreamers, technophiles, and the simply curious."[5]

- August 5, 2013—Phoenix Fund announces plan to invest $200 million in Avalon, which makes servers used to generate bitcoins.

A central purpose of the bitcoin, according to Nakamoto, was to reduce transaction costs incurred when parties validate transactions and mediate disputes.[6] To that end, the bitcoin system builds on open source computing, in which all bitcoin users work together to validate transactions, either by running a program on an individual's own computer implementing the bitcoin protocol or by creating an account on a bitcoin website that runs the protocol for users. The original creators of bitcoin used it for working on Internet-related tasks, *e.g.*, trading bitcoin for programming help. However, bitcoin earned increasing acceptance in other contexts. Early on, bitcoin was commonly used for online drug markets or casinos.[7] That gave bitcoin a somewhat tarnished reputation which still persists in some quarters. But it is now accepted by legitimate organizations, not only for charitable donations,[8] but also by a host of businesses.

III. How Bitcoins Are Obtained.

There are two ways to acquire bitcoins: mine them, thereby creating new bitcoins, or trade for existing bitcoins. One newspaper reported in July 2013 that a majority of bitcoin users who were interviewed in San Francisco bought bitcoins instead of mining them.[9] Either way, the person needs Internet access in order to connect to what is known as the "Bitcoin Network." We will discuss both of these approaches.

[5] Paul Vigna, *Bitcoin and the Rise of a Digital Counterculture*, WALL ST. J. (July 31, 2013)

[6] *See* Nakamoto at 1.

[7] Derek A. Dion, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker Cash*, 2013 UNIV. ILL. J. L. TECH & POLY, 165, note 32 ["Dion"].

[8] Dion at note 33.

[9] Cameron Scott, *New Money*, 32 S.F. WEEKLY No. 25 (July 10-15, 2013) 9, 10.

A. “Mining” For Bitcoins.

1. How Mining Works.

To understand mining for bitcoins in the bitcoin system, it is first necessary to know the operation of the “Blockchain.” This is a transaction database that is shared by all nodes that participate in a system based on the bitcoin protocol. There is only one Blockchain, and the first block in the chain is called the “genesis block.” A full copy of the Blockchain contains every transaction ever executed in bitcoin, allowing one to ascertain how much value belonged to each address at any point in history. Generation of a new bitcoin by mining results in new blocks being added to the Blockchain and new bitcoins being issued to the miners. To accomplish this, miners engage in a set of prescribed complex mathematical calculations. Miners that succeed in adding a block to the Blockchain automatically receive a fixed number of bitcoins as a reward for their effort. This reward system is the method by which new bitcoins enter into circulation.

To begin mining, a user can download and run Bitcoin Network mining software, which turns the user’s computer into a “node” on the Bitcoin Network that validates blocks. All bitcoin transactions are recorded as separate blocks in the Blockchain, with each block containing the details of some or all of the most recent transactions that are not memorialized in prior blocks and keeping 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 predetermined length (the “hash value”) using the SHA-256 cryptographic hash algorithm. To “solve” or “calculate” a block, a miner must repeat this computation with a different nonce until the miner generates a SHA-256 hash of a block’s header that has a value less than or equal to the current target set by the Bitcoin Network. 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 and constantly increase their computing power to improve their likelihood of solving for new blocks.

The cryptographic hash function that a bitcoin miner uses is one-way only. It also is, in effect, irreversible: hash values are easy to generate from input data (*i.e.*, valid recent network transactions, Blockchain and nonce), but neither a miner nor a participant can determine the original input data solely from the hash value. This makes it difficult at first for a miner to generate a new valid block with a header less than the target prescribed by the Bitcoin Network, but other miners can easily confirm a proposed block by running the hash function just once with the proposed nonce and other input data. 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, and the miner who has solved such block receives the reward of a fixed number of bitcoins (plus any transaction fees paid by transferors whose transactions are recorded in the block). This “hashing” process is akin to a mathematical lottery in which miners with devices having greater processing power (*i.e.*, the ability to make more hash calculations per second) being more likely to succeed. As more miners join the Bitcoin Network and its processing power increases, the Bitcoin Network adjusts the complexity of the block-solving equation to ensure that one newly-created block is added to the Blockchain approximately every ten minutes.

A legitimate bitcoin miner will only build onto a block (by referencing it in blocks the miner creates) if it is the latest block in the longest valid chain. "Length" is calculated as total combined difficulty of that chain, not number of blocks, though this distinction is only important in the context of a few potential attacks. A chain is valid if all of the blocks and transactions within it are valid, and only if it starts with the genesis block.

From any block on the chain, there is only one path back to the genesis block. But there can be forks in the chain. One-block forks are created from time to time when two blocks are created just a few seconds apart. When that happens, generating nodes build onto whichever one of the blocks they received first. Whichever block ends up being included in the next block becomes part of the main chain because that chain is longer.

Blocks in shorter (or invalid) chains are not used for anything. When the bitcoin client switches to another, longer chain, all valid transactions of the blocks inside the shorter chain are re-added to the pool of queued transactions and will be included in another block. The reward for the blocks on the shorter chain will not be present in the longest chain, so they will be practically lost, which is why there is a network-enforced 100-block maturation time for generation.

2. Incentives for Mining.

Bitcoin miners dedicate substantial resources to their activity. Given the increasing difficulty of the target established by the Bitcoin Network, miners currently must invest in expensive mining devices with adequate processing power to hash at a competitive rate. In the early bitcoin development, when a bitcoin cost only 25 cents to buy on an exchange and there were few participants, a miner could run bitcoin using only the CPU of a laptop and make a handful of new coins a day. While the very first mining devices were standard home computers, now there are computers which are specially designed solely for mining purposes. Gradually miners used their profits for faster machines. They began to use GPU-enhanced computers, which can execute tasks like the hash calculation thousands of times faster. Eventually they moved into field-programmable gate arrays, and finally rigs using an application-specific integrated circuit (ASIC) purposely built to execute the hash operation, in April 2013.[10]

On August 5, 2013, the Phoenix Fund, a Zurich-based private equity fund led by billionaire foreign-exchange trader Joe Lewis, announced a $200 million investment in Avalon, which makes high-end computer servers that are used for making bitcoins. The deal will also include Taiwan Semiconductor Manufacturing Co., which will supply the state-of-the-art microchips to power the hardware.[11] Miners also incur substantial electricity costs in order to continuously power and cool

[10] Morgan E. Peck, *The Bitcoin Arms Race Is On!*, iSPECTRUM (May 6, 2013).

[11] Harriet Agnew, *Famed Trader Backs Bitcoins*, WALL ST. J. (Aug. 5, 2013), C3.

their devices while solving for a new block. It is estimated that the aggregate electricity costs of mining across the Bitcoin Network exceed $300,000 every 24 hours.

3. Mining Pools.

Because the Bitcoin Network's mining protocol makes it more difficult to solve for new blocks as the computer processing power dedicated to mining increases (in order to maintain a 10 minute per block average), the difficulty of finding a valid hash value has grown exponentially since the first block was mined. As of August 2013, the likelihood that a single individual is able to mine bitcoins is extremely low. This has spawned development of mining "pools," in which multiple miners act cohesively and combine their processing power to solve blocks. When a pool solves a new block, the participating mining pool members split the resulting reward based on the processing power each contributed to the solution. Mining pools provide participants with access to smaller, but steadier and more frequent, bitcoin payouts. It was estimated that in late August 2013, about 11.5 million bitcoins were in existence, with the amount steadily increasing.[12] MyMiner is a bitcoin mining project which operates "mining farms" in China where it claims the electricity costs are "extremely low."[13]

4. Mathematically Controlled Supply.

The Bitcoin Network is designed so that the reward for adding new blocks to the Blockchain decreases over time and the production (and reward) of bitcoins will eventually cease. Once such rewards cease, it is expected that miners will need to be compensated in transaction fees to provide adequate incentive for them to continue mining. The amount of transaction fees will be based upon the structural requirements necessary to provide sufficient revenue to incentivize miners, as counterbalanced by the need to retain sufficient bitcoin users (and transactions) to make mining profitable. Transaction fee rules are already built into the Bitcoin Network protocol; however, users currently may opt not to pay transaction fees (depending on the bitcoin software they use) and miners may choose not to enforce the transaction fee rules since, at present, the bitcoin rewards are far more substantial than transaction fees. As of June 2013, transaction fees generally accounted for only about one percent of miners' total revenue.

The method for creating new bitcoins is mathematically controlled in a manner so that the supply of bitcoins grows at a limited rate pursuant to a pre-set schedule. The number of bitcoins awarded for solving a new block is automatically halved every 210,000 blocks. Thus, the fixed reward for solving a new block is presently 25 bitcoins per block, which will decrease by half to become 12.5 bitcoins around the year 2017. This deliberately controlled rate of bitcoin creation means that the number of bitcoins in existence will never exceed 21 million and that Bitcoins cannot be devalued through excessive production unless the Bitcoin Network's source code (and the

[12] Blockchain.info/charts/total-bitcoins, visited August 30, 2013.

[13] MyMiner.com.

underlying protocol for bitcoin issuance) is altered. It is estimated that more than 90% of the 21 million bitcoins will have been produced by 2020.

B. Trading For Bitcoins.

Anyone who wants to trade for bitcoins generally must have Internet access to connect to the Bitcoin Network. Bitcoin transactions between persons occur very rapidly (within seconds). The transactions can be made directly between end-users without need for a third-party intermediary, although entities exist that provide third-party intermediary services. To prevent the possibility of double-spending a single bitcoin, a user must notify and update the Bitcoin Network of the transaction. The Bitcoin Network ensures against double-spending by memorializing every transaction by virtue of the Blockchain, described in Subsection A. above.

As discussed earlier, the Blockchain is a history of time-stamped transactions. When a transaction is made, it is time-stamped and cannot be modified. This not only notarizes the transaction, it also prevents and prevents bitcoins from being double-spent.[14] The Blockchain database is shared by all nodes participating in the system. Because a full copy of a currency's Blockchain contains every transaction ever executed in bitcoin currency which enables one can find out how much value belonged to each address at any point in history. Every block contains a hash of the previous block. Each block is guaranteed to come after the previous block chronologically, because the previous block's hash would otherwise not be known. Each block is also computationally impractical to modify once it has been in the chain for a while, because every following block would also have to be regenerated.

A user planning to engage in bitcoin transactions must first install on a computer (or mobile device) a bitcoin software program that will allow the user to generate the digital "wallet," which is analogous to a bitcoin account in which to store bitcoins. The wallet may be either stored in a person's own computer by the bitcoin software or hosted on a third-party website. The Bitcoin Network software program and the digital wallet enable the user to connect to the Bitcoin Network and engage in the purchase, sale and receipt of bitcoins.

The user who downloads a Bitcoin Network software program becomes a "node" on the Bitcoin Network that assists in validating transactions. As noted, a user may in the alternative retain a third party to create a digital wallet to be used for the same purpose. A user can have an unlimited number of digital wallets, and each wallet includes a unique address and verification system consisting of both a "public key" and a "private key," which are mathematically related. Because the bitcoin relies upon peer-to-peer networking and cryptography, the system is a distributed model resistant to central control. Each wallet is based upon key pairs, *i.e.*, a set of public and private keys. The public keys generate an "address" consisting of a string of letters and numbers approximately 27 to 34 characters long. The private keys are for the purpose of authorizing bitcoin transactions. Although the address has no information about the user, the transactions are traceable

[14] Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in Bitcoin*, unpublished paper cited in Dion at 167.

by means of the public key. This means that a bitcoin can be traced through each address in which it was held, even though the ownership of each such address will remain anonymous. In a bitcoin transaction, the bitcoin recipient must provide its public key, which serves as an address for the digital wallet, to the party initiating the transfer. This activity is not unlike a recipient providing an address in wire instructions to a payor so that cash may be paid to the recipient's account.

The bitcoin recipient, however, does not make public its related private key or provide it to the other party to the transaction, because the private key authorizes both access to and transfer of funds in that digital wallet to other users. That means that a user who loses his or her private key permanently loses access to the bitcoins contained in the associated digital wallet. Likewise, bitcoins are irretrievably lost if the wallet containing them is deleted and no backup of the public and private key relating to that wallet has been made. In the data packets distributed from bitcoin software programs to confirm transaction activity, each bitcoin user must "sign" transactions with a data code derived from entering the private key into a "hashing algorithm," which signature serves as validation that the transaction has been authorized by the owner of the bitcoins.

There are several ways to trade in bitcoin. One is to identify someone willing to send bitcoins and offer to pay for them with conventional currency. Once a price is set, the seller transfers the bitcoins to the buyer's wallet. Another (and more formal) avenue of trading is to use a bitcoin exchange.[15] Traders can seek an e-commerce intermediary to facilitate a cash payment into cash payment out from an exchange. As with conventional currency exchanges, price is not usually individually negotiated, but is rather based on the aggregate supply of and demand for bitcoins in the system.[16] Using an exchange adds to the transaction cost, but it is both more efficient and better monitored (*See* Section VI, *infra.*)

IV. Using Bitcoin in Commerce.

A customer at a retail store can make a payment in bitcoin using a smartphone that scans a barcode provided by the retailer. Although an officer of the National Retail Federation (a trade group largely comprised of big chains) questions the consumer's motivation to use bitcoins as compared to credit cards, merchants note that credit card fees can be as high as 3%, compared to less than 1% for bitcoins.[17] Moreover, bitcoin transactions are final, while credit card charges can be disputed.[18] Since bitcoin is a currency run by the people who use it, the value of bitcoins is determined by the marketplace; in other words, whatever someone will take for a bitcoin is what it is worth.

[15] Bitcoin Exchanges, http://www.bitcoinexchanges.net.

[16] Dion, note 28.

[17] Sarah E. Needleman*, Banking on Bitcoin's Novelty*, WALL ST. J. (June 27, 2013) B4.

[18] *Id.*

BitPay, Inc., an Atlanta firm formed in 2011 to process bitcoin payments, by 2013 reportedly had signed up more than 8,000 merchants world-wide, all of whom are small companies.[19] BitPay says it is available in every country and in over 30 different currencies. It works over ethernet, wi-fi and 3G/4G data networks. It represents that it can handle payments multiple ways: (1) PC-to-website; (2) phone-to-website; (3) mobilewebsite; (4) phone-to-phone; (5) phone-to-card; and (6) tablet point-of-sale.

In June 2012, BitPay Inc. reportedly set what was then a new record for internet payment processing with bitcoin.[20] The majority of the sales were generated by Butterfly Labs, Kansas City, in connection with the release of its new application-specific integrated circuit (ASIC) cryptographic processors. BitPay claimed to have bested PayPal and Dwolla to become the exclusive online payment processor for this new product line, with orders and payments from 17 different countries, including Belgium, Russia, Finland, Poland, and the Philippines. BitPay reported that, within 24 hours it processed over $250,000 worth of bitcoin payments, shattering its previous record of $31,000 in a single day. BitPay claimed its "payment service is unique in the marketplace" and that with its system, "an internet merchant can accept a payment from any country on the planet, instantly, with zero risk of fraud."[21]

In February 2013, Ginbase reported selling one million bitcoins in a single month at over $22 per bitcoin. As of mid-2013, data on specific users of bitcoins is largely anecdotal, but among who are known accept bitcoins for goods or services range from Buyer's Best Friend Wholesale & Mercantile, Inc., a specialty grocery business in San Francisco, and Aaron Rollins, a cosmetic surgeon in Beverly Hills, to A Class Limousine Travel and Tours, Inc., of Bridgewater, N.J., and a sushi restaurant in the eastern San Francisco Bay Area.

V. Venture Capital and Bitcoin.

In the past two years, startups focused on marketing bitcoin services have begun to attract serious venture capital. In January 2013, BitPay announced it had completed a seed round funding from several angel investors, including the founder of SecondMarket. Other fledgling businesses, like Coinbase, Inc., Coinsetter, Inc. and CoinLab, Inc., also have raised millions of dollars from prominent venture capital firms and angel investors.[22] In April 2013, a group led by venture firm Andreeson Horowitz and others invested more than $2 million in OpenCoin, Inc.[23] On May 7, 2013

[19] *Id.*

[20] Orlando, FL (PRWEB) June 26, 2012

[21] Anthony Gallippi, the co-founder and CEO of BitPay, Inc, quoted in PRWeb, *BitPay Shatters Record for Bitcoin Payment Processing* (June 26, 2012), at http://prweb.com/printer/9637829.htm. "No other payment processor can do this. American Express cannot do this, PayPal cannot do this, Mastercard cannot do this. BitPay can."

[22] Sarah E. Needleman and Spencer E. Ante, *Bitcoin Startups Begin to Attract Real Cash*, WALL. ST. J. (May 8, 2013) B4.

[23] *Id.*

Coinbase announced closing of a $5 million "A" round led by Union Square Ventures. Coinbase operates an online service that allows users to buy and store bitcoin in a digital wallet and pay merchants for goods and services. It claimed to have about 116,000, members who converted $15 million of real money into bitcoin, with dollar conversions increasing by about 15% a week.[24] According to Coinbase's co-founder, "we are in land-grab mode."[25]

Jeremy Liew, a partner with Lightspeed Venture Partners, which has invested in three virtual currency startups including OpenCoin, has said he's "incredibly bullish" on bitcoin because it allows for cost-free micro-transactions—such as buying a single candy bar—that would be too small for other electronic payments. "The appeal of zero transaction costs is really strong and extremely disruptive for a massive industry, the payments industry," he said.[26] A general partner at the San Francisco-based venture firm Kleiner Perkins Caufield & Byers in April 2013 said his firm was actively exploring bitcoin-related investments and had looked at more than two dozen companies.[27] He estimated that almost 100 companies were operating in the bitcoin domain, including exchanges, payment processors and bitcoin ATM operators.[28]

VI. Bitcoin Exchanges.

Among the more active bitcoin exchanges are Mr. Gox in Japan, BitBox and Bitstamp in the U.S., and Bitcurex in Poland. It was reported by Reuters that banks such as Morgan Stanley and Goldman Sachs visited bitcoin exchanges as frequently as thirty times a day.[29] In April 2013, Tokyo-based Mt. Gox Co., the largest online exchange trading bitcoin, said its services were disabled for approximately four hours by an Internet denial-of-service attack.[30] According to the exchange, "Attackers wait until the price of bitcoins reaches a certain value, sell, destabilize the exchange, wait for everybody to panic-sell their bitcoins, wait for the price to drop to a certain amount, then stop the attack and start buying as much as they can," according to the exchange.[31] Such volatility is one of the concerns about this kind of digital currency. Bitcoin rose in value from roughly $5 in June 2012 to a high of $266 in April 2013 and was down to about $108 on May 7, 2013, according to Mt. Gox data.

[24] *Id.*

[25] *Id*. (quoting Fred Ehrsam).

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] Naomi O'Leary, *Bitcoin: The City Traders' Archaic New Toy*, Reuters (Sep. 8, 2012).

[30] *Id.*

[31] *Id.*

VII. Bitcoin as Means of Avoiding Credit Card Fraud.

The amount of credit card fraud is staggering, estimated at $190 billion per year, according to a recent article in Forbes. The majority of this fraud occurs in situations where the credit card is not physically present, such as internet payments. BitPay claims that using bitcoin in a payment processing service, the multi-billion dollar fraud problem can be eliminated and risk-free internet payments can be processed from any country. BitPay claims that since August of 2011, shortly after its launch, it has been the world leader in payment processing for bitcoin currency. Over 600 merchants are currently using BitPay's services, to sell all types of products, ranging from computers, to internet access, to video games, and even some homemade baklava.

BitPay asserts that when companies which decide to accept bitcoin as a form of payment try to do it themselves, they expose themselves to accounting uncertainties, security risks, and volatility risks. BitPay claims that its service takes all of those risks off of the merchant. It claims to guarantee the exchange rate and the security, by paying a direct deposit into the merchant's bank account every day and keeping full records of the exchange rates for their accounting purposes.

BitPay is but one of many merchant services in the global bitcoin economy. There are estimated to be approximately 12 currency exchanges around the world, where consumers and businesses can buy and sell bitcoins in exchange for their local currency. There are also about 10 different bitcoin digital wallet programs, which let users access and use bitcoins from their computer or mobile device. Because the technology is open source, new services are being created every week.

VIII. The Winklevoss Bitcoin Trust.

On July 1, 2013, the Winklevoss Twins filed a registration statement with the SEC for the Winklevoss Bitcoin Trust, a form of electronically-traded fund. The Winklevoss Twins' SEC filing describes a bitcoin as "one type of a Digital Math-Based Asset that is issued by, and transmitted through, an open source, cryptographic protocol platform known as the Bitcoin Network." The filing calls the Bitcoin Network "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." The filing states that bitcoins can be used to pay for goods and services or can be converted to fiat currencies, such as the U.S. dollar at rates determined on "bitcoin exchanges." The filing notes that third party service providers, such as bitcoin exchanges, may charge significant fees for processing transactions. The SEC filing contains over 17 pages of "Risk Factors," observing that the value of bitcoins is determined by the supply of and demand for bitcoins in the bitcoin exchange market, as well as the number of merchants that accept them.

The Winklevoss filing also concedes that bitcoins have little use in real-world retail and commercial markets compared with their "relatively large use by speculators." Chuck Jaffe pointed out in an email alert on Marketwatch.com that "If you can't actually spend bitcoins without converting them to conventional currency, one could argue that they aren't so much a currency as a form of scrip, a temporary money that had some value but that could become worthless overnight due to any number of structural, economic or market conditions."[32]

Jaffe also noted that the Winklevoss Twins themselves have been buying up bitcoins, and that their own stash may serve as the seed coins for the fund. Jaffe opined that even if the brothers "truly believe in the future of bitcoin—any every interview or statement they've given suggests they think bitcoin is revolutionary—an investor can't help but feel that the ETF is a way for them to backstop their own investment." According to Jaffe, "Ultimately, if Bitcoin Trust helps people interested in the currency to access and trade it, it's a plus even if it's not a commercial success. If bitcoin proves durable and lives up to the potential its supporters say it has, then the Winklevoss boys will cash in big time and be heavily imitated."[33]

Jaffe says the Twins "face a long, uphill battle just to get this fund to market; from there, chances are good it will still be viewed for years as a granular, niche fund—more like a fund that specializes in stocks from Bulgaria than one that has mainstream applications."[34] Jaffe quoted Morningstar analyst Steven Pikelny as saying that the Winklevoss ETF "is a total gimmick. Bitcoins are very illiquid, and the current trading infrastructure is riddled with security/efficiency problems. . . . If you actually want exposure to bitcoins, it's probably a better idea to buy them directly. And if you can't figure out how to do that, you probably don't have any business owning bitcoins in the first place."[35]

Industry watchers laughed just over a decade ago at the first gold exchange-traded funds, saying funds backed by hard assets were a gimmick, but all the today gold ETFs combined constitute are the world's fourth largest holder of gold, behind only the United States, Germany and the International Monetary Fund. Perhaps those are two good comparisons for the Winklevoss Bitcoin Trust. But as Jaffe notes, gold funds were backed by hard assets. The bitcoin fund cannot do that, because bitcoins are digital.[36] The Bitcoin Trust could be looked at as just another currency fund, just with the unique—some would call it imaginary—currency of the bitcoin behind it. Until you can cash them, however, that value is both speculative and ephemeral.

[32] The registration statement shows that the Twins claim a proprietary method for storing bitcoin holdings—they will charge a yet-to-be-specified management fee for maintaining this virtual storage—which would, in turn, make bitcoin holdings more liquid.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.* Liquidity is important here because bitcoins have a volatile history. In the last year alone, they have traded between $13 and $266; Mt. Gox, the largest bitcoin exchange, had them trading in the $80-to-$90 range last week. *Id*.

IX. Regulatory Issues.

A. Potential Prohibition by the U.S. Government.

It is conceivable that the U.S. could seek to prohibit the issuance or use of bitcoin within its jurisdiction. For example, in March 2011, the U.S. convicted Bernard von NotHaus on federal counterfeiting, forgery, criminal fraud, and conspiracy charges. He had been selling his own physical coins called "Liberty Dollars," which resembled U.S. currency. But unlike the digital bitcoin, the counterfeiting and forgery statutes involved in the von NotHaus case are directed at *physical* currencies. They prohibit "falsely" making, forging, or counterfeiting "any coin or bar in resemblance or similitude" of U.S. coins, knowingly passing or possessing any forged or counterfeit coin or bar (18 USC 485), and making "coins of gold or silver or other metal or alloys of metals, intended for use as current money" (18 USC 486).

The press release by the U.S. Department of Justice on the von NotHaus conviction stated that the U.S. Constitution "delegates to Congress the power to coin money and to regulate the value thereof … in order to establish and preserve a uniform standard of value and to insure a singular monetary system for all purchases and debts in the United States." The release went on to state that Congress also has concurrent power to restrain the circulation of money which is not issued under its own authority in order to protect and preserve the constitutional currency for the benefit of all citizens of the nation. Therefore, according to the press release, "[i]t is a violation of federal law for individuals, such as von NotHaus, or organizations … to create private coin or currency systems to compete with the official coinage and currency of the United States."[37]

Accordingly, bitcoin does not presently implicate criminal activity due to its virtual nature. But in the opinion of the Department of Justice, Congress could enact laws to prohibit or restrict the use of bitcoin. Even then, there could be a question whether U.S. law would apply to bitcoins issued outside the U.S.

B. FinCEN Regulatory "Guidance."

As alluded to earlier, on March 18, 2013 the Financial Crimes Enforcement Network (FinCEN), a bureau within the U.S. Treasury Department, issued regulatory "guidance" on centralized and decentralized "virtual currencies." It classified digital currencies and other digital payment systems like bitcoin as "virtual currencies" on the basis they are not legal tender under any sovereign jurisdiction. It stated that a "user of virtual currency" is not a "money services business" (MSB) and hence not subject to Federal MSB regulation, reporting or record-keeping regulations. However, FinCEN went on to hold that U.S. entities which generate "virtual currency" (such as bitcoins) are MSBs if they sell their generated currency for national currency, *i.e.*, for "real currency or its equivalent." Accordingly, "miners" of bitcoin may need to register as MSBs and comply with applicable MSB regulations if they are within the U.S. and sell generated

[37] *See* http://www.fbi.gov/charlotte/press-releases/2011/defendant-convicted-of-minting-his-own-currency.

bitcoins for dollars. If entities that generate bitcoins are MSBs, they may also have to cope with various state laws regulating money service businesses.

Some observers claim that FinCEN's regulations are having a disruptive effect on the bitcoin system.[38] An article in the online American Banker asserted that at least three bitcoin exchanges in the U.S. had elected to shut down as a result of FinCEN's guidance.[39] Although the FinCEN director has said that the guidance aims to protect digital currency systems from abuse and ensure that information is available to prosecute "criminal actions," the guidance does not apply to everyday users of bitcoin.[40] The bitcoin exchanges cited by American Banker as having "suspended operations indefinitely" include Bitme, BTC Buy, and Bitfloor. Of these, Bitfloor was already registered as an MSB with FinCEN, but was not state-licensed as a money transmitter.

In May, the Department of Homeland Security seized an account controlled by the Japanese-based bitcoin exchange, Mt. Gox, on the theory that Mt. Gox was operating as an unlicensed MSB. Mt. Gox subsequently registered as an MSB with the U.S. Treasury. Purportedly, the pressure on Mt. Gox "opened a door for rivals," such as Bitstamp.[41] All the controversy surrounding regulation of bitcoin has prompted bitcoin enthusiasts to form a self-regulatory group called the Committee for the Establishment of the Digital Asset Transfer Authority, which plans to set technical standards that aim at preventing money-laundering and insuring compliance with laws.[42]

Carol R. Van Cleef, a partner specializing in emerging payments and antimoney-laundering-compliance at the Washington, D.C., law firm Patton Boggs LLP, says that government financial reporting regulations likely will make it difficult for virtual-currency startups. The Commodity Futures Trading Commission was reportedly discussing whether Bitcoin might fall under its regulatory jurisdiction.[43] On August 26, 2013 representatives from at least seven governmental agencies met with the Bitcoin Foundation, which is the main bitcoin trade group. The general counsel of the Foundation was scheduled to make a presentation and answer questions from representatives of the Federal Reserve, Treasury Department, Federal Deposit Insurance Corp., Office of the Comptroller of the Currency, Internal Revenue Service, Federal Bureau of Investigation and Secret Service.[44]

[38] Jon Matonis, *FinCEN's New Regulations Are Choking Bitcoin Entrepreneurs*, AMERICAN BANKER (April 25, 2013), online at www.americanbanker.com/bankthink/fince-regulations-choking-bitcoin-entrepreneurs.

[39] *Id.*

[40] *Id.*

[41] Vigna, *supra* note 4. *See also* Romain Dillet, *Feds Seize Assets From Mt. Gox's Dwolla Account, Accuse It of Violating Money Transfer Regulations*, TECHCRUNCH.COM (May 16, 2012)

[42] Robin Sidel, *Virtual Currency Enthusiasts to Launch Self-Regulatory Group*, W. ST. J. (July 30, 2013).

[43] *Id.*

[44] Robin Sidel, Bitcoin Group, Regulators to Meet, S. ST. J. (Aug. 25, 2013) C3.

C. State License Laws

Several states, including California and New York, have reportedly warned bitcoin-related companies that they may be violating local money-transaction laws.[45] California, one of 50 states with laws affecting money transmitters, has available in the files of the California Department of Financial Institutions a letter dated July 1, 2013 to the Department from the law firm of Perkins Coie on behalf of the Bitcoin Foundation, which addresses not only whether the Foundation is subject to the California Money Transmission Act but whether that Act should have any application to bitcoins.

The Perkins Coie letter notes that the California Money Transmission Act prohibits "engage[ing] in the business of money transmission," "or advertis[ing], solicit[ing], or hold[ing] itself out as a provid[ing] money transmission in this state" without a license or exemption from licensure.[46] Specifically, California defines money transmission as including any of the following:

1. "selling or issuing payment instruments;"
2. "selling or issuing stored value;" and
3. "receiving money for transmission.[47]

Under the express wording of the statute, the California Money Transmission Act regulates "the business of money transmission . . . *in this state*"—namely, California.[48] Perkins Coie therefore contends that an entity would need to have business operations in California to be subject to the Department of Financial Institutions' ("DFI"s) jurisdiction.

Even if an entity were not in the business of selling bitcoin to consumers, Perkins Coie argued, the entity would not be regulated as a seller or issuer of payment instruments because a bitcoin is not a payment instrument under California law. In California, a payment instrument is "a check, draft, money order, traveler's check or other instrument for the transmission or payment of money or monetary value, whether or not negotiable."[49] A payment instrument "does not include a credit card voucher, letter of credit, or any instrument that is redeemable by the issuer for goods and services provided by the issuer or its affiliate."[50] "Money" is defined as "a medium of exchange that is authorized or adopted by the United States or a foreign government."[51] "Monetary value" is

[45] *Id.*

[46] Cal. Fin. Code §2030.

[47] Cal. Fin. Code §2003(o).

[48] Cal. Fin. Code §2030 (emphasis added).

[49] Cal. Fin. Code §2003(q).

[50] *Id.*

[51] Cal. Fin. Code §2003(n).

defined as "a medium of exchange, whether or not redeemable in money."[52] The terms "issue" and "issuer" have different meanings in the payment instrument and stored value contexts. With regard to payment instruments, these terms refer to "the entity that is the maker or drawer of the instrument in accordance with the California Commercial Code and is liable for payment."[53]

The California Commercial Code defines "instrument "as a negotiable instrument,[54] distinguished as either a "note" or "draft," depending on whether it involves a "promise" or an "order."[55] Both notes and drafts must involve a written instruction or undertaking.[56]

On July 7, 2001, the California Department of Financial Institutions had issued a letter regarding "Sale of ATM-Accessible Cards" that interpreted the term "payment instrument":

> [I]t has been our view that the term "other instrument" as used on Section 33059 means a *paper* instrument, like check or draft which is governed by Division 3 ("Division 3") the California Uniform Commercial Code ("UCC") . . . we have taken the view that for purposes of the Payment Instrument Law, an "instrument" is a *written, signed* document that it is similar in nature to a check or a draft, even though not negotiable. We have, therefore, not viewed electronic media, such as stored value cards, as payment instruments.[57]

Perkins Coie argued to CFI that the foregoing letter of the Department of Financial Institutions confirms that a product can only be an "instrument" if it involves a writing. Since bitcoins are not written or signed notes or drafts, Perkins Coie contends they are not payment instruments regulated by the California Money Transmitter Act. They go on to argue that even if bitcoins are classified as "instruments," there exists no "issuer" of bitcoins under California law because no entity acts as the "maker or drawer" of bitcoins, and no entity is fundamentally liable for payment. The term

[52] Cal. Fin. Code §2003(m).

[53] Cal. Fin. Code §2003(k).

[54] A negotiable instrument means "an unconditional promise or order to pay a fixed amount of money, with or without interest or other charges described in the promise or order, if it is all of the following: (1) payable to bearer or to order at the time it is issued or first comes into possession of a holder. (2) Is payable on demand or at a definite time. (3) Does not state any other undertaking or instruction by the person promising or ordering payment to do any act in addition to the payment of money, but the promise or order may contain (i) an undertaking or power to give, maintain, or protect collateral to secure payment, (ii) an authorization or power to the holder to confess judgment or realize on or dispose of collateral, or (iii) a waiver of the benefit of any law intended for the advantage or protection of an obligor." Cal. Comm. Code §3014(a).

[55] Cal comm.. Code §3014(e).

[56] Cal. Comm. Code § 3103(a)(6) (for a draft, an "order" means "a written instruction to pay money signed by the person giving the instruction"); Cal. Comm. Code §3103(a)(9) (for a note, a "promise" means "a written undertaking to pay money signed by the person undertaking to pay").

[57] California DFI precedent letter ruling – 01-94 Sale of Stored Value Cards in California is Not Subject to the Payment Instruments Law (July 7, 2001) (emphasis added).

"maker" means "a person who signs or is identified in a note as a person undertaking to pay.[58] A "drawer" is "a person who signs or is identified in a draft as a person ordering payment."[59] No single entity in the bitcoin ecosystem can be identified as an entity undertaking to pay a fixed sum of real currency for particular bitcoins. Thus, there is no issuer of bitcoin that would be subject to licensure as a money transmitter under California law.The letter concludes that, even if the Bitcoin foundation were in the business of selling bitcoin to consumers, it should not be regulated as a seller of payment instruments because, for the reasons stated above, bitcoin is not a payment instrument.

D. Patriot Act: Criminal Indictment of Liberty Reserve.

On May 28, 2013, an indictment against the Liberty Reserve, S.A., a Costa Rican currency exchange, and seven of its executives, was handed down by the grand jury in Manhattan. It alleged that the operators of the global bitcoin currency exchange ran a $6 billion money-laundering operation online, in violation of Section 311 of the USA Patriot Act, and was a central hub for criminals trafficking in everything from stolen identities to child pornography.

Liberty Reserve traded in virtual currency and provided the kind of anonymous and easily accessible banking infrastructure increasingly sought by criminal networks, law enforcement officials said.[60] Over seven years, it was allegedly responsible for laundering billions of dollars, conducting 55 million transactions that involved millions of customers around the world, including about 200,000 in the United States. Prosecutors claim that criminal investigation division in Washington said at a news conference that the case heralds the arrival of "the cyber age of money laundering," in which criminals "are gravitating toward digital currency alternatives as a means to move, conceal and enjoy their ill-gotten gains."[61]

According to the indictment, Liberty Reserve had a complicated system designed to allow people to move sums large and small around the world with virtual anonymity. The U.S. Attorney in Manhattan asserted that "the only liberty that Liberty Reserve gave many of its users was the freedom to commit crimes—the coin of its realm was anonymity, and it became a popular hub for fraudsters, hackers and traffickers."[62]

Liberty Reserve was incorporated in Costa Rica in 2006 by Arthur Budovsky, who renounced his United States citizenship in 2011, and was arrested in Spain on May 24, 2013. He was among the seven executives indicted, all of whom were charged with conspiracy to commit

[58] Cal. Comm.. Code §3103(a)(5).

[59] Cal. Comm.. Code §3103(a)(3).

[60] Mark Santora, William K. Rashbaum and Nicole Perloff, *Online Currency Exchange Accused of Laundering $6 Billion*, N.Y. TIMES (May 28, 2013).

[61] *Id.*

[62] *Id.*

money laundering, conspiracy to operate an unlicensed money-transmitting business, and operating an unlicensed money-transmitting business.

While Liberty Reserve was incorporated outside the United States, federal officials used a provision in the Patriot Act to target the organization and other financial institutions with whom they conducted business. Prosecutors said it was the first time the provision had been used to prosecute a virtual currency provider.According to the indictment, to transfer money using Liberty Reserve, a user needed only to provide a name, address and date of birth. But users were not required to validate their identity. Thus, essentially all a customer needed to open an account was an e-mail address. One undercover agent was allegedly able to register accounts under names like "Joe Bogus" and describe the purpose of the account as "for cocaine" without being questioned. That no-questions-asked verification system made Liberty Reserve the premier bank for cybercriminals, according to the prosecutors.

E. Securities Laws.

On July 23, 2013, the Securities and Exchange Commission announced that it had filed an action in the U. S. District Court for the Eastern District of Texas, charging a Texas man and his company with defrauding investors in a bitcoin-based Ponzi scheme. The SEC alleged that Trendon T. Shavers, founder and operator of Bitcoin Savings and Trust (BTCST), had offered and sold Bitcoin-denominated investments through the Internet using the monikers "*Pirate*" and "*pirateat40*." Shavers raised at least 700,000 bitcoin in BTCST investments, which amounted to more than $4.5 million based on the average price of bitcoin in 2011 and 2012, when the investments were offered and sold. The value of 700,000 bitcoin allegedly exceeded $60 million on the day the action was filed.

According to the SEC, Shavers promised investors up to 7% weekly interest based on BTCST's market arbitrage activity, which supposedly included selling to individuals who wished to buy bitcoin "off the radar" in quick fashion or large quantities. The SEC charged that BTCST was a "sham" and a "Ponzi scheme," in which Shavers used bitcoin from new investors to make purported interest payments and cover investor withdrawals on outstanding BTCST investments. Shavers also diverted investors' bitcoin for day trading in his account on a Bitcoin currency exchange, and exchanged investors' bitcoin for U.S. dollars to pay his personal expenses. "Fraudsters are not beyond the reach of the SEC just because they use Bitcoin or another virtual currency to mislead investors and violate the federal securities laws," announced Andrew M. Calamari, Director of the SEC's New York Regional Office.

According to the SEC's complaint, Shavers sold BTCST investments over the Internet to investors in states including Connecticut, Hawaii, Illinois, Louisiana, Massachusetts, North Carolina and Pennsylvania. Shavers allegedly posted general solicitations on a website dedicated to bitcoin discussions, with such false assurances about his investment opportunity as "It's growing, it's growing," "I have yet to come close to taking a loss on any deal," and "risk is almost 0." Contrary to those representations to investors, the SEC alleges BTCST was not in the business of buying and selling Bitcoin at all. It alleges that Shavers instead paid 507,148 bitcoin in investor withdrawals and purported interest payments and he transferred at least 150,649 bitcoin to his personal account at an online bitcoin currency exchange. Shavers suffered a net loss from his day trading, but realized net proceeds of $164,758 from his sales of 86,202 bitcoin. Shavers then allegedly transferred $147,102 from his personal account at the online Bitcoin currency exchange to accounts he controlled at an online payment processor as well as his personal checking account. He used this money to pay his rent, utilities, and car-related expenses as well as for food and retail purchases and gambling. All of this allegedly violated the anti-fraud and registration provisions of the securities laws, specifically Sections 5(a), 5(c) and 17(a) of the Securities Act of 1933, Section 10(b) of the Securities Exchange Act of 1934 and Exchange Act Rule 10b5.

X. Intellectual Property Rights.

Given the diverse nature of the mining mechanisms and the time-stamped exchange mechanisms associated with bitcoins, it would be difficult to write patent claims that could be enforced manageably against miners and users, and it is not apparent that any such patent applications have been filed. There are, however, many patents and applications that disclose inventions that use as a premise the existence of a medium of exchange in something other than what we think of as the usual currencies. A brief search of current U.S. and WIPO databases produces a list of just over 500 patents and applications (a few of them a PCT duplicate of a corresponding U.S. application) that employ the phrase “digital currency.” Some of these applications were filed as early as the mid-1990s, but the numbers appear to increase with the passage of time. Their subject matter ranges widely, from inventions designed to improve security in online transactions to ways of trading anonymously to systems for providing the “rewards” in various types of gaming. Some also address ways of expanding the use of the traditional telephone cards and gift cards. Hundreds of patents and applications describe inventions useful in creating and entering virtual worlds such as Second Life, many seeking to establish methods and mechanisms for using virtual currencies as part of the process. Although few of these inventions purport to be replacing more traditional currencies on a broad level, as many of the proponents of bitcoins appear to suggest, their number and diversity suggests that this is a phenomenon to be watched and that is likely to grow.

Bitcoins, themselves, which have been in existence for only about four years, are mentioned in at least 40 published patent applications and at least one issued patent. As with the more generic collection of inventions dealing with virtual currencies, the range of proposed uses for bitcoins ranges widely from gaming to more efficient transactions to enabling anonymity. One of the most interesting and informative of these is an application published December 23, 2011, Publication No. 2013/0166455, filed by Douglas Feigelson of Cincinnati, Ohio. The application describes a device in which bitcoins can be recorded in what are dubbed “bitbills,” to allow the user to have a portable version of her bitcoin account. Quite clearly people are looking for ways to make these virtual currencies a part of mainstream commerce.

XI. The Future . . .?

The economist Paul Krugman stated earlier this year that, unlike gold or paper fiat currencies, bitcoin derives its value solely from a self-fulfilling expectation that others will accept it as payment. Another economist, John Quiggin, contends that bitcoin "is perhaps the finest example of a pure bubble" and that it provides a conclusive refutation of the Efficient Markets Hypothesis. Others see bitcoin as a major development in virtual currency. There are many areas where the future of bitcoin will be developed: Is it an investment? How will bitcoin transactions be taxed? Is it a legitimate currency or, as one commentator has suggested, "the cyber equivalent of rare postage stamps"? Stay tuned.