BITCOIN FINANCIAL REGULATION: SECURITIES, DERIVATIVES, PREDICTION MARKETS, & GAMBLING

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

[*] Senior Research Fellow, Mercatus Center at George Mason University. J.D., George Mason University School of Law, 2005; B.A., Political Science, Florida International University, 1999. The authors would like to thank Eli Dourado, Patrick O'Sullivan, and Jeff Garzik for their thoughtful input and Jacob Hamburger for his research assistance.

[**] Associate Professor of Law, New York Law School. B.A. 1998, University of California at Berkeley; J.D. 2002, University of Southern California.

[***] Research Associate, Mercatus Center at George Mason University. B.S., Economics, Florida State University, 2011.

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 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 Commodities and Exchange Act because such derivatives would likely involve physical delivery (as opposed to cash settlement) and would not be capable of being centrally cleared. 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 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. In particular, given that physical settlement of a commodity derivatives transaction likely means that it is excluded from regulation by the Commodities Futures Trading Commission, virtual settlement of Bitcoin transactions should likewise trigger a lighter regulatory framework. 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 adaption.

This Article is structured as follows. Part I presents a brief sketch of the 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, 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.

I. BITCOIN AND THE FIRST WAVE OF REGULATION

Bitcoin is a new Internet protocol, a peer-to-peer network, and a digital currency unit. Following the protocol, the network operates to maintain a global public ledger of bitcoin transactions.[1] As we will see in later sections, there are many different applications that this technology enables. To date, however, it is simple payments and money transfer that has captured the public's imagination, and it is therefore 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."[2] While that description is accurate, it can be misleading because it is at once 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).[3] 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.[4]

Virtual or digital currencies are nothing new. From in-game currencies like World of Warcraft Gold[5] or Linden Dollars,[6] to vendor-specific

[1] Lowercase vs. uppercase

[2] Francois R. Velde, Bitcoin: A Primer, 317 *Chicago Fed Letter* (2013).

[3] Jerry Brito & Andrea Castillo, Bitcoin: A Primer for Policymakers, (1st ed. 2013).

[4] Jerry Brito, It's More Than Money, Cato Unbound, July 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 Magazine, February 24, 2014, http://reason.com/archives/2014/02/24/is-bitcoin-the-key-to-digital-copyright.

[5] Laurence H.M. Holland, Making Real Money in Virtual Worlds, Forbes Magazine, August 7, 2006, http://www.forbes.com/2006/08/07/virtual-world-

currencies like Facebook Credits,[7] Microsoft Points,[8] 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. What makes Bitcoin unique is that unlike all digital currencies that preceded it, a central authority, such as a company or government, does not issue Bitcoin and no central authority is required to verify a transfer from one individual to another.[9] Instead, Bitcoin employs cryptography and peer-to-peer networking to eliminate the need for third parties.[10] Comparing Bitcoin to traditional payments and money transfer systems helps explain the distinction.

Before Bitcoin's invention in 2008, online transactions always required a trusted third-party intermediary.[11] 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 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,[12] and 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.

---

jobs_cx_de_0807virtualjobs.html.

[6] Spencer Reiss, Virtual Economics, MIT Technology Review, December 1, 2005, http://www.technologyreview.com/article/404979/virtual-economics/.

[7] Miguel Helft, Facebook Hopes Credits Make Dollars, New York Times (New York), September 23, 2010 at B1.

[8] Ben Gilbert, Microsoft Points from Xbox 360 transfer to Xbox One as real money, 'equal or greater in Marketplace value,' Engadget, June 12, 2013, http://www.engadget.com/2013/06/12/microsoft-points-conversion-xbox-one/.

[9] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, *White Paper*, (2008).

[10] Id.

[11] Jerry Brito & Andrea Castillo, Bitcoin: A Primer for Policymakers, (1st ed. 2013).

[12] David Chaum, Achieving Electronic Privacy, Scientific American Magazine (New York), August 1992, at 96–101.

Bitcoin does this by distributing the necessary ledger among all the users of the system via a peer-to-peer network. Every transaction that occurs in the Bitcoin network is registered in a distributed public ledger, which is 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 double-spending is prevented, through the clever use of public-key cryptography.[13] 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. When Alice decides to transfer bitcoins to Bob, she creates a message, called a "transaction," which contains and Bob's public key and how many coins she is sending. 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. Public-key cryptography ensures that all computers in the network have a constantly updated and verified record of all transactions within the Bitcoin network, which prevents double-spending and fraud.

Out of technical necessity, transactions on the Bitcoin network are not denominated in dollars or euros or yen as they are on PayPal, but are instead denominated in bitcoins. This makes it 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 as is 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 a algorithmically pre-determined rate baked into the protocol.[14]

---

[13] Christof Paar, Jan Pelzl, and Bart Preneel, *Introduction to Public-Key Cryptography*, in Understanding Cryptography: A Textbook for Students and Practitioners, ch. 6 (Christof Paar and Jan Pelzl, eds., New York: Springer 2010). (New York: Springer, 2010), *sample available at* http://wiki.crypto.rub.de/Buch/download/Understanding -Cryptography-Chapter6.pdf.

[14] 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:

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 is a central authority needed to verify 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.[15] 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 from Overstock.com[16] to the Sacramento Kings[17] to WordPress.com[18] have begun accepting payment in bitcoin, and startups like BitPesa plan to use the Bitcoin network to facilitate international remittances.[19] By disintermediating traditional financial networks like PayPal, Visa, and Western Union, Bitcoin offers three main advantages: 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,[20] and the

---

Brito & Castillo; Velde.

[15] Alex Liu, Beyond Bitcoin: A Guide to the Most Promising Cryptocurrencies, Motherboard, November 29, 2013, http://motherboard.vice.com/blog/beyond-bitcoin-a-guide-to-the-most-promising-cryptocurrencies.

[16] Cade Metz, The Grand Experiment Goes Live: Overstock.com Is Now Accepting Bitcoins, Wired Magazine, January 9, 2014, http://www.wired.com/business/2014/01/overstock-bitcoin-live/.

[17] Cade Metz, Sacramento Kings Crowned First Pro Sports Team to Accept Bitcoin, Wired Magazine, January 16, 2014, http://www.wired.com/business/2014/01/sacramento-kings-bitcoin/.

[18] Jon Matonis, What's Your Bitcoin Strategy? WordPress Now Accepts Bitcoin Across the Planet, Forbes Magazine, November 16, 2012, http://www.forbes.com/sites/jonmatonis/2012/11/16/whats-your-bitcoin-strategy-wordpress-now-accepts-bitcoin-across-the-planet/.

[19] Richard Boase, BitPesa Uses Bitcoin to Slash Kenyan Remittance Costs, CoinDesk, November 28, 2013, http://www.coindesk.com/bitpesa-uses-bitcoin-slash-kenyan-remittance-costs/.

[20] Paul Downs, What You Need to Know About Credit Card Processing, New York Times, March 25, 2013, http://boss.blogs.nytimes.com/2013/03/25/what-you-need-to-know-about-credit-card-processing/.

average cost of international remittances is 8.5 percent,[21] a Bitcoin transaction can cost less than 1 percent.[22] Second, Bitcoin transactions can be much faster. For example, while international wire transfers can take days to complete, Bitcoin transactions take roughly ten minutes.[23] 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,[24] such transactional prior restraint would not be possible on the Bitcoin network because there is no intermediary.

Bitcoin is in many ways a disruptive technology,[25] and sensing a great profit opportunity venture capitalists and entrepreneurs are at present 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[26] and crowdfunding,[27] 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[28] and Russia.[29]

---

[21] World Bank, Remittance Prices Worldwide, accessed March 26, 2014, http://remittanceprices.worldbank.org/.

[22] Note that the tradeoff for the low transaction costs of a bitcoin transaction is the lack of insurance and perks that are paid for with traditional payment systems' higher fees.

[23] Average transaction times are viewable at: blochain.info, Average Transaction Confirmation Time, accessed March 26, 2014, http://blockchain.info/charts/avg-confirmation-time.

[24] Kevin Poulsen, PayPal Freezes WikiLeaks Account, Wired Magazine, December 4, 2010, http://www.wired.com/threatlevel/2010/12/paypal-wikileaks/.

[25] Timothy Lee, Bitcoin is a Disruptive Technology, Forbes Magazine, April 9, 2013, http://www.forbes.com/sites/timothylee/2013/04/09/bitcoin-is-a-disruptive-technology/.

[26] Pete Rizzo, Bitcoin Micropayments Get Big Moment as Chicago Sun-Times Paywall Experiment Goes Live, CoinDesk, February 1, 2014, http://www.coindesk.com/micropayments-chicago-sun-times-paywall-live/.

[27] Eric Blattberg, Crowdtilt launches free, open source crowdfunding solution and it supports Bitcoin, VentureBeat, February 20, 2014, http://venturebeat.com/2014/02/20/crowdtilt-launches-free-open-source-crowdfunding-solution-and-it-supports-bitcoin/.

[28] Max Raskin, Dollar-Less Iranians Discover Virtual Currency, BusinessWeek, November 29, 2012, http://www.businessweek.com/articles/2012-11-29/dollar-less-

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.[30]

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 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 FinCEN's regulations implementing the Bank Secrecy Act.[31] As a result, such businesses are obligated to register with FinCEN as money services businesses (MSBs) and comply with "know your customer" rules, put in place robust anti-money-laundering programs, and file Suspicious Activity Reports.[32]

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.[33] 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.[34] 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

---

iranians-discover-virtual-currency.

[29] Russian authorities say Bitcoin illegal, Reuters, February 9, 2014, http://www.reuters.com/article/2014/02/09/us-russia-bitcoin-idUSBREA1806620140209.

[30] Eli Dourado, Can the War on Drugs Bootstrap Bitcoin?, blog post, June 4, 2011, http://elidourado.com/blog/can-the-war-on-drugs-bootstrap-bitcoin/.

[31] US 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, March 18, 2013), http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

[32] Id.

[33] Marco Santori, Bitcoin Law: Money transmission on the state level in the US, CoinDesk, September 28, 2013, http://www.coindesk.com/bitcoin-law-money-transmission-state-level-us/.

[34] Greg Farrell, N.Y. Subpoenas Bitcoin Firms in Probe on Criminal Risk, Bloomberg, August 12, 2013, http://www.bloomberg.com/news/2013-08-12/n-y-regulator-subpoenas-firms-over-bitcoin-crime-risks.html.

new "BitLicense" tailored specifically for virtual currencies.[35]

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.[36] According to the seizure warrant, the company had not registered with FinCEN as a money services businesses and had stated in its bank application that it was not engaged in money services.[37] 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.[38] 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.[39]

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.[40] Other federal regulators are also developing guidance to explain how their regulations apply to Bitcoin. For example, the Federal Election Commission

---

[35] Cater Dougherty, New York Vying With California to Write Bitcoin Rules, Bloomberg, January 27, 2014, http://www.bloomberg.com/news/2014-01-27/new-york-duels-california-to-write-bitcoin-rules.html.

[36] 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.

[37] Seizure Warrant – In the Matter of the Seizure of The contents of one Dwolla account (D. Md. May 14, 2013) (13-1162 SKG), http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-Gox-Dwolla-Warrant-5-14-13.pdf.; Affidavit in Support of Seizure Warrant (D. Md. May 9, 2013) (13-1085SAG), http://thegenesisblock.com/wp-content/uploads/2013/08/Gox-Wells-Fargo-Seizure-Warrant.pdf.

[38] Sealed Complaint – United States of American v. Robert M. Faiella, a/k/a "BTCKing," and Charlie Shrem, No. 14-MAG-0164 (S.D.N.Y. January 24, 2014), http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR/Faiella, %20Robert%20M.%20and%20Charlie%20Shrem%20Complaint.pdf.

[39] Id.

[40] Department of Treasury Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001, January 30, 2014, http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf; Department of Treasury Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, FIN-2014-R002, January 30, 2014, http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf.

has been looking at the question of bitcoin campaign contributions,[41] and the Internal Revenue Service recently issued guidance on the tax treatment of bitcoins.[42] 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, looking at Bitcoin-related financial instruments and markets.

II. Regulation of Bitcoin-Related Financial Instruments

There is some debate about whether bitcoins qualify as currency, securities, commodities, or a new asset class altogether.[43] Whatever the answer, the fact is that as the Bitcoin economy develops one should expect to see demand for Bitcoin-related financial instruments to emerge, and 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.[44] 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.[45] In that time, the price reached a high of $1,147.25 on December 4th, and experienced single-day gains of $198.09,[46] and losses of $208.[47] This volatility obviously presents a

[41] Benjamin Goad, FEC: No bitcoins in federal campaigns, The Hill, November 21, 2013, http://thehill.com/blogs/regwatch/technology/191096-fec-no-bitcoins-in-federal-campaigns.

[42] John D. McKinnon and Ryan Tracy, IRS Says Bitcoin Is Property, Not Currency, Wall Street Journal, March 25, 2014, http://online.wsj.com/news/articles/SB10001424052702303949704579461502538024502.

[43] Reuben Grinberg, Bitcoin: An Innovative Alternative Digital Currency, *4 Hasting Sci.& Tech. L.J.* 160 (2011).

[44] Law Library of Congress, Global Legal Research Center, Regulation of Bitcoin in Selected Jurisdictions, Report for Congress, LL File No. 2014-010233, January 2014, http://www.hsgac.senate.gov/download/regulation-of-bitcoin-in-selected-jurisdictions.

[45] 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, accessed March 27, 2014, http://www.coindesk.com/price/#2012-12-31,2013-12-30,close,bpi,USD.

[46] Gains for trades between the closing prices on November 17 and November 18, 2013. See: Bitcoin Price Index Chart, CoinDesk, accessed March 27, 2014,

challenge to anyone looking to transact using Bitcoin.

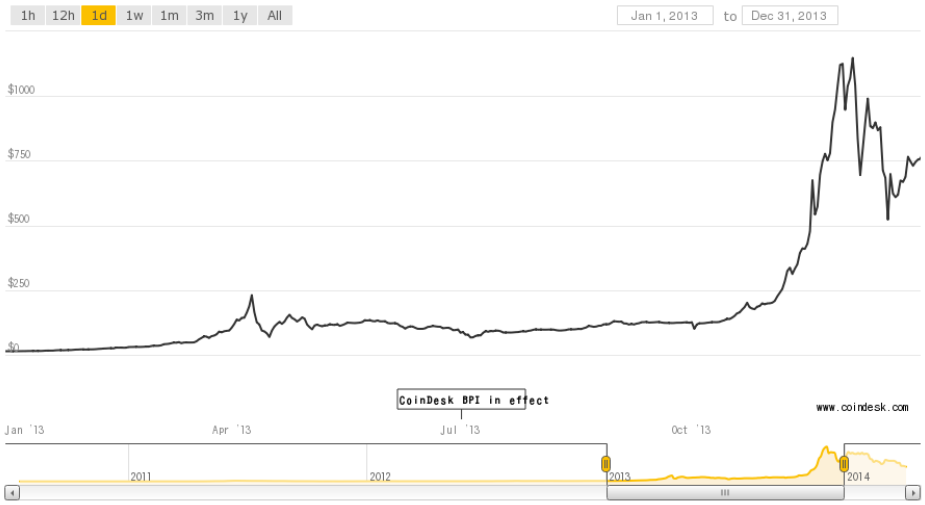

Figure 1 *– Bitcoin-dollar exchange rate for 2013.*

There is nothing inherently volatile about Bitcoin, however.[48] Its volatility is likely attributable to the fact that it is a new currency, still in the process of discovering its stable price.[49] Additionally, as a nascent currency, it is very thinly traded and as a result a single large-enough 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.

Despite this volatility, tens of thousands of merchants accept bitcoins for payment.[50] The reason is that while Bitcoin's present volatility may

---

http://www.coindesk.com/price/#2012-12-31,2013-12-30,close,bpi,USD.

[47] Losses for trades between the closing prices on December 5 and December 6, 2013. See: Bitcoin Price Index Chart, CoinDesk, accessed March 27, 2014, http://www.coindesk.com/price/#2012-12-31,2013-12-30,close,bpi,USD.

[48] 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, blog, January 20, 2014, http://elidourado.com/blog/bitcoin-volatility/.

[49] Timothy B. Lee, These four charts suggest that Bitcoin will stabilize in the future, Washington Post, February 3, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/03/these-four-charts-suggest-that-bitcoin-will-stabilize-in-the-future/.

[50] BitPay Announces Bitcoin Payroll API, BusinessWire, January 13, 2014,

make it an unstable store of value, it can nevertheless serve as an excellent medium of exchange.[51] 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."[52] 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.[53] 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."[54]

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,[55] 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.[56] 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.[57] For its services, Coinbase charges Overstock a fee of about 1%, which is less than the fees associated with other electronic payments such as credit cards.[58]

However, that 1% fee by itself might not be enough to cover the exchange rate risk that Coinbase faces. At the moment, Coinbase is hedging

---

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, December 29, 2013, http://blog.coinbase.com/post/71607045439/new-coinbase-for-android-and-coinbase-merchant-app.

[51] Marc Andreessen, Why Bitcoin Matters, New York Times, January 21, 2014, http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.

[52] Id.

[53] Rob Wile, Bitcoin Is Experiencing Its Longest Stretch of Price Stability In a While, Business Insider, January 29, 2014, http://www.businessinsider.com/bitcoin-volatility-slows-2014-1.

[54] Id.

[55] Will Knight, Show Me the Bitcoins, MIT Technology Review, February 2014, http://www.technologyreview.com/graphiti/524796/show-me-the-bitcoins/.

[56] Cade Metz, The Grand Experiment Goes Live: Overstock.com Is Now Accepting Bitcoins, Wired Magazine, January 9, 2014, http://www.wired.com/business/2014/01/overstock-bitcoin-live/.

[57] Id.

[58] What fees does Coinbase charge for merchant processing?, Coinbase support, February 5, 2014, http://support.coinbase.com/customer/portal/articles/1277919-what-fees-does-coinbase-charge-for-merchant-processing-.

using algorithmic trading.[59] Other merchant services companies, like Founders-Fund-backed BitPay, seem to employ a similar approach.[60] 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.[61] 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 forwards, futures, 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 and Exchange Act (CEA).[62] However, because Bitcoin derivatives would likely involve physical delivery (as opposed to cash settlement) and would not be capable of being centrally cleared, they would not be subject to the full scope of CFTC regulation, if any.

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 specific price.[63] 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 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 forward contract would still require the buyer to sell at what would be below-market prices. Futures contracts are by

[59] Cade Metz, The Grand Experiment Goes Live: Overstock.com Is Now Accepting Bitcoins, Wired Magazine, January 9, 2014, http://www.wired.com/business/2014/01/overstock-bitcoin-live/.

[60] Greg Simon, Exclusive Interview with Bitpay CEO Tony Gallippi, December 28, 2013, http://knowmadiclife.com/blog/2013/12/28/exclusive-interview-with-bitpay-ceo-tony-gallippi.

[61] Cade Metz, The Next Big Thing You Missed: There's a Sure-Fire Way to Control the Price of Bitcoin, Wired Magazine, January 14, 2014, http://www.wired.com/business/2014/01/bitcoin-derivatives/.

[62] CEA, 7 USC §1 et seq.

[63] Futures contract, CFTC Glossary, U.S. Commodity Futures Trading Commission Education Center, accessed March 27, 2014, http://www.cftc.gov/consumerprotection/educationcenter/cftcglossary/; John C. Hull, Options, Futures, and Other Derivatives 6 (6th ed. 2006)

definition highly standardized and trade on exchanges. Accordingly, trading a futures contract requires parties to open an account with a futures exchange and abide by its requirements such a posting collateral when entering the contract (initial margin) and paying more collateral if the market value of the contract decreases (variation margin). This is often done through an intermediary known as a futures commission merchant.

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.[64] 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."[65] The definition of commodity includes interest rates, foreign exchange rates, indices, and even weather events.[66] Futures contracts for commodities are subject to the provisions of the CEA and are regulated by the CFTC and entities that have self-regulatory responsibilities, including exchanges and the National Futures Association (NFA). The key regulatory aspect of futures is that they are standardized with respect to all terms except for price,[67] and can only trade on regulated exchanges.[68]

The CEA categorizes regulated futures exchanges as a type of designated contract market and as such they are required to comply with 23 "core principles."[69] These principles effectively require them to establish

[64] Id. See also *CFTC v. Erskin* (6th Cit. 2008) (defining and distinguishing futures and forwards contracts), http://caselaw.findlaw.com/us-6th-circuit/1106725.html.

[65] 7 U.S.C. § 1a(9). Two interests that fall outside of the definition of commodity include onions and motion picture box office receipts. Id.

[66] *See* CEA Section 1a(19), 7 U.S.C. §1a(19) (defining "excluded commodity" to include a wide range of financial interests); CFTC Glossary, Weather Derivative (definitive "weather derivative" as "A derivative whose payoff is based on a specified weather event, for example, the average temperature in Chicago in January"), http://www.cftc.gov/consumerprotection/educationcenter/cftcglossary/glossary_wxyz.

[67] Under some circumstances a non-standardized contract may be categorized as a futures contract. In re Bybee, 945 F.2d 309, 312-13 (9th Cir. 1991).

[68] CEA § 6(a).

[69] CEA § 5(b-x), 7 USC § 7(d). A DCM 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, CFTC Glossary. http://www.cftc.gov/consumerprotection/educationcenter/cftcglossary/glossary_co; Core Principles and Other Requirements for Designated Contract Markets 77 Fed. Reg. 36612 (CFTC June 19, 2012), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2012-12746a.pdf.

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.[70] Regulated exchanges are available to retail investors. A similar regulatory framework applies to derivatives clearing organizations.[71] 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,[72] introducing brokers,[73] commodity pool operators,[74] and commodity trading advisers.[75] 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.[76]

Bitcoins likely fall under the CEA's broad definition of commodity. Accordingly, any futures contract referencing bitcoins will be subject to the full scope of regulation under the CEA. 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

[70] See also 7 U.S.C. 6g(e) (requiring exchanges to publicly disclose daily trading volume).

[71] 7 USC § 7a-1(c)(2).

[72] CEA 1a(28); 7 USC 1a(28) (defining FCM).

[73] 7 U.S.C. 1a(31) (defining introducing broker).

[74] 7 U.S.C. 1a(11) (defining commodity pool operator); Harmonization of Compliance Obligations for Registered Investment Companies Required to Register as Commodity Pool Operators, 78 Fed. Reg. 52308 (CFTC Aug. 22, 2013).

[75] 7 U.S.C. 1a(12) (defining commodity trading advisor); CFTC v. Equity Financial Group LLP, 572 F.3d 150 (3d Cir. 2009).

[76] 7 U.S.C. 6d(a)(1) (FCM registration requirements); 7 U.S.C. 6d(a)(2) (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) (requiring FCMs and introducing brokers to implement conflicts-of-interest systems); 7 U.S.C. 6g (reporting and recordkeeping requirements for futures commission merchants, introducing brokers, and floor brokers and traders); 7 U.S.C. 6f(c)(2) (risk assessment recordkeeping requirements for futures commission merchants); 7 U.S.C. 6d(g) (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) (registration requirements for CTAs and CPOs); 7 U.S.C. 6o(1) (prohibiting fraud by commodity trading advisers and commodity pool operators); 77 Fed. Reg. 20127-20215 (CFTC Apr. 3 2012) (obligations of futures commission merchants); 7 U.S.C. 6n(3)(A) (recordkeeping requirements for commodity trading advisers and commodity pool operators); 77 Fed. Reg. 11252 (CFTC Feb. 24 2012) (compliance obligations for commodity pool operators and commodity trading advisers).

would have to come into compliance with the wide-ranging and costly regulation required of futures exchanges by the CEA.

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.[77] In a currency forward, for example, one party agrees to trade the currency with another at a later date at a pre-specified exchange rate.[78] Currency forwards are one of the most widely used and liquid financial instruments.[79] Forwards are generally heavily negotiated to be tailored to the specific risks and other terms that parties are concerned about. The distinction between a futures and a forward is not always clear and often depends detailed analysis of the facts and circumstances of the contract. The general distinction is that, compared to futures, forwards are non-standardized, do not trade on an exchange, and are intended for actual delivery of the commodity (as opposed to cash settlement).[80] Other courts have articulated the distinction as being that futures markets are for the sale of contracts while forward markets are for the sale of commodities.[81]

Importantly, forward contracts are not subject to CFTC regulation.[82] The court in *CFTC v. Erskine* explained the underlying policy:

---

[77] Forward Contract, CFTC Glossary, U.S. Commodity Futures Trading Commission Education Center, accessed March 27, 2014, http://www.cftc.gov/consumerprotection/educationcenter/cftcglossary/; Hull, supra note 63, at 3-4.

[78] 7 U.S.C. 1a(24).

[79] Swap, CFTC Glossary, U.S. Commodity Futures Trading Commission Education Center, accessed March 27, 2014, http://www.cftc.gov/consumerprotection/educationcenter/cftcglossary/.

[80] Forward contract, CFTC Glossary, U.S. Commodity Futures Trading Commission Education Center, accessed March 27, 2014, http://www.cftc.gov/consumerprotection/educationcenter/cftcglossary/. See also CFTC v. Erskin (6th Cir. 2008) (defining and distinguishing futures and forwards contracts), http://caselaw.findlaw.com/us-6th-circuit/1106725.html; 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*);* In re Grain Land Cooperative, [2003-2004 Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 29,636 (CFTC Nov. 25, 2003).

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

[82] CEA § 1a(27) (excluding sales "of any cash commodity for deferred shipment or delivery" from the term "future delivery"); U.S. Commodity Futures Trading Com'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").

> 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 . . . 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.[83]

Accordingly, to the extent a contract delivers bitcoins at a date after the sale (and not their cash equivalent), and is being used by a party to manage price risk, it would likely be considered a forward and be excluded from the CEA. Unlike agricultural commodities, bitcoins are easily transferrable between parties. Indeed, it is easier to transfer bitcoins than their cash-equivalent. And unlike financial interests such as interest rates or index prices, bitcoins are not pure intangibles where ownership is not possible.[84] In addition, as a means of payment and other financial services,[85] bitcoins have inherent value. The digital nature of bitcoins along with their near costless transferability suggests that most transactions involving future delivery of bitcoin should be categorized as forwards not futures.

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.[86] 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.[87] 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.[88] 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

[83] CFTC v. v. Ross Erskine, et al., No. 06-3896., (6th. Cir. Jan. 9, 2008), http://caselaw.findlaw.com/us-6th-circuit/1106725.html.

[84] Bitcoins would likely fall under the "exempt commodity" category under the CFTC's regulatory framework, as do precious metals.

[85] For a discussion of the emerging uses of Bitcoin beyond a means of payment, see infra Section III.

[86] Hull, supra note 63, at 149.

[87] 7 U.S.C. 1a(25).

[88] Katy Burne, New Derivative Guards Against Bitcoin's Price Swings, WSJ.com, March 24, 2014.

the value of Bitcoin drops relative to the dollar. Trade a swap that references an index of virtual currencies would be another way to hedge Bitcoin price risk.

The 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.[89] Swaps must be cleared by a regulated central counterparty clearinghouse[90] and be traded on either a designated contract market or a swaps execution facility, unless no designated contract market or swaps execution facility makes the swap available for trading.[91] Swaps contracts are not available to retail investors; parties to a swaps contract must be an eligible contract participant.[92] In practice, parties to a swaps contract will enter a trade with an futures commission merchant who will in turn transact 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.[93] 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.[94] 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.[95] All users of swaps are prohibited from engaging in fraud or manipulative behavior.[96]

---

[89] Further Definition of "Swap," "Security-Based Swap," and "Security-Based Swap Agreement"; Mixed Swaps; Security-Based Swap Agreement Recordkeeping;, 77 Fed. Reg. 48,208 (August 13, 2012).

[90] CEA Section 2(h)(1)(A). 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).

[91] CEA Section 2(h)(8). See also Core Principles and Other Requirements for Swap Execution Facilities, 78 Fed. Reg. 33476 (June 4, 2013), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2013-12242a.pdf.

[92] CEA Section 2(e).

[93] 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).

[94] 76 Fed. Reg. 43,851 (July 22, 2011) (large trader reporting).

[95] CEA Section 2(h)(7)(A), 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.

[95] Melissa Jurgens, Clearing Exemption for Swaps Between Certain Affiliated Entities, 17 CFR Part 50, RIN 3038-AD47 (April 1, 2013) http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/federalregister040113.pdf.

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

As of March 2014, the CFTC has applied the clearing requirement to standard interest rate swaps and certain index credit default swaps.[97] This determination was based on what swaps were actually being cleared by clearing organizations.[98] In addition, the Treasury Department has exempted certain physically settled foreign exchange swaps and forwards from the clearing and trading mandate.[99] 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 decrease systemic risk.[100] It is not clear what swaps the CFTC will determine qualify for an exemption or will subject to mandatory clearing requirement in the future. Uncleared swaps are still subject to mandatory margin requirements. Not all swaps can be cleared in practical or economic sense. Swaps that are capable of being cleared must possess a sufficient degree of standardization and transaction volume.

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 lacking sufficient volume, though they will be uncleared and subject to the margin requirements of uncleared swaps. The Tera Group swap described above fits categorization as an uncleared swap. Nonetheless, Tera is reportedly also seeking regulatory approval for swap that trades on its regulated swaps execution facility, TeraExchange.[101] In addition, to the extent bitcoin swaps are structured to resemble exempted foreign exchange swaps (or forwards), they may likewise be exempted from mandatory clearing and trading.

The use of Bitcoin swaps by merchants is 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 just as they would be exposed to exchange-rate risk from selling products overseas. The commercial end-user exemption may also apply to a wide range of Bitcoin-related business, including those that are built on top of the block chain.

---

[97] Sauntia S. Warfield, Clearing Requirement Determination Under Section 2(h) of the CEA, 17 CFR Parts 39 and 50, RIN 3038-AD86 (November 29, 2012) http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/federalregister112812.pdf.

[98] Id. at 13.

[99] 77 Fed. Reg. 69,694 (Nov. 20, 2012).

[100] Id.

[101] Nermin Hajdarbegovic, Tera Group Hopes to Offer First Bitcoin Swap, Coinbase, March 25, 2014.

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 pre-specified price and only has value if that price is below the market price. A put option works the opposite way.[102] A call option would enable a merchant selling in 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.[103] Accordingly, options are generally regulated as swaps.[104] However, just as CFTC regulation does not reach forwards based largely on their physical delivery of commodities, options that entail physical delivery are likewise exempt from CFTC regulation, but only if they are traded between entities that include financially sophisticated parties and commercial users.[105] Accordingly, bitcoin options used by qualifying entities would be exempt from CFTC regulation because they would likely be structured to involve physical delivery. This means that, as between a merchant and another sophisticated party, the Bitcoin options being offered on Derivabit would not be regulated as swaps because they are structured to result in physical delivery of bitcoins if exercised by the option holder.[106] Ordinary individuals would be prohibited from using Derivabit, however, unless it registered and complied with the rules of a regulated trading venue open to

[102] Hull, supra note 63, at 6.

[103] 7 U.S.C. 1a(47)(A)(i). Definition of "swap" includes options on physical commodities (whether or not traded on a DCM). CEA section 1a(47)(A)(i), 7 U.S.C. 1a(47)(A)(i). The definition of swap excludes options on futures (which must be traded on a DCM. CEA section 1a(47)(B)(i), 7 U.S.C. 1a(47)(B)(i). Options on securities are regulated by the securities laws.

[104] Commodity Options, 77 Fed. Reg. 25320, 25325 (April 27, 2012), ("commodity options will be permitted to transact subject to the same rules applicable to any other swap"), 17 CFR Parts 3, 32, and 33, 77 F.R. 82 (April 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. 25320 (CFTC Apr. 27 2012) (regulating commodity options dealers).

[105] Commodity Options, 77 Fed. Reg. at 25326, 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 25326-25328. Other exempt commodity options include those embedded in forward contracts. See CFTC Division of Market Oversight Responds to Frequently Asked Questions Regarding Commodity Options, (September 30, 2012) https://forms.cftc.gov/_layouts/TradeOptions/Docs/TradeOptionsFAQ.pdf.

[106] Derivabit Guide, (stating that "underlying [Bitcoin] is fully available if the call option holder chooses to exercise the option"), https://derivabit.com/guide.

retail investor (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.

Finally, if Bitcoin is categorized as foreign exchange by the CFTC and offered to retail investors, any foreign exchange futures, options, and options on futures would require the retail investor's counterparty to register as a futures commission merchant or a retail forex dealer.[107]

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. It has been argued that in some respects buying bitcoins is very much like buying shares in a financial services startup.[108] 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.[109] A research note from Bank of America reached a more conservative price target of $1,300 by assuming that Bitcoin takes a 10% share of money transfers and e-commerce transactions.[110] 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.[111]

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

[107] 17 C.F.R. 5.1, 5.3. 17 CFR 5, 76 *F.R.* 176 (September 12, 2011), http://www.cftc.gov/LawRegulation/DoddFrankAct/Rulemakings/DF_20_FXSwaps/index.htm.

[108] Joe Weisenthal, Why Bitcoin Has Value, Dec. 30, 2013, http://www.businessinsider.com/why-bitcoin-has-value-2013-12; Stan Larimer, Bitcoin and the Three Laws of Robotics, Let's Talk Bitcoin!, 2013, http://letstalkbitcoin.com/bitcoin-and-the-three-laws-of-robotics..

[109] Robert McMillan, Silicon Valley VC Thinks a Single Bitcoin Will Be Worth $100,000, Wired Magazine, January 15, 2014, http://www.wired.com/wiredenterprise/2014/01/chrisdixon/.

[110] David Woo, Ian Gordon, and Vadim Iaralov, Bitcoin: a first assessment, Bank of America Merrill Lynch Research Report, December 5, 2013.

[111] Bitcoin Investment Trust Investor Presentation, February 2014, Page 6, http://www.bitcointrust.co/#Deck.

bitcoins can be a laborious affair with little room for error.[112] 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.[113] As a result, entrepreneurs have begun to develop instruments that allow investors to more easily gain 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 Bitcoin Investment Trust (BIT), which is describes as "a private, open-ended trust that is invested exclusively in bitcoin and derives its value solely from the price of bitcoin."[114] According to its investor presentation, it is modeled on the SPDR Gold ETF, but is a private fund open only to accredited investors.[115] The fund was seeded with a $2 million investment by SecondMarket.[116] Meanwhile, Winklevoss Capital is seeking regulatory approval for an exchange traded fund to invest in bitcoins.[117] Such an ETF would be open to any investor seeking exposure to bitcoins and would also have advantages relative to trading bitcoins directly.[118] It could also benefit

[112] Quentin Fottrell, To secure your bitcoins, print them out, Wall Street Journal MarketWatch, February 26, 2014, http://www.marketwatch.com/story/to-secure-your-bitcoins-print-them-out-2014-02-26.

[113] Noel Randewich and Julie Gordon, Bitcoin owners find safe place for digital currency: on paper, Reuters, February 27, 2014, http://www.reuters.com/article/2014/02/28/us-bitcoin-mattress-idUSBREA1R00P20140228.

[114] Simon Foxman, Once again the Winklevoss twins get beaten launching their big idea: a bitcoin trust, Quartz, September 26, 2013, http://qz.com/128442/once-again-the-winklevoss-twins-get-beaten-to-launching-their-big-idea-a-bitcoin-trust/.

[115] Bitcoin Investment Trust Investor Presentation, February 2014, http://www.bitcointrust.co/#Deck.

[116] Emily Spaven, SecondMarket launches Bitcoin Investment Trust, invests $2 million, CoinDesk, September 26, 2013, http://www.coindesk.com/secondmarket-launches-bitcoin-investment-trust-invests-2-million/.

[117] 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 (October 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, February 2, 2014, http://www.bloomberg.com/news/2014-01-30/winklevosses-lawyer-in-talks-with-sec-over-bitcoin-etf.html

[118] Yulia Chernova, Winklevoss Twins Face Competition From SecondMarket's New Bitcoin Trust, Wall Street Journal Venture Capital Blog, September 25, 2013, http://blogs.wsj.com/venturecapital/2013/09/25/winklevoss-twins-face-competition-from-secondmarkets-new-bitcoin-trust/.

Bitcoin by making price discovery much more efficient and transparent.[119]

The Winklevoss Bitcoin ETF is structured as a New York common law trust.[120] 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.[121] 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.[122] The trust's aim is for its shares to achieve a weighted average price of bitcoins minus fees.[123] Its public disclosure document states that the shares of the trust "are designed for investors seeking a cost-effective and convenient means to gain exposure to Bitcoins with minimal credit risk."[124]

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.[125]

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.[126] Although an offering pursuant to Rule 506 does

---

[119] Id.

[120] 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 1, http://www.sec.gov/Archives/edgar/data/1579346/000119312513279830/d562329ds1.htm.

[121] S-1, at i.

[122] S-1, at 1.

[123] S-1, at 1.

[124] S-1, at 2. For other purported benefits of the ETF see pages 37-39.

[125] 15 U.S.C. § 77e (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 (stating general requirements regarding preparation and filing of the registration statement); 15 U.S.C. § 77j (information required in prospectus); Regulation S-K, 17 C.F.R. Part 229 (stating requirements applicable to the content of the non-financial statement portions of registration statements).

[126] 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

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 the 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.[127] 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.[128]

Exchange-traded funds (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.[129] Like public company stock, ETF shares are usually traded through a broker.[130] ETFs invest in, or track, the performance of a wide variety of securities, commodities, and indices, and may actively or passively managed. The potential benefits of ETFs to investors include gaining access to wide range of investments and sectors through a liquid instrument with low fees.[131] ETFs have growth spectacularly in the past decade and by year-end 2012 managed $1.3 trillion in assets.[132] 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.[133] 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

---

for the last two years of at least $200,000 (or $300,000 in joint spousal income). 17 C.F.R. § 230.501(a).

[127] 15 U.S.C. § 77q(a).

[128] 15 U.S.C. § 78j; Rule 10b-5, 17 C.F.R. § 240.10b-

[129] 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) (permitting shares that meet generic exchange listing requirements to be listed without SEC approval), Rule 19b-4. Unique ETFs may require an exchange filing a listing rule for SEC approval.

[130] ETFs also sell creation units to authorized participants.

[131] Investment Company Institute, Investment Company Fact Book (53rd ed., 2013), ch. 3, http://www.icifactbook.org/fb_ch3.html.

[132] Id.

[133] 15 U.S.C. 78a. When it comes to filing a registration statement disclosure, ETFs registered under the Company Act must comply with Form N-1A and ETFs registered under the Securities Act must comply with Form S-1.

Investment Company Act and its regulations.[134] Among other effects, obtaining relief allows an ETF to trade creation units with authorized participants, 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. Creating an ETF may take several months to over a year to obtain the necessary regulatory approval.

Actively managed ETFs are permitted to use derivatives, but such use must be subject to board review and approval and must be disclosed in a manner consistent with SEC guidance.[135] An ETF investing in futures must be registered under the CEA as a commodity pool required to comply with CFTC disclosure requirements.[136] Shares of the Winklevoss Bitcoin ETF are registered under the Securities Act. However, because bitcoins are not regulated as commodity futures or securities, the Winklevoss Bitcoin ETF is not registered under the Company Act and is not a commodity pool under the CEA.[137]

Investment advisers (managers) to funds that invest in Bitcoin ETFs or Bitcoin trusts are regulated by the SEC under the Investment Advisers Act of 1940 (Advisers Act).[138] 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.[139] Investment

[134] Investment Company Act §§ 2(a)(32), 5(a)(1) (requiring require shares of an open-end fund to be redeemable daily); 22(d), 22c-1 (requiring issuers to sell redeemable securities only at the current offering price, and to redeem only at the current NAV); 22(e) (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) (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) (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).

[135] Elizabeth G. Osterman, Moratorium Lift, Securities and Exchange Commission Office of Investment Company Regulation, December 6, 2012, http://www.sec.gov/divisions/investment/noaction/2012/moratorium-lift-120612-etf.pdf.

[136] 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.

[137] 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.

[138] 15 U.S.C. § 80b-1 et seq.

[139] Advisers Act §§ 80b-3(b), 80b-3(l), 80b-3(m); Exemptions for Advisers to Venture

advisers are subject to the provisions of the Advisers Act prohibiting advisers from making any material misstatements, misleading omissions, and other fraudulent statements to investors or prospective investors.[140] These statements include statements regarding investment strategies, experience and credentials, risks associated with the fund, or valuation of the fund's assets.[141]

The Advisers Act also requires registered managers to electronically file and keep current Form ADV with the SEC.[142] 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 hedge 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.[143] 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.[144]

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.[145] Similar to forex trading, Bitcoinica allowed customers to short sell within a chosen leverage range.[146] For example, if a trader wanted to bet against Bitcoin, he could essentially borrow bitcoins from Bitcoinica (in actuality, another

---

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).

[140] 17 C.F.R. § 275.206(4)-(8)

[141] Prohibition of Fraud by Advisers to Certain Pooled Investment Vehicles, 72 Fed. Reg. 44756, 44759 (Aug. 9, 2007) (to be codified at 17 C.F.R. pt. 275).

[142] 17 C.F.R. §§ 275.203.1, 275.204-1.

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

[144] Compliance Programs of Investment Companies and Investment Advisers, Advisers Act Release No. 2204, Investment Company Act Release No. 26,299, 68 Fed. Reg. 74714 (Dec. 24, 2003).

[145] Jon Matonis, Bitcoinica Registers in New Zealand for Bitcoin Margin Trading, Forbes, April 21, 2012, http://www.forbes.com/sites/jonmatonis/2012/04/21/bitcoinica-registers-in-new-zealand-for-bitcoin-margin-trading/.

[146] Id.

trader who wished to go long, but Bitcoinica was the ultimate counterparty) and sell them.[147] 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.[148]

Although Bitcoinica was registered as a financial services provider in New Zealand,[149] 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.[150] 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.[151] Despite persistent security issues,[152] Bitcoinica hosted an average monthly volume of roughly 1.2 million BTC at its peak.[153] 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 order fund.[154] The company entered into receivership in August 2012 and was liquidated shortly thereafter.[155] Tong had by this point announced he was leaving the

[147] 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, Bitcointalk.org forum post, December 29, 2011, accessed February 11, 2014, https://bitcointalk.org/index.php?topic=55970.msg665945#msg665945.

[148] Jon Matonis, Bitcoinica Registers in New Zealand for Bitcoin Margin Trading, Forbes, April 21, 2012, http://www.forbes.com/sites/jonmatonis/2012/04/21/bitcoinica-registers-in-new-zealand-for-bitcoin-margin-trading/.

[149] Id.

[150] Zhou Tong, Show HN: Bitcoinica – Advanced Bitcoin Trading Platform, HackerNews forum post, September 8, 2011, https://news.ycombinator.com/item?id=2973313.

[151] Zhou Tong, Bitcoinica – Advanced Bitcoin Trading Platform, Bitcointalk.org forum post, September 9, 2011, accessed February 11, 2014, https://bitcointalk.org/index.php?topic=42267.msg517128#msg517128.

[152] Tim Worstall, Another Theft at Bitcoinica, Forbes Magazine, May 12, 2012, http://www.forbes.com/sites/timworstall/2012/05/15/another-bitcoin-theft-at-bitconia/.

[153] Jon Matonis, Bitcoinica Registers in New Zealand for Bitcoin Margin Trading, Forbes, April 21, 2012, http://www.forbes.com/sites/jonmatonis/2012/04/21/bitcoinica-registers-in-new-zealand-for-bitcoin-margin-trading/.

[154] Zhou Tong, [Emergency ANN] Bitcoinica site is taken offline for security investigation, Bitcointalk.org forum post, May 11, 2012, accessed February 11, 2014, https://bitcointalk.org/index.php?topic=81045.msg894277#msg894277.

[155] Justin Porter, Tihan Seale Announces Bitcoinica Liquidation, Bitcoin Magazine,

Bitcoin space for good.[156]

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.[157] The company later filed with the Securities and Exchange Commission plans to raise another $1.5 million in venture capital.[158] 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.[159] 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.[160]

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.[161] The Federal Reserve promulgated Regulation T under that authority to prevent investors from taking on too much credit when purchasing or holding securities.[162] Regulation T establishes minimum margin requirements,[163] but exchanges

---

August 2, 2012, http://bitcoinmagazine.com/1872/tihan-seale-announces-bitcoinica-liquidation/.

[156] Zhou Tong, I'm Leaving Bitcoin, Bitcointalk.org forum post, May 13, 2012, accessed February 11, 2014, https://bitcointalk.org/index.php?topic=81581.msg897948#msg897948.

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

[158] Ari Levy, Bitcoin Trading Exchange Coinsetter Files to Raise $1.5 Million, Bloomberg, December 27, 2013, http://www.bloomberg.com/news/2013-12-27/bitcoin-trading-exchange-coinsetter-files-to-raise-1-5-million.html.

[159] Learn More, Coinsetter information page, accessed February 12, 2014, https://www.coinsetter.com/beta

[160] Unclescrooge, [OFFICIAL]Bitfinex.com first Bitcoin P2P lending platform for leverage trading, Bitcointalk.org forum post, June 8, 2013, accessed February 11, 2014, https://bitcointalk.org/index.php?topic=229438.0; FAQ, Bitfinex.com, accessed February 11, 2014, https://www.bitfinex.com/pages/support.

[161] 15 U.S.C. § 78g(a).

[162] Regulation T ''imposes, among other things, obligations, initial margin requirements, and payment rules on securities transactions.'' 12 C.F.R. 220.1(a).

[163] 12 C.F.R. 220.12(a) (limiting extension of credit to 50 percent of a security's market value).

and other organizations may establish additional requirements.[164] 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 the Federal Reserve has no jurisdiction over Bitcoin,[165] implying it is unlikely that it would assert authority over bitcoin margin trading 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 there are today several unregulated exchanges actively trading commodity futures contracts and company shares denominated in bitcoins. These exchanges tend not to be registered with, nor 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. Similarly, there are gambling sites online that denominate bets in bitcoins and suggest that gambling laws do not apply to them.

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 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, there is a strong demand for instruments that allow one to bet against the price of bitcoin. Ideally, such an instrument would be a dollar/bitcoin currency swap, or a futures 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 have begun to offer bitcoin futures contracts and options that are bought and sold not for dollars or any other fiat currency, but for bitcoins.[166] Indeed, many early experiments in

[164] 12 C.F.R. 220.1(b)(2).

[165] Sophie Knight & Takaya Yamaguchi, Japan Says Any Bitcoin Regulation Should Be International, Feb. 27, 2014.

[166] 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

providing bitcoin-denominated derivatives markets have already launched, blossomed, and failed.[167]

One of the most prominent of the bitcoin-denominated futures markets is ICBIT.se, which launched in January of 2012.[168] In April of 2013, the company reported a customer base of roughly 5,000 registered users and around $50,000 in revenue per month.[169] 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.[170] ICBIT therefore merely acts as a facilitator, rather than counterparty, of bitcoin-denominated financial instruments. This business model is at odds with traditional futures markets in which the exchange also performs the clearing function. 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.[171]

MPEx is another longstanding Bitcoin-denominated derivatives market that has facilitated futures-like trading since 2011. Like ICBIT, MPEx has

---

of margin trading. Simone Foxman, *How to Short bitcoins (if you really must)*, QUARTZ, April 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, available at http://finance.fortune.cnn.com/2013/12/05/betting-against-bitcoin-bubble.

[167] 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, accessed February 12, 2014, http://wiki.bitcoin-otc.com/wiki/Beginners_Guide.

[168] Fireball, ICBIT – New Exchange, Bitcointalk.org forum post, January 21, 2012, accessed February 11, 2014, https://bitcointalk.org/index.php?topic=60548.msg705207#msg705207

[169] Cyrus Farviar, 'Taming the Bubble': investors bet on Bitcoin via derivatives markets, Ars Technica, April 11, 2013, http://arstechnica.com/business/2013/04/taming-the-bubble-investors-bet-on-bitcoin-via-derivatives-markets/.

[170] The ICBIT.se website FAQ directs to a Bitcointalk forum post. See: Super T, *Unofficial* ICBIT (BTC Futures Trading) – Help & FAQ's, Bitcointalk.org forum post, April 1, 2013, accessed February 11, 2014, https://bitcointalk.org/index.php?topic=164255.0.t

[171] 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/.

been dogged by rumors and complaints from disgruntled customers.[172] Others, however, praise MPEx for its simple but elegant execution and long-term vision.[173] MPEx is considerably less user-friendly than other existing Bitcoin derivatives markets. Indeed, the creator intentionally designed the platform to weed out novice investors and foster a higher-caliber exchange community.[174] The website is sparse and users must interact with the service through an embedded command line terminal.[175] 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.[176] 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.[177] MPEx does not appear to be incorporated or registered with any regulatory body, but it does provide several hypothetical escape plans in the event of a take down on their website FAQ.[178]

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.[179] 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.[180] For each open position taken, users

[172] 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, February 5, 2013, accessed February 11, 2014, http://trilema.com/2013/because-most-people-are-idiots-in-spite-of-never-manning-up-and-admitting-to-it/

[173] A Review of MPEx, the Bitcoin Stock Exchange, Loper OS blog, February 3, 2013, accessed February 11, 2014, http://www.loper-os.org/?p=1108.

[174] Mircea Popescu, So what's the plan with MPOE/MPEx?, Trilema blog, February 3, 2013, accessed February 11, 2014, http://trilema.com/2013/so-whats-the-plan-with-mpoempex/.

[175] MPEx, English FAQ, accessed February 11, 2014, http://mpex.co/faq.html

[176] Id.

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

[178] Id.

[179] Seal, [ANN] BTC.sx – Leveraged trading made easy, Bitcointalk.org forum post, April 27, 2013, accessed March 26, 2014, https://bitcointalk.org/index.php?topic=188735.msg1955964#msg1955964

[180] Danny Bradbury, BTC.SX revives bitcoin margin trades, CoinDesk, May 23, 2013, http://www.coindesk.com/btc-sx-revives-bitcoin-margin-trades/

must hold deposits equal to the size of the trade multiplied by the price and multiplied by a measure of current market volatility.[181] 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.[182] 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[183] and reported 2,000 registered users.[184] By January of 2014, BTC.sx reported $35 million in total trading since its launch and an active user base of 3,300 traders.[185]

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"[186] and explains that for a party using their platform to short Bitcoin against the dollar, "if rate goes down he would *get as many Bitcoins as it's needed* to buy $6000 on the spot market."[187] Likewise, the settlement term for MPEx's X.Eur contract contemplates physical delivery of bitcoins and not cash.[188] In addition, the Bitcoin derivatives platforms do not also

[181] FAQ, BTC.sx support, accessed March 26, 2014, https://btc.sx/about/faq.

[182] 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. Let's say this deposit amount 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, 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 deposit insurance 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.

[183] Daniel Cawrey, Bitcoin Derivatives Platform BTC.sx Surpasses $13.5m in Trades, CoinDesk, November 25, 2013, http://www.coindesk.com/bitcoin-derivatives-platform-btc-sx-trades/.

[184] Id.

[185] George Samman, The World's First Bitcoin Derivatives Platform Surpasses US$35M in Trades, PRWeb, January 21, 2014, http://www.prweb.com/releases/Bitcoin/Trading/prweb11494016.htm.

[186] See https://icbit.se/BUJ4.

[187] About ICBIT Derivatives Market, https://icbit.se/futures.

[188] See http://mpex.co/?mpsic=X.EUR ("intends to market make an Euro based Bitcoin

serve as a clearinghouse for their customers' trades, which is an essential aspect of a futures exchange. On the other hand, there is no bright line between forwards and futures. The contracts being offered by the platforms are highly standardized and 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 concerns, such as mining equipment manufacturers, but also include Bitcoin-denominated gambling sites like Satoshi Dice[189] and BitBet.[190]

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.[191] Nevertheless, they have proven to be a useful way to fundraise small amounts of capital for interesting projects. They do not seem, however, to be in compliance with securities and exchange regulations. 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.[192] The original GLBSE service was quite basic and

---

future with physical delivery for the foreseeable future ").

[189] 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, March 20, 2014, http://www.coindesk.com/sec-making-inquiries-mpex-satoshidice/.

[190] Mircea Popescu, How does one list on MPEx?, Trilema, October 3, 2012, http://trilema.com/2012/how-does-one-list-on-mpex/.

[191] Olivia Solon, Founder reflects on the closure of Bitcoin stock exchange GLBSE, Wired UK, October 13, 2013, http://www.wired.co.uk/news/archive/2013-10/24/bitcoin-exchange-collapse-glbse.

[192] For frame of reference, GLBSE was founded at around the same time that the infamous 10,000 BTC pizza was purchased. See: Vitalik Buterin, Interview With GLBSE's James McCarthy/Nefario, Bitcoin Magazine, October 15, 2012, http://bitcoinmagazine.com/2578/interview-with-glbses-nefario/.

customers used a command line terminal interface to browse listings and buy or sell shares.[193] 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.[194] Another major player in GLBSE, Lambert Investment Funds,[195] also suddenly pulled itself from the GLBSE directory after several of its investments were revealed to be illusory.[196]

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.[197] During May of 2012, GLBSE listed 10 major stocks valued at a sum of over $650,000.[198]

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 exchange platform from November 2011 to August 2012. BTCST was a popular listing on

[193] GLBSE later offered a user-friendly interface and enhanced features to expand functionality and increase its customer base. Nefario, GLBSE 2.0 open for testing, Bitcointalk.org forum post, January 21, 2012, accessed February 17, 2014, https://bitcointalk.org/index.php?topic=60489.0.

[194] Vitalik Buterin, Interview With GLBSE's James McCarthy/Nefario, Bitcoin Magazine, October 15, 2012, http://bitcoinmagazine.com/2578/interview-with-glbses-nefario/.

[195] Lambert Investment Funds was not a company, but an investment fund that was also traded on GLBSE. See: Peter Lambert, GLBSE:LIF, Bitcointalk.org forum thread, August 5, 2011, accessed February 17, 2014, https://bitcointalk.org/index.php?topic=34634.

[196] 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 forum thread, January 17, 2012, accessed February 17, 2014, https://bitcointalk.org/index.php?topic=35775.msg698197#msg698197

[197] Vitalik Buterin, Global Bitcoin Stock Exchange Shuts Down for Good, Bitcoin Magazine, October 10, 2012, http://bitcoinmagazine.com/2549/global-bitcoin-stock-exchange-shuts-down-for-good/.

[198] GLBSE Valuations, The Bitcoin Trader Blog, May 13, 2012, http://www.thebitcointrader.com/search/label/GLBSE.

GLBSE,[199] and it promised investors returns of up to 1% per day, or 7% per week.[200] 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.[201] At its peak, the scheme had attracted investments of about $7 million, according to Shavers.[202]

On July 23, 2013, the SEC filed a complaint against Shavers and Bitcoin Savings and Trust, alleging that BTCST was a Ponzi scheme,[203] contrary to Shavers' many assurances to his customers that BTCST was a legitimate operation.[204] "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."[205] 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."[206] 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 an "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.[207] Under this test, a wide variety of investments have found to be securities.[208] Shavers argued that the first

[199] Adrianne Jeffries, Suspected Multi-Million Dollar Bitcoin Pyramid Scheme Shuts Down, Investors Revolt, The Verge, August 27, 2012, http://www.theverge.com/2012/8/27/3271637/bitcoin-savings-trust-pyramid-scheme-shuts-down

[200] Securities and Exchange Commission v. Shavers, No. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013), https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf.

[201] Id.

[202] Vitalik Buterin, The Pirate Saga: And So It Ends, Bitcoin Magazine, August 30, 2012, http://bitcoinmagazine.com/2126/the-pirate-saga-and-so-it-ends/.

[203] Securities and Exchange Commission v. Shavers, No. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013).

[204] Trendon Shavers, If my business is illegal then anyone trading coins for cash and back to coins is doing something illegal. :), Bitcointalk.org forum post, January 19, 2012, accessed March 24, 2014, https://bitcointalk.org/index.php?topic=50822.385;wap2.

[205] Securities and Exchange Commission v. Shavers, No. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013).

[206] Id.

[207] SEC v. W.J. Howey Co., 328 U.S. 293, 298-99 (1946).

[208] For example, the First Circuit held that virtual shares in imaginary companies sold

prong of the test failed because Bitcoin was not money.[209] 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.[210]

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."[211] 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.[212]

Around the same time, GLBSE operator James McCarthy[213] sought legal counsel to ensure compliance with existing regulations as his side project grew into a going concern.[214] After his lawyers convinced him that GLBSE ran afoul of existing anti-money laundering and know your customer rules, McCarthy abruptly shut the exchange for good on October 4, 2012.[215] McCarthy attempted to ensure the return of investor funds, but some customers nevertheless likely lost investments.[216] Like so many other

---

in dollars on a virtual exchange as part of a video game were "investment contracts" subject to securities regulation. SEC 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 (2011) Unregulated Stock Markets in Second Life. Southern Economic Journal: July 2011, Vol. 78, No. 1, pp. 6-29.

[209] Securities and Exchange Commission v. Shavers, No. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013).

[210] Id.

[211] Id.

[212] Craig K. Ellwell, M. Maureen Murphy, and Michael V. Seitzinger, Bitcoin: Questions, Answers, and Analysis of Legal Issues, Congressional Research Service Report No. 7-5700, December 20, 2013, http://www.fas.org/sgp/crs/misc/R43339.pdf

[213] James McCarthy did not fully control GLBSE. Rather, GLBSE was owned by a parent company, Bitcoin Global, which is itself a multi-shareholder enterprise. For details, see: theymos, Nefario, Bitcointalk.org forum post, October 6, 2012, accessed February 17, 2014, https://bitcointalk.org/index.php?topic=115669.0.

[214] Vitalik Buterin, Global Bitcoin Stock Exchange Shuts Down for Good, Bitcoin Magazine, October 10, 2012, http://bitcoinmagazine.com/2549/global-bitcoin-stock-exchange-shuts-down-for-good/.

[215] Id.

[216] McCarthy estimates that 95% of GLBSE customers were compensated. See Olivia

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.[217] 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.[218] 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.[219] 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.[220] Indeed, BitFunder's creator was acutely cognizant of the legal challenges his exchange faced from the day he first announced the project.[221] Fearing SEC investigation following the BTCST takedown,[222] 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 website by December 1 of that year.[223] (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.[224]

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

[217] Id.

[218] Ukyo, [BitFunder] Asset Exchange Marketplace + Rewritable Options Trading, Bitcointalk.org forum post, December 10, 2012, accessed February 18, 2014, https://bitcointalk.org/index.php?topic=130117.0.

[219] Kadhim Shubber, Bitcoin stock exchange BitFunder announces closure, *CoinDesk*, November 12, 2013, http://www.coindesk.com/bitcoin-stock-exchange-bitfunder-announces-closure/.

[220] Ukyo, Re: [BitFunder] Asset Exchange Marketplace - Official Launch, Bitcointalk.org forum post, December 11 2012, accessed February 18, 2014, https://bitcointalk.org/index.php?topic=130117.msg1393343#msg1393343.

[221] Id.

[222] Investor Alert: Ponzi Schemes Using Virtual Currencies, 7 *SEC Pub.* 153 (July 23, 2013), http://investor.gov/sites/default/files/ia_virtualcurrencies.pdf.

[223] Kadhim Shubber, Bitcoin stock exchange BitFunder announces closure, *CoinDesk*, November 12, 2013, http://www.coindesk.com/bitcoin-stock-exchange-bitfunder-announces-closure/

[224] Ukyo, Re: [BitFunder] Asset Exchange Marketplace - Official Launch,

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.[225] 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.[226] 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.[227] 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.[228] BTC-TC also emphasized its legal registration in Belize as an international company.[229] 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:
> - 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.)[230]

This scant legal cover proved inadequate to protect BTC-TC and the exchange shut down in September of 2013, citing regulatory concerns.[231]

Bitcointalk.org forum post, November 4, 2013, accessed February 18, 2014, https://bitcointalk.org/index.php?topic=130117.msg3482565#msg3482565

[225] Jonathan Stacke, Bitcoin Securities Exchange BTC-TC Shutters $12M Operations, Cites Regulatory Environment, The Genesis Block, September 23, 2013, http://thegenesisblock.com/btc-trading-corp-shutters-operations-cites-regulatory-environment/.

[226] Id.

[227] Why BTC-TC Rocks, FAQ, accessed March 26, 2014, https://btct.co/.

[228] Deprived, Re: [BTCTC] BTC Trading Corp. -- All new virtual exchange up at https://btct.co/, Bitcointalk.org forum post, November 19, 2012, accessed February 18, 2014, https://bitcointalk.org/index.php?topic=125629.msg1346121#msg1346121.

[229] Why BTC-TC Rocks, FAQ, accessed March 26, 2014, https://btct.co/.

[230] Why BTC-TC Rocks, FAQ, accessed March 26, 2014, https://btct.co/faq.

[231] Jonathan Stacke, Bitcoin Securities Exchange BTC-TC Shutters $12M Operations, Cites Regulatory Environment, The Genesis Block, September 23, 2013, http://thegenesisblock.com/btc-trading-corp-shutters-operations-cites-regulatory-

As with BitFunder, BTC-TC outlined a closing plan for issuers and shareholders to settle or reconcile outstanding balances.[232]

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.[233] As with MPEx futures trading, users must pay an upfront registration fee and a small percent commission on trades.[234] MPEx currently lists four companies selling shares, including MPEx itself.[235] 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.[236] The operator of MPEx even provides periodic shareholder reports in the popular Bitcointalk forums[237] and his own personal blog.[238] The popular gambling site, Satoshi Dice, sold shares of the company on MPEx from April of 2012 until July of 2013.[239] 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.[240] Popescu, who posted his

---

environment/.

[232] Id.

[233] A Review of MPEx, the Bitcoin Stock Exchange, Loper OS blog, February 3, 2013, accessed February 11, 2014, http://www.loper-os.org/?p=1108.

[234] As of February 2013, MPEx garnered 2/3 of its profits from registration fees. Id.

[235] http://mpex.co/, accessed March 26, 2014.

[236] See, for instance, the listing agreement for BitBet: http://mpex.co/?mpsic=S.BBET, accessed March 26, 2014.

[237] MPOE-PR, Re: Investing in Mircea Popescu's Options Emporium, Bitcointalk.org forum post, September 29, 2012, accessed February 18, 2014, https://bitcointalk.org/index.php?topic=64962.msg1230084#msg1230084; and

[238] Mircea Popescu, Six Month MPOE Financial Results, February 20, 2012, accessed February 18, 2014, http://trilema.com/2012/sa-ne-jucam-de-a-investitiile-n-bitcoini/#comment-78745.

[239] 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 forum post, August 20 2012, accessed February 18, 2014, https://bitcointalk.org/index.php?topic=101902.0; and Emily Spaven, Bitcoin company acquisitions begin: Gambling site SatoshiDice sells for $11.5m, CoinDesk, July 18, 2013, http://www.coindesk.com/bitcoin-company-acquisitions-begin-gambling-site-satoshidice-sells-for-11-5m-126315-btc/.

[240] Carter Doughtery, Gambling Website's Bitcoin-Denominated Stock Draws SEC Inquiry, Bloomberg, March 20, 2014, http://www.bloomberg.com/news/2014-03-19/gambling-website-s-bitcoin-denominated-stock-draws-sec-inquiry.html.; Daphna A.

correspondence with the SEC on his blog, responded by questioning the SEC's jurisdiction over his business and its authority to make any requests.[241]

3. Regulating Bitcoin-Denominated 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, 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.[242] Similarly, any investment in bitcoins that takes place through a contract that satisfies the 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 reconsider bringing the full scope of its regulation to a transaction that involves a Bitcoin-denominated instrument whose underlying is also Bitcoin-denominated, which we can call Bitcoin-universe transactions. An example of a Bitcoin-universe transaction would be a Bitcoin-denominated credit default swap that references a Bitcoin-denominated loan.

One approach for regulators would be to completely exclude Bitcoin-universe transactions from regulation, just as forwards and private investment funds are excluded from the CEA and the Company Act, respectively. Another approach would be 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

---

Waxman, SEC Letter to Mircea Popescu in Re: SatoshiDICE (NY-8954), March 3, 2014, http://trilema.com/wp-content/uploads/2014/03/2014-0303-popescu-mpex.pdf.

[241] Mircea Popescu, Interacting with fiat institution: a guide, Trilema, March 18, 2014, http://trilema.com/2014/interacting-with-fiat-institution-a-guide/.

[242] See supra Section II.A.

securities and commodity trade options are regulated.

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. 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. Although Bitcoin universe transactions *could* lead to economic losses, the extent to which, if any, may be highly remote and contingent. It would depend on the value of Bitcoin relative to a fiat currency, the willingness of merchants and other users to accept Bitcoin as a method of payment, and the extent to which Bitcoin is used for functions beyond a payment system.[243] Whether a bitcoin loss leads to real economic loss also depends on whether a party actually converts their bitcoins to real currency or property, something that should not be taken for granted. Bitcoin-universe transactions may leave parties with less bitcoins, but so does an ordinary direct transfer of bitcoins between wallets or paying a fee to use a Bitcoin service such as a storage service—neither of which would fall under the purview of the CFTC or SEC. By treating Bitcoin-universe as no different from traditional financial instruments that may result in a loss in real wealth, regulators would implicitly be permitting form to triumph over substance.

The following chart displays the unique nature of Bitcoin-universe 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:

	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-universe transactions

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

[243] See infra Section III.

There is already legal precedent for treating Bitcoin-universe transactions differently. Despite the court's opinion in *Shavers*, the approach taken by FinCEN—the federal regulator of money services business—provides grounds for not regulating or granting an exemption for Bitcoin-universe transactions. 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.[244] It further distinguishes *convertible* virtual currency as a virtual currency that either has an equivalent value in real currency or acts as a substitute for real currency.[245] Under FinCEN regulation of money service businesses, only companies that transmit convertible virtual currencies or exchange convertible virtual currencies into real ones are subject to regulation.[246] Bitcoin miners and those that trade convertible virtual currencies for their own investment purposes are not regulated.[247] This approach suggests that transactions that "stay" within the bitcoin economy—which would include Bitcoin-universe transactions—are unique and should not be subject to the same level of regulation.

The CFTC in particular should find the argument for excluding or exempting Bitcoin universe transactions from the CEA to be particularly compelling. By statute and regulation, most physically-settled transactions are not subject to the full scope of CFTC regulations, if any. Insofar as the cash versus physically settled distinction applies to Bitcoin derivatives, Bitcoin-universe transactions clearly fall within the category of physical settlement. In a Bitcoin-universe transaction, each party transacts in and pays (or receives) only bitcoins. Accordingly, for all the reasons the CFTC places such strong weight on physical settlement as grounds for excluding contracts from regulation, it should do so for virtual settlement 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

[244] Department of Treasury Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001, January 30, 2014, http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf.

[245] Id.

[246] Id.

[247] See FinCEN Ruling FIN-2014-R001, Application of FinCEN's Regulations to Virtual Currency Mining Operations (Jan. 30, 2014), 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, (Jan. 30, 2014), accessible at: http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf.

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. As a result, prediction markets are often designed for the express purpose of uncovering these prices, and not merely to facilitate wagering.[248]

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 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. In 2012, the CFTC sued the prediction market Intrade for violating the Commission's ban on off-exchange options trading.[249] 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

[248] Adam Ozimek, The Regulation and Value of Prediction Markets, March 12, 2014, Mercatus Center Working Paper, http://mercatus.org/publication/regulation-and-value-prediction-markets

[249] 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, November 26, 2012, http://www.cftc.gov/PressRoom/PressReleases/pr6423-12.

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."[250] Intrade suspended its operations in the U.S., and within months the site had shut down.[251]

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.[252] 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."[253]

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.[254] It operates under the auspices of two CFTC no-action letters that are contingent on the market's non-profit and academic status.[255] The letters also place a number of restrictions on the market.[256] For example, no individual is allowed to invest more than $500, and individual markets are limited to a pre-determined range of

[250] Id.

[251] The CFTC continues to target predictions markets. See: Katherine Mangu-Ward, The Death of Intrade, Reason Magazine, December 2013, http://reason.com/archives/2013/11/25/the-death-of-intrade.; Jamila Trindle, Regulators Sue Prediction Site, Allege Illegal Options, Wall Street Journal, June 6, 2013, http://online.wsj.com/news/articles/SB10001424127887324798904578529241482337164.

[252] Jason Abbruzzese, CFTC bans election-based derivatives contracts, FT, April 3, 2012, http://www.ft.com/intl/cms/s/0/dcf08b92-2a70-11e1-9bdb-00144feabdc0.html#axzz2vaSTU2d.

[253] CFTC Issues Order Prohibiting North American Derivatives Exchange's Political Event Derivatives Contracts, CFTC Press Release, April 2, 2012, http://www.cftc.gov/PressRoom/PressReleases/pr6224-12.

[254] Paul Gomme, Iowa Electronic Markets, Federal Reserve Bank of Cleveland Report, April 15, 2003, https://www.clevelandfed.org/research/commentary/2003/0415.pdf.

[255] Andrea M. Corcoran, CFTC Letter to Professor George Neumann, CFTC Letter No. 91-04a, Division of Trading and Markets, February 5, 1992, 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, June 18, 1993, http://www.cftc.gov/files/foia/repfoia/foirf0503b004.pdf.

[256] Id.

participants.[257] In addition, pursuant to authority granted to it by the Dodd-Frank Wall Street Reform and Consumer Protection Act,[258] 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."[259]

The regulatory environment has been similarly hostile to online gambling. The Wire Act[260] 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,[261] and the Illegal Gambling Business Act (IGBA)[262] 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.[263] It also requires payment processors, such as money transmitters and credit cards providers, to block payments to gambling sites.[264]

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

---

[257] Id.

[258] 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.

[259] 17 CFR 40.11

[260] 18 U.S.C. § 1084

[261] 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 Attorney General, Criminal Division, September 20, 2011, http://www.justice.gov/olc/opiniondocs/state-lotteries-opinion.pdf.

[262] 18 U.S.C. § 1955

[263] 31 U.S.C. §§ 5361–5367.

[264] Id.

why it is the perfect payment method for online action in the U.S.[265]

Other gambling sites include SatoshiDice.com, SatoshiBet, and dozens more.[266] 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. While there is no uniform federal standard, state laws generally require that gambling transactions have three elements: prize, chance, and consideration.[267] 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.[268] 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.[269] 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.[270]

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

---

[265] Information for U.S. Bettors, Coinbet.cc customer service, accessed March 26, 2014, http://www.coinbet.cc/pages/us-bettors#.Ux9IiOddXzc.

[266] Bitcoin wiki, s.v. Gambling, accessed March 26, 2014, https://en.bitcoin.it/wiki/Category:Gambling.

[267] See, *Midwestern Enters. v. Stenehjem*, 2001 ND 67, ¶17, 625 N.W.2d 234, 237 (2001) ("The three elements of gambling are generally recognized as consideration, prize, and chance.").

[268] *United States v. Davis*, 690 F.3d 330 (5th Cir. 2012).

[269] 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).

[270] *Securities and Exchange Commission v. Shavers*, No. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013).

growing consensus that bitcoins can be used 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 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 bitcoins 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[.][271]

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.[272] Bitcoins are also likely to be considered "funds" under a similar analysis to that in *Bitcoin Savings and Trust*.[273] Therefore, accepting bitcoins transmitted by or 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.[274]

The more difficult case is when there is no intermediary involved

[271] 31 U.S. Code § 5363

[272] US 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, March 18, 2013), http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

[273] See supra

[274] 31 U.S. Code § 5364

between the consumer and the gambling business. 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.[275] 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,[276] 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."[277] 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[.]"[278] Therefore, it would be 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

[275] 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, February 15, 2014, http://www.coindesk.com/roger-ver-blockchain-past-present-future/.

[276] 31 U.S. Code § 5363 (2)

[277] Emphasis added.

[278] Emphasis added.

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.[279] 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.[280] This design means that no accounts or deposits are 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[281] 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,[282] and DiceOnCrack.[283]

---

[279] Megan Geuss, Firm says online gambling accounts for almost half of all Bitcoin transactions, ArsTechnica, August 24, 2014, http://arstechnica.com/business/2013/08/firm-says-online-gambling-accounts-for-almost-half-of-all-bitcoin-transactions/.

[280] Because all transactions are public, users can verify that the house is paying out fairly -- unlike traditional casinos.

[281] Jon Matonis, Bitcoin Casinos Release 2012 Earnings, CoinDesk, January 22, 2013, http://www.forbes.com/sites/jonmatonis/2013/01/22/bitcoin-casinos-release-2012-earnings/.

[282] Bitlotto, [BITLOTTO] Mar 1 draw over $2000 or 50BTC! Tickets now 0.1 BTC for Apr 5, Bitcointalk.org forum post, August 3, 2011, accessed April 2, 2014, https://bitcointalk.org/index.php?topic=34007.0.

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.[284] 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[285] ("Win in the price is higher in:" and "Win if the price of 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 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).[286] According to the website FAQ, BTCOracle has processed at least 3,000 options trades since the service launched in April of 2013.[287]

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. 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.[288]

---

[283] TTBit, DiceOnCrack.com | If you thought dice was addicting…, Bitcointalk.org forum post, October 24, 2012, accessed April 2, 2014, https://bitcointalk.org/index.php?topic=120239.0.

[284] BTCOracle, FAQ, BTCOracle Customer Service, accessed March 26, 2014, http://btcoracle.com/faq.php.

[285] 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.

[286] BTCOracle, FAQ – "How does it work?", BTCOracle Customer Service, accessed March 26, 2014, http://btcoracle.com/faq.php.

[287] BTCOracle, FAQ – "Can you trust us? Who are you?", BTCOracle Customer Service, accessed March 26, 2014, http://btcoracle.com/faq.php.

[288] 31 U.S. Code § 5361 - Congressional findings and purpose

III. 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. Conceived of in this way, the Bitcoin block chain then becomes more than just a payment system. It can be a completely decentralized and perfectly reconciled property registry.

Additionally, transactions using the Bitcoin protocol are programmable, which means that they can be automated.[289] For example, Bitcoin allows for multisignature, or "m-of-n," transactions that require any *m* number of *n* signatures to complete.[290] 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.[291]

Substituting Bitcoin for a trusted third party will likely meet the demand of a wide range of sellers and merchants. The use of a third party financial institution to ensure delivery and payment among anonymous parties currently takes place through the long-standing and widespread practice of an intermediary issuing an instrument known as a commercial letter of credit. A letter of credit assures a seller of payment by requiring a buyer to pay a trusted financial institution to take on the obligation to pay the

[289] Gavin Andresen, Pay to Script Hash, *Bitcoin Improvement Proposal 0016*, March 1, 2012, https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki.

[290] Gavin Andresen, Bitcoin Faucet Hacked, blog, March 2012, http://gavintech.blogspot.com/2012/03/bitcoin-faucet-hacked.html.

[291] 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 video, uploaded by QueuePolitely on September 27, 2012, accessed March 21, 2014, http://www.youtube.com/watch?v=mD4L7xDNCmA.

seller.[292] At the same time, a letter of credit transaction assures the buyer that it will not have to pay the seller until the seller ships the goods. The practice requires the seller to deliver substantial documentation to the intermediary evidencing proof of shipment before the seller is paid. Letters of credit are mostly used in international goods transactions, where trust between contracting parties is relatively low. Letters of credit can be expensive, and range from 0.5 to 3 percent based upon the structure of the transaction, whether additional bank intermediaries are used, and the creditworthiness of the parties. Like credit card payments, using Bitcoin as a substitute for the third party verification function of letters of credit could entail a substantial cost savings to merchants.

The simplest application of multisignature transaction is a 2-of-3 transaction. Bitcoins are sent to an address controlled by three parties:[293] perhaps the buyer, the seller, and a third party arbitrator. 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.[294] The third party's signature provides the second needed signature to complete the 2-if-3 transaction.

This kind of multisignature transaction can be used to provide escrow-like services[295] for bitcoin transactions as well as for real world assets.

[292] Uniform Commercial Code Section 5-108(b) (requiring an issuer of a letter of credit to honor by payment); 5-102(a)(3) (defining beneficiary as party that issuer of letter is required to pay upon presentation of documents); 5-102(a)(8) (defining honor as being satisfied by payment).

[293] 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, Bitcointalk.org forum post, May 18, 2012, https://bitcointalk.org/index.php?topic=82213.msg906833#msg906833.

[294] While this third party can technically be any person, early businesses have looked to provide professionalized mediation services through 2-of-3 transactions. For one example, see: Bitrated, FAQ, accessed March 26, 2013, https://www.bitrated.com/faq.html.

[295] Note that multisignature transactions are not like a 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.

Suppose Alice orders an original painting from Bob.[296] 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 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 it is received by Dan and Alice. 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.

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,[297] 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

[296] 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 video, uploaded by QueuePolitely on September 27, 2012, accessed March 21, 2014, http://www.youtube.com/watch?v=mD4L7xDNCmA.

[297] For a deeper explanation of oracles, see: Mike Hearn, Contracts - Example 4: Using external state, Bitcoin wiki, accessed March 21, 2014, https://en.bitcoin.it/wiki/Contracts#Example_4:_Using_external_state.

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.[298] Conceivably, a custom-designed oracle could simply monitor news data feeds, such as 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.[299] 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 exchange.

The case of an inheritance is a simple example to illustrate how oracles and multisignature transactions can be combined.[300] Let's say that Alice wishes to bequeath an inheritance to her granddaughter Erin. She wants the inheritance to be dispersed either on Erin's 18th birthday or after Alice dies, whichever date comes first. It would be easy enough for Alice to create a conditional transaction that will not complete until a certain agreed-upon future "lock time." Alice would merely need to specify that the transaction should be considered pending until Erin's 18th birthday, after which date Erin can sign her private key to retrieve the inheritance. In order to also cover the death condition, Alice can create another transaction, this time a multisignature transaction, to which herself, Erin, and an oracle are all parties. The oracle would be programmed to check official death registries for an official record of Alice's death. If Alice dies before Erin's 18th birthday, the oracle will receive an input that Alice's death record has been registered in the public databases. This input will induce the oracle to sign the transaction, along with Erin, to transfer the bitcoins to Erin's account. If Alice does not die before Erin's 18th birthday, Erin can simply sign the transaction that Alice gave her after the date of her birthday. Since the lock time date has passed, it will be considered valid by the block chain, so the

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

[299] http://www.coindesk.com/reality-keys-bitcoins-third-party-guarantor-contracts/

[300] This example is taken from a use case originally developed by Mike Hearn. See: Mike Hearn, Contracts - Example 4: Using external state, Bitcoin wiki, accessed March 21, 2014, https://en.bitcoin.it/wiki/Contracts#Example_4:_Using_external_state.

bitcoins are transferred to Erin.

Eventually, the block chain could even serve as a distributed title registry for real world assets through the use of "smart property."[301] Physical, non-BTC assets can be represented on the block chain through the use of "colored coins."[302] 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.[303] 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 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.

A. 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.[304] One solution that has

---

[301] Nick Szabo, The Idea of Smart Contracts, White Paper, 1997, http://szabo.best.vwh.net/idea.html.

[302] For a deeper explanation of colored coins, see the white paper: Yoni Assia and Leor Hakim, Colored Coins - BitcoinX, White paper, accessed March 21, 2014,https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit.

[303] Mike Hearn, Smart Property, Bitcoin wiki entry, accessed March 26, 2014, https://en.bitcoin.it/wiki/Smart_Property.

[304] Chris Odom, Chris Odom on OpenTransactions, presentation at the Miami Bitcoin Conference 2014, January 25, 2014, accessed March 21, 2014, https://soundcloud.com/mindtomatter/miami-2014-chris-odom-on-1

been proposed is a federated server system and software library known as Open Transactions.[305] To briefly summarize, the Open Transactions system uses multisignature transactions, triple entry accounting,[306] and Truledger receipt systems[307] to regulate bitcoin deposits and transfers throughout a federated system of servers.[308] This federated model, along with Open Transaction's digital software library of complex transactions available for users to employ,[309] 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 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" experiments that are in various phases of development include Mastercoin,[310] Counterparty,[311] and Ethereum.[312] Each project differs in terms of the tools and specific functions that are prioritized, but they all aim to extend the Bitcoin protocol's core capabilities of block chain-based peer-to-peer asset exchange to complex financial instruments and even real world assets.

This is where things get interesting. These three tools—multisignature

---

[305] Id.

[306] Ian Grigg, Triple Entry Accounting, White Paper, 2005, accessed April 7, 2014, http://nakamotoinstitute.org/literature/31/html/.

[307] Bill St. Clair, Truledger in Plain English, White Paper, 2008, accessed April 7, 2014, http://nakamotoinstitute.org/literature/32/html/.

[308] Justus Ranvier, Voting Pools: How to Stop the Plague of Bitcoin Heists, Thefts, Hacks, Scams, and Losses, Bitcoinism blog, December 6, 2013, accessed March 11, 2014, http://bitcoinism.blogspot.com/2013/12/voting-pools-how-to-stop-plague-of.html.

[309] Open Transactions wiki, s.v. List of Classes, accessed March 26, 2014, http://opentransactions.org/wiki/index.php?title=List_of_Classes.

[310] J.R. Willet, Maran Hidskes, David Johnston, Ron Gross, Marv Schneider, and Peter Todd, The Master Protocol / Mastercoin Complete Specification, White Paper Version 0.4.5.1 Smart Property Fundraisers Edition, accessed March 26, 2014, https://github.com/mastercoin-MSC/spec.

[311] PhantonPhreak, The Counterparty Protocol, White Paper, accessed March 26, 2014, https://github.com/PhantomPhreak/Counterparty.

[312] Vitalik Buterin, et al., A Next Generation Smart Contract and Decentralized Application Platform, Ethereum White Paper, accessed March 26, 2014, https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper.

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 does 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 give the reader 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 company. She has a strong background in chip 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[313] or Keyhotee.[314] 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

[313] David Gilson, What are Namecoins and .bit domains?, CoinDesk, June 18, 2013, http://www.coindesk.com/what-are-namecoins-and-bit-domains/.

[314] Daniel Larimer, Introduction to Keyhotee, Invictus Innovations Presentation, posted to YouTube on October 24, 2013, accessed March 21, 2014, http://www.youtube.com/watch?v=3pZaTdEtK-8.

#bitcoin-otc open order book[315] or can create a broadcast on the peer-to-peer messaging space Bitmessage.[316] 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.[317] This may take the form of colored coins representing shares of the company, a programmable and algorithmically self-enforcing contract shared among all shareholders,[318] 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.

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.[319] Alice broadcasts a message to Bitmessage stating that she thinks the price of Google stock will rise by 20% by six months from that day and that she is willing to wager 0.5 BTC on her prediction.

[315] OTC Order Book, #bitcoin-otc, accessed March 26, 2014, http://bitcoin-otc.com/vieworderbook.php.

[316] Jonathan Warren, Bitmessage: A Peer-to-Peer Authentication and Delivery System, White Paper, November 12, 2012, https://bitmessage.org/bitmessage.pdf.

[317] Open Transactions wiki, s.v. Smart contracts, accessed March 26, 2014, http://opentransactions.org/wiki/index.php?title=Smart_contracts.

[318] This concept is known as a "decentralized autonomous corporation" (DAC) or a "decentralized autonomous organization" (DAO). [1] 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 Magazine, September 2013, http://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/.

[319] Jerry Brito, Bitcoin: More than Money, Reason Magazine, December 2013.

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 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.[320] 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 likelihoods 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.[321]

---

[320] Nick Szabo, The Idea of Smart Contracts, White Paper, 1997, http://szabo.best.vwh.net/idea.html.

[321] Ed Felten, Bitcoin Research in Princeton CS, Freedom to Tinker, November 29,

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[322] or box office revenues,[323] 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.[324] A group of researchers from the University of Warsaw have already theoretically described[325] and successfully executed[326] 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

---

2013, https://freedom-to-tinker.com/blog/felten/bitcoin-research-in-princeton-cs/.

[322]

[323]

[324] See, for example: Andrew Chi-Chih Yao, How to Generate and Exchange Secrets, 27th Annual Symposium on the Foundations of Computer Science, IEEE, 1986, http://www.csee.wvu.edu/~xinl/library/papers/comp/Yao1986.pdf.; and Oded Goldreich, Silvio Micali, and Avi Wigderson, How to Play Any Mental Game: or, A Completeness Theorem for Protocols with Honest Majority, Proceedings of the nineteenth annual ACM symposium on Theory of computing, ACM, 1987, http://www.math.ias.edu/~avi/PUBLICATIONS/MYPAPERS/GMW87/GMW87.pdf.

[325] Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski and Łukasz Mazurek, Secure Multiparty Computations on BitCoin, Cryptology ePrint Archive: Report 2013/784, January 13, 2014, http://eprint.iacr.org/2013/784.

[326] 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.

> dishonest parties behave, the honest parties will never get cheated. More precisely, each honest party can be sure that, once the game starts, it will always terminate and will be fair."[327]

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.

B. 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 the Internet.[328] These include ISPs, search engines, payment processors, and DNS registrars. And Jack Goldsmith & Tim Wu have written that content providers cannot evade

---

[327] Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski and Łukasz Mazurek, Secure Multiparty Computations on BitCoin, Cryptology ePrint Archive: Report 2013/784, January 13, 2014, http://eprint.iacr.org/2013/784.

[328] Zittrain, J. (2006). A History of Online Gatekeeping. *Harvard Journal of Law and Technology,* 19(2), 253-298.

control by simply avoiding intermediaries because "the elimination of intermediaries is in many cases the same thing as the elimination of the underlying conduct."[329] 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.[330] That was indeed what happened after the RIAA successfully sued Napster for contributory copyright infringement.[331] 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.[332] These included FastTrack, Gnutella, and eventually BitTorrent, which is completely decentralized.[333] 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, and PayPal froze the organization's account.[334] They did so likely under political pressure. WikiLeaks began accepting bitcoin donations in 2011,[335] and today such a

[329] Goldsmith & Wu, Who Controls the Internet, at 69.

[330] Annemarie Bridy, *Is Online Copyright Enforcement Scalable*, 13 Vanderbilt Journal of Entertainment & Technology Law 695 (2011), 699-701.

[331] Id.

[332] Id.

[333] Id.

[334] Greenberg, A. (2010, Dec. 7). Visa, MasterCard Move to Choke WikiLeaks. *Forbes*. Retrieved from http://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/

[335] Greenberg, A. (2011, June 14). WikiLeaks Asks for Anonymous Bitcoin Donations. *Forbes*. Retrieved from http://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-

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,[336] while adaptation is the change an organism or species undergoes to become better suited to a new environment.[337] In several works, Adam Thierer has applied these concepts to information technology as alternatives to precautionary regulation or prohibition, either of technology of information.[338]

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.[339] He argues quite convincingly that the best approach 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.[340] The alternative—a precautionary principle for information—would be too costly and trade too much potential innovation for safety, he argues.[341]

For our purposes, we need not make any normative claims about "top-

---

bitcoin-donations

[336] http://en.wikipedia.org/wiki/Resilience_(ecology)

[337] http://en.wikipedia.org/wiki/Adaptation

[338] 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

[339] *Id.* at 356-57.

[340] *Id.*

[341] *Id*. at 361.

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, policymaker's next best options 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,[342] and then also pursued individual file-sharers.[343] 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 the easily copied music, to difficult-to-replicate performances and branded goods.[344] 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.[345] 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 independent artists, may thrive better than ever, and we see evidence of this.[346] 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

[342] David Kravets, *Dec. 7, 1999: RIAA Sues Napster*, WIRED, Dec. 7, 2009, *at* http://www.wired.com/2009/12/1207riaa-sues-napster/

[343] Donald Harris, *The New Prohibition: A Look at the Copyright Wars Through the Lens of Alcohol Prohibition*, 80 TENN. L. REV. 101 (2012).

[344] Raustalia and Sprigman, Knockoff Economy, p 222(?)

[345] Id at 183(?) Also: "Total revenues from live shows grew from $7.3 billion in 2006 to $10.3 billion in 2011."

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

information access and use.[347] "Still, after the initial panic," he writes, "we almost always embrace the service that once violated our visceral sense of privacy."[348] It happened with the introduction of cameras 100 years ago,[349] and more recently with the introduction of ad-supported Gmail.[350] 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.[351]

The point it not that policymakers should give up once intermediary control becomes ineffectual; quite the contrary. It's 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 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.

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

[347] Larry Downes, A Rational Response to the Privacy "Crisis," Cato Institute Policy Analysis No. 716 (Jan. 7, 2013), *available at* http://www.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf

[348] *Id.*

[349]

[350]

[351] Prolexic --- see Fatal System Error by Menn.

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 adaption.