2014

Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling

Jerry Brito
jerry.brito@nyls.edu

Houman B. Shadab
New York Law School

Andrea Castillo

Recommended Citation

THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

ARTICLE

BITCOIN FINANCIAL REGULATION:
SECURITIES, DERIVATIVES, PREDICTION MARKETS,
AND GAMBLING†

Jerry Brito[*], Houman Shadab,[**] and Andrea Castillo[***]

The next major wave of Bitcoin regulation will likely be aimed at financial instruments, including securities and derivatives, as well as prediction markets and even gambling. While there are many easily regulated intermediaries when it comes to traditional securities and derivatives, emerging bitcoin-denominated instruments rely much less on traditional intermediaries such as banks and securities exchanges. Additionally, the block chain technology that Bitcoin introduced for the first time makes completely decentralized markets and exchanges possible, thus eliminating the need for intermediaries in complex financial transactions.

In this Article we survey the type of financial instruments and transactions that will most likely be of interest to regulators, including traditional securities and derivatives, new bitcoin-denominated instruments, and completely decentralized markets and exchanges. We find that Bitcoin derivatives would likely not be subject to the full scope of regulation under the Commodity Exchange Act to the extent that such derivatives involve physical delivery (as opposed to cash settlement) or are non-fungible and not independently traded. We also find that

some laws, including those aimed at online gambling, do not contemplate a payment method like Bitcoin, thus placing many transactions in a legal gray area.

Following the approach to virtual currencies taken by the Financial Crimes Enforcement Network, we argue that other financial regulators should consider exempting or excluding certain financial transactions denominated in Bitcoin from the full scope of their regulations, much like private securities offerings and forward contracts are treated. We also suggest that to the extent that regulation and enforcement becomes more costly than its benefits, policymakers should consider and pursue strategies consistent with that new reality, such as efforts to encourage resilience and adaptation by existing institutions.

TABLE OF CONTENTS

I. INTRODUCTION

Bitcoin presents a unique challenge to policymakers. On the one hand, because it is an open protocol and a decentralized network, there is no company or central server that can be regulated. On the other hand, there are a number of emerging new intermediaries operating on the Bitcoin network that are certainly susceptible to regulation and enforcement. These include exchanges, merchant processors, and money transmitters that provide Bitcoin services to consumers. To date, Bitcoin-related regulation has largely been focused on the application of "know your customer," anti-money-laundering rules, as well as consumer protection licensing, on these new intermediaries.

The next major wave of Bitcoin regulation will likely be aimed at financial instruments, including securities and derivatives, as well as prediction markets and even gambling. While there are many easily regulated intermediaries when it comes to traditional securities and derivatives, emerging bitcoin-denominated instruments rely much less on traditional intermediaries. Additionally, the underlying block chain ledger technology that Bitcoin introduced for the first time makes completely decentralized markets and exchanges possible, thus eliminating the need for intermediaries in complex financial transactions.

In this Article we survey the type of financial instruments and transactions that will most likely be of interest to regulators, including traditional securities and derivatives, new bitcoin-denominated instruments, and completely decentralized markets and exchanges. We find that bitcoin derivatives would likely not be subject to the full scope of regulation under the Commodity Exchange Act to the extent that such derivatives involve physical delivery (as opposed to cash settlement) or are non-fungible and not independently traded. We also find that some laws, including those aimed at online gambling, do not contemplate a payment method like Bitcoin, thus placing many transactions in a legal gray area.

Following the approach to virtual currencies taken by the Financial Crimes Enforcement Network, we argue that other financial regulators should consider exempting or excluding certain financial transactions denominated in Bitcoin from the full scope of their regulations, much like private securities offerings and forward

contracts are treated. We also suggest that to the extent that the cost of regulation and enforcement grows to outweigh its benefits, policymakers should consider and pursue strategies consistent with that new reality, such as efforts to encourage resilience and adaptation by existing institutions.

This Article is structured as follows. Part I presents a brief sketch of Bitcoin technology and describes the first wave of Bitcoin-related regulation. Part II analyzes the legal treatment of traditional securities and derivatives that are either bitcoin-backed or which have bitcoins as the underlying asset, as well as non-traditional bitcoin-denominated securities, derivatives, prediction markets, and gambling. Finally, Part III considers the implications of completely decentralized markets and exchanges made possible by Bitcoin and other emerging technologies.

II. BITCOIN AND THE FIRST WAVE OF REGULATION

Bitcoin is an Internet protocol, a peer-to-peer network, software client, and a digital currency unit. Following the protocol, the network maintains a global public ledger that records Bitcoin transactions. As we will see in later sections, there are many different applications that this technology enables. To date, however, it is the simple payments and money transfer that has captured the public's imagination, and therefore that is what has drawn regulators' attention. In this section we will present a brief overview of Bitcoin as a payments or money transfer system, and the first wave of regulation that addressed those applications.

A. Bitcoin in Brief

Bitcoin is frequently described as a "digital currency."[1] While that description is accurate, it can be misleading as it is both too broad and too narrow. It is too broad because Bitcoin is a very particular kind of digital currency called a cryptocurrency (indeed, it is the first of its kind).[2] On the other hand it is too narrow because although currency is one aspect of the Bitcoin system, Bitcoin is more broadly an Internet protocol with many applications beyond payments or money transfer, such as recording property titles and

---

1. Francois R. Velde, *Bitcoin: A Primer*, 317 CHICAGO FED LETTER 1, 1 (2013).

2. Jerry Brito & Andrea Castillo, *Bitcoin: A Primer for Policymakers*, at 1 (2013), http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf.

authenticating documents.[3] Bitcoin's unique peer-to-peer properties allow it to simultaneously serve as a currency and a distributed ledger system.

Virtual or digital currencies are nothing new. From in-game currencies, like World of Warcraft Gold[4] or Linden Dollars,[5] to vendor-specific currencies like Facebook Credits,[6] Microsoft Points,[7] or even airline miles, digital currencies have been around for well over a decade. Even the dollars in one's PayPal account are essentially digital currency. Bitcoin is unique from the digital currencies that preceded it because it does not require a central authority, such as a company or government, to issue bitcoins or verify transfers between individuals.[8] Instead, Bitcoin employs secure communication techniques (cryptography) and peer-to-peer networking to eliminate the need for third parties.[9] Comparing Bitcoin to traditional payments and money transfer systems helps explain the distinction.

Before the introduction of the Bitcoin system in 2009, online transactions always required a trusted third-party intermediary.[10] For example, if Alice wanted to send $100 to Bob over the Internet, she would have had to rely on a third-party service like PayPal or MasterCard. Intermediaries like PayPal keep a ledger of account holders' balances. When Alice sends Bob $100, PayPal deducts the amount from her account and adds it to Bob's account.

Without such intermediaries, digital money could be spent twice. Imagine there are no intermediaries with ledgers, and digital cash is simply a computer file, just as digital documents, such as

---

3.   Jerry Brito, *It's More Than Money*, CATO UNBOUND (Jul. 12, 2013) http://www.cato-unbound.org/2013/07/12/jerry-brito/its-more-just-money;   Jerry Brito, *Is Bitcoin the Key to Digital Copyright?*, REASON MAG. (Feb. 24, 2014) http://reason.com/archives/2014/02/24/is-bitcoin-the-key-to-digital-copyright.

4.   Laurence H.M. Holland, *Making Real Money in Virtual Worlds*, FORBES MAGAZINE (Aug. 7, 2006), http://www.forbes.com/2006/08/07/virtual-world-jobs_cx_de_0807virtualjobs.html.

5.   Spencer Reiss, *Virtual Economics*, MIT TECH. REV. (Dec. 1, 2005) http://www.technologyreview.com/article/404979/virtual-economics/.

6.   Miguel Helft, *Facebook Hopes Credits Make Dollars*, N.Y. TIMES, Sept. 23, 2010 at B1.

7.   Ben Gilbert, *Microsoft Points from Xbox 360 transfer to Xbox One as real money, "equal or greater in Marketplace value,"* ENGADGET (Jun. 12, 2013), http://www.engadget.com/2013/06/12/microsoft-points-conversion-xbox-one/.

8.   Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, White Paper at 1 (2008), https://bitcoin.org/bitcoin.pdf.

9.   *Id.*

10. Jerry Brito & Andrea Castillo, *Bitcoin: A Primer for Policymakers*, at 1 (2013), http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf.

photos or Word documents are computer files. Alice could send $100 to Bob by attaching a money file to a message. But just as with email, sending an attachment does not remove it from one's computer. Alice would retain a perfect copy of the money file after she had sent it. She could then easily send the *same* $100 to Charlie. In computer science, this is known as the "double-spending" problem.[11] Until Bitcoin, it could only be solved by employing a ledger-keeping trusted third party.

Bitcoin's invention is revolutionary because for the first time the double-spending problem can be solved without the need for a third party. Bitcoin does this by distributing the necessary ledger among all the users of the system through a peer-to-peer network. Every transaction that occurs in the Bitcoin network is registered in a distributed public ledger called the "block chain." New transactions are checked against the block chain to ensure that the same bitcoins have not been previously spent, thus eliminating the double-spending problem. The global peer-to-peer network, composed of thousands of users, takes the place of an intermediary; Alice and Bob can transact online without PayPal.

Transactions are verified and secured through the clever use of public-key cryptography.[12] Public-key cryptography requires that each user be assigned two "keys," one private key that is kept secret like a password, and one public key that can be shared with the world. The mathematical relationship between a given public key and the corresponding private key allows users to verify bitcoin ownership (that is, that the owner holds the private key) by simply checking a public key using the Bitcoin software. Let's say Alice wants to transfer one bitcoin to Bob. She creates a message to the network, called a "transaction," stating that she would like to transfer 1 BTC from her public address to Bob's public address. She then "signs" it with her private key and broadcasts the message over the network. By looking at Alice's public key, anyone can verify that the transaction was indeed signed with her private key, that it is an authentic exchange, and that Bob is the new owner of the funds. The transaction—and thus the transfer of ownership of the bitcoins— is recorded, time-stamped, and displayed in one "block" of the block chain by a network of voluntary "miners" that contribute their

---

11. David Chaum, *Achieving Electronic Privacy*, SCIENTIFIC AMERICAN MAG. (Aug. 1992), at 96–101.

12. *See generally* CHRISTOF PAAR & JAN PELZL, UNDERSTANDING CRYPTOGRAPHY: A TEXTBOOK FOR STUDENTS AND PRACTITIONERS ch. 6 (Springer 1st ed. 2010) *sample available at* http://wiki.crypto.rub.de/Buch/ download/Understanding-Cryptography-Chapter6.pdf.

computer's processing power to the system. This process ensures that all computers in the network have a verified record of all transactions within the Bitcoin network that is updated by miners roughly every ten minutes.

Transactions on the Bitcoin network are not denominated in dollars or any other country's currency as they are on PayPal, but are instead denominated in bitcoins. This makes Bitcoin a virtual currency in addition to a decentralized public ledger. The value of the currency is not derived from gold or government fiat, but from the value that people assign to it. The dollar value of a bitcoin is determined on an open market, just like the exchange rate between different world currencies. The number of bitcoins that are issued— that is, the size of the money supply—is not determined by any person, company, or central bank, but instead grows at an algorithmically pre-determined rate baked into the protocol.[13]

For these reasons, Bitcoin is unlike any digital currency that preceded it. Bitcoin is not just a virtual unit of account, but also a decentralized system for transferring value. It is a *cryptocurrency*, which means that a central authority does not issue the currency nor verify its transactions. Transactions are instead recorded in a decentralized and distributed public ledger and are cryptographically verifiable. Bitcoin was the world's first cryptocurrency, and since its invention other cryptocurrencies have emulated its model.[14] As we'll see in Part III, *infra*, because Bitcoin is at root a decentralized and distributed public ledger, and because it is programmable, it has the potential to facilitate completely decentralized security exchanges, prediction markets, and gambling.

B.   The First Wave of Regulation

Payments and money transfers are the most obvious application of the distributed public ledger technology, so they were the first application of the technology to be implemented. Merchants

---

13.   The explanation of Bitcoin's mechanics presented here is a consciously abridged one. It might therefore be unsatisfying to those encountering Bitcoin for the first time. Readers looking for a more-detailed explanation of Bitcoin's operation should consult: Velde, *supra* note 1, at 1-2; Brito & Castillo, *supra* note 2, at 4-9.

14.   Alex Liu, *Beyond Bitcoin: A Guide to the Most Promising Cryptocurrencies*, MOTHERBOARD (Nov. 29, 2013), http://motherboard.vice.com/blog/beyond-bitcoin-a-guide-to-the-most-promising-cryptocurrencies.

from Overstock.com[15] to the Sacramento Kings[16] to WordPress.com[17] have begun accepting payment in Bitcoin, and startups like BitPesa plan to use the Bitcoin network to facilitate international remittances.[18] By disintermediating traditional financial networks like PayPal, Visa, and Western Union, Bitcoin offers three main utilities: it can be cheaper, faster, and censorship-resistant.

First, Bitcoin transaction costs are much lower than those of traditional financial networks. While credit card networks charge merchants fees in the range of 3 to 4 percent of the total amount of a transaction,[19] and the average cost of international remittances is 8.5 percent,[20] a Bitcoin transaction can cost less than 1 percent.[21] Second, Bitcoin transactions can be much faster. For example, while international wire transfers can take days to complete, Bitcoin transactions take roughly ten minutes.[22] Finally, Bitcoin is censorship-resistant. For example, while PayPal froze the accounts of WikiLeaks after it released secret State Department cables, and prevented its customers from making donations to the group,[23] such transactional prior restraint would not be possible on the Bitcoin network because there is no intermediary.

---

15. Cade Metz, *The Grand Experiment Goes Live: Overstock.com Is Now Accepting Bitcoins*, WIRED MAG. (Jan. 9, 2014), http://www.wired.com/2014/01/overstock-bitcoin-live/.

16. Cade Metz, *Sacramento Kings Crowned First Pro Sports Team to Accept Bitcoin*, WIRED MAG. (Jan. 16, 2014), http://www.wired.com/2014/01/sacramento-kings-bitcoin/.

17. Jon Matonis, *What's Your Bitcoin Strategy? WordPress Now Accepts Bitcoin Across the Planet*, FORBES MAG. (Nov. 16, 2012), http://www.forbes.com/sites/jonmatonis/2012/11/16/whats-your-bitcoin-strategy-wordpress-now-accepts-bitcoin-across-the-planet/.

18. Richard Boase, *BitPesa Uses Bitcoin to Slash Kenyan Remittance Costs*, COINDESK (Nov. 28, 2013), http://www.coindesk.com/bitpesa-uses-bitcoin-slash-kenyan-remittance-costs/.

19. Paul Downs, *What You Need to Know About Credit Card Processing*, N.Y. TIMES (Mar. 25, 2013), http://boss.blogs.nytimes.com/2013/03/25/what-you-need-to-know-about-credit-card-processing/.

20. *Remittance Prices Worldwide*, WORLD BANK, http://remittanceprices.worldbank.org/ (last visited Mar. 26, 2014).

21. Note that the tradeoff for the low transaction costs of a bitcoin transaction is the lack of insurance, consumer protection measures like AML/KYC checks, and perks that are paid for with traditional payment systems' higher fees.

22. The market standard for Bitcoin transactions that minimize double-spend probability is roughly one hour. Average transaction times are viewable at: *Average Transaction Confirmation Time*, BLOCKCHAIN.INFO, http://blockchain.info/charts/avg-confirmation-time (last visited Mar. 26, 2014).

23. Kevin Poulsen, *PayPal Freezes WikiLeaks Account*, WIRED MAG. (Dec. 4, 2010), http://www.wired.com/threatlevel/2010/12/paypal-wikileaks/.

Bitcoin is in many ways a disruptive technology,[24] and sensing a great profit opportunity, venture capitalists and entrepreneurs are presently rushing to develop the network's infrastructure. Among the key parts of this first wave of startups are exchanges that allow consumers to trade fiat currency, such as dollars or euros, for bitcoins and vice versa; online wallets that allow consumers who do not want to run the more-complicated desktop software on their own computers to carry bitcoin balances and spend them; and merchant services, which easily allow merchants to accept bitcoin payments and have dollars deposited in their bank accounts, thus eliminating volatility risk.

Like other disruptive technologies, Bitcoin is first taking hold in spaces that are underserved by incumbents. This includes innovative areas like micropayments[25] and crowdfunding,[26] but also payments related to the online sale of illicit goods, such as drugs and firearms in the U.S. or subversive actions against oppressive regimes like Iran[27] and Russia.[28] Because Bitcoin is censorship-resistant, it can be employed for transactions that incumbent intermediaries would not process, or are not allowed by law to process. Indeed, it is possible that Bitcoin's network effects were bootstrapped by demand for use in facilitating illicit transactions.[29]

Given that the first application of the Bitcoin technology has been simple payments and money transfers, and given that the technology's censorship-resistance permits transactions that were previously restrained, it is no surprise that the first wave of regulatory activity related to Bitcoin has focused on money transmission. At the

---

24. Timothy Lee, *Bitcoin is a Disruptive Technology*, FORBES MAG. (Apr. 9, 2013), http://www.forbes.com/sites/timothylee/2013/04/09/bitcoin-is-a-disruptive-technology/.

25. Pete Rizzo, *Bitcoin Micropayments Get Big Moment as Chicago Sun-Times Paywall Experiment Goes Live*, COINDESK (Feb. 1, 2014), http://www.coindesk.com/micropayments-chicago-sun-times-paywall-live/.

26. Eric Blattberg, *Crowdtilt launches free, open source crowdfunding solution and it supports Bitcoin*, VENTUREBEAT (Feb. 20, 2014), http://venturebeat.com/2014/02/20/crowdtilt-launches-free-open-source-crowdfunding-solution-and-it-supports-bitcoin/.

27. Max Raskin, *Dollar-Less Iranians Discover Virtual Currency*, BUSINESSWEEK (Nov. 29, 2012), http://www.businessweek.com/articles/2012-11-29/dollar-less-iranians-discover-virtual-currency.

28. Gabriela Baczynska, *Russian authorities say Bitcoin illegal*, REUTERS (Feb. 9, 2014), http://www.reuters.com/article/2014/02/09/us-russia-bitcoin-idUSBREA1806620140209.

29. Eli Dourado, *Can the War on Drugs Bootstrap Bitcoin?*, ELI DOURADO BLOG (June 4, 2011), http://elidourado.com/blog/can-the-war-on-drugs-bootstrap-bitcoin/.

federal level, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued guidance in March of 2013 advising that Bitcoin exchangers and other related enterprises qualified as money transmitters under the Bank Secrecy Act.[30] As a result, such businesses are obligated to register with FinCEN as money services businesses (MSBs) in each state in which they do business. They also must comply with "know your customer" rules, put in place robust anti-money-laundering programs, and file Suspicious Activity Reports.[31]

Money transmitters must be licensed by each state in which they do business, so at the state level, financial regulators have been grappling with how existing money transmission laws and regulations apply to Bitcoin businesses.[32] New York has taken the lead in making these determinations. In August 2013, New York's Department of Financial Services subpoenaed almost two-dozen Bitcoin-related businesses, as well as investors in those businesses, seeking more information about their activities.[33] And in January of 2014, the Department held two days of hearings looking at how Bitcoin businesses should be licensed, and considering the possibility of a new "BitLicense" tailored specifically for virtual currencies.[34]

Law enforcement actions to date have also centered on money laundering and unlicensed money transmission. In May of 2013, federal agents seized $5 million from accounts belonging to Mt. Gox, which at the time was the world's largest bitcoin exchange.[35] According to the seizure warrant, the company had not registered with FinCEN as a money services business and had stated

---

30. U.S. DEP'T OF THE TREASURY, FINANCIAL CRIMES AND ENFORCEMENT NETWORK, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013), *available at* http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

31. *Id.*

32. Marco Santori, *Bitcoin Law: Money transmission on the state level in the US*, COINDESK (Sept. 28, 2013), http://www.coindesk.com/bitcoin-law-money-transmission-state-level-us/.

33. Greg Farrell, *N.Y. Subpoenas Bitcoin Firms in Probe on Criminal Risk*, BLOOMBERG (Aug. 12, 2013), http://www.bloomberg.com/news/2013-08-12/n-y-regulator-subpoenas-firms-over-bitcoin-crime-risks.html.

34. Cater Dougherty, *New York Vying With California to Write Bitcoin Rules*, BLOOMBERG (Jan. 27, 2014), http://www.bloomberg.com/news/2014-01-27/new-york-duels-california-to-write-bitcoin-rules.html.

35. Amar Toor, *US seizes and freezes funds at biggest Bitcoin exchange*, THE VERGE (May 15, 2013), http://www.theverge.com/2013/5/15/4332698/dwolla-payments-mtgox-halted-by-homeland-security-seizure-warrant.

in its bank application that it was not engaged in money services.[36] Similarly, in January of 2014, federal agents arrested Charlie Shrem, CEO of the now-shuttered exchange BitInstant, on charges of money laundering, operating an unlicensed money transmitter, and willful failure to file suspicious activity reports with FinCEN.[37] According to the criminal complaint against Shrem, he knowingly helped a bitcoin reseller exchange dollars for bitcoins to be used on anonymous online black market Silk Road.[38] In February of 2014, a U.S. Secret Service investigation of the popular in-person Bitcoin trading directory, LocalBitcoins.com, resulted in criminal charges being filed against two Florida men.[39] Both had allegedly violated anti-money laundering laws and ran unlicensed money transmission businesses.[40]

In the near term, state regulators will likely continue to develop guidelines for applying money transmission licensing rules to Bitcoin businesses. For its part, FinCEN has begun to release administrative rulings clarifying the applicability of its regulations to specific business cases.[41] Other federal regulators are also developing guidance to explain how their regulations apply to Bitcoin.[42] For example, the Federal Election Commission has been

---

36.   Seizure Warrant, In the Matter of the Seizure of The contents of one Dwolla account (No. 13-1162 SKG), (D. Md. May 14, 2013), *available at* http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-Gox-Dwolla-Warrant-5-14-13.pdf.; Aff. in Support of Seizure Warrant (No. 13-1085SAG), (D. Md. May 9, 2013).

37.   Sealed Complaint, United States v. Robert M. Faiella, a/k/a "BTCKing," and Charlie Shrem, No. 14-MAG-0164 (S.D.N.Y. Jan. 24, 2014), *available at* http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR/Faiella, Robert M. and Charlie Shrem Complaint.pdf.

38.   *Id.*

39.   Brian Krebs, *Florida Targets High-Dollar Bitcoin Exchangers*, KREBS ON SECURITY (Feb. 7, 2014), http://krebsonsecurity.com/2014/02/florida-targets-high-dollar-bitcoin-exchangers/.

40.   *Id.*

41.   U.S. DEP'T OF THE TREASURY, FINANCIAL CRIMES AND ENFORCEMENT NETWORK, FIN-2014-R001, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY MINING OPERATIONS (Jan. 30, 2014), *available at* http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf; U.S. DEP'T OF THE TREASURY, FINANCIAL CRIMES AND ENFORCEMENT NETWORK, FIN-2014-R002, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY SOFTWARE DEVELOPMENT AND CERTAIN INVESTMENT ACTIVITY (Jan. 30, 2014), *available at* http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf.

42.   As an example of what economist George Selgin calls "synthetic commodity" money, Bitcoin shares features of both commodity money and fiat money. The features that regulators choose to emphasize will therefore determine that agency's jurisdiction (or lack thereof) over Bitcoin transactions. *See* George

looking at the question of bitcoin campaign contributions,[43] and the Internal Revenue Service recently issued guidance on the tax treatment of bitcoins.[44] However, as we will argue in the following section, the next major wave of regulatory scrutiny that Bitcoin will face will not be related to money transmission, but will instead come from financial regulators, including the Securities and Exchange Commission and the Commodity Futures Trading Commission, who will be looking at Bitcoin-related financial instruments and markets.

III. REGULATION OF BITCOIN-RELATED FINANCIAL INSTRUMENTS

There is some debate about whether bitcoins qualify as currency, commodities, or a new asset class altogether.[45] Whatever the answer, the fact is that as the Bitcoin economy develops, one should expect to see demand for Bitcoin-related financial instruments emerge. Indeed, such demand is already beginning to manifest itself. In this section, we survey some of these instruments and analyze how existing law and regulation may apply to them.

A. Bitcoin Derivatives

Over the course of 2013, regulators and central banks around the world issued warnings to consumers about the risks associated with Bitcoin.[46] Chief among these risks is the currency's historical volatility. The dollar-denominated market price of one bitcoin began 2013 at around $13.41 and closed the year at around $817.12 in December.[47] In that time, the price reached a high of $1,147.25 on December 4th, and experienced single-day gains of

---

Selgin, *Synthetic Commodity Money* (Apr. 21, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118.

43. Benjamin Goad, *FEC: No bitcoins in federal campaigns*, THE HILL (Nov. 21, 2013), http://thehill.com/blogs/regwatch/technology/191096-fec-no-bitcoins-in-federal-campaigns.

44. I.R.S. Notice 14-21, 2014-21, http://www.irs.gov/pub/irs-drop/n-14-21.pdf.

45. Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 160 (2011).

46. *See generally* GLOBAL LEGAL RESEARCH CENTER, REGULATION OF BITCOIN IN SELECTED JURISDICTIONS, S. DOC. NO. 2014-010233 (2014), *available at* http://www.loc.gov/law/help/bitcoin-survey/.

47. Price data from the CoinDesk Bitcoin Price Index, which aggregates price data from multiple exchanges that meet certain criteria; in this case, Bitfinex, Bitstamp, and BTC-e. *See Bitcoin Price Index Chart*, COINDESK, http://www.coindesk.com/price/#2012-12-31,2013-12-30/,close,bpi,USD (last visited Mar. 27, 2014).

$198.09,[48] and losses of $208.[49] This volatility obviously presents a challenge to anyone looking to transact using Bitcoin.
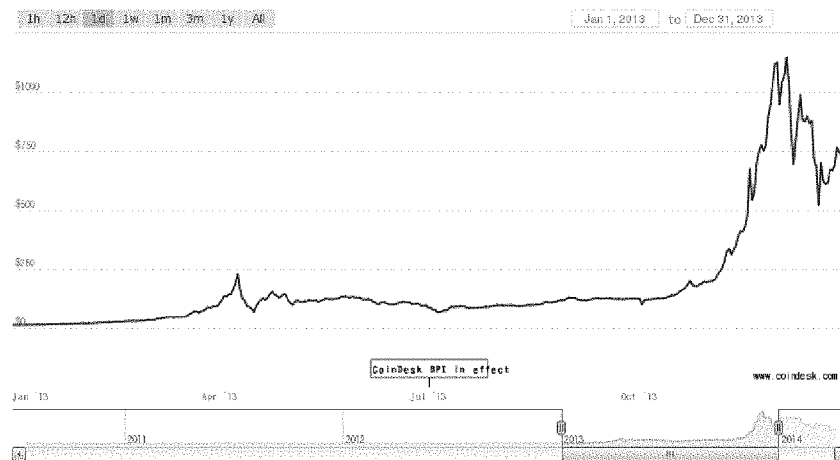
Figure 1 – *Bitcoin-dollar exchange rate for 2013.*

Bitcoin may not be inherently volatile, however.[50] Its volatility is likely attributable to the fact that it is a new currency, still in the process of discovering its stable price.[51] Additionally, as a nascent currency, it is very thinly traded and as a result a single large trade can affect the exchange price substantially. Positive news, such as major retailers announcing they will accept the currency, can make the price jump dramatically, while negative news, such as unfavorable regulatory pronouncements, can send the price plummeting. And greater media coverage of any kind will no doubt introduce more and more persons to Bitcoin for the first time and thus drive new demand for the currency.

---

48. Gains for trades between the closing prices on November 17 and November 18, 2013. *See Bitcoin Price Index Chart,* COINDESK, http://www.coindesk.com/price/#2012-12-31,2013-12-30,close,bpi,USD (last visited Mar. 27, 2014).

49. Losses for trades between the closing prices on December 5 and December 6, 2013. *See Bitcoin Price Index Chart,* COINDESK, http://www.coindesk.com/price/#2012-12-31,2013-12-30,close,bpi,USD (last visited Mar. 27, 2014).

50. Indeed, volatility has historically trended down. *See* Eli Dourado, *Bitcoin Volatility is Down Over the Last Three Years. Here's the Chart that Proves It,* ELI DOURADO BLOG (Jan. 20, 2014), http://elidourado.com/blog/bitcoin-volatility/.

51. Timothy B. Lee, *These four charts suggest that Bitcoin will stabilize in the future,* WASHINGTON POST (Feb. 3, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/03/these-four-charts-suggest-that-bitcoin-will-stabilize-in-the-future/.

Despite this volatility, tens of thousands of merchants accept bitcoins for payment.[52] The reason is that while Bitcoin's present volatility may make it an unstable source of value, it can nevertheless serve as an excellent medium of exchange.[53] As Marc Andreessen has put it, "Bitcoin can be used entirely as a payment system; merchants do not need to hold any Bitcoin currency or be exposed to Bitcoin volatility at any time."[54] This means accepting bitcoins for payment at the current exchange rate and then immediately converting those bitcoins to dollars or some other stable currency. This is what Overstock.com, one of the largest retailers to accept bitcoins, does.[55] Overstock CEO Patrick Byrne has explained that the company will not hold bitcoins saying, "Until we can hedge through some kind of derivative instrument, we don't want to take that direct exposure."[56]

An astute reader will no doubt be thinking: well, *someone* has to be holding the bitcoins. Speculators account for a large portion of bitcoin holdings,[57] but what about bitcoins that are actively being transacted? In the case of Overstock.com, the retailer is employing merchant services from Coinbase, a Silicon Valley startup backed by Andreessen Horowitz.[58] When you make a purchase at Overstock, prices are denominated in dollars, and if you pay in bitcoins, Coinbase accepts the bitcoins and deposits the dollar amount into Overstock's bank account. This means that it is Coinbase that is accepting the exchange volatility risk.[59] For its services, Coinbase charges Overstock a fee of about 1 percent,[60]

---

52. *BitPay Announces Bitcoin Payroll API*, BUSINESSWIRE (Jan. 13, 2014), http://www.businesswire.com/news/home/20140113006504/en/BitPay-Announces-Bitcoin-Payroll-API; *New Coinabase for Android, and Coinbase Merchant App Released for Android*, COINBASE BLOG (Dec. 29, 2013), http://blog.coinbase.com/post/71607045439/new-coinbase-for-android-and-coinbase-merchant-app.

53. Marc Andreessen, *Why Bitcoin Matters*, N.Y. TIMES (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.

54. *Id.*

55. Rob Wile, *Bitcoin Is Experiencing Its Longest Stretch of Price Stability In a While*, BUSINESS INSIDER (Jan. 29, 2014, 9:35 AM), http://www.businessinsider.com/bitcoin-volatility-slows-2014-1.

56. *Id.*

57. Will Knight, *Show Me the Bitcoins*, MIT TECH. R. (Feb. 2014), http://www.technologyreview.com/graphiti/524796/show-me-the-bitcoins/.

58. Cade Metz, *The Grand Experiment Goes Live: Overstock.com Is Now Accepting Bitcoins*, WIRED MAG. (Jan. 9, 2014), http://www.wired.com/2014/01/overstock-bitcoin-live/.

59. *Id.*

60. In August of 2013, Coinbase waived all merchant fees for the first $1 million in transactions, after which merchants were charged a fee of 1 percent of

which is less than the fees associated with other electronic payments such as credit cards.[61]

However, that 1 percent fee by itself might not be enough to cover the exchange rate risk that Coinbase could face in the future. At the moment, Coinbase is hedging its exposure exchange rate risk using automated, algorithmic trading.[62] Other merchant services companies, like Founders-Fund-backed BitPay, seem to employ a similar approach.[63] But this approach is not as efficient as simply engaging in a swap or futures contract. It is not surprising, therefore, that bitcoin payment processors and others are clamoring for Bitcoin derivatives.[64] Such instruments could help calm Bitcoin's volatility and could allow the network's infrastructure to further develop.

There are several types of derivatives contracts that parties seeking to reduce their exposure to Bitcoin price volatility can employ. We consider Bitcoin futures, forwards, swaps, and options. These types of Bitcoin derivatives come within the orbit of regulation by the Commodity Futures Trading Commission (CFTC) pursuant to the Commodity Exchange Act (CEA).[65] The CFTC regulates futures and swaps markets to protect buyers and sellers of derivatives, and other participants in the derivatives markets, from fraud, market manipulation, abusive practices, and systemic risk.[66] Bitcoin derivatives would likely not be subject to the full scope of regulation under the CEA to the extent such derivatives involve

the transaction value, plus any fees charged by legacy banks for ACH transactions (usually around $0.15 per transaction). *See Your first $1,000,000 USD in merchant processing is now free!*, COINBASE BLOG (Aug. 26, 2013), http://blog.coinbase.com/post/59417545262/your-first-1-000-000-usd-in-merchant-processing-is-now.

61. Coinbase compares its rates to the 2.2 percent standard favored by credit card companies. *See What fees does Coinbase charge for merchant processing?*, COINBASE SUPPORT (Feb. 5, 2014), http://support.coinbase.com/customer/portal/articles/1277919-what-fees-does-coinbase-charge-for-merchant-processing-.

62. Cade Metz, *The Grand Experiment Goes Live: Overstock.com Is Now Accepting Bitcoins*, WIRED MAG. (Jan. 9, 2014), http://www.wired.com/business/2014/01/overstock-bitcoin-live/.

63. Greg Simon, *Exclusive Interview with Bitpay CEO Tony Gallippi*, KNOWMADIC LIFE BLOG (Dec. 28, 2013), http://knowmadiclife.com/blog/2013/12/28/exclusive-interview-with-bitpay-ceo-tony-gallippi.

64. Cade Metz, *The Next Big Thing You Missed: There's a Sure-Fire Way to Control the Price of Bitcoin*, WIRED MAG (Jan. 14, 2014, 9.30 AM), http://www.wired.com/business/2014/01/bitcoin-derivatives/.

65. CEA, 7 U.S.C. § 1 et seq. (1936).

66. *Mission and Responsibilities*, U.S. COMMODITY FUTURES TRADING COMM'N, http://www.cftc.gov/About/MissionResponsibilities/index.htm (last visited Nov. 14, 2014).

physical delivery (as opposed to cash settlement) or are non-fungible and not independently traded.

1. Futures

In a futures contract, one party agrees to deliver an underlying asset or its cash-equivalent to another at a later time at a pre-specified price.[67] A party concerned with Bitcoin prices decreasing would take the "short" position in a futures contract and agree to sell Bitcoin at a specific price. For example, on January 1st one party may agree to sell 1 bitcoin on February 1st for $800. This agreement would lock in a bitcoin-to-dollar exchange rate of 0.00125 bitcoins, or BTC. A company that owns or expects to be paid in bitcoins, and is concerned about the value of bitcoins dropping against the dollar, would be protected against that risk. On the other hand, if bitcoins became more valuable after January 1st, the futures contract would still require the buyer to sell at what would be below-market prices.

Futures are standardized with respect to all terms except for price. They specify the underlying asset, the amount of the asset to be exchanged, the place and month for delivery, and the price.[68] The CFTC defines a future as "[a]n agreement to purchase or sell a commodity for delivery in the future" in which the price is determined at the outset of the agreement.[69] With few exceptions, the definition of commodity is defined broadly to include all agricultural products and "all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in."[70]

---

67. John C. Hull, Options, Futures, and Other Derivatives 6 (6th ed. 2006); *Futures Contract Definition*, CFTC Glossary, U.S. Commodity Futures Trading Comm'n Education Center, http://www.cftc.gov/consumerprotection/educationcenter/cftcglossary/ (last visited Mar. 27, 2014).

68. Hull, *supra* note 67, at 23-25; CME Group, A Trader's Guide to Futures, 13-14, http://www.cmegroup.com/content/dam/cmegroup/education/files/a-traders-guide-to-futures.pdf. Under some circumstances, a non-standardized contract may be categorized as a futures contract. *See* In re Bybee, 945 F.2d 309, 312-13 (9th Cir. 1991).

69. *Futures Contract Definition*, Glossary, U.S. Commodity Futures Trading Comm'n Education Center, http://www.cftc.gov/consumerprotection/educationcenter/cftcglossary/ (last visited Mar. 27, 2014).

70. 7 U.S.C. § 1a(9) (1936). Two interests that fall outside of the definition of commodity include onions and motion picture box office receipts. *Id.*

The CEA categorizes commodities into one of three categories: "agricultural commodities" such as soybean and wheat,[71] "excluded commodities" which are made up of financial interests such as prices and price indices, interest rates, and currencies,[72] and a catch-all category of "exempt commodities" that includes energy interests, precious metals, and measurable events such as the weather.[73] The CFTC also sometimes distinguishes commodities based upon whether they are financial or nonfinancial in nature.[74] Another distinction is between tangible commodities (such as crops and currencies) and intangible commodities (such as price indices, pollution allowances, and contractual rights).[75]

Commodity futures are subject to the CEA and regulated by the CFTC and entities that have self-regulatory responsibilities, including futures exchanges and the National Futures Association (NFA). Under the CEA, futures may only be traded on regulated exchanges.[76] Accordingly, trading a futures contract requires an account with a futures exchange and compliance with the exchange's requirements such as posting collateral when entering the contract (initial margin) and paying more collateral if the market value of the contract decreases (variation margin). Trading futures often takes place through an intermediary known as a futures commission merchant.

The CEA categorizes regulated futures exchanges as a type of designated contract market that are required to comply with twenty-three "core principles."[77] These principles effectively require

---

71. CEA § 1a(9) (1936); CFTC Glossary, Agricultural Commodity.

72. *See* CEA § 1a(19) (1936) (defining "excluded commodity" to include a wide range of financial interests).

73. CEA § 1a(20) (1936); CFTC Glossary, Exempt Commodity; CFTC Glossary, Weather Derivative (defining "weather derivative" as "[a] derivative whose payoff is based on a specified weather event, for example, the average temperature in Chicago in January").

74. 77 Fed. Reg. 48,227, 48,232-48,233 (Aug. 13, 2012) (defining nonfinancial commodities as consisting of (1) exempt commodities or agricultural commodities that are physically deliverable; and (2) intangible commodities whose ownership can be transferred and are consumable), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2012-18003a.pdf.

75. *Id.*

76. CEA § 6(a) (1936); 7 U.S.C. § 6 (1936).

77. CEA § 5(b-x) (1936), 7 USC § 7(d) (1936). A designated contract market is defined as "a board of trade or exchange designated by the CFTC to trade futures, swaps, and/or options under the CEA. A contract market can allow both institutional and retail participants and can list for trading contracts on any commodity, provided that each contract is not readily susceptible to manipulation." *Commodity Market Definition*, CFTC GLOSSARY,

exchanges to establish and enforce rules to protect customers, prevent fraud and manipulation, maintain and disclose records, and maintain fair and orderly markets by, for example, enforcing position limits.[78] Regulated exchanges are available to ordinary retail investors.[79] In addition, other futures market intermediaries are required to register with the CFTC and are subject to wide ranging regulation. These intermediaries include futures commission merchants (that serve the function of brokerages),[80] introducing brokers,[81] commodity pool operators,[82] and commodity trading advisers.[83] The CEA and CFTC regulation impose a wide variety of requirements on these intermediaries, including obligations involving disclosure, reporting, recordkeeping, ethical requirements, protection of customer funds, and capital requirements.[84]

---

http://www.cftc.gov/consumerprotection/educationcenter/cftcglossary/glossary_co; Core Principles and Other Requirements for Designated Contract Markets, 77 Fed. Reg. 36, 612 (CFTC June 19, 2012), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2012-12746a.pdf.

78. *See also* 7 U.S.C. § 6g(e) (1936) (requiring exchanges to publicly disclose daily trading volume).

79. A similar regulatory framework applies to derivatives clearing organizations. 7 USC § 7a-1(c)(2) (1936). Retail investors routinely transact off-exchange commodity transactions through the retail foreign exchange market. This is permitted so long as the retail investor's counterparty is regulated by the CFTC as an FCM or a retail foreign exchange dealer, or by another financial regulator such as the Securities and Exchange Commission. *See* CEA § 2(c)(2)(D) (1936) (regulating leveraged or margined retail commodity transactions); CFTC, Regulation of Off-Exchange Retail Foreign Exchange Transactions and Intermediaries, 75 Fed. Reg. 55,410 (Sept. 10, 2010), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2010-21729a.pdf.

80. CEA § 1a(28) (1936); 7 USC § 1a(28) (1936) (defining futures commission merchant).

81. 7 U.S.C. § 1a(31) (1936) (defining introducing broker).

82. 7 U.S.C. § 1a(11) (1936) (defining commodity pool operator); Harmonization of Compliance Obligations for Registered Investment Companies Required to Register as Commodity Pool Operators, 78 Fed. Reg. 52,308 (CFTC Aug. 22, 2013).

83. 7 U.S.C. § 1a(12) (1936) (defining commodity trading advisor); CFTC v. Equity Financial Group LLP, 572 F.3d 150 (3d Cir. 2009).

84. 7 U.S.C. § 6d(a)(1) (1936) (futures commission merchant registration requirements); 7 U.S.C. § 6d(a)(2) (1936) (FCM customer funds segregation duties); 78 Fed. Reg. 68506, Enhancing Protections Afforded Customers and Customer Funds Held by Futures Commission Merchants and Derivatives Clearing Organizations (Nov. 14, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-11-14/pdf/2013-26665.pdf; 7 U.S.C. 6d(c) (1936) (requiring FCMs and introducing brokers to implement conflicts-of-interest systems); 7 U.S.C. § 6g (1936) (reporting and recordkeeping requirements for futures commission merchants, introducing brokers, and floor brokers and traders); 7 U.S.C. § 6f(c)(2) (1936) (risk assessment

Although bitcoins fall under the CEA's definition of commodity, it is unclear what category of commodity they fall under. Bitcoins may be categorized as an excluded commodity if they are viewed as being a type of currency or other financial interest. On the other hand, there are several reasons why bitcoins should be categorized as an exempt commodity. First, bitcoins may be viewed as being similar to precious metals because they are limited in supply and capable of being physically delivered (at least in a digital sense). In addition, like metals, bitcoins are a capital good because they are used to produce other goods and services such as digital assets and contracts.[85] Second, the CFTC classifies intangible commodities as exempt commodities "if ownership of the commodity can be conveyed in some manner and the commodity can be consumed."[86] Bitcoins may accordingly be viewed as intangible exempt commodities because they can be owned and "consumed" in the sense of being spent (or traded). Finally, Bitcoins may be categorized as an exempt commodity because commodities that fail to meet the definition of an agricultural commodity or an excluded (financial) commodity are classified as exempt commodities.[87]

Accordingly, despite the unique nature of bitcoins, they fall within the definition of commodity for the purposes of futures regulation. Whether bitcoins are classified as excluded or exempt

---

recordkeeping requirements for futures commission merchants); 7 U.S.C. § 6d(g) (1936) (introducing broker registration requirement); CFTC, Minimum Net Capital Requirements for Futures Commission Merchants and Introducing Brokers, http://www.cftc.gov/IndustryOversight/Intermediaries/FCMs/fcmibminimumnetcapital; 7 U.S.C. § 6m(1) (1936) (registration requirements for CTAs and CPOs); 7 U.S.C. § 6o(1) (1936) (prohibiting fraud by commodity trading advisers and commodity pool operators); 77 Fed. Reg. 20,127-20,215 (CFTC Apr. 3 2012) (obligations of futures commission merchants); 7 U.S.C. § 6n(3)(A) (1936) (recordkeeping requirements for commodity trading advisers and commodity pool operators); 77 Fed. Reg. 11,252 (CFTC Feb. 24 2012) (compliance obligations for commodity pool operators and commodity trading advisers).

85. Old Kharif, *Bitcoin 2.0 Shows Technology Evolving Beyond Use as Money*, BLOOMBERG (Mar. 28, 2014), http://www.bloomberg.com/news/2014-03-28/bitcoin-2-0-shows-technology-evolving-beyond-use-as-money.html.

86. 77 Fed. Reg. 48,227, 48,233 (Aug. 13, 2012), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2012-18003a.pdf.

87. CEA Section § 1a(20) (1936); *Exempt Commodity Definition*, CFTC Glossary, http://www.cftc.gov/ConsumerProtection/EducationCenter/CFTCGlossary/glossary_e.

commodities may have regulatory implications for Bitcoin swaps and for contracts sold to retail investors.[88]

Any futures contract referencing bitcoins will thus likely be subject to the full scope of regulation under the CEA. At a minimum, this means that Bitcoin futures must be traded on existing regulated exchanges such as the Chicago Mercantile Exchange. Otherwise, any platform that offers Bitcoin futures would have to come into compliance with the wide-ranging and costly regulation required by the CEA for regulated futures exchanges.

2. Forwards

A forward is a contract whereby parties agree to trade an asset at a later date at a price specified in the present.[89] For example, a contract where an oil refiner pays an oil producer to deliver oil at a specific time in the future and at a specific price is a forward contract.[90] In contrast to futures, forwards are negotiated to be tailored to the specific risks and other terms that parties are concerned about and do not trade on centralized exchanges.

Importantly, forward contracts are excluded from CFTC regulation.[91] The court in *CFTC v. Erskine* summarized the policy rationale behind the forward exclusion:

> The purpose of [the] "cash forward" exception [to CFTC regulation] is to permit those parties who contemplate physical transfer of the commodity to set up contracts that

---

88. If bitcoins are classified as currency-like excluded financial commodities, they may ultimately be subject to the Treasury Department's exemption from clearing and trading applicable to foreign exchange swaps and forwards. In addition, excluded commodity bitcoins sold to retail investors would likely be regulated like retail foreign exchange transactions. However, if bitcoins are classified as exempt nonfinancial commodities, they may be completely exempt from swaps regulation if they also qualify as a forward contract intended for physical delivery. 7 U.S.C. § 1a(47)(B)(ii) (1936).

89. *Forward Contract Definition*, CFTC Glossary, U.S. COMMODITY FUTURES TRADING COMM'N EDUC. CTR., http://www.cftc.gov/ConsumerProtection/EducationCenter/CFTCGlossary/index.htm; Hull, *supra* note 67, at 3-4 (last visited Mar. 27, 2014).

90. Ronald H. Filler & Jerry W. Markham, REGULATION OF DERIVATIVE FINANCIAL INSTRUMENTS (SWAPS, OPTIONS AND FUTURES), 1-2 (2014).

91. CEA § 1a(27) (1936) (excluding sales "of any cash commodity for deferred shipment or delivery" from the term "future delivery"); U.S. Commodity Futures Trading Comm'n v. Reed, 481 F. Supp. 2d 1190 (D. Colo. 2007) ("The CFTC's exclusive jurisdiction does not extend to transactions involving the sale or physical delivery of the actual commodity, which are referred to as 'cash forwards' or 'spot' transactions.").

reduce the risk of price fluctuations, without subjecting the parties to burdensome regulations. These contracts are not subject to the CFTC regulations because those regulations are intended to govern only speculative markets; they are not meant to cover contracts wherein the commodity in question has an "inherent value" to the transacting parties.[92]

The forward exclusion originated in permitting farmers and crop buyers to lock in a price without being subject to a legislative scheme intended to curb "excessive speculation and price manipulations occurring on the grain *futures* markets,"[93] but not the grain markets themselves.[94] The forward exclusion applies not to price speculators, but to parties for whom the commodity has "inherent value;" that is, to those that actually use the underlying commodity for commercial purposes.[95]

However, the distinction between a futures and a forward is not defined by statute or regulation and may be unclear. Accordingly, courts have adopted various approaches to determine whether parties are unlawfully using off-exchange futures contracts disguised as unregulated forwards.

Traditionally, the distinction between futures and forwards turns on an analysis of the totality of the circumstances surrounding the contracts in question. Under this approach, some of the main differences between futures and forwards are that forwards are non-standardized, do not trade on an exchange, and, perhaps most importantly, are intended by the parties to physically deliver the commodity as opposed to a cash settlement of the market versus contract price difference.[96] In the words of the CFTC, the "primary purpose of a forward contract is to transfer ownership of the

---

92.   CFTC v. Erskine, 513 F.3d 309, 3179 (6th Cir. 2008).

93.   CFTC v. Co Petro Marketing Group, Inc., 680 F.2d 573, 577-78 (9th Cir. 1982) (emphasis added).

94.   Erskine, 513 F.3d at 317 ("[T]he CEA was aimed at manipulation, speculation, and other abuses that could arise from the trading in futures contracts and options, as distinguished from the commodity itself.").

95.   *Id.* at 578 (noting that wheat has "inherent value" for farmers, operators of grain elevator storage companies, and flour millers).

96.   Forward contract, CFTC Glossary, U.S. COMMODITY FUTURES TRADING COMM'N EDUC. CTR., http://www.cftc.gov/consumerprotection/educationcenter/cftcglossary/ (last visited Mar. 27, 2014); *See also* CFTC v. Erskin, 512 F.3d 309 (6th Cir. 2008) (defining and distinguishing futures and forwards contracts); In re National Gas Distributors, 556 F.3d 247 (9th Cir. 2009); CFTC v. Hanover Trading Corp., 34 F. Supp. 2d 203 (S.D.N.Y. 1999) (contracts where no delivery was contemplated were futures).

commodity and not to transfer solely its price risk."[97] Transfer of ownership may include the transfer of intangible commodities, such as pollution rights, such that a contract that transfers the ownership of an intangible may qualify as a forward contract.[98]

In *CFTC v. Co Petro Marketing Group*, the court found that contracts marketed to the public for the purchase of fuel do not require physical delivery to be futures. The court explained that purchasers of such contracts were speculators without the intent or capacity for physical delivery.[99] Other factors the *Co Petro* court considered important in finding the contracts to be futures were their high degree of standardization, and that Co Petro acted like an exchange by promising to offset its customers' contracts and standing ready to liquidate the contracts and collect customer deposits.[100] In *In re Grain Land Cooperative*, the court found that a cancellation provision in a contract for a producer to deliver grain was the decisive factor in precluding the contract from being a forward.[101] It further held that the contracts in question were futures because they were used by producers to speculate, were never intended for physical delivery, and were standardized as to quantity, delivery, and fees.[102]

More recently, courts distinguishing between futures and forwards in the context of currencies have rejected the totality of the circumstances approach. Instead, they articulate the distinction as being that futures markets are for the sale of contracts independent of commodities while forward markets are for the sale of commodities.[103] In other words: a forward contract is a "*sale* for *deferred delivery*. A futures contract, by contrast, does not involve

---

97. 77 Fed. Reg. 48,227, 48,228 (Aug. 13, 2012), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2012-18003a.pdf.   For   the purposes of being excluded from the statutory definition of "swap," the CEA defines a forward contract as "any sale of a nonfinancial commodity or security for deferred shipment or delivery, so long as the transaction is intended to be physically settled." 7 U.S.C. § 1a(47)(B)(ii) (2014).

98. *Id.* at 48232-33. Accordingly, to the extent the CFTC considers bitcoins intangible because they are digital, that property should not preclude bitcoins from being recognized as physically deliverable pursuant to bona fide forward contracts.

99. CFTC v. Co Petro Marketing Group, Inc., 680 F.2d 573, 578-79 (9th Cir. 1982).

100. *Id.* at 579-81.

101. In re Grain Land Cooperative, 978 F. Supp. 1267, 1273-74 (D. Minn. 1997).

102. *Id.*

103. CFTC v. Zelener, 373 F.3d 861, 865-66 (7th Cir. 2004); CFTC v. Giovanni Fleury, et al., No. 10-15041 (11th Cir. Jun. 27, 2012).

a sale *of the commodity* at all. It involves a sale *of the contract.*"[104] In *CFTC v. Zelener*, the court held that contracts that permitted buyers to purchase currency on a deferred basis were forwards and not futures because the contracts were not fungible (each customer purchased a unique amount and had unique settlement dates) and hence there was no trading of the contracts.[105] The contracts were found to be forwards despite the fact that they permitted customers to obtain the economically equivalent position as a futures contract by continually extending their contracts and postponing delivery of the currency.[106] *Zelener* also identified two essential characteristics of futures (as opposed to forwards) markets: the existence of a centralized (intermediary) clearinghouse that takes on counterparty risk, and the ability to exit a position by purchasing an offsetting contract from a dealer.[107]

Yet another approach to distinguishing between futures and forwards was put forward by the Sixth Circuit Court of Appeals.[108] The court in *CFTC v. Erskine* stated that "a futures contract is a contract for a future transaction, while a forward contract is a contract for a present transaction with future delivery."[109] The court argued its approach was superior to the traditional totality of the circumstances test and the *Zelener* approach because it applies to intangible commodities such as prices as well as physical commodities.[110] *Erskine* specifically defined each type of contract with a six-element set of characteristics. Applying those definitions to the contracts at issue, *Erskine* found that contracts to buy or sell foreign currencies were forwards because they were not fungible,

---

104. *Zelener*, 373 F.3d at 865 (emphasis in original).

105. *Id.* at 867. *Zelener's* classification of the contracts as forwards has not been disturbed by subsequent amendments to the CEA that expanded the CFTC's authority over retail forex transactions. *See* Secure Leverage Grp., Inc. v. Bodenstein (In re Peregrine Fin. Grp., Inc.), 510 B.R. 190, 196 (Bankr. N.D. Ill. 2014) ("Congress did not reject the holding in *Zelener* that retail forex transactions are spot contracts.").

106. *Id.* at 866-867. Pursuant to the Dodd-Frank Act, on December 2, 2011 the CFTC clarified the meaning of "actual delivery" solely for the purposes of retail commodity transactions. See Retail Commodity Transactions Under Commodity Exchange Act, 78 Fed. Reg. 52,426, Aug. 23, 2013, http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2013-20617a.pdf.

107. *Id.* at 864-868. Indeed, the definition of "commodity contract" does not include uncleared commodity transactions. *See* 7 U.S.C. § 2(c)(2)(D)(iii) (2014); 11 U.S.C. § 761(4)(F)(ii) (2014).

108. CFTC v. Erskine, 513 F.3d 309, 322-23 (6th Cir. 2008).

109. *Id.* at 322.

110. *Id.* at 321.

not traded on an exchange, did not have set unit sizes or require a particular currency, and did not have a set price or settlement date.[111] The *Erskine* court found the contracts to be forwards despite them being cash settled (no physical delivery) and permitting continuous roll over (or offsets).[112] Indeed, both of these latter two approaches to the futures/forward distinction reject the relevancy of whether the contract intends or results in physical delivery of the commodity.[113]

Just like other commodities, certain types of contracts will qualify as Bitcoin forwards, and not Bitcoin futures, and hence will not be subject to the full scope of regulation under the CEA. Depending on which of the foregoing approaches a court applies, Bitcoin derivatives are more likely to qualify as forwards to the extent such contracts involve physical delivery or are non-fungible and not independently traded.

3. Swaps

A third type of potential Bitcoin derivative is a Bitcoin swap. A swap is a contract in which each counterparty agrees to an exchange of payments related to the value or return of some underlying asset or event.[114] The structure of Bitcoin swaps may resemble a foreign exchange (FX) swap. In an FX swap, two parties borrow a foreign currency from each other and agree to pay each other back at a specified exchange rate.[115] FX swaps are used to hedge against or speculate on foreign-exchange (rate) risk. Another type of Bitcoin swap could be cash-settled and not entail the parties actually trading bitcoins and a legal currency. Tera Group, Inc., is reportedly arranging such a Bitcoin swap.[116] It would entail the parties to the swap agreeing to exchange the cash equivalent value of Bitcoin and the dollar at a future point in time. A merchant accepting Bitcoin would be able to use the swap to protect itself against a price decrease by being promised to be paid cash if the value of Bitcoin drops relative to the dollar. Trading a swap that

---

111. *Id.* at 325-26.

112. *Id.* at 322.

113. CFTC v. Zelener, 373 F.3d 861, 865 (7th Cir. 2004); *Erskine*, 513 F.3d at 322.

114. Hull, *supra* note 67, at 149.

115. 7 U.S.C. § 1a(25) (2014).

116. Katy Burne, *New Derivative Guards Against Bitcoin's Price Swings*, MONEYBEAT: WALL ST. J. (Mar. 24, 2014, 11:47 AM), http://blogs.wsj.com/moneybeat/2014/03/24/new-derivative-guards-against-bitcoins-price-swings/.

references an index of virtual currencies could be another way to hedge Bitcoin price risk.

The Securities and Exchange Commission (SEC) has exclusive jurisdiction over swaps based on securities and narrow-based indices. The CFTC has exclusive jurisdiction over most other types of swaps, including those based on commodities, currencies, and interest rates.[117] Swaps must be cleared by a regulated central counterparty clearinghouse[118] and be traded on either a designated contract market or a swaps execution facility (SEF), unless no such trading venue makes the swap available for trading.[119] The CEA defines an SEF as "a trading system or platform in which multiple participants have the ability to execute or trade swaps by accepting bids and offers made by multiple participants."[120] SEFs must comply with 15 core principles and regulatory requirements including executing trades through an order book or a request for quote system involving three or more participants.[121] In contrast to multi-dealer SEF platforms, single-dealer trading platforms are not required to register and be regulated as a SEF or a designated

---

117. Further Definition of "Swap," "Security-Based Swap," and "Security-Based Swap Agreement"; Mixed Swaps; Security-Based Swap Agreement Recordkeeping, 77 Fed. Reg. 48,208 (Aug. 13, 2012). Under the CEA, forward contracts (for nonfinancial commodities) are excluded from the definition of "swap." CEA § 1a(47)(B)(ii) (2014), 7 U.S.C. § 1a(47)(B)(ii) (2014) (excluding from the definition of swap "any sale of a nonfinancial commodity or security for deferred shipment or delivery, so long as the transaction is intended to be physically settled").

118. CEA § 2(h)(1)(A) (2014). The CFTC, either upon application by a clearinghouse or on its own initiative, may require a category of swaps to be cleared. CEA § 2(h)(2) (2014).

119. CEA § 2(h)(8) (2014). *See also* Core Principles and Other Requirements for Swap Execution Facilities, 78 Fed. Reg. 33,476 (June 4, 2013), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2013-12242a.pdf. The process of making a swap available to trade is subject to regulation. *See* CFTC, Process for a Designated Contract Market or Swap Execution Facility To Make a Swap Available to Trade, Swap Transaction Compliance and Implementation Schedule, and Trade Execution Requirement Under the Commodity Exchange Act, 78 Fed. Reg. 33606 (June 4, 2013), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2013-12250a.pdf.

120. CEA § 1a(50) (2014), 7 U.S.C. § 1a(50) (2014).

121. Core Principles and Other Requirements for Swap Execution Facilities, 78 Fed. Reg. 33,476, (June 4, 2013) http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2013-12242a.pdf.

contract market.[122] In a single-dealer platform, only one market participant is able to trade with other traders.

Swaps contracts are not available to retail investors; parties to a swaps contract must be eligible contract participants.[123] In practice, parties to a swaps contract typically enter a trade with a futures commission merchant who in turn transacts with a clearinghouse.

The two major categories of regulated entities are swaps dealers that make markets in swaps, and major swaps participants, so defined because their swaps exposures are deemed to pose a systemic risk.[124] These entities are required to register with the CFTC and are subject to a wide range of disclosure, reporting, capital, clearinghouse margin, and business conduct requirements.[125] Non-financial, commercial end-users of swaps are not subject to entity-level regulation or the mandatory clearing and trading requirement so long as they only use swaps to hedge commercial risk.[126] For example, an airline may use swaps to hedge their exposure to increases in fuel prices without being subject to the regulations. Nonetheless, all users of swaps are prohibited from engaging in fraud or manipulative behavior.[127]

As of March 2014, the CFTC has applied the clearing requirement to standard interest rate swaps and certain index credit default swaps.[128] This determination was based on what swaps were

122. Technical Comm, Int'l Org. of Securities Comm'n, REPORT ON TRADING OF OTC DERIVATIVES 29-33 (2011), *available at* http://awareness.sca.ae/Arabic/IntReports/Report_2011_02_02.pdf.

123. CEA § 2(e) (2014).

124. Further Definition of "Swap Dealer," "Security-Based Swap Dealer," "Major Swap Participant," "Major Security-Based Swap Participant," and "Eligible Contract Participant;" Final Rules, 77 Fed. Reg. 30,596 (May 23, 2012).

125. 76 Fed. Reg. 43,851 (July 22, 2011) (large trader reporting).

126. CEA § 2(h)(7)(A) (2014), CFTC Rule 50.50. See also 77 Fed. Reg. 42,560, 42,590 (July 19, 2012). End-users must comply with certain reporting requirements. *Id.*

126. Melissa Jurgens, *Clearing Exemption for Swaps Between Certain Affiliated Entities*, COMMODITY FUTURES TRADING COMM'N, 17 CFR Part 50, RIN 3038-AD47 (Apr. 1, 2013), *available at* http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/federalregister040113.pdf.

127. CFTC Regulations § 180.1-180.2; (2014); see also 76 Fed. Reg. 41,398 (July 14, 2011).

128. Sauntia S. Warfield, *Clearing Requirement Determination Under Section 2(h) of the CEA*, COMMODITY FUTURES TRADING COMM'N, 17 CFR Parts 39 and 50, RIN 3038-AD86 (Nov. 29, 2012), *available at* http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/federalregister112812.pdf.

actually being cleared by clearing organizations.[129] In addition, the Treasury Department, pursuant to its legislative authority,[130] exempted certain physically settled foreign exchange swaps and forwards from the clearing and trading mandate.[131] This is because the physical settlement risk associated with the contracts is well managed and they are short-dated such that compliance with the mandate would not reduce systemic risk.[132] It is not clear what swaps the CFTC will determine qualify for an exemption or will be subject to the mandatory clearing requirement in the future. Not all swaps can be cleared and traded in a practical or economic sense. Among other characteristics, swaps that are capable of being cleared and traded must possess a sufficient degree of standardization and trading volume.[133] Nonetheless, uncleared swaps are still subject to mandatory margin, reporting, and margin segregation requirements.[134]

Given the relatively recent adoption of Bitcoin and the alternatives to swaps as a volatility reduction device (e.g., forwards), Bitcoin swaps are not likely to be subject to the mandatory clearing requirement due to a lack of sufficient trading volume. Nonetheless, they would still be subject to the margin and other requirements for uncleared swaps. The Tera Group swap, described above, fits categorization as an uncleared swap. Tera is reportedly also seeking regulatory approval for swaps that trade on its regulated swaps execution facility, TeraExchange.[135] In addition, to the extent that Bitcoin swaps are structured and are recognized as foreign exchange swaps, they may also be exempted from mandatory clearing and

---

129. *Id.* at 13.

130. CEA § 1a(47)(E) (2014).

131. 77 Fed. Reg. 69,694 (Nov. 20, 2012). Non-deliverable foreign exchange forwards were not exempted by the Treasury Department, and therefore are subject to the clearing mandate unless the CFTC provides an exemption.

132. *Id.*

133. Technical Comm, Int'l Org. of Sec. Comm'n, REPORT ON TRADING OF OTC DERIVATIVES 22-29 (2011), *available at* http://awareness.sca.ae/Arabic/IntReports/Report_2011_02_02.pdf.

134. Margin Requirements for Uncleared Swaps for Swap Dealers and Major Swap Participants, 76 Fed. Reg. 23,732 (proposed Apr. 28, 2011), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2013-26479a.pdf; Protection of Collateral of Counterparties to Uncleared Swaps; Treatment of Securities in a Portfolio Margining Account in a Commodity Broker Bankruptcy, 78 Fed. Reg. 66621 (Nov. 6, 2013), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2013-26479a.pdf.

135. Nermin Hajdarbegovic, *Tera Group Hopes to Offer First Bitcoin Swap*, COINBASE (Mar. 25, 2014), http://www.coindesk.com/tera-group-hopes-offer-first-bitcoin-swap/.

trading.[136] Alternatively, to the extent a Bitcoin derivatives contract is structured and recognized as a contract involving a nonfinancial commodity intended for physical delivery, it will be deemed a forward contract and will hence be excluded from any aspect of swaps regulation.[137]

Merchants that accept Bitcoin are likely to fall under the commercial end-user exception to mandatory clearing and trading. This is because merchants would be entering into the swap to hedge the commercial risk associated with accepting Bitcoin as a method of payment. In principle, the use of Bitcoin swaps for this purpose is no different than a merchant using FX swaps to hedge foreign currency exchange-rate risk when it sells overseas—a well-recognized category of exempt commercial end-user.[138]

4. Options

Option contracts are a fourth type of possible Bitcoin derivative. A call option gives the purchaser the right to purchase an asset at a pre-specified price and only has value if that price is below the market price. A put option works the opposite way.[139] A call option would enable a merchant selling Bitcoin denominated goods to be protected if the price increases. A Bitcoin put option would protect against Bitcoin price declines by guaranteeing the option to sell at a pre-specified price.

Options on commodities fall within the definition of "swap" under the CEA.[140] Accordingly, options are generally regulated as

---

136. There may be some ambiguity as to whether the intent to or actual exchange of physical currencies is required to qualify as an exempt FX swap or forward. *See* Andrew Kross, *Foreign Exchange Forwards (a/k/a "Currency" or "FX" Forwards) as Swaps: The Half-Time Report (Mutual Funds, Hedge Funds, ETFs and Fund Advisers)*, THE SWAP REPORT (Aug. 7, 2012), http://www.theswapreport.com/2012/08/articles/dodd-frank-reforms-1/foreign-exchange-forwards-aka-currency-or-fx-forwards-as-swaps-the-halftime-report-mutual-funds-hedge-funds-etfs-and-fund-advisers-this-is-important/.

137. 7 U.S.C. § 1a(47)(B)(ii) (1936).

138. *See* 17 C.F.R. 50.50(c)(i)(F) (2013) (recognizing that "a swap is used to hedge or mitigate commercial risk if" such swap reduces "risks in the conduct and management of a commercial enterprise" from "[a]ny fluctuation in interest, currency, or foreign exchange rate exposures arising from a person's current or anticipated assets or liabilities").

139. Hull, *supra* note 67, at 6.

140. CEA Section 1a(47)(A)(i), 7 U.S.C. 1a(47)(A)(i) (1936). The definition of "swap" excludes options on futures (which must be traded on a designated contract market). CEA section 1a(47)(B)(i), 7 U.S.C. 1a(47)(B)(i) (1936). Options on securities are regulated by the securities laws.

swaps.[141] However, just as CFTC regulation may not reach forwards based largely on their physical delivery of commodities, options that entail physical delivery are exempt from CFTC regulation, but only if they are traded between entities that include financially sophisticated parties and commercial users.[142]

Accordingly, Bitcoin options used by qualifying entities may be exempt from CFTC regulation if they are structured to involve physical delivery. This means that, as between a merchant and another sophisticated party, the Bitcoin options being offered on Derivabit,[143] a risk management platform that connects buyers and sellers of standardized Bitcoin options and futures contracts, would not be regulated as swaps because they are structured to result in physical delivery of bitcoins if exercised by the option holder.[144] Ordinary individuals would be prohibited from using Derivabit, however, unless it registered and complied with the rules of a regulated trading venue open to retail investors (e.g., a futures exchange). This is because in the hands of ordinary investors the Bitcoin options would be viewed as swaps. However, swaps are not permitted to be offered to such investors because they do not qualify as eligible contract participants.

B. Bitcoin Securities

At the other end of the spectrum from those looking to hedge against Bitcoin's volatility are those who want to speculate in the currency. Some commentators argue that in some respects buying bitcoins is very much like buying shares in a financial services

---

141. *Commodity Options,* 77 Fed. Reg. 25,320, 25,325 (Apr. 27, 2012), ("commodity options will be permitted to transact subject to the same rules applicable to any other swap"), 17 C.F.R. Parts 3, 32, and 33, 77 F.R. 82 (Apr. 27, 2012), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2012-9888a.pdf. *See also* Commodity Options, Final Rule and Interim Final Rule, 77 Fed. Reg. 25,320 (CFTC Apr. 27 2012) (regulating commodity options dealers).

142. *Commodity Options,* 77 Fed. Reg. at 25,326, http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2012-9888a.pdf. These exempt "trade options" are still subject to CFTC rules regarding recordkeeping, reporting, anti-fraud, and anti-manipulation. *Id.* at 25,326-25,328. Other exempt commodity options include those embedded in forward contracts. *See CFTC Division of Market Oversight Responds to Frequently Asked Questions Regarding Commodity Options* (Sept. 30, 2012), https://forms.cftc.gov/_layouts/TradeOptions/Docs/TradeOptionsFAQ.pdf.

143. DERIVABIT GUIDE, https://derivabit.com/guide.

144. *Id.* (stating that "underlying [Bitcoin] is fully available if the call option holder chooses to exercise the option").

startup.[145] If Bitcoin succeeds as an innovative and low-cost payments system, then there will be much greater demand for bitcoins, thus driving up the price. Chris Dixon, a partner at Andreessen Horowitz, has suggested that bitcoins could someday be worth $100,000 each.[146] A research note from Bank of America reached a more conservative price target of $1,300 by assuming that Bitcoin takes a 10 percent share of money transfers and e-commerce transactions.[147] Another prospectus suggests that if Bitcoin were to reach the scale of PayPal, which has been recently valued at $22.8 billion, then that implies a valuation per bitcoin of $1,949.[148]

To date, investing in Bitcoin has generally meant buying and holding bitcoins, but for several reasons this is not ideal for investors. First, acquiring bitcoins in large quantities at this early stage of the currency's development can be technically daunting. Almost all bitcoin exchanges are located outside the U.S. and are largely unregulated, which introduces unnecessary counterparty risk. Second, much like gold, securely storing bitcoins can be a laborious affair with little room for error.[149] Standard practice is to make several backup copies of the private keys that control the bitcoins and then storing the hard drives containing them in safety deposit boxes in different jurisdictions around the world.[150] As a result, entrepreneurs have begun to develop instruments that allow investors to more easily gain economic exposure to bitcoins.

1. Bitcoin Funds

SecondMarket, a registered broker-dealer that specializes in the trade of private Silicon Valley startup shares, has developed the

145. Joe Weisenthal, *Why Bitcoin Has Value,* BUSINESS INSIDER (Dec. 30, 2013, 12:04 PM), http://www.businessinsider.com/why-bitcoin-has-value-2013-12; Stan Larimer, *Bitcoin and the Three Laws of Robotics,* LET'S TALK BITCOIN! (2013), https://letstalkbitcoin.com/bitcoin-and-the-three-laws-of-robotics/.

146. Robert McMillan, *Silicon Valley VC Thinks a Single Bitcoin Will Be Worth $100,000,* WIRED MAG. (Jan. 15, 2014), http://www.wired.com/2014/01/chrisdixon/.

147. David Woo, Ian Gordon & Vadim Iaralov, *Bitcoin: A First Assessment,* BANK OF AMER. (Dec. 5, 2013), https://ciphrex.com/archive/bofa-bitcoin.pdf.

148. *Bitcoin Investment Trust Investor Presentation,* Feb. 2014, Page 6, http://www.bitcointrust.co/#Deck.

149. Quentin Fottrell, *To secure your bitcoins, print them out,* WALL ST. J. MARKETWATCH (Feb. 26, 2014), http://www.marketwatch.com/story/to-secure-your-bitcoins-print-them-out-2014-02-26.

150. Noel Randewich and Julie Gordon, *Bitcoin owners find safe place for digital currency: on paper,* REUTERS (Feb. 27, 2014), http://www.reuters.com/article/2014/02/28/us-bitcoin-mattress-idUSBREA1R00P20140228.

Bitcoin Investment Trust (BIT), which it described as "a private, open-ended trust that is invested exclusively in bitcoin and derives its value solely from the price of bitcoin."[151] According to its investor presentation, it is modeled on the SPDR Gold exchange-traded fund (ETF), but is a private fund open only to accredited investors.[152] The fund was seeded with a $2 million investment by SecondMarket.[153] Meanwhile, Winklevoss Capital is seeking regulatory approval for an exchange traded fund to invest in bitcoins.[154] Such an ETF would be open to any investor seeking exposure to bitcoins and would also have advantages relative to trading bitcoins directly.[155] It could also benefit Bitcoin by making price discovery much more efficient and transparent.[156]

The Winklevoss Bitcoin ETF is structured as a New York common law trust.[157] The trust expects to sell shares to the public in reference to the price of bitcoins represented by each share and the market price of the shares.[158] The trust is passively managed, directly holds bitcoins, and may issue shares in exchange for a deposit of bitcoins or redeem investors' shares with bitcoins.[159] The trust's aim is for its shares to achieve a weighted average price of bitcoins minus fees.[160] Its public disclosure document states that the shares of the

---

151. Simon Foxman, *Once again the Winklevoss twins get beaten launching their big idea: a bitcoin trust*, QUARTZ (Sept. 26, 2013), http://qz.com/128442/once-again-the-winklevoss-twins-get-beaten-to-launching-their-big-idea-a-bitcoin-trust/.

152. *Bitcoin Investment Trust Investor Presentation*, BITCOIN TRUST, Feb. 2014, http://www.bitcointrust.co/#Deck.

153. Emily Spaven, *SecondMarket launches Bitcoin Investment Trust, invests $2 million*, COINDESK (Sept. 26, 2013), http://www.coindesk.com/secondmarket-launches-bitcoin-investment-trust-invests-2-million/.

154. Registration Statement for the Winklevoss Bitcoin Trust, Amendment No. 1 to Form S-1 Registration Statement, U.S. Securities and Exchange Commission, Registration No. 333-189752 (Oct. 8, 2013), http://www.sec.gov/Archives/edgar/data/1579346/000119312513393903/d562329ds1a.htm; Christopher Condon, *Winklevosses' Lawyer in Talks with SEC Over Bitcoin ETF*, BLOOMBERG (Feb. 2, 2014), http://www.bloomberg.com/news/2014-01-30/winklevosses-lawyer-in-talks-with-sec-over-bitcoin-etf.html.

155. Yulia Chernova, *Winklevoss Twins Face Competition From SecondMarket's New Bitcoin Trust*, WALL ST. J. VENTURE CAPITAL BLOG, Sept. 25, 2013, http://blogs.wsj.com/venturecapital/2013/09/25/winklevoss-twins-face-competition-from-secondmarkets-new-bitcoin-trust/.

156. *Id.*

157. Registration Statement for the Winklevoss Bitcoin Trust, Form S-1 Registration Statement, U.S. Securities and Exchange Commission, Registration No. 333-[] (Jul. 1 2013), S-1, at 1, http://www.sec.gov/Archives/edgar/data/1579346/000119312513279830/d562329ds1.htm.

158. *Id.* at 1.

159. *Id.*

160. *Id.*

trust "are designed for investors seeking a cost-effective and convenient means to gain exposure to Bitcoins with minimal credit risk."[161]

Trusts are governed at the state level primarily by trust statutes and common law. Because trusts that invest in Bitcoin raise funds by issuing securities, they are also governed by state and federal securities laws. As an issuer of securities, a Bitcoin trust is subject to the registration and disclosure obligations of the Securities Act. If the securities are publicly issued, the trust must file a publicly available registration statement containing a prospectus that states basic information about the trust and its investments and also audited financial statements.[162]

An issuer can avoid the registration requirement by issuing the securities privately. To qualify for a private offering, a trust may satisfy any one of the private offering exemptions provided by the Securities Act. A common exemption is provided by Rule 506 of Regulation D, which requires the issuer to limit their investor base almost exclusively to wealthy, "accredited" investors.[163] Although an offering pursuant to Rule 506 does not require the issuer to file a registration statement, to minimize liability and satisfy investor demand, a private issuer will nonetheless disclose to investors information of the type required to be in a registration statement.

Regardless of whether a trust issues its securities to the public or privately to sophisticated investors, the trust is subject to Section 17(a) of the Securities Act, which makes it unlawful for any issuer to make an untrue statement of material fact or to omit any fact so as to make a statement misleading.[164] Under Section 10(b) and Rule 10b-5 of the Exchange Act, material omissions in connection with the sale of any security are likewise prohibited.[165]

---

161. *Id.* at 2. For other purported benefits of the ETF see *infra* II.C.

162. 15 U.S.C. § 77e (1954) (prohibiting the sale of securities without filing a registration statement); 15 U.S.C. § 77aa (listing schedule of information required in a registration statement); Regulation C, 17 C.F.R. §§ 230.400 to 230.494 (2007) (stating general requirements regarding preparation and filing of the registration statement); 15 U.S.C. § 77j (1954) (information required in prospectus); Regulation S-K, 17 C.F.R. Part 229 (2007) (stating requirements applicable to the content of the non-financial statement portions of registration statements).

163. Rule 506 of Regulation D, 17 C.F.R. § 230.506 (2007). Accredited investors include institutions with at least $5,000,000 in assets and natural persons whose net worth (or whose joint net worth with a spouse) exceeds $1,000,000 or that have an annual income for the last two years of at least $200,000 (or $300,000 in joint spousal income). 17 C.F.R. § 230.501(a) (2007).

164. 15 U.S.C. § 77q(a) (1933).

165. 15 U.S.C. § 78j (2009); Rule 10b-5, 17 C.F.R. § 240.10b-5 (1948).

ETFs are typically structured as unit investment trusts or open-end investment companies with shares that are listed and traded on exchanges that are open to both retail and institutional investors.[166] Like public company stock, ETF shares are usually traded through a broker.[167] ETFs invest in, or track, the performance of a wide variety of securities, commodities, and indices, and may be actively or passively managed. The potential benefits of ETFs to investors include gaining access to a wide range of investments and sectors through a liquid instrument with low fees.[168] ETFs have grown spectacularly in the past decade and by year-end 2012 managed $1.3 trillion in assets.[169] ETF shares trade at the market price and not at the fund's net asset value.

ETF shares are securities that must be registered under the Securities Act and, because their shares are exchange-traded, ETFs must also comply with the listing requirements of the Securities and Exchange Act of 1940.[170] ETFs are also typically regulated under the Investment Company Act of 1940 because they invest in securities. To be eligible for offering and trading, an ETF must obtain relief from several prohibitions of the Investment Company Act and its regulations.[171] Among other effects, obtaining such relief allows an ETF to trade creation units with authorized participants,

---

166. ETFs must also meet exchange listing requirements and can typically do so without the exchange being required to obtain SEC approval. Exchange Act Rule 19b-4(e) (1934) (permitting shares that meet generic exchange listing requirements to be listed without SEC approval). Unique ETFs may require an exchange filing a listing rule for SEC approval.

167. ETFs also sell creation units to authorized participants.

168. INVESTMENT COMPANY INSTITUTE, INVESTMENT COMPANY FACT BOOK (53rd ed. 2013), ch. 3, http://www.icifactbook.org/fb_ch3.html.

169. *Id.*

170. 15 U.S.C. 78a (1934). When it comes to filing a registration statement disclosure, ETFs registered under the Investment Company Act must comply with Form N-1A and ETFs registered under the Securities Act must comply with Form S-1.

171. Investment Company Act §§ 2(a)(32), 5(a)(1) (1940) (requiring shares of an open-end fund to be redeemable daily); 22(d), 22c-1 (1934) (requiring issuers to sell redeemable securities only at the current offering price, and to redeem only at the current NAV); 22(e) (1934) (prohibiting a fund from suspending the right of redemption, or postponing the date of satisfaction of redemption requests for more than seven days); 17(a)(1), 17(a)(2) (1934) (prohibiting affiliated persons, principal underwriters or promoters of a fund (or affiliated persons of such persons) from selling a security or other property to, or purchasing a security or other property from, a fund); 12(d)(1) (1934) (limiting amount of shares that a registered investment company may hold of another registered investment company, and the amount of shares that one investment company may sell to another as an investment).

have its shares traded on an exchange at market prices, delay payment from share redemptions beyond seven days in some circumstances, and purchase shares in other ETFs.

Unlike other investment companies, actively managed ETFs are permitted to engage in derivatives transactions, but the transactions must be subject to board approval and must be disclosed in a manner consistent with SEC guidance.[172] An ETF investing in futures must be registered under the CEA as a commodity pool required to comply with CFTC disclosure requirements.[173] Shares of the Winklevoss Bitcoin ETF are registered under the Securities Act but will not be effective until the SEC provides final approval.[174] However, because bitcoins are not regulated as commodity futures or securities, the Winklevoss Bitcoin ETF is not registered under the Investment Company Act[175] and is not a commodity pool under the CEA.[176]

For managers of funds that invest in Bitcoin ETFs or Bitcoin trusts, the Investment Advisers Act of 1940[177] (Advisers Act) and SEC regulation apply. All U.S.-based managers of funds that invest in securities must register under the Advisers Act, unless they fall within an exemption, such as advising funds with less than $150 million in assets under management or qualifying as a foreign private adviser.[178] Investment advisers are subject to the provisions of the Advisers Act prohibiting advisers from making any material misstatements, misleading omissions, and other fraudulent

---

172. Elizabeth G. Osterman, *Moratorium Lift*, SECURITIES AND EXCH. COMM'N OFFICE OF INV. CO. REG. (Dec. 6, 2012), http://www.sec.gov/divisions/investment/noaction/2012/moratorium-lift-120612-etf.pdf.

173. ETFs that invest in commodity futures are not required to register with the CFTC as a commodity pool operator if they are registered with the SEC as an Investment Company. CFTC Regulation 4.5(a)(1), http://www.cftc.gov/IndustryOversight/Intermediaries/CPOs/cpoctaexemptionsexclusions.

174. Daniel Cawrey, Winklevoss Twins Plan NASDAQ Listing for Bitcoin ETF in New SEC Filing, COINDESK (May 9, 2014), http://www.coindesk.com/winklevoss-twins-plan-nasdaq-listing-for-bitcoin-etf-in-new-sec-filing/.

175. Investment Company Act §§ 2(a)(32) (Approved Jan. 3, 2012).

176. Registration Statement for the Winklevoss Bitcoin Trust, Form S-1 Registration Statement, U.S. Securities and Exchange Commission, Registration No. 333-[] (July 1 2013), S-1, at 22-23 and 27, http://www.sec.gov/Archives/edgar/data/1579346/000119312513279830/d562329ds1.htm.

177. 15 U.S.C. § 80b-1 et seq. (2010).

178. Advisers Act §§ 80b-3(b), 80b-3(l), 80b-3(m); Exemptions for Advisers to Venture Capital Funds, Private Fund Advisers with Less Than $150 Million in Assets Under Management, and Foreign Private Advisers, Investment Advisers Act Release No. 3111, 75 Fed. Reg. 77,190 (Nov. 19, 2010).

statements to investors or prospective investors.[179] Such statements include those regarding investment strategies, experience and credentials, risks associated with the fund, or valuation of the fund's assets.[180]

The Advisers Act also requires registered managers to electronically file and keep current Form ADV with the SEC.[181] Part 1 of Form ADV requires managers to disclose basic information relating to the firm and its business, so as to assist regulators with oversight. Part 2 of Form ADV requires a manager to disclose information relating to potential conflicts of interest and other issues, including fees and how they are calculated, client referrals, disciplinary history, and the manager's supervision of personnel. The Advisers Act also requires fund managers to keep specific business and accounting records, to protect any client assets over which the fund has legal custody, and ensure that their own personnel comply with federal securities law and regulation.[182] Rule 206(4)-7 of the Advisers Act requires fund managers to establish a compliance program that includes written policies and procedures and a designated chief compliance officer.[183]

2. Bitcoin Margin Trading

Related to securities, there have also been attempts to create platforms that allow bitcoin margin trading. One of the earliest such platforms was Bitcoinica, which offered contract-for-difference trading against the Bitcoin/USD exchange rate starting in September of 2011.[184] Similar to forex trading, Bitcoinica allowed customers to short sell within a chosen leverage range.[185] For example, if a trader wanted to bet against Bitcoin, he could essentially borrow bitcoins from Bitcoinica (in actuality, from another trader who wished to go long for whom Bitcoinica was the ultimate counterparty) and sell

---

179. 17 C.F.R. § 275.206(4)-(8) (2012).

180. Prohibition of Fraud by Advisers to Certain Pooled Investment Vehicles, 72 Fed. Reg. 44,756, 44,759 (Aug. 9, 2007) (to be codified at 17 C.F.R. pt. 275).

181. 17 C.F.R. §§ 275.203.1, 275.204-1 (2012).

182. SEC, STUDY ON INVESTMENT ADVISERS AND BROKER-DEALERS 32-34 (2011).

183. Compliance Programs of Investment Companies and Investment Advisers, Advisers Act Release No. 2204, Investment Company Act Release No. 26,299, 68 Fed. Reg. 74,714 (Dec. 24, 2003).

184. Jon Matonis, *Bitcoinica Registers in New Zealand for Bitcoin Margin Trading*, FORBES (Apr. 21, 2012), http://www.forbes.com/sites/jonmatonis/2012/04/21/bitcoinica-registers-in-new-zealand-for-bitcoin-margin-trading/.

185. *Id.*

them.[186] If Bitcoin's price were to drop, the short-seller could close out his position by buying back the borrowed bitcoins at a lower exchange rate and thereby profit by pocketing the difference. Bitcoinica made its profits by taking the spread between the traders it matched internally.[187]

Although Bitcoinica was registered as a financial services provider in New Zealand,[188] it was also representative of the ambitious-but-shoestring operations that dotted the early Bitcoin landscape. Founded by a 17-year-old computer programmer in Singapore, Zhou Tong, Bitcoinica valued expediency and experimentation over postponement and risk-aversion.[189] The response from the Bitcoin community was initially quite enthusiastic. According to Tong, Bitcoinica facilitated transactions of over 3,724 BTC within the first 24 hours of operation.[190] Despite persistent security issues,[191] Bitcoinica hosted an average monthly volume of roughly 1.2 million BTC at its peak.[192] Bitcoinica was not able to overcome the security and trust issues that plagued it, however, and it went offline in May 2012 after hackers stole a reported 18,000 BTC from the exchange.[193] The company entered into receivership in

---

186. This example was first outlined by a customer on the Bitcointalk forums and approved by Zhou Tong as an accurate explanation of Bitcoinica operations. Note that this example uses a 1:1 leverage spread for simplicity. Higher leverage spreads provide opportunities for broader spreads and higher profits. The explanation also includes a discussion of how short contracts worked on Bitcoinica. *See* Mushoz, *Bitcoinica: How It Works*, forum post, BITCOINTALK.ORG (Dec. 29, 2011), https://bitcointalk.org/index.php?topic=55970.msg665945#msg665945.

187. Jon Matonis, *Bitcoinica Registers in New Zealand for Bitcoin Margin Trading*, FORBES (Apr. 21, 2012), http://www.forbes.com/sites/jonmatonis/2012/04/21/bitcoinica-registers-in-new-zealand-for-bitcoin-margin-trading/.

188. *Id.*

189. Zhou Tong, *Show HN: Bitcoinica – Advanced Bitcoin Trading Platform*, HACKERNEWS (Sept. 8, 2011), https://news.ycombinator.com/item?id=2973313.

190. Zhou Tong, *Bitcoinica – Advanced Bitcoin Trading Platform*, BITCOINTALK.ORG (Sept. 9, 2011, 3:49 PM), https://bitcointalk.org/index.php?topic=42267.msg517128 - msg517128.

191. Tim Worstall, *Another Theft at Bitcoinica*, FORBES MAG. (May 12, 2012), http://www.forbes.com/sites/timworstall/2012/05/15/another-bitcoin-theft-at-bitconia/.

192. Jon Matonis, *Bitcoinica Registers in New Zealand for Bitcoin Margin Trading*, FORBES (Apr. 21, 2012), http://www.forbes.com/sites/jonmatonis/2012/04/21/bitcoinica-registers-in-new-zealand-for-bitcoin-margin-trading/.

193. Zhou Tong, *Bitcoinica site is taken offline for security investigation*, BITCOINTALK.ORG (May 11, 2012, 1:16:am), https://bitcointalk.org/index.php?topic=81045.msg894277#msg894277.

August 2012 and was liquidated shortly thereafter.[194] Tong had by this point announced he was leaving the Bitcoin space for good.[195]

Today, new entrants are looking to offer similar platforms for margin trading. The leading contender is probably Coinsetter, a New York City-based startup that has generated much buzz after a successful $500,000 venture capital funding round in April of 2013.[196] The company later filed with the Securities and Exchange Commission plans to raise another $1.5 million in venture capital.[197] The Coinsetter platform today is only available to beta testers, and while its full feature set is available to customers outside the U.S., accounts for U.S. customers only accept Bitcoin deposits and withdrawals, but not bank transfers.[198] While still in limited use and early development, Coinsetter aims to provide a liquid, trusted, and compliant forex-like Bitcoin exchange to suit professional short-term traders. Another new entrant is Bitfinex, which emerged in late 2012 with a focus on security and is registered as a Hong Kong limited liability corporation.[199]

The Board of Governors of the Federal Reserve System (Federal Reserve) regulates the use of margin credit pursuant to its authority under Section 7(a) of the Securities and Exchange Act.[200] The Federal Reserve promulgated Regulation T under that authority to prevent investors from taking on too much credit when purchasing or holding securities.[201] Regulation T establishes

---

194. Justin Porter, *Tihan Seale Announces Bitcoinica Liquidation,* BITCOIN MAG. (Aug. 2, 2012), http://bitcoinmagazine.com/1872/tihan-seale-announces-bitcoinica-liquidation/.

195. Zhou Tong, *I'm Leaving Bitcoin,* BITCOINTALK.ORG (May 13, 2012, 1:02 PM), https://bitcointalk.org/index.php?topic=81581.msg897948#msg897948.

196. Rip Empson, *Coinsetter Lands $500K From SecondMarket Founder & Others to Help Bring Leverage, Shorting To Trade Bitcoin,* TECHCRUNCH (Apr. 9, 2013), http://techcrunch.com/2013/04/09/coinsetter-lands-500k-from-secondmarket-founder-others-to-help-bring-leverage-shorting-to-bitcoin-trade/.

197. Ari Levy, *Bitcoin Trading Exchange Coinsetter Files to Raise $1.5 Million,* BLOOMBERG (Dec. 27, 2013), http://www.bloomberg.com/news/2013-12-27/bitcoin-trading-exchange-coinsetter-files-to-raise-1-5-million.html.

198. *Learn More,* COINSETTER INFORMATION PAGE, https://www.coinsetter.com/beta (last visited Feb. 12, 2014).

199. Unclescrooge, *[OFFICIAL]Bitfinex.com first Bitcoin P2P lending platform for leverage trading,* BITCOINTALK.ORG (Jun. 8, 2013), https://bitcointalk.org/index.php?topic=229438.0; FAQ, BITFINEX.COM, https://www.bitfinex.com/pages/support (last visited Feb. 11, 2014).

200. 15 U.S.C. § 78g(a) (2011).

201. Regulation T "imposes, among other things, obligations, initial margin requirements, and payment rules on securities transactions." 12 C.F.R. 220.1(a) (2011).

minimum margin requirements,[202] but exchanges and other organizations may establish additional requirements.[203] Because bitcoins are not securities, bitcoin margin trading platforms seem to fall outside of the scope of the Securities Act and Regulation T. In addition, on February 27, 2014, Federal Reserve Chairwoman Janet Yellen stated that, "Bitcoin is a payment innovation that's taking place outside the banking industry. To the best of my knowledge there's no intersection at all, in any way, between Bitcoin and banks that the Federal Reserve has the ability to supervise and regulate. So the Fed doesn't have authority to supervise or regulate Bitcoin in any way,"[204] implying that it is unlikely that the Fed would assert authority over bitcoin margin trading that does not involve regulated banks without a legislative directive.

C.   *Bitcoin-Denominated Instruments & Gambling*

Separate and apart from derivatives and securities based on bitcoins are derivatives and securities *denominated* in bitcoins. It may be hard to believe, but today there are several unregulated exchanges actively trading commodity futures contracts and company shares denominated in bitcoins. These exchanges tend not to be registered with, nor actively regulated by, any government agency. There are also unregulated prediction markets operating today that denominate the price of event contracts in bitcoins. These exchanges all seem to be operating under the theory that, because they do not handle government-issued currencies, they are not subject to regulation.[205] Similarly, there are gambling sites online that denominate bets in bitcoins and suggest that gambling laws do not apply to them.[206]

---

202. 12 C.F.R. 220.12(a) (2011) (limiting extension of credit to 50 percent of a security's market value).

203. 12 C.F.R. 220.1(b)(2) (2011).

204. Sophie Knight & Takaya Yamaguchi, *Japan Says Any Bitcoin Regulation Should Be International,* REUTERS (Feb. 27, 2014), http://uk.reuters.com/article/2014/02/28/us-bitcoin-mtgox-idUKBREA1Q1YK20140228.

205. For instance, the BTC-TC FAQ page responds to the question, "Is it legal for me to use this site?" by stressing that "no assets on the site are to be considered real," and "the use of this site is for educational and entertainment purposes only." *See Why BTC-TC Rocks, FAQ,* BTC TRADING GROUP, https://btct.co/faq (last visited Mar. 26, 2014).

206. For instance, the Bitcoin poker website SealsWithClubs makes the argument that "[t]here's no bank account. There's no bank of any sort that we do. We only do this one weird brand-new Internet protocol transaction that some of the nerds out there are calling money." *See* Cyrus Farivar, *"Is Online Gambling*

In this section we will look at existing derivatives and securities being offered that are denominated in bitcoins. Similarly, we'll look at event contracts being offered that are denominated in bitcoins, as well as bitcoin gambling sites. We conclude that while their regulation lie in a gray area, they are generally subject to existing laws and regulation.

1. Bitcoin-Denominated Derivatives and Markets

As we have noted, current price volatility creates a strong demand for instruments that allow one to bet against the price of bitcoin. Most likely, such an instrument would take the form of a dollar/bitcoin currency swap, or a forward contract or option that could be bought or sold for dollars. Such instruments will likely be available soon, but not before their platform providers comply with regulatory requirements as outlined in Part II.A, *supra*. Impatient with a slow regulatory process, however, a wide array of startups—including ICBIT.se, MPEx, and BTC.sx—have begun to offer bitcoin derivatives that are bought and sold not for dollars or any other fiat currency, but for bitcoins.[207] Indeed, many early experiments in providing bitcoin-denominated derivatives markets have already launched, blossomed, and failed.[208]

Legal If Bitcoins, Not Dollars, Are At Stake?", NPR (Feb. 6, 2013), http://www.npr.org/blogs/alltechconsidered/2013/02/06/171182974/is-online-gambling-legal-if-bitcoins-not-dollars-are-at-stake.

207. One way to bet against the price of Bitcoin is to borrow bitcoins, sell them, and then later buy them back at a (hopefully) lower price. Services like Bitfinex offer this kind of margin trading. Simone Foxman, *How to Short Bitcoins (If You Really Must)*, QUARTZ (Apr. 2, 2013), *available at* http://qz.com/69630/how-to-short-bitcoins-if-you-really-must. Shorting the price of bitcoin in bitcoin-denominated contracts, however, is a bit counterintuitive. Essentially one buys an option to sell an amount of bitcoins at a set dollar price, but instead of taking dollars as settlement, one takes the bitcoin-equivalent of any gains. One problem, of course, is that if one believes that the price of a bitcoin will be zero in the future, then one will not be interested in such bitcoin-settled contracts. Stephen Gandel, *How to bet against the bitcoin megabubble*, FORTUNE (Dec. 5, 2013, 6:12 AM), *available at* http://finance.fortune.cnn.com/2013/12/05/betting-against-bitcoin-bubble.

208. This summary reviews some of the more successful (or infamous) forays into Bitcoin futures trading. A considerable amount of over the counter Bitcoin futures trading has also emerged in IRC chat rooms and TOR-Based connections. *See* Bitcoin-otc wiki, S.V. BEGINNER'S GUIDE, http://wiki.bitcoin-otc.com/wiki/Beginners_Guide (last visited Feb. 12, 2014).

One of the most prominent of the bitcoin-denominated futures markets is ICBIT.se, which launched in January of 2012.[209] In April of 2013, the company reported a customer base of roughly 5,000 registered users and around $50,000 in revenue per month.[210] Users do not purchase options or futures contracts from ICBIT itself but rather are matched with other buyers or sellers who have an opposite and corresponding risk profile.[211] ICBIT therefore merely acts as a facilitator, rather than a counterparty, of bitcoin-denominated financial instruments. This business model is different from traditional futures markets in which the exchange also performs the clearing function.[212] Customers are not given any information about the traders with whom they are matched and many in the Bitcoin community have speculated that ICBIT manipulates its central order book for the personal interest of a small group of insiders.[213]

MPEx is another longstanding Bitcoin-denominated derivatives market that has facilitated futures-like trading since 2011. MPEx has been dogged by rumors and complaints from disgruntled customers,[214] but others praise the exchange for its simple but elegant execution and long-term vision.[215] MPEx is considerably less user-friendly than other existing Bitcoin derivatives markets. Indeed, the creator intentionally designed the platform to weed out novice

---

209. Fireball, *ICBIT–New Exchange*, BITCOINTALK.ORG (Jan. 21, 2012, 11:45 AM), https://bitcointalk.org/index.php?topic=60548.msg705207 #msg705207.

210. Cyrus Farviar, *"Taming the Bubble": Investors Bet on Bitcoin via Derivatives Markets*, ARS TECHNICA (Apr. 11, 2013, 8:50 PM), http://arstechnica.com/business/2013/04/taming-the-bubble-investors-bet-on-bitcoin-via-derivatives-markets/.

211. The ICBIT.se website FAQ directs to a Bitcointalk. *See* Super T, **Unofficial* ICBIT (BTC Futures Trading) – Help & FAQ's*, BITCOINTALK.ORG (Apr. 1, 2013, 8:17 PM), https://bitcointalk.org/index.php?topic=164255.0.t.

212. In other words, in which the exchange itself moves assets among traders, as opposed to merely matching traders that exchange directly with each other.

213. Greg Mulhauser, *Bitcoin Derivatives, Liquidity and Counterparty Risk*, PSYCHOLOGICAL INVESTOR BLOG (May 29, 2013), http://psychologicalinvestor.com/lib/real-markets/bitcoin-derivatives-liquidity-counterparty-risk-134/.

214. The operator responds to these criticisms on his personal blog. *See* Mircea Popescu, *Because most people are idiots, in spite of never manning up and admitting to it*, TRILEMA BLOG (Feb. 5, 2013), http://trilema.com/2013/because-most-people-are-idiots-in-spite-of-never-manning-up-and-admitting-to-it/.

215. *A Review of MPEx, the Bitcoin Stock Exchange*, LOPER OS BLOG, http://www.loper-os.org/?p=1108 (last visited Feb. 11, 2014).

investors and foster a higher-caliber exchange community.[216] The website is sparse and users must interact with the service through an embedded command line terminal.[217] MPEx provides a stripped-down platform for buyers and sellers to discover each other and trade options. Customers pay a fee to register an MPEx account that is linked with the public keys of their Bitcoin wallets. Upon registration, buyers and sellers can then direct the program to withdraw money from their Bitcoin wallet into the MPEx exchange address from which they can then issue orders.[218] Similarly, users can deposit their MPEx earnings back into their personal Bitcoin wallets, send bitcoins to another MPEx account, execute call and put orders, buy on margin, and execute batch contracts.[219] MPEx does not appear to be incorporated or registered with any regulatory body, but on its FAQs it does provide several hypothetical escape plans in the event that a government confiscates exchange servers or otherwise incapacitates the website.[220]

There is also Singapore-based BTC.sx, which does not offer derivatives per se, but is rather a bitcoin-denominated margin trading platform. It was launched in private beta in April of 2013 and full operation in June of 2013.[221] Users can deposit bitcoins to a wallet created by BTC.sx and can then speculate on Bitcoin price movements by opening long or short positions for varying lengths of time.[222] For each open position taken, users must hold deposits equal to the size of the trade multiplied by the price and multiplied by a measure of current market volatility.[223] This allows the BTC.sx platform to leverage each position at 100 times the value of the bet, allowing investors a broader possible return on each investment.[224]

---

216. Mircea Popescu, *So what's the plan with MPOE/MPEx?*, TRILEMA BLOG (Feb. 3, 2013), http://trilema.com/2013/so-whats-the-plan-with-mpoempex/.

217. *English FAQ*, MPEX, http://mpex.co/faq.html (last visited Feb. 11, 2014).

218. *Id.*

219. *Id.* MPEx also allows stock offerings and dividend payments. This function is discussed in more depth in the section on stock markets.

220. *Id.*

221. Seal, *[ANN] BTC.sx – Leveraged trading made easy*, forum post, BITCOINTALK.ORG (Apr. 27, 2013), https://bitcointalk.org/index.php?topic=188735.msg1955964#msg1955964.

222. Danny Bradbury, *BTC.SX Revives Bitcoin Margin Trades*, COINDESK (May 23, 2013), http://www.coindesk.com/btc-sx-revives-bitcoin-margin-trades/.

223. FAQ, BTC.SX SUPPORT, https://btc.sx/about/faq (last visited Mar. 26, 2014).

224. For example, let's say a user wanted to bet 1/100th of a Bitcoin that the price of Bitcoin will increase over the next day. To take this position, the user must have the proper deposit amount in their BTC.sx wallet to cover the trade and function as a de facto guaranteed stop loss order. Let's say this deposit amount

BTC.sx has proven popular and relatively successful during its short year of operation. By November of 2013, BTC.sx surpassed $13.5 million in margin trading since May of 2013[225] and reported 2,000 registered users.[226] By January of 2014, BTC.sx reported $35 million in total trading since its launch and an active user base of 3,300 traders.[227]

As indicated by the analysis in Section II.A, these Bitcoin derivatives contracts and platforms likely do not fall under the scope of CFTC regulation. First, their contracts more closely resemble unregulated, off-exchange forwards and not regulated exchange-traded futures. This is primarily because the derivatives contracts are intended to be settled "physically" with bitcoins, and not their cash equivalent. ICBIT.se states its BTC/USD-4.14 contract is "Settled in BTC, quoted in USD"[228] and explains that for a party using their platform to short Bitcoin against the dollar, "if [the] rate goes down he would *get as many Bitcoins as it's needed* to buy $6000 on the spot market."[229] Likewise, the settlement term for MPEx's X.Eur contract contemplates physical delivery of bitcoins and not cash.[230] In other words, following the approaches taken in *Zelener* and *Erskine*, these platforms offer customers the ability to trade actual bitcoins, not contracts referencing Bitcoin. In addition, the Bitcoin derivatives platforms do not also serve as a clearinghouse for their

---

is 1.5 BTC in this example. The user communicates to BTC.sx that she wants to bet 0.01 BTC on this position and BTC.sx places 1 BTC, or 100 times the position, on this bet. If the user wins the bet, she will make a handsome profit because most of her earnings are based on BTC.sx's 1BTC bet rather than her 0.01 BTC bet. If, on the other hand, the user loses the bet, her losses will be liquidated from her 1.5 BTC deposit. This allows both BTC.sx and each user to minimize risk with guaranteed stop loss orders while increasing possible returns with margin trading. *See* Joe Lee, *Bitcoin Trading Platform BTC.sx Launches Private Beta: Offering Long and Short Leveraged Bitcoin Position Trading*, PRNEWSWIRE (May 15, 2013), http://www.prnewswire.com/news-releases/bitcoin-trading-platform-btcsx-launches-private-beta-offering-long-and-short-leveraged-bitcoin-position-trading-207556691.html.

225. Daniel Cawrey, *Bitcoin Derivatives Platform BTC.sx Surpasses $13.5m in Trades*, COINDESK (Nov. 25, 2013), http://www.coindesk.com/bitcoin-derivatives-platform-btc-sx-trades/.

226. *Id.*

227. George Samman, *The World's First Bitcoin Derivatives Platform Surpasses US$35M in Trades*, PRWEB (Jan. 21, 2014), http://www.prweb.com/releases/Bitcoin/Trading/prweb11494016.htm.

228. *See* BTC/USD-4.14, https://icbit.se/BUJ4 (last visited Nov. 14, 2014).

229. *About ICBIT Derivatives Market*, https://icbit.se/futures.

230. David devout Francois, *Listing Agreement #7*, MPEx (Dec. 15, 2013) http://mpex.co/?mpsic=X.EUR ("intends to market make an Euro based Bitcoin future with physical delivery for the foreseeable future").

customers' trades, which is an essential aspect of a futures exchange. Nonetheless, there is no bright line between forwards and futures. The contracts being offered by the platforms are highly standardized and are being offered as "futures," which weigh in favor of them being treated as regulated futures.

2. Bitcoin-Denominated Securities and Exchanges

In addition to online markets facilitating the trade of bitcoin-denominated derivatives, there are sites online that essentially serve as exchanges for shares of stock denominated in bitcoin. Unable or unwilling to make use of traditional capital markets, a small but growing number of entrepreneurs turn to these exchanges to raise capital and sell stock in their companies for bitcoins. The companies and funds listed on these exchanges tend to be Bitcoin-related businesses, such as mining equipment manufacturers, but also include Bitcoin-denominated gambling sites like Satoshi Dice[231] and BitBet.[232]

Bitcoin-denominated stock exchanges have been plagued by frequent scams in which the underlying company or concern is a hoax, and there has been seemingly little recourse for investors.[233] Nevertheless, these exchanges provide individuals with more options to fundraise small amounts of capital for interesting projects. They do not seem, however, to be in compliance with securities and exchange regulations.[234] As Bitcoin expands in popularity, it is possible that these stock markets will mature and flourish if supported by an appropriate legal framework.

The now defunct Global Bitcoin Stock Exchange (GLBSE) is one of the earliest known Bitcoin-denominated stock markets. Founded in the summer of 2011, its debut serendipitously coincided with an early burst of interest in the Bitcoin project.[235] The original

---

231. In March of 2014, the SEC opened an investigation into SatoshiDice and MPEx for possible violations of US securities law. *See* Jon Southurst, *SEC Making Inquiries Into MPEx, SatoshiDice,* COINDESK (Mar. 20, 2014), http://www.coindesk.com/sec-making-inquiries-mpex-satoshidice/.

232. Mircea Popescu, *How does one list on MPEx?,* TRILEMA (Oct. 3, 2012), http://trilema.com/2012/how-does-one-list-on-mpex/.

233. Olivia Solon, *Founder Reflects on the Closure of Bitcoin Stock Exchange GLBSE,* WIRED UK (Oct. 13, 2013), http://www.wired.co.uk/news/archive/2013-10/24/bitcoin-exchange-collapse-glbse.

234. Mircea Popescu, *Interacting with a fiat institution, a guide,* TRILEMA (Mar. 18, 2014), http://trilema.com/2014/interacting-with-fiat-institution-a-guide/.

235. "The Bitcoin project" refers to the use, application, and development of Bitcoin block chain technology since it was created in January of 2009. For frame of reference, GLBSE was founded at around the same time that the infamous

GLBSE service was quite basic and customers used a command line terminal interface to browse listings and buy or sell shares.[236] Entrepreneurs could list their company on GLBSE for a registration fee and allow investors to purchase and trade shares. Listed companies could opt to pay dividends to shareholders or buy back shares at a later date.

Shareholders had no guarantees that their investments would be honored and were entirely at the mercy of share issuers. Too often, share issuers did not honor their commitments. This was the case with GLBSE's first successfully facilitated IPO. The company behind the IPO, Ubitex, secured an impressive 1,100 BTC, or roughly $10,000, in investments before its owner disappeared without a trace a few months later.[237] Another major player in GLBSE, Lambert Investment Funds,[238] also suddenly pulled itself from the GLBSE directory after several of its investments were revealed to be illusory.[239]

Despite these setbacks, companies and investors continued to trade shares on GLBSE. An updated version of the GLBSE website introduced enhanced identification and authentication options to increase user trust and company accountability.[240] During May of 2012, GLBSE listed 10 major stocks valued at a sum of over $650,000.[241]

The saga of a high-yield investment scheme known as Bitcoin Savings and Trust (BTCST) foreshadowed GLBSE's demise. It was a high-yield investment scheme that was traded on the GLBSE

10,000 BTC pizza was purchased. *See* Vitalik Buterin, *Interview With GLBSE's James McCarthy/Nefario*, BITCOIN MAG. (Oct. 15, 2012), http://bitcoinmagazine.com/2578/interview-with-glbses-nefario/.

236. GLBSE later offered a user-friendly interface and enhanced features to expand functionality and increase its customer base. *See* Nefario, *GLBSE 2.0 open for testing*, BITCOINTALK.ORG (Jan. 21, 2012), https://bitcointalk.org/index.php?topic=60489.0.

237. Buterin, *supra* note 235.

238. Lambert Investment Funds was not a company, but an investment fund that was also traded on GLBSE. *See* Peter Lambert, *GLBSE:LIF*, BITCOINTALK.ORG (Aug. 5, 2011), https://bitcointalk.org/index.php?topic=34634.

239. The LIF operator, Peter Lambert, did offer to buy back shares at a lower rate, but many investors felt defrauded by his handling of the affair. *See* Peter Lambert, *[was on GLBSE] LIF.x*, BITCOINTALK.ORG (Jan. 17, 2012, 1:23:56 AM), https://bitcointalk.org/index.php?topic=35775.msg698197#msg698197.

240. Vitalik Buterin, *Global Bitcoin Stock Exchange Shuts Down for Good*, BITCOIN MAG. (Oct. 10, 2012), http://bitcoinmagazine.com/2549/global-bitcoin-stock-exchange-shuts-down-for-good/.

241. *GLBSE Valuations*, THE BITCOIN TRADER BLOG (May 13, 2012, 7:17AM), http://www.thebitcointrader.com/search/label/GLBSE.

exchange platform from November 2011 to August 2012. BTCST was a popular listing on GLBSE,[242] and it promised investors returns of up to 1 percent per day, or 7 percent per week.[243] Its manager, a Texas man called Trendon Shavers but known online as "Pirateat40," explained that he was in the business of "selling BTC to a group of local people" and that bitcoins deposited with him would be used in an arbitrage scheme.[244] At its peak, the scheme had attracted investments of about $7 million, according to Shavers.[245]

On July 23, 2013, the SEC filed a complaint against Shavers and Bitcoin Savings and Trust, alleging that BTCST was a Ponzi scheme,[246] contrary to Shavers' many assurances to his customers that BTCST was a legitimate operation.[247] "In reality," the SEC alleged, "the BTCST offering was a sham and a Ponzi scheme whereby Shavers used new BTCST investors' BTC to pay the promised returns on outstanding BTCST investments and misappropriated BTCST investors' BTC for his personal use."[248] Shavers moved to dismiss the SEC's complaint, arguing that BTCST investments did not qualify as securities because "Bitcoin is not money, and is not party of anything regulated by the United States."[249] Since no legal tender ever changed hands, Shavers argued, the investments were not securities and the SEC had no jurisdiction over his investment scheme.

In denying Shavers's motion to dismiss, the court applied the now-classic Howey test, which finds that an instrument is a regulated "investment contract" under the Securities Act if the instrument is (1) the investment of money; (2) in a common enterprise; (3) with the expectation of profits derived solely from the efforts of others.[250]

---

242. Adrianne Jeffries, *Suspected Multi-Million Dollar Bitcoin Pyramid Scheme Shuts Down, Investors Revolt*, THE VERGE (Aug. 27, 2012, 3:43 PM), http://www.theverge.com/2012/8/27/3271637/bitcoin-savings-trust-pyramid-scheme-shuts-down.

243. Sec. & Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2013 WL 4028182 at *1 (E.D. Tex. Aug. 6, 2013).

244. *Id.*

245. Vitalik Buterin, *The Pirate Saga: And So It Ends*, BITCOIN MAG. (Aug. 30, 2012), http://bitcoinmagazine.com/2126/the-pirate-saga-and-so-it-ends/.

246. *Shavers*, 2013 WL 4028182 at *1.

247. Trendon Shavers, *If My Business is Illegal Then Anyone Trading Coins for Cash and Back to Coins is Doing Something Illegal*, forum post, BITCOINTALK.ORG (Jan. 19, 2012, 6:51 AM), https://bitcointalk.org/index.php?topic=50822.385;wap2.

248. *Shavers*, 2013 WL 4028182 at *1.

249. *Id.*

250. Sec. & Exch. Comm'n v. W.J. Howey Co., 328 U.S. 293, 298-99 (1946).

Under this test, a wide variety of investments have been found to be securities.[251] Shavers argued that the first prong of the test failed because Bitcoin was not money.[252] The court, however, disagreed finding that Bitcoin qualified as money:

> It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and as Shavers stated, used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money, and investors wishing to invest in BTCST provided an investment of money.[253]

The court also found that BTCST met the other prongs of the Howey test and, therefore, "the BTCST investments [met] the definition of investment contract, and as such, are securities."[254] If the *Shavers* case is any guide, then issuers and exchanges will not be able to escape SEC regulation by merely denominating securities in bitcoin.[255]

Around the same time, GLBSE operator James McCarthy[256] sought legal counsel to ensure compliance with existing regulations as his side project grew into a going concern.[257] After his lawyers convinced him that GLBSE ran afoul of existing anti-money laundering and "know your customer" rules, McCarthy abruptly

---

251. For example, the First Circuit held that virtual shares in imaginary companies sold in dollars on a virtual exchange as part of a video game were "investment contracts" subject to securities regulation. Sec. & Exch. Comm'n v. SG Ltd., 265 F.3d 42, 48 (1st Cir. 2001) (holding that virtual shares of stock, offered as part of a game by a foreign entity operating a virtual stock exchange qualified as SEC-regulated investment contracts). For an account of a virtual stock market, *see* Robert J. Bloomfield and Young Jun Cho, *Unregulated Stock Markets in Second Life*, 78. S. Econ. J. 6 (2011).

252. *Shavers*, 2013 WL 4028182 at *1.

253. *Id.*

254. *Id.*

255. Craig K. Ellwell, M. Maureen Murphy, & Michael V. Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, CONG. RES. SERV. REP. NO. 7-5700 (2013), *available at* http://www.fas.org/sgp/crs/misc/R43339.pdf.

256. James McCarthy did not fully control GLBSE. Rather, GLBSE was owned by a parent company, Bitcoin Global, which is itself a multi-shareholder enterprise., *See* Theymos, *Nefario*, BITCOINTALK.ORG (Oct. 6, 2012, 12:00:57 AM), https://bitcointalk.org/index.php?topic=115669.0.

257. Buterin, *supra* note 240.

shut the exchange for good on October 4, 2012.[258] McCarthy attempted to ensure the return of investor funds, but some customers nevertheless likely lost investments.[259] Like so many other first wave Bitcoin businesses, GLBSE was conceived at a time when Bitcoin was largely a hobby or seen as a fantasy. McCarthy saw GLBSE as a fun side project experimenting with what was essentially play money.[260] By the time McCarthy realized that GLBSE could be a legitimate business, it was too late to become regulatorily compliant.

A few other Bitcoin stock market exchanges have been launched and shut down. BitFunder was launched in December of 2012 and allowed listed assets to be bought and sold using bitcoins.[261] Founded in the wake of GLBSE's closing, BitFunder aimed to provide easy integration for GLBSE customers to begin trading on the new platform. A few companies, like the mining ventures ASICMiner and IceDrill, successfully raised capital by selling shares on BitFunder.[262] Users could search for shares of companies and issue bids for buying or selling. Assets were publicly listed by Bitcoin address so that shareholders and managers could more easily reconnect in the case of an exchange shutdown. The founder of BitFunder designed the exchange with the lessons of GLBSE in mind.[263] Indeed, BitFunder's creator was acutely cognizant of the legal challenges his exchange faced from the day he first announced the project.[264] Fearing SEC investigation following the BTCST takedown,[265] BitFunder announced that it would no longer do business with U.S. customers in October of 2013 and encouraged U.S. customers to move their funds out of the

---

258. *Id.*

259. McCarthy estimates that 95% of GLBSE customers were compensated. *See* Olivia Solon, *Founder Reflects on the Closure of Bitcoin Stock Exchange GLBSE*, WIRED UK (Oct. 13, 2013), http://www.wired.co.uk/news/archive/2013-10/24/bitcoin-exchange-collapse-glbse.

260. *Id.*

261. Ukyo, *[BitFunder] Asset Exchange Marketplace + Rewritable Options Trading*, BITCOINTALK.ORG (Dec. 10, 2012, 8:34 PM), https://bitcointalk.org/index.php?topic=130117.0.

262. Kadhim Shubber, *Bitcoin Stock Exchange BitFunder Announces Closure*, COINDESK (Nov. 12, 2013, 12:30 PM), http://www.coindesk.com/bitcoin-stock-exchange-bitfunder-announces-closure/.

263. Ukyo, *Re: [BitFunder] Asset Exchange Marketplace - Official Launch*, BITCOINTALK.ORG (Dec. 11 2012, 9:06 PM), https://bitcointalk.org/index.php?topic=130117.msg1393343#msg1393343.

264. *Id.*

265. *Investor Alert: Ponzi Schemes Using Virtual Currencies*, 7 SEC PUB. 153 (Jul. 23, 2013), http://investor.gov/sites/default/files/ia_virtualcurrencies.pdf.

website by December 1 of that year.[266] (It is not clear where BitFunder was based.) By November 4, 2013, BitFunder announced that it was closing for good and announced a plan for reimbursing shareholders and listed companies.[267]

Similarly, BTC-TC was another bitcoin-denominated stock market that rose to popularity after GLBSE's demise. At its peak, BTC-TC listed 39 different assets—including stocks, bonds, futures, and investment funds—and facilitated roughly $350,000 in daily activity.[268] The exchange's most popular assets were mining companies like ASICMiner and LabCoin. At the time of its shutdown, BTC-TC listed assets were valued at an estimated $15 million.[269] Like BitFunder, BTC-TC prioritized information transparency and provided asset issuers with complete lists of shareholder email addresses and share counts to facilitate reconnecting in the event of an exchange shutdown.[270] BTC-TC prided itself on being "community operated;" asset "approval and scoring" was done by community moderators that were linked to the founder's Litecoin stock market exchange, LTC-GLOBAL.[271] BTC-TC also emphasized its legal registration in Belize as an international company.[272] Still, the website's own FAQ recognized its questionable legal status, advising customers:

> Is it legal for this exchange to operate?
>
> Most countries require real securities exchanges to register and abide by a very strict set of rules. Obviously we do not have the funding to afford such registration or the overhead of administering such rules. In addition, no single country would allow such an exchange to operate globally. As such we have taken the following approach to the operation of the site:

---

266. Shubber, *supra* note 262.

267. Ukyo, *Re: [BitFunder] Asset Exchange Marketplace - Official Launch*, forum post, BITCOINTALK.ORG (Nov. 4, 2013, 9:28 PM), https://bitcointalk.org/index.php?topic=130117.msg3482565#msg3482565.

268. Jonathan Stacke, *Bitcoin Securities Exchange BTC-TC Shutters $12M Operations, Cites Regulatory Environment*, THE GENESIS BLOCK (Sept. 23, 2013), http://www.thebitcoinchannel.com/archives/23739.

269. *Id.*

270. *Why BTC-TC Rocks*, BTCT.CO FAQ, https://btct.co/ (last visited Mar. 26, 2014).

271. Deprived, *Re: [BTCTC] BTC Trading Corp. – All new virtual exchange up at*, https://btct.co/, BITCOINTALK.ORG (Nov. 19, 2012, 11:09 PM), https://bitcointalk.org/index.php?topic=125629.msg1346121#msg1346121.

272. *See supra* note 270.

- No assets on the site are to be considered real.

- Nothing is verified. (Do your research!)

- The use of this site is for educational and entertainment purposes only.

- If an asset issuer on this site defaults, you have ZERO RECOURSE. (not like you have any recourse in most international BTC situations anyway.)[273]

 This scant legal cover proved inadequate to protect BTC-TC and the exchange shut down in September of 2013, citing regulatory concerns.[274] As with BitFunder, BTC-TC outlined a closing plan for issuers and shareholders to settle or reconcile outstanding balances.[275]

 A derivatives exchange mentioned earlier, MPEx, also provides Bitcoin-denominated stock market listings. MPEx extends its strategy of discouraging novices by employing the same command line method used by its broader derivatives and options exchange.[276] As with MPEx futures trading, users must pay an upfront registration fee and a small percent commission on trades.[277] MPEx currently lists four companies selling shares, including MPEx itself.[278] Each listing has a dedicated page where prices, trades, and dividend payments are displayed along with a "listing agreement" drafted by each company operator that serves as an informal memorandum of understanding between the company and the MPEx exchange.[279] The operator of MPEx even provides periodic shareholder reports in the popular Bitcointalk forums[280] and his own personal blog.[281] The popular gambling site, Satoshi Dice, sold

---

273. *Id.*

274. Stacke, *supra* note 268.

275. *Id.*

276. *A Review of MPEx, the Bitcoin Stock Exchange*, LOPER OS BLOG (Feb. 3, 2013), http://www.loper-os.org/?p=1108.

277. As of February 2013, MPEx garnered 2/3 of its profits from registration fees. *Id.*

278. MPEX, http://mpex.co/ (last visited Mar. 26, 2014).

279. For instance, the listing agreement for BitBet. *See* MPEX, http://mpex.co/?mpsic=S.BBET (last visited Mar. 26, 2014).

280. MPOE-PR, *Re: Investing in Mircea Popescu's Options Emporium*, BITCOINTALK.ORG (Sept. 29, 2012, 2:15 AM), https://bitcointalk.org/index.php?topic=64962.msg1230084#msg1230084.

281. Mircea Popescu, *Six Month MPOE Financial Results*, TRILEMA (Feb. 20, 2012), http://trilema.com/2012/sa-ne-jucam-de-a-investitiile-n-bitcoini/#comment-78745.

shares of the company on MPEx from April of 2012 until July of 2013.[282] While still small, MPEx stock trading continues to garner investment and interest.

In March of 2014, the SEC sent a letter to MPEx's Romanian proprietor, Mircea Popescu, asking for contracts and other documents relating to the SatoshiDice.com offering.[283] Popescu, who posted his correspondence with the SEC on his blog, responded by questioning the SEC's jurisdiction over his business and its authority to make any requests.[284] The SEC and other relevant regulatory bodies will face similar challenges during the regulatory transition. The next section will consider whether and to what extent existing financial regulation should apply to certain financial transactions involving Bitcoin.

3. Regulatory Issues Facing Bitcoin-Denominated and "Bitcoin-Economy" Transactions

Given the broad definition of "commodity" and "security," it seems likely that regulators will assert jurisdiction over any transaction involving bitcoins that is structured in a manner that even resembles that of a regulated financial instrument. Accordingly, a transaction for future delivery of bitcoins, or that exchanges bitcoin-related payments, like a swap, would likely fall under the CFTC's jurisdiction to regulate Bitcoin futures and Bitcoin swaps, subject to the limitations on regulation for transactions that are physically settled or not capable of being cleared.[285] Similarly, any investment in bitcoins that takes place through a contract that satisfies the

---

282. After being sold to a private third party for $11.5 million, Satoshi Dice de-listed itself from MPEx and paid S.DICE shareholders 0.0035 BTC per share. *See* Eric Vorhees, *[CLOSED] S.DICE - SatoshiDICE 100% Dividend-Paying Asset on MPEx*, BITCOINTALK.ORG (Aug. 20, 2012, 4:14 PM), https://bitcointalk.org/index.php?topic=101902.0; Emily Spaven, *Bitcoin company acquisitions begin: Gambling site SatoshiDice sells for $11.5m*, COINDESK (Jul. 18, 2013), http://www.coindesk.com/bitcoin-company-acquisitions-begin-gambling-site-satoshidice-sells-for-11-5m-126315-btc/.

283. Carter Doughtery, *Gambling Website's Bitcoin-Denominated Stock Draws SEC Inquiry*, BLOOMBERG (Mar. 20, 2014, 12:01 AM), http://www.bloomberg.com/news/2014-03-19/gambling-website-s-bitcoin-denominated-stock-draws-sec-inquiry.html; *see also* Letter from Daphna A. Waxman, SEC, to Mircea Popescu in Re: SatoshiDICE (NY-8954) (Mar. 3, 2014) (on file with author), *available at* http://trilema.com/wp-content/uploads/2014/03/2014-0303-popescu-mpex.pdf.

284. Mircea Popescu, *Interacting with Fiat Institution: A Guide*, TRILEMA (Mar. 18, 2014), http://trilema.com/2014/interacting-with-fiat-institution-a-guide/.

285. *See supra* Section II.A.

broadly defined characteristics of an "investment contract" will fall under jurisdiction of the SEC. Indeed, as the decision in *Shavers* strongly suggests, even if the instrument is Bitcoin-denominated, regulators are likely to assert jurisdiction just as they would over a transaction denominated in legal tender. Accordingly, parties that enter into Bitcoin-denominated transactions, and venues that trade Bitcoin-denominated instruments, will be regulated by an appropriate regulator.

Nonetheless, financial regulators should consider whether and to what extent existing financial regulation should apply to certain financial transactions involving Bitcoin. In particular, regulators should consider whether the full scope of their regulation should apply to a transaction that involves a Bitcoin-denominated instrument whose underlying transaction is also Bitcoin-denominated, which we call *Bitcoin-economy transactions*. An example of a Bitcoin-economy transaction would be a Bitcoin-denominated credit default swap that references a Bitcoin-denominated loan. The purpose of financial regulation is to protect the users of financial instruments from fraud, manipulation, and other types of misconduct that results in real economic losses. Regulators should reconsider a wide-ranging regime of regulation for Bitcoin-universe transactions because such transactions do not implicate the traditional policy goals of financial regulation.

One approach for regulators would be to completely exclude Bitcoin-economy transactions from regulation, just as forwards and private investment funds are excluded from the CEA and the Investment Company Act, respectively. Another approach would be to exempt Bitcoin-universe transactions from most applicable regulation, while still imposing requirements and prohibitions relating to recordkeeping, reporting, and fraud. The latter approach would be similar to how private company securities, commodity trade options, and certain over-the-counter securities markets are regulated.[286]

The following chart displays the unique nature of Bitcoin-economy transactions. It distinguishes a transaction based upon whether the underlying interest is virtual or real and whether the transaction is denominated in real or virtual currency:

---

286. *See* OTC Markets Group, FINRA and SEC Rules, http://www.otcmarkets.com/learn/sec-finra-rules.

	Real Underlying	Virtual Underlying
Denominated in Real Currency	Traditional Securities, Futures, Swaps, Options	Securities investing in Bitcoin; Futures, Swaps, and Options on Bitcoin
Denominated in Virtual Currency	Bitcoin-denominated Securities, Futures, Swaps, Options	Bitcoin-economy transactions

Figure 2 – "Real" vs. "Virtual" framework.

FinCEN's approach to Bitcoin indicates how Bitcoin-economy transactions can be treated differently. FinCEN defines a virtual currency as a currency that operates like a currency in some environments, but does not have all the attributes of real currency.[287] It further defines a *convertible* virtual currency as a virtual currency that either has an equivalent value in real currency or acts as a substitute for real currency.[288] Under FinCEN regulation of money service businesses, only companies that transmit convertible virtual currencies or exchange convertible virtual currencies into real currencies are subject to regulation.[289] Those that transact in non-convertible virtual currencies, or use but do not transmit or exchange convertible virtual currencies, are not regulated. As a result, Bitcoin miners and those that trade bitcoins for their own investment purposes are not subject to money transmitter regulation.[290] This approach suggests that transactions that "stay" within the Bitcoin economy—which would include Bitcoin-economy transactions—are unique and should not be subject to the same level of regulation.

The fact that FinCEN regulates to protect against money laundering and financial crimes, while the SEC and CFTC regulate

---

287. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRNEYC MINING OPERATIONS, FIN-2014-R001, 1, 2 (Jan. 30, 2014), http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf.

288. *Id.*

289. *Id.*

290. *See* FinCEN Ruling FIN-2014-R001, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY MINING OPERATIONS (2014), *available at* http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf; *See* FinCEN Ruling FIN-2014-R002, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY SOFTWARE DEVELOPMENT AND CERTAIN INVESTMENT ACTIVITY 1, 4 (2014), *available at* http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf; *supra* to 287.

to protect investors and market integrity, should not prevent the latter agencies from following FinCEN's approach. Regardless of what policy concerns are at issue, transactions that stay within the Bitcoin economy do not raise the same type of risks as those that implicate real goods, services, or currencies. Indeed, the CFTC should find the argument for excluding or exempting Bitcoin-economy transactions from the CEA to be particularly compelling. Physically-settled transactions are generally not subject to the full scope of CFTC regulation precisely because they do not implicate the markets that the CFTC is concerned about, namely, futures and swaps markets. Bitcoin-economy transactions clearly fall within the category of physical (as opposed to cash) settlement and likewise do not implicate Bitcoin derivatives markets. Accordingly, the reasons the CFTC excludes physically-settled commodity contracts from regulation should apply to physically-settled Bitcoin contracts as well.

4. Prediction Markets & Gambling

In the U.S., online gambling and prediction markets have been heavily regulated, if not outright prohibited. Nevertheless, a number of online games and prediction markets have emerged that denominate their bets in bitcoins. In this section we will survey the laws and regulations that apply to online gambling and prediction markets.

Prediction markets are exchanges where individuals trade "event contracts," which specify some future event with different possible outcomes, a payment structure based on the outcome, and a contract expiration date. For example, a contract could specify "Hillary Clinton wins the U.S. presidential election in 2016" and pay out $10 if the event comes to pass or $0 if it does not. Obviously, these markets serve to allow betting on uncertain future events, but more importantly the prices they produce contain very valuable information regarding the expectations that people have about future events. As a result, prediction markets are often designed for the express purpose of uncovering these prices, and not merely to facilitate wagering.[291]

By aggregating the beliefs of market participants, prediction market prices reveal the overall market forecast of a particular event's odds of occurring. In our example, if the contract is trading

---

291. Adam Ozimek, *The Regulation and Value of Prediction Markets*, MERCATUS CTR. WORKING PAPER (Mar. 12, 2014), http://mercatus.org/publication/regulation-and-value-prediction-markets.

at a price of $5.50, then it means the market places the odds of Clinton's election at 55%. As the election unfolds, the media, political operatives, academics, and citizens can observe the prices in the market to get a sense of the relative strength of the candidates.

Beyond elections, prediction markets have been used to predict a wide variety of events, such as Academy Award and Super Bowl winners, product sales figures, flu trends, and much more. They also tend to be more accurate than polls, surveys, and other forecasting methods. Prediction markets, therefore, could serve many useful social purposes, including forecasting the probability of man-made or natural disasters; predicting political events that could affect financial markets, such as whether the "debt limit" will be raised; better forecasting IPO pricing; and allowing hedging against failure of a product the market success of which is difficult to predict, such as entertainment or pharmaceuticals.

Unfortunately, the regulatory atmosphere in the U.S. has been largely hostile to prediction markets. (More examples may be needed to support this claim. It makes sense that the Division would want oversight because the other example is basically gambling over important political processes in the nation.) In 2012, the CFTC sued the prediction market Intrade for violating the Commission's ban on off-exchange options trading.[292] As David Meister, the Director of the CFTC's Division of Enforcement, put it in a statement announcing the suit: "It is against the law to solicit U.S. persons to buy and sell commodity options, even if they are called 'prediction' contracts, unless they are listed for trading and traded on a CFTC-registered exchange or unless legally exempt. . . . Today's action should make it clear that we will intervene in the 'prediction' markets, wherever they may be based, when their U.S. activities violate the Commodity Exchange Act or the CFTC's regulations."[293] Intrade suspended its operations in the U.S., and within months the site had shut down.[294]

---

292. *CFTC Charges Ireland-Based "Prediction Market" Proprietors Intrade and TEN with Violating the CFTC's Off-Exchange Options Trading Ban and Filing False Forms with the CFTC,* CFTC PRESS RELEASE (Nov. 26, 2012), *available at* http://www.cftc.gov/PressRoom/PressReleases/pr6423-12.

293. *Id.*

294. The CFTC continues to target predictions markets. *See* Katherine Mangu-Ward, *The Death of Intrade,* REASON MAG. (Dec. 2013), http://reason.com/archives/2013/11/25/the-death-of-intrade; Jamila Trindle, *Regulators Sue Prediction Site, Allege Illegal Options,* WALL ST. J. (June 6, 2013), http://online.wsj.com/news/articles/SB100014241278873247989045785292414823 37164.

Exemptions or permission for regulated exchanges to offer such contracts have not been forthcoming. Shortly after its action against Intrade, the CFTC rejected a proposal by the regulated exchange Nadex to offer political "binary options" that would have allowed traders to bet on the outcomes of that year's presidential and congressional elections.[295] In its order, the CFTC found that "the contracts involve gaming and are contrary to the public interest, and cannot be listed or made available for clearing or trading."[296]

Today, the only legal real-money political prediction market operating in the U.S. is the Iowa Electronic Market, which is run by the University of Iowa's Tippie College of Business.[297] It operates under the auspices of two CFTC no-action letters that are contingent on the market's non-profit and academic status.[298] The letters also place a number of restrictions on the market.[299] For example, no individual is allowed to invest more than $500, and individual markets are limited to a pre-determined range of participants.[300] In addition, pursuant to authority granted to it by the Dodd-Frank Wall Street Reform and Consumer Protection Act,[301] the CFTC has issued rules banning any event contract "that involves, relates to, or references terrorism, assassination, war, gaming, or an activity that is unlawful under any State or Federal law."[302]

---

295. Jason Abbruzzese, *CFTC Bans Election-Based Derivatives Contracts*, FIN. TIMES (Apr. 3, 2012), http://www.ft.com/intl/cms/s/0/dcf08b92-2a70-11e1-9bdb-00144feabdc0.html#axzz2vaSTU2d.

296. *CFTC Issues Order Prohibiting North American Derivatives Exchange's Political Event Derivatives Contracts*, CFTC PRESS RELEASE (Apr. 2, 2012), *available at* http://www.cftc.gov/PressRoom/PressReleases/pr6224-12.

297. Paul Gomme, *Iowa Electronic Markets*, FEDERAL RESERVE BANK OF CLEVELAND REPORT (Apr. 15, 2003), *available at* http://www.researchgate.net/publication/5028658_Iowa_electronic_markets.

298. Andrea M. Corcoran, *CFTC Letter to Professor George Neumann*, CFTC Letter No. 91-04a, Division of Trading and Markets, CFTC (Feb. 5, 1992) *available at* http://www.cftc.gov/ucm/groups/public/@lrlettergeneral/documents/letter/92-04a.pdf; Andrea M. Corcoran, *CFTC Letter to Professor George Neumann*, CFTC Letter No. rf05-003, Division of Trading and Markets, CFTC (June 18, 1993), *available at* http://www.cftc.gov/files/foia/repfoia/foirf0503b004.pdf.

299. *Id.*

300. *Id.*

301. Dodd–Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376-2223 (codified as amended in scattered sections of U.S.C. titles: 2, 5, 7, 11, 12, 16, 18, 19, 20, 22, 25, 26, 28, 29, 30, 31, 41, 42, 44, 49, 112), s. 275.

302. 17 CFR 40.11 (2011).

The regulatory environment has been similarly hostile to online gambling. The Wire Act[303] prohibits the knowing use of wire communications for the transmission of bets or wagers or information assisting bets or wagers on any sporting event or contest,[304] and the Illegal Gambling Business Act (IGBA)[305] makes it a federal offense to operate gambling businesses that are illegal under state law. In addition, in 2006 Congress passed the Unlawful Internet Gambling Enforcement Act (UIGEA), which prohibits gambling businesses from accepting payments in connection with unlawful bets or wagers involving the use of the Internet.[306] It also requires payment processors, such as money transmitters and credit cards providers, to block payments to gambling sites.[307]

Despite this inhospitable regulatory environment, today there are a number of gambling and prediction market sites operating that offer wagering, event contracts, and binary options denominated in bitcoins. They seem to operate under the theory that because they only employ bitcoin, they are not subject to regulation. For example, Coinbet.cc offers poker, casino games, and sports betting to U.S. customers and claims that by using Bitcoin, its offering is legal. The website states:

> Because the ever popular cryptocurrency is not legal tender and not recognized as a legitimate form of currency by the U.S., that also means that in legal terms- online gambling with Bitcoin is not an illegal event under the Wire Act or Unlawful Internet Gambling Enforcement Act (UIGEA) which is why it is the perfect payment method for online action in the U.S.[308]

---

303. 18 U.S.C. § 1084 (2014).

304. A 2011 decision from the Department of Justice changed the scope of 18 U.S.C. § 1084 to only apply to sports betting. Virginia A. Seitz, *Whether Proposals By Illinois and New York to Use the Internet and Out-Of-State Transaction Processors to Sell Lottery Tickets to In-State Adults Violate the Wire Act*, Memorandum Opinion for the Assistant Att'y Gen, WHETHER PROPOSALS BY ILLINOIS AND NEW YORK TO USE THE INTERNET TND OUT-OF-STATE TRANSACTION PROCESSORS TO SELL LOTTERY TICKETS TO IN-STATE ADULTS VIOLATE THE WIRE ACT (Sept. 20, 2011) *available at* http://www.justice.gov/olc/opiniondocs/state-lotteries-opinion.pdf.

305. 18 U.S.C. § 1955 (2014).

306. 31 U.S.C. §§ 5361–67 (2006).

307. *Id.*

308. *Information for U.S. Bettors*, COINBET.CC CUSTOMER SERVICE, http://www.coinbet.cc/pages/us-bettors#.Ux9IiOddXzc (last visited Mar. 26, 2014).

Other gambling sites include SatoshiDice.com, SatoshiBet, and dozens more.[309] Bitcoin prediction markets include Predictious.com, BTCOracle, and Bets of Bitcoin.

It is not likely that courts will see the use of bitcoins for wagering (instead of legal tender) as a shield from prohibitions on gambling. State gambling prohibitions, which undergird federal interstate gambling laws, generally require that gambling transactions have three elements: prize, chance, and consideration.[310] The question, therefore, is whether bitcoins can serve as consideration, and courts have confronted such "token consideration" cases before. For example, in *United States v. Davis*, the defendants operated internet cafés in which customers purchased internet access time.[311] For each dollar of internet time purchased, the customer would receive 100 "entries" into a "sweepstakes." Customers could then enter the sweepstakes through several ways, one of which was playing casino-like games on the computers. The court found that the defendant's internet café was an attempt to legitimize an illegal lottery in violation of IGBA reasoning that, under Texas gambling law, the sweepstakes participants exchanged some consideration (the "entry" tokens) in exchange for the privilege to play the sweepstakes. There are several other cases that are similar to *Davis* and use a similar type of analysis.[312] So, it would not be surprising if courts were to employ an analysis like that in the *Bitcoin Savings and Trust* case and find that bitcoins are indeed money, or tokens representing money, and thus consideration.[313]

As we have seen, the CFTC views event contracts as options, and as noted in section II.A, *supra*, options must be traded at regulated exchanges and are subject to extensive requirements and restrictions. Given the growing consensus that bitcoins can be used

---

309. S.V. GAMBLING, BITCOIN WIKI, https://en.bitcoin.it/wiki/Category:Gambling (last visited Mar. 26, 2014).

310. *See* Midwestern Enters. v. Stenehjem, 625 N.W.2d 234, 237 (N.D. 2001) ("The three elements of gambling are generally recognized as consideration, prize, and chance.").

311. United States v. Davis, 690 F.3d 330 (5th Cir. 2012).

312. *See e.g.*, Telesweeps of Butler Valley, Inc. v. Kelly, 2012 WL 4839010 (M.D. Pa. 2012) (holding that a computerized casino game-style sweepstakes based on credits purchased from phone cards is considered gambling, in violation of Pennsylvania law); City of Cleveland v. Thorne, 987 N.E.2d 731 (Ohio Ct. App. 2013) (although not a federal case, the court held that offering "sweepstakes points" associated with the sale of internet time at an internet cafe violated city gambling ordinances).

313. *See* SEC v. Shavers, No. 4:13-CV-416, 2014 WL 4652121 (E.D. Tex. Aug. 6, 2013).

as money whether they fit any particular definition of money or not, it is unlikely the CFTC will find it has no jurisdiction over event contracts denominated in bitcoins. The CEA talks in terms of regulated "trading," "agreements," "contracts," and "transactions" without reference to any limitation based on the kind of consideration employed. Therefore, the CFTC may give little weight to the fact that event contract trading is carried out in bitcoins. That said, the CFTC should consider whether bitcoin-denominated event contracts qualify as "Bitcoin-universe transactions" as illustrated in Figure 2, and therefore whether the full scope of regulation under the CEA should apply to such transactions.

The analysis under UIGEA is a bit trickier, however. UIGEA does not prohibit gambling per se, but instead prohibits accepting certain types of electronic payments for online gambling. The question is whether Bitcoin transactions qualify. The relevant section of UIGEA reads:

> No person engaged in the business of betting or wagering may knowingly accept, in connection with the participation of another person in unlawful Internet gambling . . . an electronic fund transfer, or funds transmitted by or through a money transmitting business, or the proceeds of an electronic fund transfer or money transmitting service, from or on behalf of such other person. . . .[314]

Assume for the moment that the predicate "unlawful Internet gambling" violation has been established under state or federal law. The easy case is one in which "funds [are] transferred by or through a money transmitting business." Bitcoin exchanges and some online wallet services, such as Coinbase.com, are money transmitters under federal and state regulations.[315] Bitcoins are also likely to be considered "funds" under a similar analysis to that in *Bitcoin Savings and Trust*.[316] Therefore, accepting bitcoins transmitted by or

---

314. 31 U.S.C. § 5363 (2006).

315. U.S. DEPARTMENT OF THE TREASURY, FINANCIAL CRIMES AND ENFORCEMENT NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (REGULATORY GUIDANCE, FIN-2013-G001, US DEPARTMENT OF THE TREASURY, Washington, DC, Mar. 18, 2013), *available at* http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

316. *See* Adrianne Jeffries, *Suspected Multi-Million Dollar Bitcoin Pyramid Scheme Shuts Down, Investors Revolt,* THE VERGE (Aug. 27, 2012, 3:43 PM), http://www.theverge.com/2012/8/27/3271637/bitcoin-savings-trust-pyramid-scheme-shuts-down.

through one of these Bitcoin intermediaries will likely violate UIGEA. In addition, this may mean that these intermediaries may have to comply with UIGEA's requirements to preemptively block prohibited transactions.[317]

The more difficult case is when there is no intermediary involved between the consumer and the gambling business, so that the UIGEA does not apply. Some services, like Coinbase.com, hold bitcoin accounts for consumers in a custodian-like fashion, and consumers instruct the service to send bitcoins when they want to make a transaction.[318] Bitcoin's design, however, allows a user to hold her own bitcoins, just like holding cash. To do so, a user employs software known as a "wallet," which contains the user's unique keypair that controls bitcoin holdings. A wallet application can be run on a desktop PC or a smartphone. There are also web wallets, which provide users online access to a user's bitcoins. It is important to note that the providers of such web wallets, such as Blockchain.info, do not hold bitcoins for their users nor do they have any access whatsoever to any of their users' bitcoins. They also do not initiate transactions for users. They simply provide the facility for users to manage their bitcoin holdings. Whether a user employs a wallet on their desktop, smartphone, or online when they send bitcoins to another person, there is no intermediary between them.

UIGEA prohibits accepting any "electronic fund transfer" for illegal Internet gambling,[319] so the question is whether a Bitcoin transaction sent directly from the consumer to the gambling business, with no intermediary between them, qualifies as an "electronic fund transfer." Under UIGEA, electronic fund transfer "means any transfer of funds . . . which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a *financial institution* to debit or credit an account."[320] In turn, "financial institution" is defined as "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or *any other person* who, directly or indirectly, holds an account belonging to a consumer. . . ."[321] Therefore, it would be

---

317. 31 U.S. Code § 5364 (2006).

318. For a discussion of the distinction between off-block chain and on-block chain transactions, *see* Ryan Galt, *Roger Ver on Blockchain's Past, Present and Future*, COINDESK (Feb. 15, 2014, 03:50 PM), http://www.coindesk.com/roger-ver-blockchain-past-present-future/.

319. 31 U.S.C. § 5363 (2) (2006).

320. *Id.* (emphasis added).

321. *Id.* (emphasis added).

stretching the plain meaning of the statute to argue that a bitcoin wallet held on one's own smartphone is equivalent to an account held at a financial institution. To do so, a court would have to find that the "other person" that the statute contemplates is the consumer herself; that the user is *both* the "consumer" and the "financial institution" mentioned in the statute. Clearly the statute did not anticipate electronic cash without the use of intermediaries.

There is another aspect of Bitcoin's use in online gambling and prediction markets that may pose a challenge to regulators and law enforcement. Quite apart from simply denominating bets and contract prices in bitcoins, a gambling business or prediction market could employ the Bitcoin network to serve as the betting or trading infrastructure.

For example, traditional online gambling businesses or prediction markets require a user to visit a website and create an account and then deposit funds to be associated with that account via wire transfer or some other means. Once this is done, the user may gamble or speculate using their account balance, and they may later withdraw funds, including earnings, as they see fit. This is also how many bitcoin-denominated sites operate. One example is Predictious.com, where one can buy or sell contracts related to political, economic, and sporting events. To do so one must create an account and then send bitcoins to fund that account. All users' bitcoin balances are held by Predictious, and one must initiate a withdrawal to regain control of any outstanding balance. If law enforcement were to shut down such a site, users would potentially lose access to their account balances. Indeed, user balances could be subject to seizure as well.

In contrast to this traditional model, there are betting sites and prediction markets that require no account creation whatsoever, and bets are placed simply by initiating a Bitcoin transaction. SatoshiDice is probably the most popular of these block-chain-based gambling sites.[322] Playing is as easy as sending an amount of one's choosing to a static address operated by the service and immediately getting back either more or less than one's bet. Different SatoshiDice addresses have different possible payouts and corresponding odds.[323] This design means that no accounts or deposits are

322. Megan Geuss, *Firm says online gambling accounts for almost half of all Bitcoin transactions*, ARSTECHNICA (Aug. 24, 2014, 8:30 PM), http://arstechnica.com/business/2013/08/firm-says-online-gambling-accounts-for-almost-half-of-all-bitcoin-transactions/.

323. Because all transactions are public, users can verify that the house is paying out fairly – unlike traditional casinos.

necessary to play. Indeed, no website is needed either. All the SatoshiDice website does is list the betting addresses, and these are widely known. Therefore, even if SatoshiDice's.com domain were to be seized, its operations would not be affected as long as its Dublin-based[324] servers continued processing Bitcoin transactions. And if its servers were to be shut down, users would have no account balances to lose. Other sites like SatoshiDice include BitLotto[325] and DiceOnCrack.[326]

BTCOracle is a similar service that does not require registration or balances, but instead of gambling, it allows users to attempt to predict the future price of Bitcoin using binary options.[327] Unlike SatoshiDice, BTCOracle does hold balances on behalf of users, but only for pre-determined, discrete lengths of time.[328] Users can bet on whether the price of Bitcoin will go up or down within a given period of time simply by initiating a bitcoin transaction. The BTCOracle website merely serves as a directory for open options and their corresponding betting addresses. The front page of the website displays two main tables[329] ("Win if the price is higher in:" and "Win if the price is lower in:") with five different selections under each. Each table lists five options: 15 minutes, 3 hours, 1 day, 3 days, and 1 week. Each option lists a minimum and maximum Bitcoin-denominated bet along with a price multiplier that will be used to determine winnings. Finally, each "option" lists a Bitcoin wallet address and corresponding QR code. Users who wish to bet on any of these options simply send a bet amount within the predetermined range to the associated address. If the user wins the

---

324. Jon Matonis, *Bitcoin Casinos Release 2012 Earnings*, COINDESK (Jan. 22, 2013, 11:35 AM), http://www.forbes.com/sites/jonmatonis/2013/01/22/bitcoin-casinos-release-2012-earnings/.

325. Bitlotto, *[BITLOTTO] Mar 1 draw over $2000 or 50BTC! Tickets now 0.1 BTC for Apr 5*, BITCOINTALK.ORG (Aug. 3, 2011), https://bitcointalk.org/index.php?topic=34007.0.

326. TTBit, *DiceOnCrack.com | If you thought dice was addicting...*, foreign post, BITCOINTALK.ORG (Oct. 24, 2012), https://bitcointalk.org/index.php?topic=120239.0.

327. BTCOracle, *FAQ*, BTCORACLE CUSTOMER SERVICE, http://btcoracle.com/faq.php (last visited Mar. 26, 2014).

328. This means that BTCOracle users could conceivably lose their bitcoins if the site shuts down before the balance time period is up. SatoshiDice users face no such problems since the service never holds bitcoins on users' behalf.

329. Two other tables are "Win if at any time until the option is closed, the price is 10% or more higher than the starting price" and "Win if at any time until the option is closed, the price is 10% or more lower than the starting price" with three different time options: 1 day, 3 days, and 1 week. The remaining tables list running and closed executed options.

bet, the earnings, equal to the amount of the initial bet times the displayed price multiplier, will be sent back to the Bitcoin wallet from which the user sent the original bet. If the user loses, he will receive nothing (or will receive a corresponding repayment according to the odds).[330] According to the website FAQ, BTCOracle has processed at least 3,000 options trades since the service launched in April of 2013.[331]

While bitcoin-denominated prediction markets and gambling sites exist in a legal gray area, the fact that transactions are bitcoin-denominated is likely less of a legal shield than some operators imagine.[332] Nevertheless, Bitcoin will make it more difficult to enforce gambling regulations. After all, the purpose of UIGEA is to leverage intermediary payment processors to target illegal online gambling.[333]

IV. DECENTRALIZED MARKETS AND EXCHANGES

Bitcoin, at root, is a cryptographically verifiable distributed ledger system. At any moment in time, there is a fixed number of bitcoins and the block chain allows a user to prove ownership of a particular bitcoin (or fraction thereof) and to verifiably transfer ownership without the need for a single trusted third party.

To date, bitcoins have represented money at a floating exchange rate, and the Bitcoin network has been employed as a fast and inexpensive payments or money transfer system. But there is no reason why particular bitcoins (or fractions thereof) could not represent something besides money. If we conceive of bitcoins simply as tokens, then other applications become apparent. For example, we could agree that a particular bitcoin (or, indeed, an infinitesimally small fraction of a bitcoin so as to allow for many tokens) represents a house, a car, a share of stock, a futures contract, or an ounce of gold.[334] Conceived of in this way, the Bitcoin block

---

330. BTCOracle, *FAQ – "How does it work?"*, BTCORACLE CUSTOMER SERVICE, http://btcoracle.com/faq.php (last visited Mar. 26, 2014).

331. BTCOracle, *FAQ – "Can you trust us? Who are you?"*, BTCORACLE CUSTOMER SERVICE, http://btcoracle.com/faq.php (last visited Mar. 26, 2014).

332. For instance, the creator of the centralized digital currency, Liberty Dollar, was charged and eventually convicted of the federal crime of, "making, possessing, and selling his own coins." "Defendant Convicted of Minting His Own Currency," U.S. Attorney's Office, (Mar. 18, 2011) *available at* http://www.fbi.gov/charlotte/press-releases/2011/defendant-convicted-of-minting-his-own-currency.

333. 31 U.S.C. § 5361 (2006), Congressional findings and purpose.

334. The conceptual idea of smart contracts, famously proposed by Nick Szabo, was theoretically derived for Bitcoin applications by Mike Hearn. *See* Nick

chain then becomes more than just a payment system. It can be a completely decentralized and perfectly reconciled property registry, which we will explain in more detail shortly.

This section explains how Bitcoin may be used to create decentralized financial transactions. It first explains the basic components of decentralized ledger transactions; namely, multisignature transactions, escrow and arbitration, oracles that verify real-word information, and smart property. It then reviews the mechanisms and operations of decentralized securities exchanges, prediction markets, and gambling. Finally, this section explores the implications of decentralization for financial regulators and highlights the limitations of attempting to control information.

A. Decentralized Ledger Transactions

Transactions using the Bitcoin protocol are programmable, which means that they can be automated.[335] For example, Bitcoin allows for multisignature, or "m-of-n," transactions that require any m number of n signatures to complete.[336] Compared to a basic two-person transaction where bitcoins are transferred directly from one person's wallet to another's with no opportunity for chargebacks, multisignature transactions offer greater security and more complexity without the need for a trusted third party through the use of pre-established signature consensus.[337]

The simplest application of a multisignature transaction is a 2-of-3 transaction. Bitcoins are sent to an address controlled by three parties:[338] perhaps the buyer, the seller, and a third party arbitrator

---

Szabo, *The Idea of Smart Contracts*, 1997, http://szabo.best.vwh.net/idea.html; and Mike Hearn, *Smart Property*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Smart_Property.

335. Gavin Andresen, *Pay to Script Hash, Bitcoin Improvement Proposal 0016*, GITHUB (Mar. 1, 2012), https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki.

336. Gavin Andresen, *Bitcoin Faucet Hacked*, GAVIN TECH (Mar. 1, 2012), http://gavintech.blogspot.com/2012/03/bitcoin-faucet-hacked.html.

337. For an overview of the functions and applications of multisignature transactions, *see* Mike Hearn, *The Future of Bitcoin: New Applications and Rebuilding the Banking System, Presentation at the Bitcoin 2012 Conference in London*, YOUTUBE (Sept. 27, 2012), http://www.youtube.com/watch?v=mD4L7xDNCmA.

338. More technically, three normal bitcoin addresses are gathered or created and their public keys are noted. A multisignature address is then created from these three public keys using the "addmultisigaddress" command. Users can then send funds into this multisignature address using normal Bitcoin commands. *See* Gavin Andresen, *Re: [Bounty] How-to Multi signature transactions*, forum

chosen by the buyer and seller. To move the bitcoins from the jointly controlled address, two out of the three parties must sign off on the transaction. If the buyer and seller are both happy with the exchange, they both sign off on the transaction, the bitcoins are transferred to the seller, and the transaction is reconciled on the block chain. In the case of a dispute, the seller will sign off on the transfer of the bitcoins to herself, but the buyer will not. In this case, the third party arbitrator can render a decision by deciding who should get the coins and signing the appropriate transaction.[339] The third party's signature provides the second needed signature to complete the 2-of-3 transaction.

　　This kind of multisignature transaction can be used to provide escrow-like services[340] for bitcoin transactions as well as for real world assets. Suppose Alice orders an original painting from Bob.[341] Instead of using PayPal to serve as a payment processor and dispute mediator, Alice and Bob decide to arrange a multisignature bitcoin transaction with a third party arbitrator, Chuck. A multisignature address is created and Alice sends enough bitcoins to cover the price to the jointly controlled address. At no point in time can any one party move these bitcoins from the joint address. If Alice receives the painting without a dispute, Alice and Bob both sign the transaction and the bitcoins move to Bob's personal address. If Alice receives the painting but she cannot get a hold of Bob for some reason, she can direct Chuck to provide the second signature to the transaction so that the bitcoins get transferred to Bob's address. If Bob does not send the painting by the agreed upon date, Chuck and Alice will sign the transaction to return Alice's bitcoins to her personal address. In the case of a dispute, Alice and Bob can appeal to Chuck to arbitrate according to the agreed-upon terms of

---

post, BITCOINTALK.ORG (May 18, 2012, 1:20 AM), https://bitcointalk.org/index.php?topic=82213.msg906833#msg906833.

339. While this third party can technically be any person on whom the buyer and seller agree, early businesses have looked to provide professionalized mediation services through 2-of-3 transactions. For one example, *see* Bitrated, *FAQ,* https://www.bitrated.com/faq.html (last visited Mar. 26, 2013).

340. Note that multisignature transactions are not like traditional escrow services because the third party never actually takes ownership of the collateral or deposit. The bitcoins are always under the joint control of the multisignature address, so no one party can simply abscond with the funds as in traditional escrow services.

341. For an overview of the functions and applications of multisignature transactions, *see* Mike Hearn, *The Future of Bitcoin: New Applications and Rebuilding the Banking System, Presentation at the Bitcoin 2012 Conference in London,* YOUTUBE (Sept. 27, 2012), http://www.youtube.com/watch?v=mD4L7xDNCmA.

the contract. Unlike traditional escrow, at no point can Chuck run away with the money he is holding.

Arbitrators to a multisignature transaction can provide more than simple dispute mediation. In the case of rare or specialty goods, arbitrators can also serve as specialists to verify authenticity. Let's say that the painting that Bob is selling is an original Picasso. Alice and Bob now agree to designate Dan, a Sotheby's broker, to serve as the third party arbitrator. Bob carefully ships the painting to the United States, where Dan and Alice receive it. With the full weight of Sotheby's reputation behind him, Dan inspects the work to ensure its authenticity. If he determines the work is a genuine Picasso, he will provide the second signature to the transaction to transfer the bitcoins to Bob's private address. This structure allows Bob and Alice with the expertise of a specialist arbitrator along with the peace of mind that no one party can move bitcoins from the joint address.[342]

It may one day be possible to even eliminate the need to trust any individual arbitrator's or organization's professional reputation. Rather than designating a living person as the third party, users could write a program, called an oracle,[343] to only sign off on the transaction if the program receives a specified input, like a verified bit of information. An oracle is a computer server that is programmed to scour data feeds to verify whether a user-provided expression is true. Because the oracle is bound by its design to act only as programmed, there is no risk that the oracle would collude with any party as there is with a human arbitrator. Oracles can be programmed to monitor pre-existing data feeds, like official death registries, stock market tickers, weather reports, or indeed anything that can be expressed as structured data.[344] Conceivably, a custom-designed oracle could simply monitor news data feeds, such as

---

342. Substituting Bitcoin for a trusted third party will likely meet the demand of a wide range of sellers and merchants. A popular use of a third party financial institution today is to ensure delivery and payment among anonymous parties using a commercial letter of credit. *See generally* SOLUTIONS FOR EXPORTERS: AN EXPORTER'S GUIDE TO GLOBAL TRADE SERVICES, BANK OF AMERICA, MERRILL LYNCH 12-21 (2013), http://corp.bankofamerica.com/documents/16303/74434/ exporter.pdf; *See also* U.C.C. § 5-108(b) (requiring an issuer of a letter of credit to honor by payment); 5-102(a)(3) (defining beneficiary as the party that the issuer of a letter is required to pay upon presentation of documents); 5-102(a)(8) (defining honor as being satisfied by payment).

343. For a deeper explanation of oracles, *see* Mike Hearn, *Contracts - Example 4: Using external state*, BITCOIN WIKI (Aug. 31, 2014), https://en.bitcoin.it/wiki/Contracts#Example_4:_Using_external_state.

344. For instance, private companies may opt to create data sources that are specifically designed to be used by those companies' oracles.

Google News, looking for keywords that confirm some arbitrary event. Depending on the information that the oracle receives, the program will sign its own unique key to the transaction to send bitcoins to the corresponding address. One early variant of the oracle concept, Reality Keys, combines a distributed keypair service with their centrally-managed data feeds that users can combine to create custom Bitcoin contracts.[345] Eventually, oracles will not require a third-party facilitator like Reality Keys to provide trustless verification of conditional outcomes. If oracles are designed carefully enough, they can be combined with multisignature transactions to virtually eliminate the need to trust a third party in an exchange.

Eventually, the block chain could even serve as a distributed title registry for real world assets through the use of "smart property."[346] Physical, non-BTC assets can be represented on the block chain through the use of "colored coins."[347] Suppose Alice wants to transfer title of her car to Bob using the block chain. Alice can choose to "color" some fraction of a bitcoin to represent her car and serve as a "title" on the block chain. Bob transfers enough bitcoins to Alice to cover the cost of the car and Alice transfers the colored coin that represents the car to Bob. In this simple scenario, Bob and Alice would need to rely on an established legal system to recognize the legitimacy of colored coins in representing property titles. A more complex variation could make smart property titles self-enforcing.[348] Alice could one day attach a chip to the car that serves both as a key and a property title.

One way to do this is to attach a small computer or chip to real world assets that will automatically allow trustless authentication and transfer of ownership. Once Alice transfers the colored coins that represent the car to Bob's wallet, the car's chip will then update its ownership information so that Bob can now open and start the automobile. By adding a programmable chip that communicates with the block chain to a real world asset, that asset can be

---

345. Jon Southurst, *Reality Keys: Bitcoin's Third-Party Guarantor for Contracts and Deals*, COINDESK (Jan. 17, 2014), http://www.coindesk.com/reality-keys-bitcoins-third-party-guarantor-contracts.

346. Nick Szabo, *The Idea of Smart Contracts*, NICK SZABO'S PAPERS AND CONCISE TUTORIALS, 1997, http://szabo.best.vwh.net/idea.html.

347. For a deeper explanation of colored coins, *see* Yoni Assia & Leor Hakim, *Colored Coins - BitcoinX*, WHITE PAPER, https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit (last visited Mar. 21, 2014).

348. Mike Hearn, *Smart Property*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Smart_Property (last visited Mar. 26, 2014).

transferred with the same ease as any bitcoin transaction. Eventually, this concept could be applied to rental concepts, like ZipCar and Car2Go, or other extensions like hotel booking to allow secure and seamless payments and access. While still in early development, the possibilities that smart property creates are innovative and unprecedented.

B. Decentralized Applications

While the Bitcoin block chain could theoretically facilitate these complex transactions, some in the Bitcoin community have expressed doubts that the block chain can easily scale to accommodate these services without slowing or hindering other core functions.[349] One solution that has been proposed is a federated server system and software library known as Open Transactions,[350] which its creator colorfully describes as "PGP for money."[351] Open Transactions allows users to employ a full and working implementation of Chaumian blinded tokens.[352] To briefly summarize, the Open Transactions system uses multisignature transactions, triple entry accounting,[353] and Truledger receipt systems[354] to regulate bitcoin deposits and transfers throughout a federated system of servers.[355] This federated model, along with Open Transaction's digital software library of complex transactions available for users to employ,[356] allows Bitcoin users, and indeed the users of any digital currency or representation of real world assets, to harness complex transactions without the limits of the Bitcoin block chain or the need to trust any one third party. It is best thought of as an independent, compatible extension of the Bitcoin system

349. Chris Odom, *Chris Odom on OpenTransactions*, SOUNDCLOUD (Jan. 25, 2014), https://soundcloud.com/mindtomatter/miami-2014-chris-odom-on-1.

350. *Id.*

351. *Open Transactions*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Open_Transactions (last visited Oct. 23, 2014).

352. Mark Ryan, *Digital Cash*, U. BIRMINGHAM, http://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/DigitalCash.html (last visited Oct. 23, 2014).

353. Ian Grigg, *Triple Entry Accounting*, SATOSHI NAKAMOTO INSTITUTE (Dec. 25, 2005), http://nakamotoinstitute.org/literature/31/html.

354. Bill St. Clair, *Truledger in Plain English*, WHITE PAPER (2008), http://nakamotoinstitute.org/literature/32/html.

355. Justus Ranvier, *Voting Pools: How to Stop the Plague of Bitcoin Heists, Thefts, Hacks, Scams, and Losses*, BITCOINISM (Dec. 6, 2013), http://bitcoinism.blogspot.com/2013/12/voting-pools-how-to-stop-plague-of.html.

356. *List of Classes*, OPEN-TRANSACTIONS, http://opentransactions.org/wiki/index.php?title=List_of_Classes (last visited Mar. 26, 2014).

that uses federated servers to communicate complex transactions to the block chain.

Like the Bitcoin protocol, the Open Transactions system does not require a trusted third party to facilitate transactions and does not contain a single point of control that can be shut down. While the Open Transactions project was in development before Bitcoin's release, both projects' functions and philosophies are very compatible. Indeed, Open Transactions is merely one of several ongoing projects that aim to provide higher functionality to the Bitcoin protocol. Other "Bitcoin 2.0" projects that are in various phases of development include Mastercoin,[357] Counterparty,[358] and Ethereum.[359] Each project differs in terms of the tools and specific functions that are prioritized, but they all aim to extend the Bitcoin protocol or their own block chain's capabilities to asset exchange, complex financial instruments, and even real world assets.

This is where things get interesting. These three tools—multisignature transactions, real world asset registration on the block chain, and programmable contracts—can be combined with other cryptographic and peer-to-peer programs to allow for, *inter alia*, distributed securities exchanges, prediction markets, and gambling. Not only do Bitcoin and Bitcoin-related technologies disintermediate payment processors and money transfer systems like PayPal, Visa, and Western Union, they also have the potential to disintermediate the kinds of services provided by the NYSE, Intrade, or Mega Millions. In the following sections we will briefly survey each potential application to provide an idea of what is possible without going into too much technical detail.

1.   Securities Exchanges

We begin by looking at how Bitcoin and Bitcoin-related technologies can be used to create a securities exchange that is not controlled or operated by any central third party, whether registered and regulated or not. Let's say Alice wants to start a Bitcoin miner manufacturing company. She has a strong background in chip

---

357. J.R. Willet, Maran Hidskes, David Johnston, Ron Gross, Marv Schneider, & Peter Todd, *The Master Protocol / Mastercoin Complete Specification*, WHITE PAPER VERSION 0.4.5.1 SMART PROPERTY FUNDRAISERS EDITION, https://github.com/mastercoin-MSC/spec (last visited Mar. 26, 2014).

358. PhantonPhreak, *The Counterparty Protocol*, WHITE PAPER, https://github.com/PhantomPhreak/Counterparty (last visited Mar. 26, 2014).

359. Vitalik Buterin, et al., *A Next Generation Smart Contract and Decentralized Application Platform*, ETHEREUM WHITE PAPER, https://github.com/ethereum/wiki/wiki/White-Paper (last visited Mar. 26, 2014).

design and wants to manufacture and sell dedicated Bitcoin mining hardware as a business, and she wants to raise capital by selling shares of Alice's Mining Company. Having observed several instances of fraud or mismanagement on some of the centralized Bitcoin-denominated stock market platforms, Alice decides that she would like to bypass these third party platforms and sell shares of her company using multisignature transactions and programmable contracts.

First, Alice creates a verified identity for her company through a distributed naming service like Namecoin[360] or Keyhotee.[361] All addresses and pseudonyms that are associated with Alice's Mining Company are tied to this one verified identity that only Alice (or anyone with whom she shares her private key) can control. This provides prospective customers and investors with a credible identity on which she can build (or destroy) her company's reputation.

Next, Alice needs to identify and connect with prospective investors. Since Alice is not using a centralized trading platform, she cannot use the messaging spaces of such a platform to broadcast offers and discover investors. Fortunately, a number of alternative, non-centralized messaging spaces exist. Alice can broadcast shares of her company for sale on the #bitcoin-otc open order book[362] or can create a broadcast on the peer-to-peer messaging space Bitmessage.[363] These messaging spaces allow buyers and sellers to connect without the need for a third party platform to oversee the exchange. Alice can provide details about her business plan, growth projections, dividend schedule, and other relevant information to prospective buyers.

After drumming up enough investors, Alice can create a custom algorithmic contract that reflects the terms negotiated with her shareholders through the Open Transactions software library.[364] This may take the form of colored coins representing shares of the company, a programmable and algorithmically self-enforcing

---

360. David Gilson, *What are Namecoins and .bit Domains?*, COINDESK (Jun. 18, 2013), http://www.coindesk.com/what-are-namecoins-and-bit-domains.

361. Daniel Larimer, *Introduction to Keyhotee*, YOUTUBE (Oct. 24, 2013), http://www.youtube.com/watch?v=3pZaTdEtK-8.

362. *OTC Order Book*, #BITCOIN-OTC, http://bitcoin-otc.com/vieworderbook.php (last visited Mar. 26, 2014).

363. Jonathan Warren, *Bitmessage: A Peer-to-Peer Authentication and Delivery System*, BITMESSAGE (Nov. 12, 2012), https://bitmessage.org/bitmessage.pdf.

364. *Smart Contracts*, OPEN TRANSACTIONS, http://opentransactions.org/wiki/index.php?title=Smart_contracts (last visited Mar. 26, 2014).

contract shared among all shareholders,[365] or even old-fashioned physical documents representing shares. Whatever the form of the contract, Open Transactions and the Bitcoin block chain provide Alice with a number of options to publicly and credibly commit the parties to their agreed-upon financial stakes in Alice's Mining Company. Shareholders can buy or sell after market shares of Alice's Mining Company through #bitcoin-otc or Bitmessage. Alice might decide to broadcast an order book specifically for her company shares to streamline trading. Alternatively, another individual may list market activity for shares of Alice's Mining Company among a public broadcast of stock market indices.

Block chain technologies, therefore, potentially make it possible to issue stock and raise capital without the need for a centralized exchange. This has interesting implications for law and regulations that today only anticipate centralized stock exchanges.

2. Predictions Markets

Similarly, Bitcoin and Open Transactions users can buy or sell predictions without the need to remain within a centralized third party platform—that is, users can trade event contracts directly, without the need for an Intrade-type service. Let's say that Alice wishes to bet on the future price of Google stock.[366] Alice broadcasts a message to Bitmessage stating that she thinks the price of Google stock will rise by 20 percent by six months from that day and that she is willing to wager 0.5 BTC on her prediction. Other users can browse public feeds to find potentially lucrative bets. Since Bitmessage, like Bitcoin, is a pseudonymous system, users can post and enter into bets without knowing the identity of the party or parties on the other side. Those who believe that the price of Google stock will behave differently than the bet that Alice proposes can respond to Alice's message that they would like to enter the bet.

One easy way to facilitate this bet is to create a smart contract on Open Transactions that includes an oracle as a party to the

---

365. This concept is known as a "decentralized autonomous corporation" (DAC) or a "decentralized autonomous organization" (DAO). Vitalik Buterin's series for Bitcoin Magazine describes in detail the hypothetical forms and functions that DACs could take. *See* Vitalik Buterin, *Bootstrapping A Decentralized Autonomous Corporation: Parts I-III*, BITCOIN MAG. (Sept. 19, 2013), http://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i.

366. Jerry Brito, *Bitcoin: More than Money*, REASON MAG. (Dec. 2013), *available at* http://reason.com/archives/2013/11/19/bitcoin-more-than-money.

exchange. Alice, the initiator of the bet, creates a smart contract on Open Transactions to codify and enforce the bet. Each party to the bet enters into the contract along with the oracle. Bettors send their wagers to a multisignature address and agree that the bet will close at a certain date. On the closing day, the oracle will consult a pre-determined price feed, like NASDAQ, to determine which party is correct about the price of Google stock. The oracle will then automatically provide the needed signature to the transaction so that the "pot" goes to winner of the bet.

This basic example involves at least two persons monitoring for bets and engaging directly in discussions via messaging in order to enter into a bet, but this process can be automated.[367] Alice, for instance, could write a program to automatically browse broadcast feeds and enter into prediction trades that fall within some pre-determined range. If enough bettors prefer using these autonomous programs to automatically trade certain bets, it is possible that many or most of the trades made on decentralized prediction markets will come from these programs acting on their creator's behalf.

Predictions are not just useful for the individuals who believe that they can profit from their special knowledge, but also from observers who can use this information to inform their own probabilities of the likelihood of certain events. Individuals who wish to view aggregated price information on prediction market questions could program oracles to scour prediction broadcasts and display lists of going predictions and prices. These tools could allow individuals to either trade informational bets to earn potential profits or simply gauge the probabilities of future events by viewing public feeds of prediction market prices. In recognition of some of the informational benefits that publicly-viewable but non-centrally-administered prediction markets can provide, researchers at Princeton University are currently developing a theoretical design for such a system.[368]

These basic tools can allow for a dispersed ecosystem of predictions on subjects ranging from the weather, expected commodity prices, scientific discoveries, or even less savory speculations like assassinations or terrorist attacks. Contracts on heretofore prohibited events, like election outcomes[369] or box office

---

367. Nick Szabo, *The Idea of Smart Contracts*, WHITE PAPER (1997), http://szabo.best.vwh.net/idea.html.

368. Ed Felten, *Bitcoin Research in Princeton CS*, FREEDOM TO TINKER (Nov. 29, 2013), https://freedom-to-tinker.com/blog/felten/bitcoin-research-in-princeton-cs.

369. *See supra* notes 292 to 298 and accompanying text.

revenues,[370] could proliferate. The outcome of any event that can be expressed as structured data readable by an oracle could be fair game for speculation on a distributed prediction market. Like Bitcoin, this ecosystem would contain no central point of control that authorities could shut down to end trading. Also like Bitcoin, distributed prediction markets will challenge the assumptions and methods currently favored by authorities to regulate these activities.

3. Gambling

Gambling, too, could be more fully decentralized through the use of the Bitcoin protocol alone. For example, multisignature transactions can potentially allow for secure multiparty lotteries using the Bitcoin protocol without relying on a trusted third party.[371] A group of researchers from the University of Warsaw have already theoretically described[372] and successfully executed[373] this kind of lottery. They explain:

> [W]e construct protocols for secure multiparty lotteries using the Bitcoin currency, without relying on a trusted authority. By "lottery" we mean a protocol in which a group of parties initially invests some money, and at the end one of them, chosen randomly, gets all the invested money (called the pot). Our protocols can work in purely peer-to-peer environment, and can be executed between players that are anonymous and do not trust each other. Our constructions come with a very strong security guarantee: no matter how the dishonest parties behave, the honest parties will never get

---

370. 7 U.S.C. § 13-1 (2012).

371. *See, e.g.*, Andrew Chi-Chih Yao, *How To Generate And Exchange Secrets*, 27th Annual Symposium on the Foundations of Computer Science, IEEE, 162-67 (1986), *available at* http://www.csee.wvu.edu/~xinl/library/papers/comp/Yao1986.pdf; and Oded Goldreich, Silvio Micali, & Avi Wigderson, *How to Play Any Mental Game: or, A Completeness Theorem for Protocols with Honest Majority*, Nineteenth Annual ACM Symposium on Theory of Computing, 218-29 (1987), *available at* http://www.math.ias.edu/~avi/PUBLICATIONS/MYPAPERS/GMW87/GMW87.pdf.

372. Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski & Łukasz Mazurek, *Secure Multiparty Computations on BitCoin*, CRYPTOLOGY EPRINT ARCHIVE: REPORT 2013/784 (Jan. 13, 2014), http://eprint.iacr.org/2013/784.

373. Blockchain Records of a Three-Party Lottery Performed by the University of Warsaw Researchers: PUTMONEY[A]: https://blockchain.info/tx-index/96946847; PUTMONEY[B]: https://blockchain.info/tx-index/96946887; PUTMONEY[C]: https://blockchain.info/tx-index/96947563; Compute: https://blockchain.info/tx-index/96964833; ClaimMoney[C]: https://blockchain.info/tx-index/96966124.

cheated. More precisely, each honest party can be sure that, once the game starts, it will always terminate and will be fair.[374]

Let's say Alice wishes to initiate a secure multiparty lottery using the Bitcoin protocol. Alice sends a command to the block chain that opens the lottery. She specifies a closing date at which the lottery will end and submits a deposit to the transaction to ensure the lottery. The multiparty lottery generates some secret value "x" that functions as a "winning number" for the gamble. If Alice neglects to announce the winning "x" by the date indicated, Alice's deposit will be distributed among the participants and their gambles will be returned.

Alice can broadcast an announcement for the lottery in a distributed message space like Bitmessage to draw entrants. Each entrant contributes their bets into a common pool that cannot be stolen or transferred by any one player, along with a secret number "s" for each player, which serves as each player's individual "lottery ticket number." On the closing date, Alice sends a command to reveal the winning "x" while the entrants publicly reveal their "s" values. The entrant whose "s" corresponds to the winning "x" wins the pot. The winning entrant is automatically broadcast to the block chain and the winner sends a command to the block chain to claim her winnings. The lottery closes without any risk of theft or fraud.

This construction provides a successfully tested blueprint for a basic distributed lottery using only the Bitcoin block chain in a proof-of-concept test. The authors of this construction indicate that variations on this method could be used to provide complex forms of distributed gambling, like card games and board games, through the Bitcoin block chain. It may not be long before we see the first ever multi-billion dollar global lotteries online. While they may well be unofficial and illegal, they will be cryptographically verifiable and therefore completely fraud-proof.

C. Law and Decentralization

In "A History of Online Gatekeeping," Jonathan Zittrain catalogs how intermediaries serve as the obvious targets of regulation for governments seeking to control information flows on

---

374. Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski & Łukasz Mazurek, *Secure Multiparty Computations on BitCoin*, CRYPTOLOGY EPRINT ARCHIVE: REPORT 2013/784 (Jan. 13, 2014), http://eprint.iacr.org/2013/784.

the Internet.[375] These include ISPs, search engines, payment processors, and DNS registrars. And Jack Goldsmith and Tim Wu have written that content providers cannot evade control by simply avoiding intermediaries because "the elimination of intermediaries is in many cases the same thing as the elimination of the underlying conduct."[376] However, growing decentralization can in fact remove these intermediary points of control, making information even more costly to regulate.

Consider, for example, attempts to control illegal music sharing. Napster emerged as the first mainstream peer-to-peer file sharing system. Its design featured a centralized index, which was the obvious point of control that could be regulated or shut down.[377] That was indeed what happened after the RIAA successfully sued Napster for contributory copyright infringement.[378] But of course, that is not where the story ends. Napster's demise saw the rise of new file-sharing systems that did not use a centralized index.[379] These included FastTrack, Gnutella, and eventually BitTorrent, which is completely decentralized.[380] As a result, the cost of policing and controlling illegal file sharing became exponentially higher. The same may happen to bitcoin-denominated exchanges, prediction markets, and gambling.

Decentralized peer-to-peer technologies are increasingly removing layers of intermediation by avoiding centralized servers that can be regulated or shut down. Despite what Goldsmith and Wu suggest, a peer-to-peer system can eliminate intermediaries without eliminating the underlying conduct. As a result, fewer intermediary points of control will further raise the costs of controlling information while also reducing the costs of sharing it.

Bitcoin's decentralized nature already makes controlling simple payments difficult if not impossible. After WikiLeaks released the Cablegate memos, financial intermediaries including MasterCard and Visa refused to process donations for the group,

---

375. Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 253-65 (2006), *available at* http://dash.harvard.edu/bitstream/handle/1/4455491/Zittrain_History%20of%20Online%20Gatekeeping.pdf?sequence =1.-298.

376. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET 69 (2006).

377. Annemarie Bridy, *Is Online Copyright Enforcement Scalable*, 13 VAND. J. ENT. & TECH. L. 695, 699-701 (2011), *available at* http://www.jetlaw.org/wp-content/journal-pdfs/Bridy_PDF.pdf.

378. *Id.*

379. *Id.*

380. *Id.*

and PayPal froze the organization's account.[381] They did so likely under political pressure. WikiLeaks began accepting bitcoin donations in 2011,[382] and today such a financial embargo would be much more difficult. In the future, it may well be more than just simple payments that Bitcoin will make difficult to control.

This is a new world for policymakers. In the past, to achieve a public policy goal, they only needed to regulate a handful of intermediaries. The perceived benefits of the public policy goal very often outweighed the cost associated with regulating the few intermediaries. If there are no intermediaries, but only thousands or millions of users interacting peer-to-peer, then the costs of enforcement may well outweigh any perceived potential benefits of regulation. In this new world, regulators should take into consideration the increasingly high cost of information control into their cost-benefit calculus. Doing so may lead policymakers to conclude that efforts to control only make sense as a last resort.

If top-down regulation is increasingly not a cost-beneficial option for achieving public policy goals, policymakers will have to consider realistic alternatives, such as focusing on resiliency and adaptation. These are concepts borrowed from biology and ecology. Resilience is the capacity of an ecosystem to recover quickly from a shock,[383] while adaptation is the change an organism or species undergoes to become better suited to a new environment.[384] In several works, Adam Thierer has applied these concepts to information technology as alternatives to precautionary regulation or prohibition, either of technology or information.[385]

Thierer develops a continuum of possible responses to technological risks, with adaptation at the bottom, followed by resiliency and anticipatory regulation, and ending with prohibition at the top.[386] He argues quite convincingly that the best approach

---

381. Andy Greenberg, *Visa, MasterCard Move to Choke WikiLeaks*, FORBES (Dec. 7, 2010), http://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/.

382. Andy Greenberg, *WikiLeaks Asks for Anonymous Bitcoin Donations*, FORBES (Jun. 14, 2011), http://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations.

383. *Resilience (Ecology)*, WIKIPEDIA, http://en.wikipedia.org/wiki/Resilience_(ecology) (last visited Oct. 23, 2014).

384. *Adaptation*, WIKIPEDIA, http://en.wikipedia.org/wiki/Adaptation (last visited Oct. 23, 2014).

385. Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J.L. SCI. & TECH. 309 (2013), *available at* http://purl.umn.edu/144225.

386. *Id.* at 356-57.

2014]

for policy makers confronted with a new and potentially risky technology is to take a "bottom-up" approach, employing first adaptation and then resiliency strategies before considering anticipatory regulation or prohibition.[387] The alternative—a precautionary principle for information—would be too costly and trade too much potential innovation for safety, he argues.[388]

For our purposes, we need not make any normative claims about "top-down" responses to unwanted information or behaviors in order to apply Thierer's model. We need only note that if prohibition and regulation become too costly, the next best options for policymakers will be resilience and adaptation. The music industry's recent experience with online piracy presents an example of resiliency and adaptation.

Confronted with a threat to its business from new online technologies, the music industry at first engaged in a strategy of information control. It sued prominent file-sharing service Napster out of existence,[389] and then also pursued individual file-sharers.[390] These efforts did not succeed in containing the threat. BitTorrent, a decentralized and difficult-to-control network protocol, became the new file-sharing standard, and the campaign of suits against individuals was ended after it resulted in little more than widespread consumer resentment. Today, the industry continues to pursue new information control regimes, such as the proposed Stop Online Piracy Act, but it has also begun to adapt to a new environment where such control is extremely difficult.

Music producers have begun to shift what they monetize away from easily copied music, to difficult-to-replicate performances and branded goods.[391] As Mark Raustalia and Christopher Sprigman point out, concert ticket sales tripled in value from $1.5 billion to $4.6 billion between 1999 and 2009, just as the record labels' revenues were plummeting.[392] The result of this changing landscape may be that some species in the music ecosystem, such as the labels, will not survive. However, those who do adapt, especially

---

387. *Id.*

388. *Id.* at 361.

389. David Kravets, *Dec. 7, 1999: RIAA Sues Napster*, WIRED MAG. (Dec. 7, 2009), *available at* http://www.wired.com/2009/12/1207riaa-sues-napster/.

390. Donald Harris, *The New Prohibition: A Look at the Copyright Wars Through the Lens of Alcohol Prohibition*, 80 TENN. L. REV. 101 (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2095193.

391. KAL RAUSTALIA & CHRISTOPHER SPRIGMAN, KNOCKOFF ECONOMY 222 (2012).

392. *Id.* at 183 ("Total revenues from live shows grew from $7.3 billion in 2006 to $10.3 billion in 2011.").

independent artists, may thrive better than ever, and we see evidence of this.[393] More persons make their living as musicians today than ever before, and thanks in large part to the Internet, there is more music available today from more artists than ever. The music industry will therefore likely adapt without having to resort to information control.

One can imagine the same kind of adaptation in other contexts. Larry Downes notes that concerns about privacy are often the result of how quickly new information technologies can disrupt traditional patterns of information access and use.[394] "Still, after the initial panic," he writes, "we almost always embrace the service that once violated our visceral sense of privacy."[395] It happened with the introduction of cameras 100 years ago,[396] and more recently with the introduction of ad-supported Gmail.[397] In the security context, governments and private firms have been largely unable to control distributed denial of service attacks, but solutions have emerged that allow a victim to deflect or more easily absorb attack traffic.[398]

The point is not that policymakers should give up once intermediary control becomes ineffectual; quite the contrary. It is that in the face of a new technological reality that cuts off certain choices, policymakers should be prepared not to fight against the new reality, but instead to discover and pursue strategies consistent with the new reality.

As Bitcoin and related technologies make gambling, prediction markets, and financial markets decentralized and therefore not easily regulated, policymakers might find that legalizing and normalizing these activities, along with promoting education, may yield better public policy outcomes than trying to wage losing battles. They might also find that some of the rationales for regulation no longer apply in a decentralized and

---

393. Michael Masnick & Michael Ho, *The Sky is Rising: A Detailed Look at the State of the Entertainment Industry*, FLOOR64 (Jan. 2012), *available at* https://www.documentcloud.org/documents/562830-the-sky-is-rising.html.

394. Larry Downes, *A Rational Response to the Privacy "Crisis,"* CATO INST. POL'Y ANALYSIS No. 716 (Jan. 7, 2013), *available at* http://www.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf.

395. *Id.*

396. Adam Thierer, Privacy Law's Precautionary Principle Problem, 66 ME. L. REV. 486, 482 (2014), *available at* http://www.mainelawreview.com/wp-content/uploads/2014/06/05-Thierer.pdf.

397. Adam Thierer, *The Pursuit of Privacy in a World Where Information Control is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 420 (2013), *available at* http://www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_409_Thierer.pdf.

398. Prolexic — *see* JOSEPH MENN, FATAL SYSTEM ERROR (2010).

disintermediated context. For example, gambling and market regulations are often aimed at protecting consumers by attempting to eliminate information asymmetries, but because decentralized peer-to-peer exchanges have no intermediaries, and because they are inherently public and transparent, there can be no such asymmetry.

V. Conclusion

Bitcoin presents a unique challenge to policymakers. To date, Bitcoin-related regulation has largely been focused on the application of "know your customer," anti-money-laundering rules, as well as consumer protection licensing, on these new intermediaries. The next major wave of Bitcoin regulation will likely be aimed at financial instruments, including securities and derivatives, as well as prediction markets and even gambling. Following the approach to Bitcoin taken by FinCEN, we conclude that other financial regulators should consider exempting or excluding certain financial transactions denominated in Bitcoin from the full scope of the regulations, much like private securities offerings and forward contracts are treated. We also suggest that to the extent that regulation and enforcement becomes more costly than its benefits, policymakers should consider and pursue strategies consistent with that new reality, such as efforts to encourage resilience and adaptation.