Oklahoma Journal of Law and Technology

Volume 10 | Number 1

January 2014

Regulatory Overview of Virtual Currency

Nicholas Godlove

Regulatory Overview of Virtual Currency

© 2014 Nicholas Godlove, J.D.[*]

Introduction: Will Bitcoins Become a New Global Currency?

Probably not.

Whether due to their apparent ease in facilitating money laundering and procuring illegal substances without involving established financial institutions, or merely because they have received a lot of press lately, Bitcoins[1] have increasingly come under scrutiny by the regulatory agencies of various state, federal and international governments.[2] In all statements so far, these regulatory bodies have been intentionally vague and speculative regarding how and when such enforcement would take place.[3] Several tremulous steps taken by committees on the nascent technology have been characterized by fundamental misconceptions as to the nature of virtual currency.[4] The questions that have been left unanswered include: Is there a purpose to be served in such regulation? And, how would such regulation be conducted? This article seeks to provide preliminary answers to those questions, and to posit a framework for considering virtual currency in a regulatory framework that will grow as the incipient technology develops.

---

* Faculty Associate, School of Criminology and Criminal Justice, Arizona State University, Phoenix, Ariz. Previously law clerk for the Hon. Judge H. Russell Holland, Federal District of Alaska. I would like to thank my mentor Professor Joel Dobris at the University of California, Davis, my family, and Douglas Rennie for their assistance in the writing of this article.

1. "Bitcoins" in this article will be used to refer to the Bitcoin network and concept exclusively; "bitcoins" refers to an actual unit of the Bitcoin exchange; "Coins" (with a capital "C") refers to Bitcoins and its derivative virtual currency, including Dogecoins, Flexcoins, etc. When I refer to Bitcoins, I mean the specific algorithms and processes by which this virtual currency is used. When I refer to the concept in general, I will use the more generic phrase "virtual currency," although some in the tech community use the expression "digital currency" to denote the same concept.

2. New York State Currency Regulatory Board, California Attorney General's Office, Japanese Federal Government.

3. Fin. Crimes Enforcement Network, Dep't of the Treasury, *Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FINCEN (No. FIN-2013-G001, Mar. 18, 2013), http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf [hereinafter Treasury Guidance FIN-2013-G001].

4. *See e.g.*, Fed. Election Comm'n, Draft Advisory Opinion 2013-15 (Conservative Action Fund) (Nov. 7, 2013), *available at* http://saos.nictusa.com/aodocs/201315.pdf.

This article will begin with an overview of the most successful virtual currency created to date –Bitcoin- and explain its progeny: virtual currency created by substantially duplicating the coding and ideas of the Bitcoin. From there, the article will describe how virtual currency abuts current regulatory law, and how it may develop in the future. Finally, I will propose framework for a regulatory environment that will regulate virtual currency in its current form and continue to serve future developments.

Bitcoin is a decentralized, peer-to-peer network for the exchange of unique serial numbers. Possession of these numbers is exclusive to the owner of the Coin, owned by them in an encrypted file. Bitcoins allow for secure transfer of ownership without the need for a trusted third party. The unit of the network is bitcoin, or BTC, which has been alternatively argued to be a currency, commodity, or method of exchange. The Bitcoin network launched in 2009 after years of development by Satoshi Nakamoto, an individual or group whose identity is still debated.[5]

The network began with the publication of a mathematical proof which spurred "miners" to use software programs that follow the mathematical formula to produce bitcoins. The formula and software are freely available for anyone to use. There is a finite amount of bitcoins that may be produced and as more bitcoins are created, the mathematical computations required to create more become increasingly difficult. Bitcoins can be traded or used to buy goods and services. All bitcoin transactions are recorded in the "block chain" - a massive and transparent ledger of each and every bitcoin transaction maintained by the miners. There is no central authority that oversees Bitcoin.

Background: Virtual Currency in General

I. How Virtual Currency Differs from Traditional Money Transmission

A. Current E-Transmission of Money

1. Electronic Funds Transfers

Electronic funds transfers ("EFTs") have been established and common since the 1980s, and they have become an inextricable part of the global economy. Virtual currency is distinct from previous electronic funds transfers by the elimination of a heretofore-unthinkable step: No dollars are

5. A man who has been living under the name Satoshi Nakamoto for decades has been identified in Northern California, but whether he is the developer in whole or in part remains an open question.

ever routed through centralized financial organizations. This distinction leads to several radical departures between the regulatory outcome of the two methods, and an understanding of the current enforcement regime is necessary in order to understand what changes must occur if the system can apply to virtual currency.

Article 4A of the UCC, promulgated by the ALI and National Conference, enacted in all fifty states and endorsed by the Fed,[6] forms the backbone of large money payments from one business or financial institution to another though electronic means.[7] The Electronic Fund Transfer Act governs point-of-sale transactions in which retail customers pay for purchases by use of an access or debit card at a retail store, ATM transactions; direct deposit; and preauthorization withdrawals.[8] Wire transfers (typically in small amounts) are covered under money transmission laws by the states but not governed by Article 4A.

EFTs necessarily involve a bank account in the transferor's country, and a separate account in the transferee's country. Each bank must conduct itself according to local laws, and the transfers thus fall into several enforcement regimes.[9] For example, a business in California buying widgets in China must send the payment from their California bank, which implicates California banking and business codes, federal banking secrecy acts, and federal money laundering regimes. Once the money reaches a bank in China with an agreement with the California bank, it must place the money in the correct account in accordance with Chinese banking law. This is the simplest possible example, but even this simple transfer precipitates substantial legislative oversight, without much protecting the beneficiary.[10]

---

6. U.C.C. art. 4A (amended 2012).
7. *Id.*.
8. 15 U.S.C. § 1693a(6) (2012).
9. U.C.C. § 4A-302.
10. Mark Sneddon, *The Effect of Uniform Commercial Code Article 4A on the Law of International Credit Transfers*, 29 LOY. L.A. L. REV. 1107 (1996), *available at* http://digitalcommons.lmu.edu/llr/vol29/iss3/11.

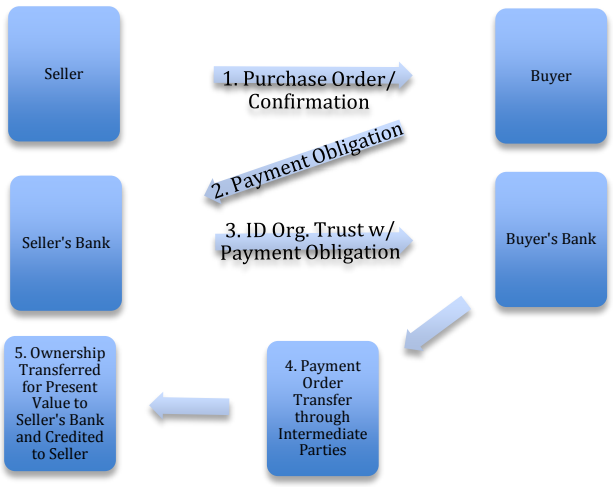

Fig 1: Traditional Electronic Funds Transfer

How are millions of dollars transferred from New York to California in a few hours? Perhaps a "Two bank transfer" occurs, which is actually two payment orders: first, from the Buyer to their bank, and second, from the buyer's bank to the beneficiary's bank.[11] Usually in these cases, the banks have settlement agreements through "cross accounts" or a "common account" which they have agreed on prior to this exchange. Another manner of large money transfer is a "CHIPS" transfer, if both the originator's' and beneficiary's' banks are participants in the Clearing House Interbank Payments System of the New York Clearing House Association. Or, if the banks have accounts in privity with the Fed, they may use Fedwire to settle their accounts.

A funds transfer involves a series of payment orders, defined in 4A-103(a)(1) as "an instruction of a sender to a receiving bank . . . to pay, or cause another bank to pay, a fixed or determinable amount of money to a beneficiary ***." As a result of "acceptance" of a payment order, the rights and obligations of the participants is defined under Article 4A.[12] Acceptance obligates the receiving bank to execute a payment order by sending it to a receiving bank, and itself becoming a sender.[13] Eventually

11. EARNEST T. PATRIKIS, THOMAS C. BAXTER, JR. & RAJ K. BHALA, WIRE TRANSFERS 140 (1993)
12. U.C.C. § 4A-209.
13. *Id.* § 4A-209(a), 302(a)(1), 402(c).

the final receiving bank, the beneficiary's bank, receives the payment order and becomes liable for the amount of the payment order to the beneficiary.[14] Speed of processing takes precedence over assignment of liability. Payment orders under 4A are not intended to require banks to engage in inquiries as to whether conditions have been satisfied, and banks act essentially as functionaries.[15] Banks that accept the payment order must ensure that they send it, which makes the wholesale money wire transfer system cheap, speedy, and final. Summary judgments are permitted on Article 4A.[16]

Funds transfers are very efficient for moving large amounts of money. Fraudulent payment orders are therefore a concern. Fraudulently executed orders may cause a chain of banks to transfer payment orders to an account controlled by the thief in another bank. Under 4A a receiving bank that executes a payment order is not acting as an agent of the sender.[17] But the agency doctrines of actual, implied, and apparent authority are difficult to apply to these larger, more impersonal functionary transactions. In the funds transfer realm, the key concept is whether such payments were "authorized," albeit in a different context than authority as exists in agency law. Thus, in order to facilitate banks' willingness to transfer millions, billions, and trillions of dollars quickly all over the world, banks that execute payments that "test" can send the order without fear of liability.[18] So long as the banks use a security procedure that is commercially reasonable and the receiving bank proves that it accepted the order in good faith after verifying the order in compliance with that security procedure, the payment order is effective, whether or not the customer actually authorized it.[19] Thus, customers accept most of the risk of loss, although banks have the burden or ensuring that they use reasonable security procedures.

2. Credit Card Payments

Credit card payments are the most useful methods for payments made by consumers in smaller dollar amounts. The transfers are surprisingly similarly unsecure as electronic funds transfers. Indeed, little has changed

14. *Id.* § 4A-404(a).

15. Centre-Point Merchant Bank v. Am. Express Bank, 913 F. Supp. 202, 208 (S.D.N.Y. 1996).

16. Aleo Intl., Ltd. v. Citibank, 612 N.Y.S.2d 540 (S. Ct. N.Y. Cty., 1994).

17. U.C.C. § 4A-212.

18. *Id.*

19. *Id.* § 4A-203.

in the actual technology of transferring funds from the 1980s framework. Other than bouncing the signals off a satellite instead of through sea cables, US systems still use the relatively unsecure format-preserving 58k encryption of credit card information in terminal-to-terminal sales, while only purchases over the Internet use the more secure 128-bit pseudo-random hexadecimal encryption but lack authentication features.

"Universal" credit cards issued by financial institutions provide unsecured short-term credit to cardholders to permit them to purchase from a universe of merchants and sellers that are not associated with the card. The merchant or seller is faced with several risks in honoring a credit card. First, the person may not be authorized to use the card, and the credit line that looks legitimate may not be paid through. Second, the issuer may have revoked the card. Third, the amount of credit given by the issuer to the cardholder may not be sufficient to cover the amount of the purchase. Usually, however, the risk for some or all of the purchase is taken by the issuer, which charges a fee to compensate for the risk. Fees to the merchant for receiving a payment through the issuer are called the "interchange fee," and generally average about 1.5% of the sales price.

Cardholders enjoy dramatically limited statutory liability to charges not in excess of $50, if the issuer has given adequate notice of the potential liability and provided a method whereby the user can be identified as the authorized user for unauthorized use of their cards.[20] "Unauthorized Use" means a use of a credit card by a person other than the cardholder who does not have actual, implied, or apparent authority for such use and from which the cardholder receives no benefit.[21] Apparent authority is the most commonly litigated situation; as apparent authority for use may arise through a cardholder's negligence.[22]

States have also hotly debated the consumer protections inherent in credit cards since their origins in the 1960s, such as the extent to which consumers may chargeback their payments if goods are delivered in a defective state or never delivered. The 1974 Fair Credit Billing Act, now the Consumer Credit Protection Act,[23] regulates the rights between cardholders and card issuers. These provisions allow issuers to make agreements governing relationships with merchants, merchant banks, and issuing banks, allowing limited recourse and chargeback in the case of a

20. 15 U.S.C. § 1643 (2012).

21. *Id.* § 1602.

22. Minskoff v. Am. Express Travel Related Servs. Co., Inc., 98 F.3d 703 (2d Cir. 1996).

23. 15 U.S.C. § 1666.

dispute.[24] However, there are geographic limitations on the cardholder's use of defenses to payment against the issuer.

3. Current Payment Process on the Internet

Most Internet sales are currently paid for by credit cards, which are leading to increasing losses as security problems mount. Typical online sales are considered "card-not-present" transactions as opposed to face-to-face sales, where brick-and-mortar stores may verify the identity of the cardholder. Internet sales leave the merchant liable for the loss.[25] More Internet transactions are charged back than retail transactions and stolen credit card numbers can be easily used to make purchases.[26] Credit card numbers are easily stolen and sold, each stolen credit card being worth approximately $25 on the international black market. The hacker who stole millions of credit card numbers from Target made several million dollars selling them on the Internet.

Already several obvious reasons emerge for preferring a virtual currency, which lead to several non-obvious reasons that signal a real reason for the global transactional market to make a shift. Before computers became ubiquitous, the fundamental organization of business monetary transfer was largely the same as today. Inventory, price lists, payroll, accounts receivable all recorded on a ledger or series of ledgers. American law and accounting rules mean every business must know exactly what its current prices are, inventory, shipping, accounts receivable, payable and a multitude of other factors. Computers built specifically for calculating these business transactions can now read in large amounts of data and apply operations to that data. These mainframes manage gargantuan amounts of data and process transactions continually. Today, a large portion of operations are done in-memory, as opposed to punch-cards and reel-to-reel tape, but businesses operate in the same fundamental way because in order to have transactional integrity, everything has to be checked against and applied to the ledger. Everything must eventually be tallied in a centralized system prevent double-booking or double-spending.[27]

---

24. *Id.* §1666i.

25. Thomas E. Weber, *What Do You Risk Using a Credit Card to Shop on the Net*, WALL. ST. J., Dec. 10, 2001, at B1.

26. Julia Angwin, *Credit-Card Scams Bedevil E-Stores*, WALL. ST. J., Sept. 19, 2000, at B1.

27. *Cf.* Joshua A. Kroll, Ian C. Davey & Edwward W. Felten, The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries (paper delivered at the Twelfth Workshop on

In the same fashion, credit cards run similar ledgers, except a card's balance is applied to an individual or organization's personal credit account. After locking the account to prevent tampering with transmissions, the card issuer will inspect the transaction for signs of fraud, deduct money from the customer's balance and credit the merchant, take fees, and the ledger will have the transaction recorded, then unlocked, which will send a return signal to the merchant that the transaction was successful. Because it is centralized to a single point of authority, the entire process takes only a few milliseconds. The complexity of computers, network, and engineering involved in this system is tremendous.

B. How Virtual Currency Works on a Technical Level

1. The Bitcoin's Block-Chain

Surprising to those who think of Bitcoins as anonymous currency, virtual currency is inextricably linked with a public ledger of transfer.[28] In fact, the very foundation of the Bitcoin's existence is bound with a public record of every exchange of every coin between transferors and transferees, published to all other users on the network, forming a chain that can be tracked the creation of the currency.[29] This list of all transfers, going back to the "Genesis Block" of original Bitcoins, is called the "Block chain."[30]

2. The Bitcoin Transfer Process

Bitcoin is essentially a unique serial number that gets hashed[31] using public-key cryptography whenever an owner wants to send a payment to a transferee. The transferor has a ledger indicating their ownership of a certain Bitcoin, which they have in their turn received via a series of transfers from the original Genesis block, each transfer of which is recorded and hashed again. Once the transferor declares they want to make a payment, they encrypt their owned serial number and announce to whom they want to make a transfer.[32] The public announcement is secure because all the vital information is encrypted, including the verification of the serial

---

the Economics of Information Security (WEIS 2013), Washington, D.C., June 11-12, 2013), *available at* http://www.weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf.

28. There are virtual currencies that do not use public ledgers in existence but they are not highly utilized and do not meet the definition of currency for this article.

29. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2009), *available at* https://bitcoin.org/bitcoin.pdf.

30. *Id*.

31. Encrypted, in the most generic sense.

32. NAKAMOTO, *supra* note 29.

number. The ingenious trick is that the verification is done by the public and discoverable, as computers on the network figure out what nonce[33] has been used with the public key. Other computers on the network, unrelated to the transaction, can verify the transfer by finding the nonce, which is relatively easy to discover within a few minutes by brute-forcing algorithms. By doing so, the transfer is verified as legitimate and at the same time a record of the transfer is made and distributed to the network, although the identities of the transferor and transferee are still encrypted and, theoretically, unknowable.[34] This means that all transferees of Bitcoins are on the public ledger, although their identities are encrypted. The block chain of Bitcoin owners has grown to 25 GB as of today.

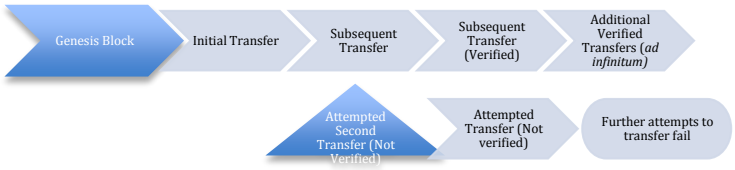

Fig 2: Hash Chain

Where do Bitcoin serial numbers come from? Actually, there are no stable serial numbers that correspond to any particular bitcoin. Transaction hashes fulfill the role of the serial number. In any transaction, the transferee receives a unique hash of their public key and the transferor's bitcoin serial number, which in turn was the output of an earlier transaction. Each transfer hashes the old serial number into a new one, which can only be transferred by the new owner.[35]

There are two implications to Bitcoin's use of transaction hashes instead of serial numbers. First, Bitcoins are not separate, persistent "coins" of unique serial numbers, rather each Bitcoin is better thought of as a series of transactions that show up in the block chain. The second, and more important result of operating in this way is that it obviates the need for any central authority to issue or verify the serial numbers.[36] Instead, the serial numbers are self-generated, merely by hashing previous numbers from prior transactions.

---

33. Permutation of the public key.
34. NAKAMOTO, *supra* note 29.
35. This owes to the unique nature of public-key cryptography. The details of how this works are incredibly innovative, but beyond the scope of this article. *See id.*
36. *Id.*

In fact, it's possible to keep following the chain of transactions further back in history than just the previous transfer. Ultimately, this process must terminate. The chain of transfers can be followed back to one of two originating transactions. The first possibility is that the ledger tracks back to the first Bitcoin transaction, contained in the so-called Genesis block, the original bitcoins. This is a special transaction, having no inputs, but a 50 bitcoin output. In other words, this transaction established the initial money supply.[37] The Genesis block is treated separately by Bitcoin clients, and although the details can be more complex than the standard transaction, we can think about these transfers in a similar fashion to subsequent transactions described above. The important thing to remember is just that anyone can create a Genesis block of a Bitcoin-like virtual currency by making an initial transaction.[38] From there, subsequent transfers can be made by the initial transferees to anybody.

The second (and more likely) possibility would be to track the coin back to a "coinbase transaction." Except for the Genesis block, every block of transactions in the block chain starts with a special coinbase transaction. Coinbase transactions are created to reward the third party miners who confirm others' transactions. They are designed to reward that miner for validating that block of transactions. The hash uses a similar but not identical format to the Genesis transaction described above. Coinbase transactions are rewards to incentivize the other users of the network to donate their resources verifying transfers between other, anonymous, users. Unfortunately, they are set to expire after a given period of time or number of transfers, effectively capping the upper-bound of the given currency, preventing the creation of new currency in that ledger.[39]

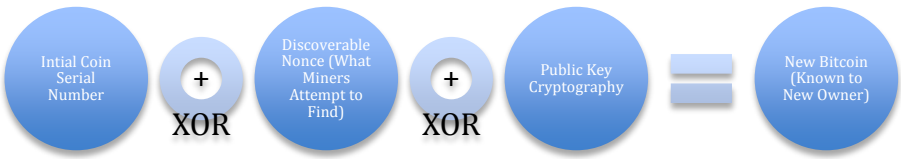

Fig 3: Hash numbers between transfers

37. *Id.*
38. *Id.*
39. *Id.*. In 2024, miners will cease to be compensated for facilitating transfers, and "mining" will either cease entirely or be done in return for bounties offered by the transferring parties in return for verification.

3. What This Means

How anonymous is Bitcoin? Many people claim that Bitcoin can be used anonymously. This claim has led to the formation of marketplaces such as the Silk Road (and various successors), which specialize in illegal goods. However, the claim that Bitcoin is anonymous is a myth.[40] The block chain is public, meaning that it is possible for anyone to see every Bitcoin transaction ever, back to the Genesis block or coinbase transaction. Although Bitcoin addresses aren't immediately associated with real-world identities, computer scientists have done much work figuring out how to de-anonymize "anonymous" social networks. The block chain is a marvelous target for these techniques. The great majority of Bitcoin users will be identified with relatively high confidence and ease in the near future.

The confidence interval linking block chain transferees and individuals will be enough to achieve probable cause for further investigation of discovered individuals, but not high enough to generate convictions without more evidence. But law enforcement will soon be able to identify likely targets whom they suspect of illegally using virtual currency. Furthermore, identification will be retrospective, meaning that someone who bought drugs on Silk Road in 2011 will still be identifiable on the basis of the block chain whenever these techniques are developed. These de-anonymization techniques are well known to computer scientists, and therefore to the NSA, and likely eventually will be used by law enforcement.

The existence of this public ledger is essential to ensuring that Bitcoins cannot be double-spent, which means that the ledger is, absent some currently-unforeseeable technological development,[41] a necessary function of the currency. The implications of this are nontrivial, and it is vital to understand that this ledger must exist for secure virtual currency to exist, to understand how any likely possible regulatory scheme may be implemented. Any discussion of "virtual currency" that does not include the

---

40. Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System*, *in* SECURITY AND PRIVACY IN SOCIAL NETWORKS 197 (Yaniv Altshuler et al. eds., 2013), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6113303&isnumber=6113084

41. *See* Patricia Everacre, Isabelle Simplot-Ryl & Issa Traoré, *Double Spending Protection for E-Cash Based on Risk Management*, *in* INFORMATION SECURITY 394 (Mike Burmester, Gene Tsudik, Spyros Magliveras & Ivana E. Ilić eds., 2011) (Lecture Notes in Computer Science No. 6531), *available at* http://dx.doi.org/10.1007/978-3-642-18178-8_33/.

public ledger is either misinformed or discussing a technology that cannot in good faith be called virtual currency.[42]

The last significant development in virtual currency is the creation of various online currency exchanges.[43] These exchanges permit the trading of actual cash into various cryptocurrencies (which now number over one hundred), and the exchange of these currencies. An exchange will also take possession of Coins owned by a customer and hold them in trust. An exchange can make paper trades on Coins held in trust, offer them for sale, and (supposedly) hold Coins safely. In theory, virtual currency exchanges permit buyers, sellers, and speculators to come to a consensus on Coin price similar to traditional stock and commodity markets. In practice, Bitcoin exchanges are targets for hackers and thieves, and are often operated dishonestly and openly operate with security holes amounting to negligence,[44] while speculators end up eating their hats on uncontrolled currency losses.[45] Even the Winklevoss twins, who have become famous for suing Mark Zuckerberg, are venture capitalists attempting to generate support for their Bitcoin payment processing system.[46] Several more legitimate currency exchanges have since been created with a focus on security and efficiency, the most important of which is Coinbase, which has attracted $25 million in venture capital.[47]

---

42. At least, this is the case barring further cryptographic developments.

43. Mt. Gox and Flexcion were two of the largest early adopters, but both have closed their doors after being hacked. Cryptsy, a U.S.-based exchange, shows the same signs of mismanagement but is currently still operational. Vircurex, a Chinese exchange, and Kraken, a UK and U.S. located exchange, are also both operating at the time of this publication.

44. *See, e.g.*, CoinLab, Inc. v. Mt. Gox KK Et Al, No., 2:13-cv-00777 (W.D. Wash. Oct. 4, 2013).

45. *Reddit Hat Eat*, YOUTUBE (Mar. 26, 2014), *available at* http://youtu.be/mjiX7xiFD-o/.

46. Colleen Taylor, *With $1.5M Led by Winklevoss Capital, BitInstant Aims to Be the Go-To Site to Buy and Sell Bitcoins*, TECHCRUNCH.COM (May 17, 2013), *available at* http://techcrunch.com/2013/05/17/with-1-5m-led-by-winklevoss-capital-bitinstant-aims-to-be-the-go-to-site-to-buy-and-sell-bitcoins/.

47. For information about Coinbase, see ABOUT COINBASE, https://coinbase.com/about/ (last visited July 9, 2014). *See also* ATLAS [NORTH AMERICA], https://atlasats.com (last visited July 9, 2014); PERSEUS, http://perseustelecom.com (last visited July 9, 2014).

II. Use of Virtual Currency Today and Tomorrow

A. What Advantages Do Public Ledger Virtual Currencies Have Over Single-Point Payments?

1. Cost Advantage

The first and most justifiable reason a virtual currency should exist and enjoy frequent use is the convenience and safety of such payment methods. Public ledger payments are inconvenient, but they are inconvenient at a constant rate. The costs of Bitcoins do not scale upward for large payments as opposed to small payments, or for international payments as opposed to local payments. Indeed, the major reasons for Bitcoin adoption involves harmless, if nerdy, hobby trading. Small-scale sales of durable goods (hobby collectibles which I will consider a kind of commodity) is not economical when factoring in exchange rates and international payment fees. Virtual currency somewhat mitigates these problems.

Additional problems with long-distance sales include international escrow in the age of the internet: a stable international payment system would make international purchasing, labor and regulatory costs much easier to minimize by globally sourcing the cheapest location regardless of local currency. In fact, it is conceivable that with large-scale trading hubs, international currency arbitrage will become radically altered in the future. Bitcoin is the first invention of a method of transfer between unknown parties without needing recourse to a trusted third party.

For example, Bitcoin or other digital currencies might enable individuals to transfer money as seamlessly as sending an email, while reducing money transfer and currency conversion fees. Payments between unknown parties can take place without regard to which countries those parties live in. This is a significant step forward for the global market.

Businesses may use Bitcoins to accept non-cash payments for the same percentage fee regardless of purchase amount ($5M or $0.05). Again, this makes virtual currency much more lucrative for business-owners seeking a global market, and allows competitive advantage on the global stage without international barriers to transaction caused by the use of intermediaries such as banks or credit card companies. As payment costs scale upward, international money transferors charge fees that begin to outgrow profits, like tariffs reducing the efficiency of the global market.

Travelers may conceivably buy goods abroad without paying cross-border fees typically charged by banks. However, it is important to note that the future could look different as rising regulatory and operating costs for Bitcoin and potentially falling costs for the conventional players as they are

forced to compete could narrow the cost savings in using virtual currency. Just as a flurry of new entrants – such as Square, Groupon, and PayPal - encouraged payment networks and payment processors to develop a mobile payments strategy, traditional payment players will likely develop virtual currency strategies.

Currently, consumers pay a money transfer fee as a percentage of the total amount transferred: approximately 10% on average. Money transfer networks, such as Western Union, charge these fees for accessing their network, as well as to cover agent commissions and foreign exchange conversion fees. Today, Bitcoin could theoretically reduce these fees to 1% by bypassing traditional money transfer systems and instead enabling transfers directly between two Bitcoin wallets. As a result, annual net savings for consumers could theoretically amount to over $43 billion based on the World Bank's estimate of global money transfers.[48] But any savings in this context usually involves at least one of the parties being unbanked, which would make converting bitcoin into local currency very difficult. And in countries where access to a bank, or conversion of foreign currency has been limited, virtual currency is likely to face similar challenges.[49] The tight control China has taken to devalue the Yuan has led it to become the first nation to outlaw banks from trading in Bitcoin. This makes conversion of Yuan into Bitcoin much more difficult than simply using a traditional payment method.

Clearly, the biggest hurdle to widespread adoption of virtual currency would be maintaining its cost-advantage over traditional payment methods. In fact, as we consider the regulatory structure of virtual currency, we will either see any development stymied by over-reaching regulation, or we must create a regulatory system that fosters this development by maintaining its competitive edge over traditional payment schemes.

The use of virtual currency will only grow if it can maintain its cost-advantage over traditional payment methods. The most likely area where virtual currencies can maintain this advantage is through global product sourcing. Thus, the value of virtual currency can be computed:

48. Roman Leal, *Is Bitcoin the Future of Payments?*, TOP OF MIND (Goldman Sachs Global Investment Research Paper), Mar. 11, 2014, Issue 21, at 18.

49. *Id*.

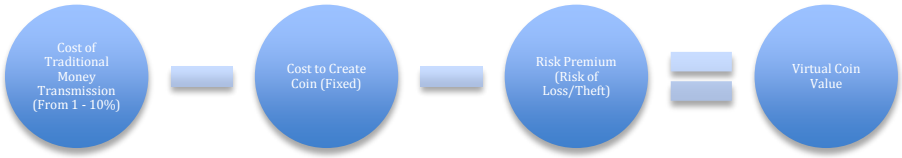

Fig. 4: Calculating the Real Value of a Bitcoin[50]

2. Ease of Use in Illegal or Sensitive Transactions

A second, and less justifiable reason for use of virtual currency, but one that has led to a large part of its adoption, is the avoidance of banking regulations and laws. Bank secrecy laws, especially the reporting requirements that have been implemented since 9/11, have led to burdensome and invasive reporting requirements.[51] But despite their poor implementation and unintended consequences, there is no legitimate reason to avoid these requirements except money laundering and tax evasion. And, indeed, Bitcoins have become a fairly robust platform by which to engage in illegal transactions.

There is an "underground" Internet, known as the TOR network,[52] which exists mainly to provide anonymity through multiple layers of blind identity encryption. This network, outside of the traditional Internet, has been used to buy and sell black market goods, but until recently the major hurdle to implementation has been the inability to anonymously ensure payment. Bitcoins have led to a Silk Road website on the TOR network by providing the anonymous payment scheme needed to conduct illicit deals. The Silk Road and its progeny, underground Internet hubs for the sale of drugs and

---

50. CTM1 (the cost of traditional money in a transaction) minus CCC (the fixed cost to create the coin) minus RP (the risk premium associated with losses, thefts, frauds) equals VCV (the value of a virtual coin).

51. Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses, 31 C.F.R. § 1010.100(ff) (2011) (the "MSB Rule"). This defines an MSB as

> a person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities listed in paragraphs (ff)(1) through (ff)(6) of this section. This includes but is not limited to maintenance of any agent, agency, branch, or office within the United States.

52. The Onion Router, so-called because its Russian-doll layers of encryption are likened to the layers of an onion.

other contraband, spring into existence as fast as the DEA and FBI can shut them down.[53] In October 2013, the U.S. government shut down the Silk Road website and seized $28 million in Bitcoins,[54] but a second Silk Road came online soon afterwards. In fact, it seems likely that the convenience of virtual currency and anonymity of the TOR underground network will lead to a persistent online black market from this point onward.

The U.S. Senate has held hearings aimed at discovering whether these so-called crypto-currencies are a tool for drug dealers and money launderers to do business beyond official scrutiny, and stat regulators have held panels on how best to manage the panorama of new virtual currencies. Bitcoins can be "legal means of exchange" according to officials from the U.S. Justice Department, which recognizes "that virtual currencies, in and of themselves, are not illegal."[55] Fed Chairman Ben S. Bernanke wrote to the Senate committee the U.S. central bank has no plans to regulate the currency: "Although the Federal Reserve generally monitors developments in virtual currencies and other payments system innovations, it does not necessarily have authority to directly supervise or regulate these innovations or the entities that provide them to the market."

The use of virtual currency in money laundering enterprises is concerning. The goal of traditional money laundering is to channel money through a source of intermediary so as to conceal its source.[56] Prosecuting virtual currency exchanges has little chance of diminishing the use of virtual currency in money laundering.[57]

---

53. Press Release, U.S. Immigration & Customs Enforcement, HSI Seizes Silk Road Underground Black Market Website (Oct. 2, 2013), *available at* http://www.ice.gov/news/releases/1310/131002baltimore.htm.

54. Press Release, U.S. Immigration & Customs Enforcement, Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website (Oct. 25, 2013), *available at* http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website.

55. Max Raskin, *U.S. Agencies to Say Bitcoins Offer Legitimate Benefits*, BLOOMBERG (Nov. 18, 2013, 4:08 PM CT), http://www.bloomberg.com/news/2013-11-18/u-s-agencies-to-say-bitcoins-offer-legitimate-benefits.html (quoting Mythili Raman, Acting Assistant Attorney General at Justice Department's Criminal Division, at the Committee on Homeland Security and Governmental Affairs).

56. OFFICE SPACE (Twentieth Century Fox 1999).

57. Catherine Martin Christopher, *Whack-a-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Laundering*, 18 LEWIS & CLARK L. REV. 1 (2014), *available at* https://law.lclark.edu/live/files/17113-lcb181art1christopherpdf.

3. The Public Ledger

A third reason for the use of virtual currency is the public creation of a transfer ledger as part of the Bitcoin transfer process. Bitcoins cannot be transferred without a public key encrypted transfer ledger. Despite their reputation as anonymous, encrypted records of every transfer back to the initial creation of the currency exists and is public. It is very likely that these records will be (or have already been) decrypted to discover the record of their sale. This kind of ledger paradoxically makes the laundering of virtual currency or purchase of illicit goods much riskier than certain international money transfer procedures.

This should be a boon to law enforcement agencies who seek to understand the flow of the black market. Even assuming that the identities of the transferors remains anonymous, the raw data regarding transfer is available publicly. This will enable the research into the extremely nebulous and difficult-to-penetrate world of the illegal marketplace. Merely the existence of this public ledger will benefit law enforcement as it will offer insights into areas where enforcement is lax, or where resources would be more efficiently applied.

Another benefit to law enforcement in the virtual currency is the ease by which this value may be seized. Currently, the largest single owner of bitcoins, after the creator, is the FBI.[58] Seized from illegal TOR networks, bitcoins can be obtained by physically seizing the servers on which the wallets are held, or virtually, by forcing a transfer of publicly available bitcoins. Law enforcement agencies with jurisdiction need only probable cause to seize property connected with criminal enterprise, and as the technology to track sales and the identities of users develops, methods to seize Coins that have been used to facilitate illicit sales will become routine. If routine seizure of Coins used in illicit transactions becomes standard, the cost of using virtual currency to engage in illegal activity will rise.

Traditional money laundering techniques generally cost about 10% of the money to be cleansed. Thus, law enforcement needs only to find and seize a relatively small portion of the money used in illegal transfers before the costs rise to a level that will deter virtual currency from being used in this

58. Press Release, FBI, Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website (Oct. 25, 2013), *available at* http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website.

fashion. I will elucidate in a future article the methods by which this may be achieved.

4. Cryptographic Security and Account Protection

If a Bitcoin is stolen, the only loss has been the value of the coin. It exists as a unit of exchange itself, and not an account or balance. The amount of value that can be lost to a hacker is limited to the amount that is kept online, while those kept in offline "wallets," which are really just computer memory storage units kept unconnected to the internet, cannot be seized. While there are other ways of potentially taking offline Coins, having an upper bound on loss can be comforting.

The pure technological marvel of virtual currency is exciting. The implementation of the Bitcoin and the cryptographic ideas embodied within are fascinating and ingenious. The use of virtual currency embodies, for some in the technical community, the radical democratization and anti-authoritarian ideology that techno-futurists covet.[59] Whether these goals are laudable or misguided is beyond the scope of this article.

B. What Disadvantages Do Bitcoins Have?

1. Theft

The major downside of virtual currency is the other side of the coin to its major advantage: the ease of transfer makes them easily stolen. There is very little consumer protection at any level of a Bitcoin transaction. Losses from theft, fraud, or failure to live up to a contract will generally go unrecovered.

Bitcoins can be attacked in several methods. The most dangerous point of contact is in the exchange, when Bitcoins are offered up for sale and can be transferred at this point. This has led to some commentators to believe that regulation should focus on the exchange phase. Bitcoins themselves enjoy 128-bit public-key security: they are equally secure as any encrypted website or online purchase in terms of pure cryptography. The issues that have arisen have all been human error. Mt. Gox and FlexCoin were badly programed for security.[60] The owners of the sites probably committed criminal malfeasance leading to the losses from the sites. [61] Poorly picked

59. Sarah Jeong, *The Bitcoin Protocol as Law, and the Politics of a Stateless Currency*, SSRN (May 8, 2013), http://ssrn.com/abstract=2294124.

60. Leaked code purported to belong to Flexcoin shows key failures to meet industry-standards regarding privacy. The first warning sign may have been when the secret passkeys for customer's Coins were used as plaintext web addresses.

61. Greene v. MtGox Inc., No. 1:14-cv-1437 Doc. 1, at 5 (N.D. Ill. Feb. 27, 2014).

passwords and sloppy programming account for the vast majority of stolen Bitcoins. Once stolen, Bitcoins are effectively gone and cannot be returned, even though the block chain has recorded the theft.

In early November of 2013, researchers at Cornell University published a paper asserting that the virtual currency can be broken if the system of mining algorithms can be successfully exploited by a group of sufficiently selfish miners who obtain a majority control of the current mining pool. [62]

Authorities in the United States have cracked down on the criminal use of virtual currencies in a few cases, but those have been isolated situations in which the coins have been used for illegal purposes in the real world, like money laundering and trade in illicit goods. The owner of the Silk Road, a website where drugs and weapons could be bought with Bitcoins, was arrested earlier this year after attempting to procure an assassination of a business rival.[63]

But for crimes contained within the Bitcoin network — like thefts from apparently reputable online wallets where Bitcoins are stored — there has been almost no accountability.

Unauthorized transfer of bitcoins is very easy when few precautions are taken, but can be made extremely difficult if some relatively straightforward precautions are put into place. Bitcoins are secured using Public Key Infrastructure (PKI), which simply means that some encryption code – a "private key" or password - is established for every public Bitcoin address, and that private key must be used to decrypt and spend Bitcoins. This private key is really nothing more than a text file with gibberish written inside. Theft occurs when an unauthorized user accesses that text file, which enables them to spend the bitcoin. Theft is by far the biggest security vulnerability. But loss is also a concern; there have been many instances of individuals accidentally losing the private keys that allow them to spend their Bitcoins. If the text file is deleted with no backups, the bitcoin cannot be spent, and the result is that it becomes useless and loses its value.

Exchanges face more problems, because they are known sites offering continually available Coins. On March 2, 2014 Flexcoin was attacked and robbed of all coins in the hot wallet. The attacker made off with 896 BTC transferring them into two anonymous addresses. Flexcoin released a notice that simply stating that, because it did "not have the resources, assets, or

62. Ittay Eyal & Emin Gun Sirer, *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*, CORNELL UNIV. LIBRARY ARXIV.ORG (Nov. 15, 2013), http://arxiv.org/pdf/1311.0243v5.pdf.

63. Paid in Bitcoin, naturally.

otherwise to come back from this loss, [the Flexcoin exchange would close its] doors immediately." A small notice in the terms of use offered the following cryptic waiver of liability: "Legal Notice: We are not a true bank that accepts USD or any national currency, only bitcoins which by their nature are not regulated, we're not FDIC insured or regulated by any government entity." The Alberta-based Flexcoin simply declared bankruptcy after determining that two of its accounts had been hacked.

The largest exchange, Mt. Gox, which had been losing Coins over the course of several months, first deducted their losses from customer accounts, and then declared bankruptcy. Being based in Japan, where virtual currency is looked upon unfavorably, chances of customers obtaining recourse are slim.

The largest Bitcoin payment processor in Europe, BIPS, has been hacked for a loss of about $1 million worth of Bitcoins, including coins that were in the personal online wallets of customers. The company,stated that it would be "unable to reimburse Bitcoins lost unless the stolen coins are retrieved." While Danish police were examining the case BIPS further stated that the authorities could "not classify this as a theft due to the current nonregulation of Bitcoin."[64]

The People's Bank of China, among five Chinese agencies released a notice that they would not use virtual currency that citizens of the country would still be allowed to buy and sell, but it warned that participants "assume the risks themselves."[65] This lack of protection is likely a calculated disincentive for the use of virtual currency in China, ensuring that Chinese banks retain tight control of the Yuan.[66]

Fraud may also be (and has been) perpetrated by an exchange client: an exchange sends money to a client, but the client says that they never received it; when the exchange tries to find the transaction using the Bitcoin hash, which is the record in the block chain that allows you to identify the transaction, the exchange cannot find it because it has been changed by the client. Since the exchange cannot find the hash, their program assumes there was an error with their system and a second transfer is attempted.

---

64. Nathaniel Popper, *In the Murky World of Bitcoin, Fraud Is Quicker Than the Law*, N.Y TIMES, Dec. 5, 2013, http://dealbook.nytimes.com/2013/12/05/in-the-murky-world-of-bitcoin-fraud-is-quicker-than-the-law/?_php=true&_type=blogs&_r=0.

65. Monetary Policy Analysis Grp. of the People's Bank of China, China Monetary Policy Report: Quarter Four, 2013 (Feb. 8, 2014), *available at* http://www.pbc.gov.cn:8080/image_public/UserFiles/english/upload/File/2013MPR-afterNancy(1).pdf

66. Lou Yao-xiong, Wu Jun, *Analysis of Legal Issues of Bitcoin*, 15 J. BEIJING UNIV. POSTS & TELECOMMUNICATIONS 25 (2013) (Social Sciences Edition).

Dishonest clients may use this fraud to double and triple dip while rapidly sending the command withdrawing their money, receiving consecutive transfers. This vulnerability is known as "malleability." While this vulnerability of the Bitcoin protocol allowing this type of fraud has been known for several years, and the Bitcoin Foundation has offered protocol fixes that prevent properly-run exchanges from facing this fraud, several exchanges have been bankrupted after the fix was released. Mt. Gox and FlexCoin operated a version of the protocol that inadequately addressed the malleability issue. However, malleability should no longer be considered an exploitable problem, despite many exchanges confirming malleability thefts.

There has already been one major possible attack on Bitcoin elaborated, which would involve one person obtaining control of a major portion of the Coin mining computer network and maliciously holding back portions of the block chain. This attack, while potentially serious, is beyond the scope of the article, except to note in passing that other attacks may be discovered in the future that pose significant risks to the currency.

The risk of theft, where liability should fall, and what waivers consumers can be expected to accept will be discussed below.

2. Poor Speed and Excessive Resource Use

The second major downside of Bitcoins, and any currently foreseeable virtual currency, is its inefficiency. Bitcoins are tremendously inefficient in three ways: Time, Computing Resources, and Transmission Data. Coins "cost" a lot of computing power to simulate trust by brute-force solving algorithms to verify trades.[67] This uses a massive amount of energy; and to encourage users to make this sacrifice, users must be paid in inflationary currency. Bitcoin is far less efficient than our current banking and credit card system for most trades. No transfer can take place without the brute force computations to verify the transfer, which means they must always take more time than a single-point transfer will. Lowering the time it takes to make such a transfer would be untenable, as it would open the Bitcoin up to several vulnerabilities that would render them useless. Unfortunately, Coins will always cost resources to transfer, and those resources must always be paid by (presumably neutral) third-parties. Those parties must be paid, either through inflation or direct payment, in order for the system to function.

---

67. William J. Luther, *CryptoCurrencies, Network Effects, and Switching Costs* (Mercatus Ctr., Working Paper No. 13-17, 2013).

When you distribute the business ledger, you can no longer simply talk to a single point of authority (as exists for credit card transactions, elaborated above), and all transactions must wait until they are verified by anonymous other players on the network. Instead of it taking a few milliseconds, it takes several minutes to get back an answer. Transactions in Bitcoin are designed to take about ten minutes to process, and attempts to speed this up would make the system insecure. Less time would permit double-spending of bitcoins or permit users with large relative computing power to solve multiple transfers without publicly verifying them and ruining the network by thereby destroying the incentive for others on the network to verify transfers.[68]

Currently, Coin trading volume is low, but the volume of trading has little effect on the timing or resource costs of Bitcoin. Again, it is the double-edged sword of virtual currency that all "costs" of a transfer remain fixed, whether the payment is for one dollar or one million dollars. Whether trading volume is low or high, the protocol itself is limited to 7 transactions per second. For comparison, a major retailer could engage in 5,000 transactions per second on Black Friday. Wal-Mart's 10 million transactions between 8 p.m. and midnight on Black Friday of 2012 would take Bitcoin system more than 800 days to record.[69] Bitcoins must remain limited to relatively infrequent purchasing systems, which again make them useful for globalized product purchases and not much else.

3. Third Party Mining

The last problem with Bitcoins is that they require third parties to do work in order to generate the block chain. The third party computers brute-force a cryptographic solution to the problem posed by the transaction, which has been summarized to the public as "solving difficult math problems." In order to incentivize third parties to use their resources, this stage of the transaction has been termed mining, because miners receive payments of new Bitcoins for successfully solving the math problems. New

68. Matthias Herrmann, Implementation, Evaluation and Detection of a Doublespend-Attack on Bitcoin (Apr. 24, 2012) (unpublished Master's thesis, Department of Computer Science, ETH Zürich, *available at* http://e-collection.library.ethz.ch/eserv/eth:5606/eth-5606-01.pdf.

69. Jessica Wohl, Reuters, *Walmart Says It Has Best Black Friday Ever Despite Protests, Crowds*, HUFFPOST BUSINESS (Nov. 23, 2012), http://www.huffingtonpost.com/2012/11/23/walmart-best-black-friday_n_2178541.html.

Bitcoins are generated when miners solve a transaction and the miner owns those new Bitcoins.[70]

If virtual currency becomes widespread, new developments either in technology, in law, or agreements by major institutions, will be required to solve the 51% problem identified by cryptographers.[71]

Currently, mining generates a tremendous amount of money (in the form of Bitcoins). The temptation to create value merely by expending computer processing power is so great that there exists a market for Bitcoin mining computers.[72] There are also already criminal hackers who have used computers in an unauthorized manner in order to mine Bitcoins. A New Jersey software company created a botnet to mine coins.[73] And a computer science student at Harvard exceeded his authorization to use a supercomputer to mine Dogecoins.[74]

Presently 3,600 bitcoins are created per day, which totals to 1,314,000 new Coins each year. This means Bitcoin currently has a monetary inflation rate of over 10% per annum. All of the new Coins are owned by the miners to incentivize them to process and verify other users' transactions. There are about 60,000 transactions per day on the bitcoin network. That accounts for an upper bound of 4,000 new coins created per day, if blocks are confirmed slightly quicker than an average of ten minutes each. For each transaction on the bitcoin network, miners receive 1/15th of a bitcoin. When bitcoin was worth $1,000 each miner earned $66 in virtual currency for every network transaction they solved.

---

70. A. Bogliolo, P. Polidori, A. Aldini, W. Moreira, P. Mendes, M. Yildiz, C. Ballester & J. Seigneur, Virtual Currency and Reputation-Based Cooperation Incentives in User-Centric Networks, paper delivered at the 8th International Wireless Communications and Mobile Computing Conference (IWCMC), Aug. 27-31, 2012), *available at* http://iee explore.ieee.org/stamp/stamp.jsptp=&arnumber=6314323&isnumber=6314161.

71. Eyal & Sirer, *supra* note 62; *see also* Nicolas Houy, *It Will Cost You Nothing to "Kill" a Proof-of-Stake Crypto-Currency* (Groupe D'analyse de Théorie Économique, Working Paper No. WP 1404, Jan. 2014), *available at* http://halshs.archives-ouvertes.fr/ docs/00/94/50/53/PDF/1404.pdf.

72. Daniel Plohmann & Elmar Gerhards-Padilla, Case Study of the Miner Botnet (papewr delivered at the 4th International Conference on Cyber Conflict (CYCON) (2012)), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6243985&isnum ber=6243954.

73. Complaint, Hoffman v. E-Sports Entm't (Super. Ct. of N.J. Nov. 19, 2013), *available at* http://nj.gov/oag/newsreleases13/E-Sports_Complaint_Consent-Judgment.pdf.

74. Danny Lee, *Harvard University Student Hijacks Computer to Mine Dogecoin Currency*, SOUTH CHINA MORNING POST, Feb. 26, 2014, http://www.scmp.com/news/world/ article/1434773/harvard-university-student-hijacks-computer-mine-dogecoin-currency.

Ultimately, it costs the network from $40 to $70 per transaction, in the form of inflation. Compare this to normal credit cards, where the average transaction fee is $2 or $3. Bitcoin transactions cost up to 20 times as much as credit card transactions. Right now, this cost is being masked through monetary inflation. Take the inflation out of the system, and all of those costs would have to be paid in transaction fees. This economic system can never achieve stability.[75]

There are methods of mitigating or eliminating this aspect of virtual currency,[76] but public ledger virtual currencies can never completely eliminate the tragedy of the commons and all transfers between peers will require that others do work for their benefit.[77] It may be that a system of contracts or traditional arrangements will come into shape similar to the EFT network that currently exists between banks.[78]

III. Virtual Currency: Currency, Commodity, or Contract?

A. Currency?

To begin thinking generally about the regulatory schemes we may envision, let us first determine what we are discussing. Having provided a general overview of the Bitcoin, what it is and how it works, let us try to categorize it.

A Bitcoin doesn't have any backing government or even regulatory body protecting its value or ensuring its legitimate use. This is the most obvious distinction against its being considered a currency. It has not been issued by any governmental body, or even an organization with quasi-authoritarian status.[79] Additionally, it is not used with the level of frequency or confidence to be considered a means of transaction. It is not a currency.

---

75. Jörg Becker, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer & Rainer Böhme, *Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency*, *in* THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY 135 (Rainer Böhme ed., 2013) *available at* http://link.springer.com/chapter/10.1007/978-3-642-39498-0_7.

76. Simon Barber, Xavier Boyen, Elaine Shi & Ersin Uzun, *Bitter to Better — How to Make Bitcoin a Better Currency*, STANFORD UNIV.: APPLIED CRYPTO GROUP, http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf (last visited July 2, 2014).

77. Moshe Babaioff, Shahar Dobzinski, Sigal Oren & Aviv Zohar., On Bitcoin and Red Balloons (Feb. 2012), *available at* http://research.microsoft.com/pubs/156072/bitcoin.pdf.

78. See ETFs described *supra*.

79. .François R. Velde, *Bitcoin: A Primer*, CHICAGO FED LETTER (Fed. Reserve Bank of Chi.), Dec. 2013, No. 317.

Eric Posner believes Bitcoins are a form of commodity; albeit one unregulated by the government:

> There is a long history of unregulated currencies. Gold has been an unregulated currency at various times and in various places. In prison camps, cigarettes have served as currency. In the United States in the 19th Century, in some states, the currency was basically unregulated; people would set up banks that issued bank notes that circulated. Sometimes you get an unregulated currency simply because there is no government. Sometimes you get an unregulated currency because there is a government but it does not control the money supply very well or the government is corrupt and people do not trust the official currency. Bitcoin just seems to be another version of this. It is a lot like gold, in fact. The difference, of course, is that it is digital rather than a heavy, unwieldy object. That means that it could serve the same purposes as gold in terms of a currency, but much more efficiently because it does not have any mass and can be sent easily from place to place.[80]

Posner has some legal precedent on his side: A Texas federal district court ruled that Bitcoins were a currency for the purpose of determining jurisdiction.[81] But the most commonly used definitions of currency: Is the currency widely accepted as a medium of exchange and does it share a common value? In the case of Bitcoins, both definitions must be considered flexibly. Bitcoins are widely accepted as medium of exchange in sheer geographic area (they have been used in forty countries at least), which puts them in a different arena than pseudo-currencies like cigarettes or company script. And they share a common value in the sense that their purported fair market value is available on a live exchange at all times. But this is not the whole story.

FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of

---

80. *Interview with Eric Posner*, TOP OF MIND (Goldman Sachs Global Investment Research Paper), Mar. 11, 2014, Issue 21, at 4.

81. *See* discussion *supra* text accompanying notes 88-89.

issuance."[82] The IRS has also come out against Bitcoins' status as currency.[83]

In my judgment Bitcoins are not currency because they do not represent stable measurements of value. The value of a Bitcoin is far too speculative to be considered currency. Bitcoins famously have an upper bound built into the system: By 2024 no new Bitcoins will be made and all mining payments will be done through payment of existing Bitcoins. This is designed to prevent runaway inflation.

Believers in this system tend to underestimate the costs. "Big miners and mining pools would be stupid to do things that undermine confidence in bitcoin and make their investment worth less. I predict history will repeat itself, and the current panic over GHash.IO will self-correct over the next few weeks."[84] But the booms and crashes in the currency, reflecting its speculative value, belie the truth.

In effect, Bitcoin can never be a currency because its value can never achieve stability. Disregarding the lack of a stabilizing central bank, even in an ideal free market the pressures inherent to the Bitcoin will necessarily create radical price differences on a continual basis. My theory has thus far been borne out by the bubble, bust, and recovery of Bitcoins to date. With no stable measure of value, Bitcoins can never be used as currency.

B. Commodity?

Is Bitcoin a commodity? It has more characteristics in common with commodities than with currency, except for the most essential: It has no inherent value. Virtual property can have value,[85] but the natural value of Bitcoin is nothing, or close to nothing, and values above equivalent transactions fees on arbitrage are purely speculative.

"Commodity" defines any item that "accommodates" our physical wants and needs. And one of these physical wants is the need for a store of value. Throughout history humans have used different commodities as a store of value (cocoa beans, pork bellies, oranges, or most commonly: gold).[86] In contrast, a security is any instrument that is "secured" against something

82. 31 C.F.R. 1010.100(m) (2011).

83. IRS Pub. Notice 2014-21 (2014), *available at* http://www.irs.gov/pub/irs-drop/n-14-21.pdf.

84. Robert McMillan, *Bitcoin Stares Down Impending Apocalypse (Again)*, WIRED (Jan. 10, 2014), http://www.wired.com/2014/01/ghash/ (inteview with Gary Andresen).

85. Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593 (E.D. Penn. 2007).

86. Dominic Wilson & Jose Ursua, *Is Bitcoin a Currency? No*, TOP OF MIND (Goldman Sachs Global Investment Research Paper), Mar. 11, 2014, Issue 21, at 6.

else. As a currency is usually secured by a commodity or a government's ability to tax and defend, it is considered to be a security. By these definitions, bitcoin is a commodity, and not a currency, while Bitcoin with a capital "B" is the technology, or network, that bitcoin moves across.[87] The analogy would be Shale technology versus shale oil.

Still, bitcoins can be sold *as* investment instruments. A Southlake oil and gas company ran afoul of Texas securities regulators after raising capital through the bitcoin.[88] The Texas State Securities Board ordered Balanced Energy to stop selling securities on the grounds that it had failed to disclose to its investors the risk of financing operations through a virtual currency subject to large fluctuations in value.[89] Clearly virtual currency can achieve value if intrinsically tied to some other, real value or venture. In such cases, virtual currency is a form of readily traded stock or method of establishing ownership of a more traditional commodity, like oil or gold.

> It is almost universally accepted that any commodity that would make a good store of value should be stable over time (non-reactive). Though not as stable as gases, gold and other precious metals are the least reactive elements that are in solid form. Bitcoin is "reactive" since software change has occurred in the past. There are thousands of bitcoin miners that maintain the Bitcoin network by using their computing power to verify transactions and place them in a block chain. If a majority of this computing power switched their software to adopt a change, then effectively that new software would become the standard and any verification using the old software would be rejected. Gold also has nearly no competing substitutes that can erode its value. Silver is more reactive and plentiful than gold. Palladium is far less dense. While platinum can compete with gold on most physical attributes, it is too rare and has catalytic properties that bid it away from investment demand. Competition is likely bitcoin's weakest point, as its position was only secured by being the first mover. However, primary competitors – Litecoin and Ripple – are not yet a serious threat. Litecoin is bitcoin's silver

87. Jeff Currie, *Bullion Bests bitcoin, Not Bitcoin*, TOP OF MIND (Goldman Sachs Global Investment Research Paper), Mar. 11, 2014, Issue 21, at 7.

88. Sec. & Exch. Comm'n v. Shavers, 4:13-CV-416, 2013 WL 4028182 (E.D. Tex. filed Aug. 6, 2013).

89. *Id.*

> and is less valuable and secure. Ripple is an exchange that supports multiple commodities including bitcoin, gold and silver.[90]

I say this because, as far as I can see, the only true value of a virtual currency is the ease with which it can be used in payment, both intra and internationally. Virtual currency, as I've said above, easily facilitates international payments and avoids several costs and delays that come with traditional international banking. The difference between these costs and the cost of using a method of virtual currency are the value of that virtual currency, and a Bitcoin can be said to have this value. In a world like ours today, where the costs of international payment are high and the costs of using a virtual currency are (theoretically) low, Bitcoin technology, and thus bitcoins, have some inherent absolute value.

C. Contracts Transferring IP

But how should we consider this economic value? I've already explained why Bitcoins are not currency, nor are they commodities. They are best thought of as contracts stipulating the creation and ownership of new intellectual property. The promise to send someone a Bitcoin is a service, and the newly created serial number hash is a new copyright. Bitcoins are more similar to contracts for loans or expense accounts than they are to mechanisms of finance or securities. This means that regulatory agencies that start from the preconception of regulating methods of international commerce are destined to fail unless they begin with an a priori framework of international contract and IP protection. Some authors have argued that online property should be held to traditional property law forms for mere simplicity; that permitting electronic ownership to be governed by contract would be conceptually difficult to function.[91] While this means such considerations are more difficult initially, once such mechanisms are in place they will be very easy to modify and adapt as technology advances or methods of use change.[92]

---

90. Currie, *supra* note 87.

91. Juliet M. Moringiello. *Towards a System of Estates in Virtual Property*. SSRN (July 23, 2008), http://ssrn.com/abstract=1070184 (Widener Law School Legal Studies Research Paper No. 08-22).

92. *See, e.g.*, Jack M. Balkin, *Law and Liberty in Virtual Worlds*, 49 N.Y.L. SCH. L. REV. 63 (2004-2005) (how jurisdictional issues and commercial disputes in virtual worlds may be litigated in the future).

The protected material of a Bitcoin is the gibberish saved in the text file that the current owner possesses.[93] This text file can be used to hash a new file when the Coin is transferred, kept safe and hidden offline to store the bitcoin, or sent to an online currency exchange that will hold the bitcoin in trust. Random characters on a text file can certainly enjoy the same copyright protections[94] as an original novel.[95] Fixation may take the form of printed zeros and ones.[96] The originality requirement is more than satisfied, because the random numbers are indeed the result of pseudorandom processes, the hashing of which takes systematic effort by the worker's computer.[97]

The Copyright Act grants copyright owners the exclusive right "to prepare derivative works based upon the copyrighted work."[98] Congress defined derivative works as those "based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted."[99] Works "consisting of editorial revisions, annotations, elaborations, or other modifications which, as a whole, represent an original work of authorship" are also considered "derivative works."[100] The derivative work right can stretch to the point where the

93. 17 U.S.C. § 101 (2012) ("Literary works" are works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied).

94. *Id.* § 102(a) (copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device).

95. Any "physical rendering" of the fruits of the author's creativity will "fix" the work in a "tangible medium of expression." Goldstein v. California, 412 U.S. 546 (1973).

96. White-Smith Music Publishing Co. v. Apollo Co., 209 U.S. 1 (1908); Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240 (3d Cir. 1983); MAI Systems Corp. v. Peak Computer Inc., 991 F.2d 511 (9th Cir. 1993).

97. Feist Publ'n, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340 (1991); Toro Co. v. R & R Prods. Co., 787 F. 2d 1208 (8th Circ. 1986); *see also* Bleistein v. Donaldson Lithographing Co., 188 U.S. 239 (1903).

98. 17 U.S.C. § 106(2).

99. *Id.* § 101.

100. *Id.*

resulting work bears little resemblance to the original.[101] Thus, the derivative work right prohibits "the unauthorized use of expressive elements in subsequent works, regardless of whether such use involves any 'copying' in the ordinary sense of the term."[102] Accordingly, person who has no authority to make a derivative work cannot copyright such a work.[103]

Each time a Bitcoin is transferred and the hash chain is extended, a new derivative work is created. Although the derivatives are created by the former owners, transferor, and miners, the derivatives are all owned by the person who owns the copyright in the original work. That person is necessarily the transferee---i.e., the new owner of the Bitcoin. The prior owners still own their works, but those works are random characters on a text file that have no value anymore because they cannot be used to make further payments.[104] Only the latest version of the Coin (the one that has been publicly verified as the latest on the block chain) is the work of IP with any value. The owner of the derivative work does not legally prejudice the original owner's ownership of the underlying work, but in practical fact the creation of a new Coin upon transfer renders them unable to use the Coin they possess.

Obviously, all parties working in the Bitcoin network have agreed (by virtue of their entrance into the system) that they disclaim ownership of the Coins they create for transfer. The new Coins are created pursuant to the terms of the sales contract that has been agreed to prior to the creation of the Coin.[105] Thus, the agreement to sell something in exchange for a Bitcoin necessarily includes the understanding that the Buyer will create a derivative work upon transfer. The block chain created by miners is the paid-for addition to a compilation for which they disclaim any rights by publication.[106]

Bitcoins, in their current form, comfortably fit into the realm of written works for which copyright protection applies upon creation. Bitcoin hash numbers are the material to be protected. They are unique, created by

---

101. *See, e.g.*, Castle Rock Entmt., Inc. v. Carol Publ'g Group, Inc., 150 F.3d 132, 138 (2d Cir. 1998) (finding the fact that a quiz book could infringe the *Seinfeld* television series).

102. Lateef Mtima, *So Dark the Con(tu) of Man: The Quest for a Software Derivative Work Right in Section 117*, 70 U. PITT. L. REV. 1, 57 (2008).

103. Gracen v. Bradford Exch., 698 F.2d 300, 303 (7th Cir. 1983).

104. *See, e.g.*, Cmty. for Creative Non-Violence v. Reid, 490 U.S. 730 (1989).

105. *See* Playboy Enters., Inc. v. Dumas, 53 F.3d 549 (2d Cir.), *cert. denied*, 516 U.S. 1010 (1995); Dumas with Schiller & Schmidt, Inc. v. Nordisco Corp., 969 F. 2d 410 (7th Cir. 1992) (Posner, J.).

106. N.Y. Times Co., Inc. v. Tasini, 533 U.S. 483 (2001).

resource-intensive processes, and each Bitcoin is created for commercial purposes. Ownership lasts beyond the useful life of the Coin.

Sales contracts can also include speculative venture.[107] Bitcoins are not illusive; they clearly have some value and even just the transmission of random code is worth enough to the transferee that such contracts are not illusive. The property right for this kind of virtual currency does not exist until the new Coin comes into being; once the transfer has been confirmed and the transferee seizes the new Coin hash number.[108] Purchases fall into the jurisdiction of traditional contract law: they are a swap of whatever the buyer is making in exchange for a promise to generate IP under the seller's employ.

IV. Present and Future Regulatory Scheme of Virtual Currency

A. Current Regulatory Environment

1. Legal Use of Virtual Currency

The US Constitution[109] and the Stamp Payments Act of 1862[110] give the Federal Government the exclusive authority to create official coinage and currency of the United States. Printing a currency that is meant to compete with or confuse people about which is the legal tender is a crime.[111] But the use of bartering, prepaid cards and other stores of value and virtual currency is permitted as long as applicable laws are complied with.[112] The notion of lenity and general usage indicates that the creation and promotion of virtual currency does not violate any current statutes.[113] Contracts stipulating payment in virtual currency simply specify the method by which value established upon the U.S. dollar is to be paid.[114]

---

107. United Hous. Found., Inc. v. Forman, 421 US 837 (S.Ct. 1975).

108. Pierson v. Post, 3 Cai. R. 175, 2 Am. Dec. 264 (N.Y. 1805).

109. U.S. CONST. art. 1, § 10.

110. 18 U.S.C. § 336 (2012). The Stamp Act has been cited by several scholars as potentially rendering Bitcoins illegal. However, the law is likely inapplicable.

111. Michael Socarras & Lata Nott, *Does the Constitution Have Anything to Say About Bitcoin and Money Laundering?*, TMT PERSPECTIVES (Feb. 28, 2014), http://www.tmtperspectives.com/2014/02/28/does-the-constitution-have-anything-to-say-about-bitcoin-and-money-laundering/.

112. United States v. Van Auken, 96 U.S. 366 (1878).

113. Anchorage Cen D. Co. v. Van Wormer & Rodrigues, Inc., 443 P. 2d 596 (Alaska 1968).

114. Emery Bird Thayer Dry Goods Co. v. Williams, 98 F. 2d 166 (8th Cir. 1938), *judgment set aside on other grounds*, 107 F.2d 965 (8th Cir. 1939).

However, there is currently no regulatory scheme to protect consumers of virtual currency, nor is there a system to prevent virtual currency from being used to buy illicit goods or launder money. The current applicable laws are as follows.

There is the general protection against hacking. Federal laws prevent unauthorized computer entry. Notably, because Bitcoins are not money, theft of them from computers is more violative because of the unauthorized entry than because of the theft. It would be interesting to see prosecution against a Bitcoin thief, as the prosecutor would have difficulty establishing the fair market value of such an intangible. Unlike most software, there is no readily identifiable fair market value because the frequency of trade is so low and there is no centralized producer offering goods for regular sale. It would be like attempting to determine the fair market value of a particular stock when trading occurred rarely and through disparate, unknown parties. It would be more productive to charge the suspect for the mere act of exceeding their authority and engaging in fraud,[115] or into a computer involved in a financial institution, such as a virtual currency exchange.[116]

Additional applicable statutes include, of course, federal prohibitions against money laundering, and state regulatory schemes under the federal Banking Secrecy Act. The use of Bitcoin in such a scheme is problematic.

In the event that the malleability problems ("the 51% problem") plaguing virtual currency becomes widespread, it is possible that antitrust penalties imposed by the Department of Justice will be the only source of relief for the aggrieved public.[117]

2. Illegal Use of Virtual Currency

It is feared that new methods of virtual currency will "help criminals launder massive amounts of money. More girls will be sold as sex slaves, more rhinos will be poached, and every other large-scale transnational crime that you can name is going to become a lot easier if criminals have a way to transfer very large amounts of money completely anonymously."[118]

---

115. 18 U.S.C. § 1030.

116. *Id.* § 1030(e)(2).

117. Unlawful monopoly under the Sherman Act, 15 U.S.C. § 2; illegal restrictive dealing agreements prohibited by section 3 of the Clayton Act, 15 U.S.C. § 14; and unlawful agreements in restraint of interstate trade in violation of section 1 of the Sherman Act, 15 U.S.C. § 1. *See* Eyal & Sirer, *supra* note 62.

118. E.J. Fagan, *Bitcoin and International Crime (Commentary)*, BALT. SUN, Nov. 25, 2013, http://www.baltimoresun.com/news/opinion/oped/bs-ed-bitcoin-20131125,0,3265347.story

Some countries, such as Denmark and China, have already announced that stolen bitcoins are not going to be investigated. The risks lie entirely on the consumers if their meaningless gibberish files are lost, stolen, or corrupted. But even this system is untenable in the long term. Capital ventures are being funded through virtual currency already, illicit purchases are being tendered, and insurance companies may be called upon to pay for losses in virtual currency. Simply ignoring them or calling them prima facie without value is a blasé to the current state of reality, and will become ludicrously neglectful if virtual currencies continue to develop.

This neglect will create geographical "black holes" where virtual currency is nether protected nor investigated, which will in turn lead to their increased use in illicit purchases and to launder money from other countries. The existence of these regulatory black spots must be ended or overcome by the United States if virtual currency can continue to be used productively but under the banner of the law. I propose the following developments to ensure that virtual currency does not become synonymous with illegality.

B. Future Regulatory Development

1. How Virtual Currency as IP Logically Orders the System

If we consider each virtual currency transaction to be a contract obligating one party to the creation of intellectual property owned by the other party, a conception of the ideal regulatory scheme becomes more comprehensible. It also makes obvious how attempts to regulate virtual currencies as forms of currency or commodity are inadequate.

To regulate virtual currency as a form of commodity would be to regulate the speculation of an item of trivial value. Once the market stabilizes on virtual currency, proposed regulatory framework will become redundant. The recent price bubble of Bitcoins is a byproduct of several recent developments, but any proposed legislative solution would be unnecessary at this time. I reject the regulation of Bitcoins in particular and virtual currency in general in the commodity arena as an unnecessary solution to a nonexistent problem. I remain open to modifying this assertion if digital currencies remain at their hyper-inflated price points beyond their current status as novelties.

How much SEC involvement would be tolerated or desirable in virtual currency? To consider virtual currency a security would likely engender regulatory barriers sufficient to destroy the system in its nascent form and lock out future development. Might Bitcoins be considered securities, though? Certainly, their nominal price is based almost purely on their

speculative value. And the broad definition under the '33 and '34 Acts may encompass at least some offers to sell virtual currency.[119]

The problem lies with the "Supreme Court's apparent inability to comprehend thoroughly and to address analytically, consistently with the language, legislative history, and underlying policies of the securities acts, the important issues of federal securities regulation."[120]

The Bitcoin network as a whole may have been created in order to sell retained bitcoins once the price increased. But if Satoshi Nakamoto is truly the creator of Bitcoin, they were not created in a speculative venture but instead from a love of cryptography and the ease of payment opportunities it offered. The Bitcoin publication documents certainly do not "offer or endorse" bitcoins as securities or investment contracts.[121] The increase in bitcoin prices seems to be a surprise to the creators. A Bitcoin is more like a collectable trading card than a stock. It is more like an antique chair than a real estate venture. The fact that the price has increased after the initial sale is not reason enough to consider the entire product line to be a security.

Still, form is less important than economic reality when defining whether an investment contract or note is in fact a security (and thus merits SEC protection).[122] Are not bitcoins a profit-seeking venture to which clients undertake a certain amount of risk? Certainly, those who buy bitcoins with dollars risk their capital: The market price for Coins may decrease or they may be unable to find subsequent purchasers to whom they may sell their Coins. But are Bitcoin purchasers buying an investment, or consuming digital goods?[123] Bitcoins may not have much utility, but they are not themselves instruments dependent on the efforts of others.[124] And once bitcoins are purchased, there is no vertical common enterprise between the promotor and the new owner; each new owner no longer needs to maintain a relationship with the old owner, and the transferor's duty to and ownership of the transferee's new coin is nil. And there is no horizontal

---

119. Securities Act of 1933, 15 U.S.C. § 77a-77z (2012); Securities Exchange Act of 1934, 15 U.S.C. § 78e-78mm (2012).

120. Marc I. Steinberg & William E. Kaulbach, *The Supreme Court and the Definition of "Security": The "Context Clause, "Investment Contract" Analysis, and Their Ramifications*, 40 VAND. L. REV. 489, 492 (1987).

121. To offer or endorse something as a security can make it a security for federal jurisdictional purposes.

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

123. *Cf.* Grenader v. Spitz, 537 F.2d 612 (2d Cir.), *cert. denied*, 429 U.S. 1009 (1976); United Hous. Found., Inc. v. Forman, 421 U.S. 837 (1975).

124. *See* Sec. & Exch. Comm'n v. ETS Payphones, Inc., 408 F.3d 727 (11th Cir. 2005).

commonality between bitcoin investors. Under any jurisdiction's test, the Bitcoin network is not an investment scheme.

However, certain sales of virtual currency, or virtual currencies based upon and backed by corporate interest certainly *can* be considered securities. In these cases, the virtual currency will look substantially similar to investment notes or other traditional investment contracts.[125] I will discuss the implications of this kind of arrangement below.

If we then resolve ourselves that Bitcoin hashes are original expression and thus properties protected under copyright, several necessary legal conclusions follow. First, the transmitted encryption is automatically protected under American law, and identical copies by others can be assumed to violate the original owner's rights. The authorship of a Bitcoin hash would be relatively easy to prove if one were to take the matter to court: They could simply enter the record created when they published the transfer. Of course, this has the effect of negating the pseudo-anonymity for which Bitcoins are currently valued. This also means that damages can be calculated as follows in the event of loss due to theft or fraud.

2. Calculating Damages

Subsequent transferees from an initial unapproved transfer will receive a different hash, which renders their Bitcoin substantially distinct from the initial Bitcoin that was unlawfully taken. So the person seeking to recover damages for an unauthorized "taking" of their currency under the protections of copyright must find the actual identity of the primary transferee. If a suit is successful, because Bitcoins are unregistered by their nature statutory damages will be unavailable and the suitor must seek actual damages. The primary difficulty in proving actual damages will be in determining the true value of the lost Bitcoins because fair market value is deceptively illusive. Although public trading "prices" exist for Bitcoin, trading frequency is currently extremely limited except in periods of high volatility when prices change very rapidly. Thus, litigants will have to dispute about what the actual fair market value of the stolen coins were in every suit. Large thefts have historically coincided with dramatic price drops in the Bitcoin exchange. Additionally, the current difficulty in obtaining cash or goods for Bitcoins makes their real value particularly contentious.

---

125. Sec. & Exch. Comm'n v. Shavers, 4:13-CV-416, 2013 WL 4028182 (E.D. Tex. filed Aug. 6, 2013).

Bitcoins offer the unique case where an exact replacement of the lost, stolen, or destroyed IP will fully restore the plaintiff. There have already been cases where defendants have been ordered to transfer bitcoins.[126] While injunctions ordering transfer of coins may be the preferred method of dealing with the situation, monetary damages need to be further normalized before definitive statements can be made.

Theft of a bitcoin, or more precisely an unauthorized transfer of an owned Coin by accessing the Coin's secret number and using it to generate a new hash in the new owner's possession, can be difficult to trace and difficult to prove. But assuming a case comes to court in the near future, what value has the thief stolen, and what reparations will make the victim whole?

If we think of the damages as relief for forms of copyright infringement, damages may be calculated as for any standard software infringement case. Statutory damages are unavailable because virtual currency is not a protected publication.[127] Instead, courts would determine actual damages. Calculating damages by comparing the plaintiff's income before and after the infringement would be very difficult to apply to Bitcoin theft, unless the plaintiff is engaged in widespread currency exchange (like a Mt. Gox).[128]

Instead courts may calculate damages by based on what the copyright owner would have received had she sold or licensed the work instead of having it stolen. The only numbers that need to be determined are the number of infringements and the value of the work. This still may be difficult, however, because of the problems associated with pricing a work if it has not been commercially sold (e.g. – a piece of original art from an artist's private collection). Virtual currency will use this method of calculation for relief, although valuation would be more difficult than it may originally seem.

Actual Damages are difficult to claim because the plaintiff must prove to the court that their amount claimed for Actual Damages is accurate.[129] Plaintiffs need forensic accountants testify as their expert witness, who are often opposed by forensic accountants for the defendants who can testify that the damages are lower than the plaintiff claims. Many records controlled by the plaintiff may become a part of the public record. It is

126. Bitvestment Partners LLC v. Coinlab, Inc. et al, 1:2013cv07632 (N.Y.S.D. filed Oct. 29, 2013).

127. 17 U.S.C. § 504 (2012).

128. CoinLab, Inc. v. Mt. Gox, Case 2:13-cv-00777-MJP, Doc. 21 (Oct. 4, 2013).

129. Recourse may be made to such sites as COINOMETRICS, http://www.coinometrics.com/bitcoin/ (last visited July 2, 2014).

possible to have the plaintiff's financial records kept private from the general public (if the court is convinced there is good cause to do so), but the plaintiff will have no choice in turning over financial records to the opposing party.

Plaintiffs with strong documentation showing lost profits have stronger cases than those without them; but bitcoins are sold only once. Historical sales records are very important for showing expected sales, but plaintiffs will only be able to show their sales of other Coins, or the market value of Coins sold at the time of the theft. In this case, the loss would be equal to the value of a future Bitcoin sale that has been stymied by the theft, less the original purchase price of the coin.[130] This requires that the plaintiff make some kind of showing that they *would have* sold the Bitcoin at a particular time *but for* the theft. The value and timing could be calculated in a fashion similar to the damages assessed to plaintiffs in securities cases where plaintiffs were misled. Any documentation that was done in the normal course of business will carry more weight than documents generated specifically for the infringement claim.

In general, it seems that the remedies for lost virtual currency are currently inadequate, even forgoing for the moment the difficulty in tracking down the perpetrators in online theft.

3. How the Current System is Inadequate

The downsides of leaving this regime as-is are tremendous.[131] Another objection, which is in my belief fatal to Bitcoins in their current form, is the fact that copyright protections render Bitcoins extremely vulnerable to overseas theft. There is very little agreement between the United States and other countries where Bitcoins are primarily traded, and obtaining protection for original expression in foreign jurisdictions can be arduous and take longer than a similarly placed foreign transfer of funds. Remember, in this article I consider Bitcoins' primary competition to be regulated bank transfers. A second objection under copyright would be the privacy aspect. Remember how one of the benefits of Bitcoin is the public transfer chain, with encrypted names of transferors. However, in order to press ownership under an IP regime, transferors would have to make their transfer and the encryption used to create the hash key public. This not only reveals the formerly-anonymous transferor, but also makes it much more likely that prior and subsequent bricks of the transfer chain can be

130. Actual damages relieves only lost profits, not lost value.

131. Sarah Jeong, *The Bitcoin Protocol as Law, and the Politics of a Stateless Currency*, SSRN (May 8, 2013), http://ssrn.com/abstract=2294124.

discovered and their anonymity can be compromised. This is a significant disadvantage to Bitcoin protection and actually makes them less desirable than traditional banking transfers for those seeking some degree of anonymity.[132] At best, plaintiffs would win the case by tracking down the thieves (already a difficult proposition) and after intensive fact-based litigation recover their actual damages by opening their accounting ledgers to the opposing parties.

C. Proposed Regulations

1. The Regulation of the Exchange E-Economy

The major reason Bitcoin is unsustainable for wider adoption is the lack of government support. While the freedom promised by virtually exchanged and cryptographically backed money may be ideologically appealing, monetary relations are too closely interwoven with other economic, political and social relations to be managed well by any institution with less sway than a government.[133] The detailed work of money creation can be delegated to independent central banks and to a credit system of regulated private banks, but the ultimate authority of any functioning monetary system will always be the ultimate political authority.

Attempts to create private currency only succeed in spaces where there is no effective government: During revolutions, in remote geographical locations, or in the black market. These situations all use private currency only as a last resort. Bitcoin exemplifies some of the problems of private money: Its value is uncertain, its legal status is unclear, and it could easily become valueless if users lose faith. And there is a legitimate fear that if Bitcoin ever starts to demonstrate true market value, governments will either ban it or destroy its competitive advantage with overregulation.

As the Bitcoin experiment develops the government should seek to foster its innovative advances while seeking to protect consumers and limit its potential use for illegal activity.[134] The major structural framework I propose is to include virtual currency in the state and federal legislative framework as we consider the future of virtual currency. I will explicate in a later article my proposed format for the next generation of virtual currency, one which more closely resembles enforceable contracts. To

---

132. Reid & Harrigan, *supra* note 40.

133. Jim Harper, *Understanding Regulators' Warnings*, BITCOIN FOUND. BLOG (Mar. 20, 2014), https://bitcoinfoundation.org/2014/03/20/understanding-regulators-warnings/.

134. But see Auroracoin, the virtual currency that has been created and promulgated by the Icelandic government and distributed to its citizens. AURORACOIN, http://auroracoin.org/ (last visited July 2, 2014).

regulate digital currencies as contracts of minute duration leads to elegant and worthwhile consequences.

Initiation		**Processing**				
Front-End Infrastructure		*Back-End Infrastructure*				*Clearing Agencies*
Instrument	Channel	Transmission	Gateways	Routing Rules	Message Format	Clear Settle

Fig. 5: Traditional Money Transmission Network

First, contract dispute between states and nations are relatively common and the body of protections and remedies is straightforward. Copyright protections are speculative and cannot be clearly envisioned at the time of transfer. Tort remedies for theft and misuse of the Bitcoin are similarly difficult to envision. If virtual currency is going to be used by legitimate and risk-averse parties, the certainty and precognition available from contract remedies are essential. This works both ways: the transferor/owner will be able to predict future possible remedies from misuse or loss; and this helps those who seek to take coins of uncertain origin: They understand the absolute limits of their potential liability. The certainty for all participants from a legal standpoint is essential if virtual currency is going to be a respectable alternative to current transfers.

Another positive benefit to virtual currency existing in the form of contract is the flexibility of such arrangements. It has proven remarkably easy to create virtual currency modeled after Bitcoin. Each derivative virtual currency has a unique reason for its existence and a unique chain of transfers leading back to an initial source. But there is no reason these currencies need to exist in perpetuity, and there is no reason the creation of a new currency needs to lead to new regulatory structure simply because the new currency features some option or feature that has not been anticipated by the existing regulatory scheme. Consider for example a new Bitcoin derivative, the GodloveCoin, which offers the feature of including call options from various banks around the world. This feature would baffle a regulator seeking to keep the market stable and free from illicit transactions under any proposed Bitcoin scheme. But under future disputes in court, considering the GodloveCoin in a contract litigation, the judge would simply rely on existing precedent at the time of the creation of the contract and apply the Bitcoin cases in an analogous manner.

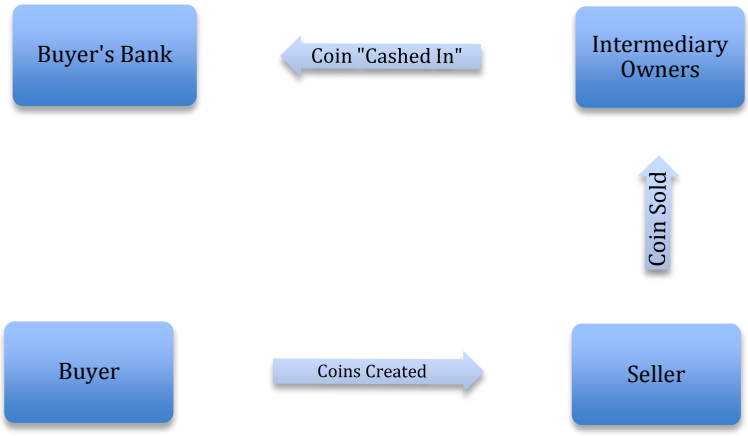

Fig. 6: Proposed Bank-Backed Virtual Currency Transmission Structure

Thus consider the Bitcoin and its progeny as forms of money transmission through value-infused software IP rather than currency or commodity. Contract allows the flourishing of virtual currency with as many names and functions as there are different needs between interested parties. The production of such coins has been shown to be easy, and future production will become trivial. Such coins would exist until their purpose has been exhausted, and the use of these, with the call option on various banks, would allow the future Coins to be fully called once the transactions have been wrapped up. The call option can exist as long as the banks with which such Coins have been created in conjunction with exist.

2. What Features Future Virtual Currency Must Include

Messages can be embedded in the "coinbase" of a block. The Bitcoin genesis block contains the headline from the front page of a newspaper and subsequent user “Luke-Jr” used his Coin pool to embed Bible quotes and prayers into the block chain. In this fashion, regulations should exist that require certain information to be embedded in the block chain from the initial creation of the Coin. Federal law should be enacted that requires certain public statements to be embedded, which can be accessed by owners of the Coins once they own possession. Embedded messages can be either encrypted or unencrypted. A blanket requirement that certain information be included in all virtual currencies created and transferred is the minimum regulation that solves nearly all of the problems identified with virtual currency.

Unencrypted messages should include the same kinds of disclosures that are currently required for users to create money transfer accounts, as well as some hybrid disclosures modeled on those required for initial public offerings of securities.

At least one federal district court has found that it has subject matter jurisdiction over cryptocurrency pursuant to sections 20 and 22 of the Securities Act of 1933, and sections 21 and 27 of the Exchange Act of 1934.[135] The jurisdiction was created through the unique manner in which the virtual currency at issue was endorsed and offered. The court correctly determined that, in these circumstances, virtual currency can be sold as an investment contract and is therefore under SEC jurisdiction:

> The term "security" is defined as "any note, stock, treasury stock, security future, security-based swap, bond ... [or] investment contract ..."[136] An investment contract is any contract, transaction, or scheme involving (1) an investment of money, (2) in a common enterprise, (3) with the expectation that profits will be derived from the efforts of the promoter or a third party.[137] First, the Court must determine whether the BTCST investments constitute an investment of 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.
>
> Next, the Court looks at whether there is a common enterprise. To show a common enterprise, the Fifth Circuit requires interdependence between the investors and the promotor, which "may be demonstrated by the investors' collective reliance on the promotor's expertise even where the promotor receives only a flat fee or commission rather than a

---

135. Sec. & Exch. Comm'n v. Shavers, 4:13-CV-416, 2013 WL 4028182 (E.D. Tex. filed Aug. 6, 2013).

136. *Id.* at *2 (quoting 15 U.S.C. § 77b).

137. *Id.* (quoting Sec. & Exch. Comm'n v. W.J. Howey Co., 328 U.S. 293, 298-99 (1946)); Long v. Shultz Cattle Co., 881 F.2d 129, 132 (1989).

> share in the profits of the venture." . . . .[138] That interdependence is established in this case because the investors here were dependent on Shavers' expertise in Bitcoin markets and his local connections.[139] In addition, Shavers allegedly promised a substantial return on their investments as a result of his trading and exchanging Bitcoin. Therefore, the Court finds that there is a common enterprise.
>
> Finally, the Court considers whether there is an expectation that profits will be derived from the efforts of the promotor or third party. The Court finds that this prong is also met. At the outset, Shavers allegedly promised up to 1% interest daily, and at some point during the relevant period the interest promised was at 3.9%. Clearly any investors participating in the BTCST investments were expecting profits from the efforts of Shavers.[140]

From the three factors, it is clear that Bitcoins were being sold as securities in this instance. In any future instances where cryptocurrencies are sold in similar fashions, the SEC should indeed gain jurisdiction to proceed. However, this is not a radical step. The SEC has jurisdiction over sales of real estate, rental property, and cooperative ventures, if they are sold in a form that resembles speculative contracts or other common enterprises for profit.[141] But it should be clear from these factors that sale of bitcoins do not usually fall within the definition of securities. Only when virtual currency is created to facilitate a common speculative enterprise should they be determined to be securities.

Consider why virtual currencies generally do *not* satisfy the three factors that would create SEC jurisdiction. First, while the court above did consider bitcoins to be currency, they are generally not considered so.[142] Second, the Bitcoin network, or other networks, typically constitute peer-to-peer contracts between private parties in the settlement of some payment, and

---

138. *Id.* (quoting *Long*, 881 F.2d at 141).

139. Author's note: Even when strict vertical commonality is required, contracts in the nature of this case will satisfy the definition of a security. Looser commonality requirements in other jurisdictions may be satisfied with arrangements that organize investors in less dependent ways.

140. *Shavers*, 2013 WL 4028182. at *2-3.

141. Reves v. Ernst & Young, 494 U.S. 56 (1990).

142. IRS Pub. Notice 2014-21 (2014), *available at* http://www.irs.gov/pub/irs-drop/n-14-21.pdf.

form an exchange of limited duration which does not constitute a common enterprise *unless* the sale is explicitly (or in some cases implicitly by virtue of the promotor's expertise) offered as part of one. Third, as this article argues, virtual currency has very little inherent value. The fact that speculators have latched onto virtual currency at this time as a commodity does not make it so; Magic: the Gathering cards are not securities simply because their price can fluctuate rapidly on the open market. Virtual currencies are not inherently speculative; only when their value is tied to some other concrete store of value, such as government currency or traditional commodities (in the case at issue, oil), will they be considered securities for jurisdictional purposes.

3. What Changes Are Needed to Buttress Existing State and Federal Regulatory Subject Matter Jurisdiction to Allow Consumer Protection?

As discussed, the Securities and Exchange Commission currently has the jurisdiction to investigate particularly egregious cases of speculative sale of virtual currency. The IRS already has the jurisdiction to investigate the gains and losses stemming from the ownership of virtual currency. And courts have already disposed of civil cases between aggrieved parties on virtual currency exchange networks. I would encourage lawmakers to limit what legislation they consider proposing at this early stage, and require *only* that newly created coins include encrypted information and disclosures. That would go a long way to alleviate consumer protection worries: All transferred virtual currency should include embedded messages should include consumer disclosures and addresses of recourse.

A more radical proposal would be to require future virtual currencies to be backed by some store of value. New Virtual Coins could only be created by licensed money transmitters, and sold to the public as methods of transferring ownership of the value they represent. Coins could be prohibited from sale unless they contained information that could be used to draw upon funds, either in a bank account or from the issuing body itself.

Messages *encrypted* into Bitcoins are in a hexadecimal nonce, not plaintext embedded messages. They cannot be read unless the issuer and the reader have some agreed-upon encoding independent of the chain itself. With ASCII this is a trivial concern for those with the agreed-upon encoding, but if anyone else downloads a block the text will be illegible.

How is this useful? All owners of the coin beyond the initial issuer would have access to an encoded file within their GodloveCoin that they could access but not read. This message would be a draw order (upon a bank account, for example, or entitling the owner to an ounce of gold). If

submitted to the bank, the bank would only be able to decode the file if the decryption algorithm had been shared by the issuer. Anyone submitting the order could be confirmed and the money could be withdrawn in real dollar after the bank receives possession of the Coin and decrypts the order. This would mean that the Coins have a terminal point: whenever an owner uses them to "cash out" at the bank where the issuer created the account joined to the Coin upon creation. Federal regulators should require this kind of system to be used in the creation of coins; and seize those on the open market that do not have these protections. This will proximately cause the stabilization and permit adequate regulation of virtual currency.

D. When Should Regulators Enter?

1. Every Transaction, or at the Beginning and End of the Chain?

The central question is: What types of firms should be regulated; and which transactions should draw agency involvement? The two general answers are that regulators can either regulate each transfer of virtual currency between owners, or merely regulate the beginning and end of the chain. I believe that regulation can achieve all the desired functions by regulating only the beginning and end of the chain except for institutional owners, for reasons that follow below.

Why should regulators not enter during each transmission? First, it is invasive. Police monitoring of each cash and debit transaction would be considered undue involvement in the lives of citizens, and may implicate federal Constitutional rights. Second, such involvement would be expensive and burdensome, costing both government resources and stifling innovation. Third, such regulatory involvement would be practicably difficult to effectuate, more so than regulation of a single-point transaction network, due to the peer-to-peer qualities of virtual currency.

Financial regulators would find it nearly impossible to provide oversight for every single individual, peer-to-peer transaction unless there is evidence of specific criminal or civil wrongdoing. Such instances would not need regulatory oversight, and could be dealt with in the current court tort system, or through specific causes of action to be discussed at a later date.

Miners are a vital part of the ecosystem, but regulators have determined that they do not meet the threshold for proactive oversight. The US Treasury's FinCEN issued a release stating this fact: Miners and individual investors do not merit oversight.[143] This is the first broad stroke in laying down where regulation should begin, and is a positive step in keeping the

143. Treasury Guidance FIN-2013-G001, *supra* note 3.

regulation to a minimum.[144] We do not, for instance, require policing of every single individual transaction involving cash. But should we, as some suggest, only regulate transactions where virtual currencies are exchanged for dollars and other traditional currencies? [145]

Institutional investors, however, do merit increased oversight. Any organization the offers itself as a virtual currency exchange, or operates as one, *or* creates and offers a new virtual currency, should be required to register in their state, and every state in which their customers operate, as money transmission services. The laws governing money transmission services vary by state, but all require some minimum level of capital backing and consumer protections, as well as reporting requirements to limit money laundering and illicit purchasing.

Without this minimum level of oversight virtual currency has a capacity to scale up money laundering in a way that is not possible with physical cash. Law enforcement is already aware of these issues and has expressed concern.[146] The accelerating growth of virtual currencies in online and brick and mortar transactions and illicit networks can leave a gaping loophole for misconduct if this technology gains wider adoption. When it comes to using physical cash for illegal activity, criminals are constrained in certain respects to what they can physically carry and transport. There are no such limitations when it comes to virtual currencies. If we adopt an end-point terminal regulatory schema, and require institutions to monitor and report suspicious transactions internally, we will have to be assured that it reasonably limits money-laundering potential.

2. Preventing Money Laundering at the Termination of Virtual Currency

The United States Treasury Department recently enacted new rules to regulate Bitcoin and other virtual currencies, making it subject to the same level of scrutiny as other forms of currency. That's bad news for anyone looking to launder money using Bitcoin, but it could be good news for proponents of virtual currency for legitimate purposes. Examples of regulated activities "include, in part, (1) the transfer of funds between a customer and a third party by permitting a third party to fund a customer's

144. *Id*.

145. *NYDFS Virtual Currency Hearing*, N.Y. DEP'T OF FIN. SERVS (Jan. 28, 2014), http://www.dfs.ny.gov/about/hearings/vc_01282014_indx.htm.

146. Money Transmitter Div., Cal. Dep't of Fin. Insts., Developments and Issues in MSB Supervision (Aug. 25, 2011) (graphics presentation at a 2011 Conference of State Bank Supervisors Legal Seminar), *available at* http://www.csbs.org/development/Documents/MSB SupervisionVenchiarutti.pdf.

account; (2) the transfer of value from a customer's currency or commodity position to the account of another customer; or (3) the closing out of a customer's currency or commodity position, with a transfer of proceeds to a third party. Since the definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies, the same rules apply to brokers and dealers of e-currency and e-precious metals.[147] Typically, this involves the broker or dealer electronically distributing digital certificates of ownership of real currencies or precious metals, with the digital certificate being the virtual currency. However, the same conclusions would apply in the case of the broker or dealer issuing paper ownership certificates or manifesting customer ownership or control of real currencies or commodities in an account statement or any other form. These conclusions would also apply in the case of a broker or dealer in commodities other than real currencies or precious metals. A broker or dealer of e-currencies or e-precious metals that engages in money transmission could be either an administrator or exchanger depending on its business model.[148]

The Treasury rules treat Bitcoin and its ilk regulated in a similar fashion to how the government deals with traditional money-order services like Western Union.[149] Individuals trading in Bitcoins need not concern themselves with reporting requirements, but businesses dealing with them, such as exchanges, will be required to keep more detailed records of the transactions. Transactions over $10,000 must be reported.[150] A user of virtual currency is not an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person.[151] An administrator or

147. Fin. Crimes Enforcement Network, Dep't of the Treasury, *Guidance: Application of the Definition of Money Transmitter to Brokers and Dealers in Currency and Other Commodities*, FINCEN (No. FIN-2008-G008, Sept. 10, 2008), http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2008-g008.pdf. The guidance also notes that the definition of money transmitter excludes any person, such as a futures commission merchant, that is "registered with, and regulated or examined by . . . the Commodity Futures Trading Commission." *Id.*

148. Treasury Guidance FIN-2013-G001, *supra* note 3.

149. *Id*.

150. *Id.*

151. *Id.*

exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN's regulations.[152]

Transfer of virtual currency into cash needs to be regulated, as well. Virtual currency purchases for consumer goods do not need to be investigated; it would be impractical for money launderers to purchase thousands of model train sets with dirty money. At the point in the chain where virtual currency is traded for readily-seized value, regulators need to be ready to enter. This end-of-chain transaction is where regulators should spend most of their time, and lawmakers should consider imposing strict requirements. This is the most important step of the chain because easy-to-transfer-but-difficult-to-spend virtual currency is converted into difficult-to-transfer-but-easy-to-spend gold or cash.

As a bare minimum, legislators should require that virtual currency *cannot* be converted into cash or gold except at banks or other licensed financial institutions. A more strict regulation (which I endorse) would prevent Bitcoins from being converted to cash or gold entirely, *unless* they are transferred to their creator's bank. In such regime, all virtual currency would need to be created in connection with an originating bank, and embedded text in the Coins would tell owners at which bank the Coin may be "cashed out;" owners who wish to convert their Coins would transfer ownership to the bank, after which the bank would verify the Coin and release the funds to the owner. Banks would be required to report suspicious transactions, as detailed below.

3. Taxation

Bitcoins also pose regulatory difficulty to the income tax code. How should they be taxed? Again, a regulatory schema that limits itself to the start and end points of coins would be superior, as it would fit seamlessly into the federal tax regime. "Bitcoin is not a currency," despite the protestations of some supporters, and "[u]sers of Bitcoin should not think that it is exempt from taxation or outside the tax system. There's nothing that Bitcoin allows anyone to do that they can't already do in the regular banking system ... Libertarians, drug dealers, and tinfoil hatters like Bitcoin because it is not issued by a central government, but the irony is that it is more controllable and more traceable than the U.S. bank notes . . . ."[153]

The only true cases on point comes from Barter Systems, a company that allowed customers to trade in hard assets in return for "trade units" issued

152. *Id.*

153. Lee Shepard predicted the IRS response in a *Tax Notes* article several weeks before the IRS Publication laying out IRS treatment of Bitcoins.

by the firm. The U.S. tax court ruled that Barter Systems was required to report transactions involving these trade units and that the exchange should be taxed on the fair market value of property received in exchange for trade units.[154] According to Tax Attorney Lee Sheppard, "Bitcoin is analogous to the trade units considered in Barter Systems Inc. of Wichita. It is a privately issued medium of exchange accepted only in constrained circumstances and not backed by any promise of the issuer. Colvin treated the trade units as property in analyzing their use. The same analysis applies to Bitcoin."[155] And indeed the IRS later confirmed that for federal tax purposes, virtual currency is treated as property.

General tax principles applicable to property transactions apply to transactions using virtual currency. The basis of virtual currency that a taxpayer receives as payment for goods or services is the fair market value of the virtual currency in U.S. dollars as of the date of receipt.[156] One who purchases ten BTC for $100 will receive ten bitcoins each with a $10 basis.

For sale of virtual currency for U.S. tax purposes, transactions must be reported in U.S. dollars. Therefore, taxpayers will be required to determine the fair market value of virtual currency in U.S. dollars as of the date of payment or receipt. If a virtual currency is listed on an exchange and the exchange rate is established by market supply and demand, the fair market value of the virtual currency is determined by converting the virtual currency into U.S. dollars (or into another real currency which in turn can be converted into U.S. dollars) at the exchange rate, in a reasonable manner that is consistently applied.

If the fair market value of property received in exchange for virtual currency exceeds the taxpayer's adjusted basis of the virtual currency, the taxpayer has taxable gain. The taxpayer has a loss if the fair market value of the property received is less than the adjusted basis of the virtual currency.

The character of the gain or loss generally depends on whether the virtual currency is a capital asset in the hands of the taxpayer. A taxpayer generally realizes capital gain or loss on the sale or exchange of virtual currency that is a capital asset in the hands of the taxpayer. For example, stocks, bonds, and other investment property are generally capital assets. A taxpayer generally realizes ordinary gain or loss on the sale or exchange of virtual currency that is not a capital asset in the hands of the taxpayer.

---

154. Barter Sys., Inc. of Wichita v. Comm'r, 1990 T.C. Memo 125 (T.C. 1990).
155. Lee A. Sheppard, *Busting the Bitcoin Myths*, 142 TAX NOTES 896 (Mar. 3, 2014).
156. Burnet v. Logan, 283 U.S. 404 (1931).

Inventory and other property held mainly for sale to customers in a trade or business are examples of property that is not a capital asset.[157]

A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property. For example, a person who in the course of a trade or business makes a payment of fixed and determinable income using virtual currency with a value of $600 or more to a U.S. non-exempt recipient in a taxable year is required to report the payment to the IRS and to the payee.[158] Examples of payments of fixed and determinable income include rent, salaries, wages, premiums, annuities, and compensation.

Generally, a person who in the course of a trade or business makes a payment of $600 or more in a taxable year to an independent contractor for the performance of services is required to report that payment to the IRS and to the payee on Form 1099-MISC, Miscellaneous Income.[159] Payments of virtual currency required to be reported on Form 1099-MISC should be reported using the fair market value of the virtual currency in U.S. dollars as of the date of payment.

Generally, a person who in the course of a trade or business makes a payment of $600 or more in a taxable year to an independent contractor for the performance of services is required to report that payment to the IRS and to the payee on Form 1099-MISC, Miscellaneous Income. Payments of virtual currency required to be reported on Form 1099-MISC should be reported using the fair market value of the virtual currency in U.S. dollars as of the date of payment. The payment recipient may have income even if the recipient does not receive a Form 1099-MISC. See the Instructions to Form 1099-MISC and the General Instructions for Certain Information Returns for more information. For payments to non-U.S. persons, see Publication 515, Withholding of Tax on Nonresident Aliens and Foreign Entities.

These IRS regulations are not surprising considering that for tax purposes, gross income is defined as "income from whatever source derived."[160] Barter of goods and services count as taxable income so a virtual currency should also be considered as such, and not a currency

---

157. See IRS Pub. Notice 2014-21 (Apr. 14, 2014), *available at* http://www.irs.gov/irb/2014-16_IRB/ar12.html, for more information about capital assets and the character of gain or loss.

158. *Id.*

159. *Id.*

160. 26 U.S.C. § 61 (2012).

(considering the fluctuations in price inherent in the virtual currency network).

The IRS ruling does, however, pose problems for Bitcoin miners. Those who mined hundreds of Coins when the value of bitcoins was $300 and sold them when the exchanges were valuing BTC at over $1,000 have realized taxable gain of several hundred dollars per Coin.[161] Those who mined bitcoins when the fair market value for each Coin exceeded $1,000 and fell to less than $500 have a good amount of capital losses they may claim. It may behoove the IRS to consider further limitations to capital gains and losses on virtual currency, lest a future article detail methods by which unscrupulous traders may generate large paper losses with virtual currency in order to deduct from their taxes.

E. How Future Regulations Will Begin to Work in Practice

1. Which Laws Need to Be enacted at the Minimum

Ideally, all virtual currency, such as Bitcoin and its derivative variants, will be required to include plaintext consumer disclosures in plaintext as riders attached to each file. Furthermore, any new derivative coin created from now on must include encrypted messages in each Coin in the Genesis block with a withdrawal order at a specific bank where the creator operates an account. The private key unlocking the message would be shared with the bank by the creator, and any subsequent owner of the Coin would thus be enabled to transfer ownership of the Coin to the bank and receive cash transferred from the account. If I wanted to create a new Coin and call it GodloveCoins, I would need to be a licensed money transmitter[162] with a bank account containing sufficient funds, communicate my private key to the bank, and let the account wait in trust for ownership of the GodloveCoin. Creating and owning the GodloveCoin Genesis block, I could now transmit ownership to the bank from anywhere in the world and receive access to the proportionate funds. Or, if I transferred them to a new owner, that owner and any subsequent owner down the block chain, could "cash in" the GodloveCoin with my bank.

An obvious point about GodloveCoin concept is that it limits the amount of new regulatory structure government needed to prevent virtual money

161. However, the IRS has permitted those in extraordinary circumstances to explain their reason for failing to pay taxes on their Bitcoin gains in 2013/2014.

162. Because "a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter," creators of virtual currency must be registered as money transmitters.

laundering and protect consumers of virtual currency. The least possible change to existing framework needs to be done, which should make privacy advocates, limited government advocates, and 'Net libertarians happy. Resolution of disputes between parties has been discussed above. Government notification in the GodloveCoin scheme happens only in the case of irregular banking withdrawals of cash or suspicious transfers at online currency exchanges. GodloveCoins could theoretically be traded across the entire globe time and time again without triggering any flags if they are traded legitimately. In such a case, the public ledger would be saved and recorded by law enforcement but not used to track transactions or decrypted to identify owners. Users would act in a relatively unrestricted environment, using petty amounts of GodloveCoin as cash, changing hands and transferring the options to draw upon the cash in the account, or sell ownership of the Coin itself. It is also probable that banks would become the primary organizations conducting the 'mining' required to resolve transfers, which will keep their transfers safe and secure the network against concentrated malicious hackers.[163] Banking regulatory schemes would come into play only when the coins were drawn upon. In such a case, the Coins would be turned into real cash. At this point, standard banking regulations trigger. Transmissions would only be regulated in the creation and centralized exchanging of virtual currency.

2. The GodloveCoin in the Proposed Regulatory Scheme

Let's take a hypothetical example. The Godlove Corporation in California, USA wants to buy a thousand widgets from Manufacturing Ltd. in New York. Manufacturing Ltd. buys its raw material from Oil Inc. in Oman. And Oil Inc. has a banking account in New York State. Godlove Corp. creates a million GodloveCoins for the purchase of the widgets. Godlove Corp. has accounts in a California bank with some established minimum amount, in this case $1M. The created Coins are all tied to the account, and each GodloveCoin contains encrypted code entitling the owner to draw of one dollar from the account. The private keys used to encode the message are transmitted to the bank. The GodloveCoins are all transferred to Manufacturing Corp. Manufacturing Corp., intending to buy some raw materials to begin the order, "cashes in" half the coins by transferring ownership to the bank. The hash numbers are sent to the bank, where they are decrypted into valid draw orders with the secret key. Manufacturing Corp. withdraws half a million dollars from the local bank and has them

163. This would solve the 51% Miner attack problem.

transferred to their bank. The other half of the GodloveCoins are transferred to Oil Inc. in Oman in order to buy raw materials. Oil Inc. receives the new hash numbers, which are verified on the public block chain, and immediately transfers the Coins to its subsidiary corporation in California. In California, the GodloveCoins are resolved as above and the funds are withdrawn. Now that all of the Coins have been transferred to the bank, and the account is empty, the bank's fiduciary duty to preserve the private key and manage a private wallet for the Coins ends and the data can be destroyed. The ability to draw in New York on a purchase made in California is old news, but here has been done in a more efficient, quicker, and less costly fashion. Godlove Corps.' bank in California will make a payment to Oil's bank in Oman, perhaps with an EFT. If there are any suspicious indicia, they will be revealed to the bank now and reported to the proper authorities. The GodloveCoin, created for a particular purchasing arrangement, is now worthless and trading among further parties, whether authorized or not, will be pointless. Any future transfers will be rejected, as the checksum will not validate.

The advantages are numerous: no money has been lost to currency exchange: The half-million dollars drawn from New York have the same value as the half-million sent from California. Additionally, the records of exchange are public and the identities of the transferees, if known to the participants, can be easily traced and deduced, but would be much more difficult for outsiders to link or determine the identities of the participants. From the standpoint of the federal government, such transfers are acceptable because money laundering and banking notification requirements are triggered.

Suspicious Activity Reports (SARs) have become the primary source of information from financial institutions and other reporting sources (casinos, currency exchanges, etc.) to assist in anti-money laundering efforts. SARs increased from 52,000 in 1996 to 288,000 in 2003.[164] Nearly half of these were characterized as "violations of the Bank Secrecy Act (BSA) / Structuring / Money Laundering."[165] Law enforcement officials consider SARs more useful and informative in the identification of suspicious activity than many other sources. Additionally, there are examples of money laundering being discovered by small banks that *failed* to file SARs. Great Eastern Bank of Florida, with deposits of $55 million failed to alert

164. PETER REUTER & EDWIN M. TRUMAN, INST. FOR INT'L ECON., CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 108 (2004).

165. *Id*.

authorities of the structured deposits of some customers. FinCEN investigated and determined willful violations based on the lack of reporting or vague details when SARs were filed.[166] Virtual Currency exchanges, and banks that "cash in" virtual currency will be under reporting requirements, which will include reporting of customers who appear to be involved in money laundering or structuring.

If the block transfer looks suspicious, investigators will have the option of requesting further information and looking at the investigation. The origin of the Coins will be obvious and regulators will be able to request information from the creator of the coins. Regulators will also be able to see the record of transfers and, while the identities of the block-chain recipients will be anonymous (initially), any suspicious transfers will become immediately apparent. Thus, the ability to determine if money laundering, tax evasion, or purchase of illicit goods will be inherent in the system, with reporting requirements similar to the current financial scheme, while permitting innovation, freedom, and limiting of costs that offer so much promise in the emerging realm of virtual currency.

3. How Proposed Virtual Currency Would Assist International Purchases

What about governments that restrict virtual currency to cash transactions? China, for example, has chosen to limit the use of Bitcoins to Yuan exchanges. It was really no surprise given China's stringent capital controls.[167] But the move was interesting in the context of China's recent history. QQ Messenger, the most popular messaging application in China with currently 800 million users, at one time embedded its own virtual currency ("QQ coin"). In 2009, the PBOC issued guidance that said it was illegal to trade QQ coin for fear that it was being used for illicit purposes. Conversely, the PBOC issued guidance that Bitcoin may be traded by private persons, but traditional financial institutions and third-party payment processors may not deal with virtual currency.

China maintains a tight control of the Yuan, and officials recognize that virtual currencies may be used as arbitrage tools against the currency. It is

166. Assessment of Civil Money Penalty, *In re* Great E. Bank of Fla., No. 2002-02 (Fin. Crimes Enforcement Network, Dep't of the Treasury Sept. 4, 2002), *available at* http://www.fincen.gov/news_room/ea/files/geassessfinal.pdf

167. To see an example of the intellectual contortions that such stringent regimes engender, such as an argument that virtual currency is distinct from virtual coinage, see Sun Guang-zhi, *Study on Virtual Currency*, 11 TECHNOLOGICAL DEV. ENTERPRISE 30 (2006) (published in Beijing, China).

unlikely that virtual currency will ever been permitted to exchange into Yuan, unless Chinese international policy dramatically shifts. However, there is no reason that U.S.-bank-backed virtual currencies may not be used by individuals in China before transfer back to U.S. firms. Such currencies could in fact find several favorable niches in the Chinese market.

4. How Proposed Virtual Currency Would Prevent Theft

Let us imagine, then, a scenario similar to the hypothetical example above, except that this time an international firm steals the GodloveCoins. A criminal syndicate in Russia that seeks to use the virtual currency to launder money now owns half of the Coins. The first problem the syndicate faces is that the coins are tied to known bank accounts in America. Once the theft is reported, the accounts can be closed or watched for draw orders. Payment between Manufacturing Ltd. and Oil Inc. has not been completed, and the parties, aware that the account is now frozen to Coin withdrawals, may arrange alternative payment (an EFT, for example). Even if the criminal syndicate attempts to use the Coins to draw upon the accounts before the parties have been alerted to the theft, an inspection of the public ledger by the bank should indicate the unusual provenance of the Coins. This will, of course, trigger banking reporting requirements. Large transfers between accounts will be tracked, as in the normal course of business. Attempts to withdraw money may signal to law enforcement that they should investigate, whereupon it is a trivial matter to backtrack the public chain of transfers from the bank account to the initial release. Again, this is public information which makes it much quicker and easier to access for law enforcement than traditional bank records across the globe, and methods of decrypting the anonymity will make indexing such transfers fairly trivial.

The only downside to this proposed regime would be in the use of grey-market virtual currency: Currency tied to secret bank accounts in countries with above-average banking privacy laws; or coins created to foil attempts to decrypt the identities of transferors such as those that are automatically routed through botnets. The trade-off of such proposed grey-market currency would be a decreased trust by the parties using them. Such denominations would necessarily be small, and their fair market value, would either be substantially lower than the amount to be called upon from the bank account, limiting the competitive advantage from such coins compared to traditional forms of money laundering; or, if decoupled from the actual accounts, meaning the entire value of the currency would be retained in the form of speculative investment, and for such currency, the

only value that could be extracted from such Coins would be in the form of illicit goods, such as laundered petty cash, drugs, etc.

V. What Needs to Be Addressed

Clearly, the future of virtual currency is exciting and difficult to predict. But by determining probable future developments, and gently prodding the developers of these products toward development in the areas outlined above, I predict a stable and useful product may result. Such currency would enjoy significant cost and time-savings over current methods of purchase and payment over the internet, which is a vitally needed development in the increasingly globalized world. And, given the outlines above, government regulation would not stifle such development.[168] In fact, certain enjoyable legal protections would be extended to virtual currency, offering the kind of legitimate backing and protections that can lead to widespread adoption by the general community. Here are specific proposals for applying existing rules for money transmitters or banks, which have generally served consumers well when vigorously enforced. Indeed, certain aspects of virtual currency could dovetail with existing regulations. That said, our agency will likely have to proceed with issuing some form of specially tailored BitLicense that adapts those rules to the world of virtual currency.

A. Consumer Education, Protection, and Disclosures

1. The Need for Disclosures

Consumers should be aware that many virtual currencies do not provide for chargebacks. Disclosures encoded in the plaintext of virtual currency, or the website operated by the creator, should clearly tell consumers that transactions are, for the most part, irreversible. In other words, there is generally no "money back guarantees" for crypto-currencies.[169] Such guarantees would need to come from reputable businesses in jurisdictions where traditional consumer lawsuits are routine in order for consumers to feel secure relying them.

Consumers should also be warned about the importance of keeping their "private keys" private – as well as the potential consequences if they fail to

---

168. Brian W. Smith & Ramsey J. Wilson, *How Best to Guide the Evolution of Electronic Currency Law*; 46 AM. U. L. REV. 1105 (1996-1997).

169. *But see* Ethan E. White, *Massively Multiplayer Online Fraud: Why the Introduction of Real World Law in a Virtual Context Is Good for Everyone*; 6 NW. J. TECH. & INTELL. PROP. 228 (2007-2008).

do so. Given the irreversibility of most transactions, if a consumer has their private key stolen, they could easily lose their virtual currency irretrievably. The legal notice issued by Flexcoin should be examined as an inadequate disclosure, which should fall under the legal minimum for future standards.[170]

Moreover, consumers should be informed about the documented volatility of virtual currency and the potential for loss of dollar-denominated principal if they hold onto that virtual currency for an extended period of time. Because virtual currencies can be so easily traded, creators should be aware that their products will rarely be limited to sophisticated investors. Like mutual funds or retirement plans, the obligation rests on the seller to ensure that consumers understand the nature of these financial instruments.

If the United States intends to promote itself as the central location in which virtual currency can be bought, sold, and invested upon, it must first ensure that average consumers are provided with strong, clear, concise disclosures, just as it has in the securities and banking realms.

How should these disclosures be made? Unlike Paypal or credit card providers (where a central authority controls the payments and acts as the intermediary between parties), there is by definition no intermediary in virtual currency. Users do not need to sign a contract with their terms and conditions, including disclosures, in order to receive coins. And, in the wake of increasingly flourishing variants of the Bitcoin as alternative virtual currency, there is no single easily recognized authority from which disclosures could be made.

2. Virtual Currency Disclosures

The largest burden to make initial disclosures to consumers should be on the initial creator of the virtual currency. In the initial public offering (even if the entirety of the currency is immediately transferred to a single source), the currency will need to be bundled with a short plaintext disclosure directing any owner to a website containing the public disclosures. This page would need to be maintained by the creator of the Coin for the duration of the Coin's life, until such time as the accounts are tapped and the Coins expire. This will lead to a form of continuing liability for the

170. "Legal Notice: We are not a true bank that accepts USD or any national currency, only bitcoins which by their nature are not regulated, we're not FDIC insured or regulated by any government entity." Note that Flexcoin closed its doors after reporting the loss of millions of dollars from its online virtual currency wallets.

creator of Coins, and would lessen the incentive to create coins for any but large institutions.

A second way disclosures could be made would to bundle the plaintext disclosures with each Coin; a checksum would make altering the plaintext difficult, as the Coins would not authenticate on transfer if the public disclosures have been altered. The downsides are technical: This would increase the size of each transfer, and would potentially make the encryption of the cyphertext less secure. It would also make it impossible to change the public disclosure for the life of the Coin; neither the owner nor the initial creator could alter these disclosures without rendering the Coin unable to transfer (as, being altered, the Coins would not authenticate on transfer).

Other places public disclosures could be made are in the transfers themselves. This would have the advantage of limiting liability for the creator of the Coin to the initial transfer only without leaving a trail of continuing liability and necessity to monitor and update disclosures of created Coins. Disclosures could be done automatically, if regulators required any front-end software to make such warnings during transmission. This would be a 'click-through' contract of the type that consumers never read while updating iTunes or installing Photoshop. Most of the home-brewed Bitcoin software is currently woefully programmed and would not meet standards of consumer safety if sold retail. It would be the place of some "killer-app" or possibly website that would corner the market on exchanges and included click-through disclosures on transfer to make such a form of consumer protection viable. It is possible that regulatory structure could require new exchange software to include certain mandated disclosures that end-users would see upon installation or use of the software.

The last potential form of consumer disclosure would be on an ad-hoc basis between parties of a transfer. If Coins were limited mainly to large institutional users (as anticipated in the GodloveCoin hypotheticals), the parties could be relied upon to negotiate disclosures and apportionment of liabilities between themselves without regulation. Such disclosures would rapidly converge on commonly used boilerplate, and variations of these contracts could become commonly copied for use among less sophisticated consumers or investors. If large institutions do begin to adopt virtual currency, regulatory agencies would be well-served by adopting a wait-and-see attitude to allow private parties to experiment and determine where apportionment of liability should lie, and what disclosures are offered or sought.

Until more development occurs, it would be premature to seek to name the kinds of disclosures consumers would need in the use of virtual currency. General outlines can be named, but the devil's in the details. At the very least, standard disclosures made by more traditional e-payment methods that could not be made for virtual currency can be listed here, and their implications laid out. First, the avoidance of ACH or other clearing houses during payment mean consumers cannot count on suspicious transfers being caught before they are made. Consumers' coins that are available online are insecure, and this dovetails into the second major disclosure that consumers cannot be expected to find: there are no chargebacks, no refunds, and no returns possible for stolen digital currencies. Consumers need to be aware that their currency is as untraceable as cash and as insecure as their email. This is the price of pseudo-anonymous, easily transferable block-cypher virtual currency. This is an inextricable fact of the currency; and attempts to provide consumer protection would eliminate many of the aspects of virtual currency that make it desirable in the first place.

Just as credit card companies protects their customers from fraud and assume the risk for fraudulent use of credit card accounts, there could be large institutions that assume the liability for use of Coins. Such companies would keep the Coins in their own accounts and credit consumers with Coins but keep them and make largely paper trades, except to trusted outsiders. These virtual currency exchanges would (as discussed above) be required to register as money transmitters and held by the Treasury to anti-money laundering requirements, but would assume the additional responsibilities of ensuring that purchases made from certain trusted sources included agreed-upon consumer protections. Users of the Coins who made purchases from trusted sites and used Coins held for them by an exchange could enjoy the same guarantees and return policies as consumers in large retail stores.

B. Protection from Theft, Prevention of Illicit Purchase

1. Can Consumers Waive Liability Against Unauthorized Transfer?

One of the biggest questions with virtual currency exchanges is whether they will insure against unauthorized transfers. An "Unauthorized Transaction" is a type of error that occurs when money is sent from the customer's account that they did not authorize and that they do not benefit from. An obvious example of unauthorized transaction would be a hacker who steals a customer's password, and uses the password to access and initial a virtual currency transfer, possibly from a currency exchange site.

However, it is standard policy that anyone entrusted with password access to a Coin by that Coin's owner may use that Coin as an agent of the owner, and that a currency exchange would not consider transfers made to be unauthorized, even if they did not benefit the owner.[171]

2. Currency Exchange Protections Against Unauthorized Transfer

PayPal, the most successful online money transmission service, protects its users against "Other Errors" that occur when money is either incorrectly taken from customer accounts and when transactions are incorrectly recorded in their accounts. PayPal protects customers when: sent payments are incorrectly debited from their account; an incorrect amount is credited to a customer's account; if a transaction is missing from or not properly identified in the account statement; the customer receives an incorrect amount of money at an ATM; and if there is a computational or mathematical error by PayPal. PayPal further provides that its customers authorize PayPal to handle all disputes, claims, chargebacks, and reversals as set forth in the User Agreement. Because PayPal is a centralized money transmission service, such an agreement makes sense for it.

The unauthorized transaction protection is most likely to be the point on which consumers and exchanges differ. Bitcoins are unlike other methods of payment in their ability to be rapidly transferred and difficult to trace, which makes chargebacks impossible. Thus, stolen Bitcoins (any transferred without owner or trustee authorization) are gone. Who should risk this loss? Bitcoins have been stolen through two major security breaches thus far: poor security in the front-end and poor password protection by the owners. When Bitcoins are kept in trust on an exchange and stolen because of lax or poor site security, the exchange should clearly be liable for the loss. And for Bitcoins held locally on owner's computers and stolen because of poor password protection or one of several methods of unauthorized entry on the computer and transfer, the owner who left the security hole on their own computers should bear the risk (they left the door 'unlocked' and are responsible for their own theft. But what about Bitcoins left in trust on an exchange that are lost due to the owner's poor choice in password, or by publicly revealing their password? In such cases, the exchange should still be held liable by default, unless the users of the exchange have agreed previously to accept responsibility for the loss or theft of their Coins due to poor password protocol. This is likely to become

171. *See PayPal User Agreement*, PAYPAL, https://www.paypal.com/us/webapps/mpp/ua/useragreement-full (last visited July 2, 2014). This is general agency law.

a standard term of use for future exchanges, and will shift the burden of liability to the person most "responsible" for the security hole that allowed the unauthorized transfer. This is another reason to disallow exchanges that do not have significant reserves, like registered money transmitters.

3. Arbitration Clauses

It seems likely to me that future Coins will include arbitration clauses in their plaintext. Arbitration by the acceptance of a ticket is permitted,[172] so acceptance of a Coin likely includes agreement to the arbitration clauses contained therein. This could be used to save money or be used against the consumers in disputes.

The Federal Arbitration Act requires that federal substantive law applies when the arbitration agreement is connected to a transaction involving interstate commerce.[173] Whether the arbitration agreement is connected to a transaction involving interstate commerce is a factual determination in each case.[174] Under the FAA, on the motion of a party, a court must stay proceedings and order the parties to arbitrate the dispute if the court finds that the parties have agreed in writing to do so.[175] A party seeking to compel arbitration must show (1) that a valid agreement to arbitrate exists between the parties and (2) that the specific dispute falls within the scope of the agreement.[176]

Arbitration clauses may be avoided if their application would be unconscionable. Under California law, unconscionability has both procedural and substantive components.[177] The procedural component can be satisfied by showing (1) oppression through the existence of unequal bargaining positions or (2) surprise through hidden terms common in the context of adhesion contracts.[178] The substantive component can be

172. Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585 (1991).

173. State Farm Mut. Auto. Ins. Co. v. Coviello, 233 F.3d 710, 713 n.1 (3d Cir. 2000); Marciano v. MONY Life Ins. Co., 470 F. Supp. 2d 518, 524 (E.D. Pa. 2007) (Robreno, J.); *see also* 13B CHARLES ALAN WRIGHT, ARTHUR R. MILLER & EDWARD H. COOPER, FEDERAL PRACTICE AND PROCEDURE § 3569, at 173 (2d ed. 1984) ("[I]n a diversity suit . . . , the substantive rules contained in the [Federal Arbitration] Act, based as it is on the commerce and admiralty powers, are to be applied regardless of state law.").

174. *State Farm*, 233 F.3d at 713 n.1.

175. 9 U.S.C. §§ 3, 4, 6. (2012).

176. Trippe Mfg. Co. v. Niles Audio Corp., 401 F.3d 529, 532 (3d Cir. 2005); PaineWebber, Inc. v. Hartmann, 921 F.2d 507, 511 (3d Cir. 1990).

177. Davis v. O'Melveny & Myers, 485 F.3d 1066, 1072-73 (9th Cir. 2007); Comb v. PayPal, Inc., 218 F. Supp. 2d 1165, 1172 (N.D. Cal. 2002).

178. *Comb*, 218 F. Supp. 2d at 1172.

satisfied by showing overly harsh or one-sided results that "shock the conscience."[179] The two elements operate on a sliding scale such that the more significant one is, the less significant the other need be.[180] However, a claim of unconscionability cannot be determined merely by examining the face of the contract; there must be an inquiry into the circumstances under which the contract was executed, and the contract's purpose, and effect.[181]

Typical cryptocurrency arbitration clauses, if they become popular, will fall under the guidance of *Comb v. PayPal*.[182] Arbitration clauses will only be binding if included in the *original* Genesis block of the Coin. Those who attempt to attach arbitration clauses to their Coins on resale, after their initial creation, will be changing the terms of the agreement upon which the Coins were created, and courts will be correct to reject such arbitration clauses.[183] Even if such clauses are included at the creation of the virtual currency, they will be unconscionable adhesion contracts (and thus correctly rejected by courts) *unless* the party seeking arbitration shows that the purchaser was a sophisticated user in a competitive market for their Coins.[184]

However, even if instant agreement is procedurally unconscionable, it may nonetheless be enforceable if the substantive terms are reasonable.[185] For instance, adhesion contracts on Coins should be mutual, which means neither the buyer and seller should enjoy an unfair advantage in the choice of arbitration over the other.[186] Arbitration clauses should specify the fees and relative position of the parties in arbitration so that an unknown and unidentified risk of excessive fees will not be sufficient to defeat a valid arbitration clause.[187]

---

179. *Id*.

180. *Id*.; *see also* Armendariz v. Found. Health Psychcare, 6 P.3d 669 (2000) ("[T]he more substantively oppressive the contract term, the less evidence of procedural unconscionability is required to come to the conclusion that the term is unenforceable, and vice versa.").

181. *Comb*, 218 F. Supp. 2d at 1172.

182. *Id*.

183. *Id*. at 1171.

184. Dean Witter Reynolds, Inc. v. Superior Court, 211 Cal. App. 3d 758, 769 (Ct. App. 1989).

185. *See* Craig v. Brown & Root, Inc., 84 Cal. App. 4th 416, 422-23 (Ct. App. 2000) (finding contract of adhesion to arbitrate disputes enforceable).

186. *Comb*, 218 F. Supp. 2d at 1174-75; Stirlen v. Supercuts, Inc., 51 Cal. App. 4th 1519, 1536 (Ct. App. 1997).

187. Green Tree Fin. Corp.-Ala. v. Randolph, 531 U.S. 79 (2000).

4. Illicit Purchase

What about the use of Coins in illicit purchases? We should look at the ways that current Internet money transmitters restrict users' ability to purchase illicit goods. The PayPal user terms of service prohibits activities that:

> (1) violate any law, statute, ordinance or regulation, (2) relate to transactions involving (a) narcotics, steroids, certain controlled substances or other products that present a risk to consumer safety, (b) drug paraphernalia, (c) items that encourage, promote, facilitate or instruct others to engage in illegal activity, (d) stolen goods including digital and virtual goods (e) items that promote hate, violence, racial intolerance, or the financial exploitation of a crime, (f) items that are considered obscene, (g) items that infringe or violate any copyright, trademark, right of publicity or privacy or any other proprietary right under the laws of any jurisdiction, (h) certain sexually oriented materials or services, (i) ammunition, firearms, or certain firearm parts or accessories, or (j) ,certain weapons or knives regulated under applicable law, (3) relate to transactions that (a) show the personal information of third parties in violation of applicable law, (b) support pyramid or Ponzi schemes, matrix programs, other "get rich quick" schemes or certain multi-level marketing programs, . . . (d) are for the sale of certain items before the seller has control or possession of the item, (e) are by payment processors to collect payments on behalf of merchants, (f), . . . (4) involve the sales of products or services identified by government agencies to have a high likelihood of being fraudulent. violate applicable laws or industry regulations regarding the sale of (a) tobacco products, or (b) prescription drugs and devices.[188]

Paypal also prevents its use in connection with gambling or lottery sales, although the use of virtual currency in gambling should be restricted already though preexisting federal and state laws.[189]

These restrictions are important but largely unenforceable in virtual currency. The difference is that, for virtual currency, there is no central clearing house that could easily identify and prevent the transmission of

188. *PayPal Acceptable Use Policy,* PAYPAL, https://cms.paypal.com/c2/cgi-bin/?cmd=_render-content& content_ID=ua/AcceptableUse_full (last visited July 9, 2014).

189. 18 U.S.C. § 1301 (2012).

money to illegal goods. Again, the burden would for the most part lies with the escrow houses; but in peer-to-peer transmission, all escrow is bypassed. The only realistic burden is the increased risk of theft or fraud, for which the consumer who bypassed the safety of an escrow house would have no recourse. Additionally, such restrictions would be overly burdensome on the use of virtual currency, and such stipulations as restricting payment before the possession has control or possession of the item being sold would severely restrict their functionality.

It would be far better for such restrictions to be determined by the creators of virtual currency and embedded in the public disclosures. It would then fall to the owner's responsibility to check the terms of service and use the virtual currency only as the terms provide. Such restrictions would be largely unenforceable but consumer protections and law enforcement could be better served by focusing on other methods.

C. Safety and Soundness Requirements

1. Should Exchanges Hold Reserves and How

The capital, collateral, net worth, and investment requirements of virtual currency are currently under debate. Who should retain sufficient capital and collateral to secure end users against loss and theft? The Bitcoin exchanges that currently exist have no capital reserves, and simply deduct losses from theft, fraud, and embezzlement from their users' accounts. Such practices are damaging to consumer confidence and likely criminal. But should these exchanges, acting like money transmission services, be bound to reimburse users for their losses? How? Should end-users or issuers be required to maintain collateral or capital reserves upon which their virtual currency can be drawn?

Traditional money transmitters and banks have to abide by certain net worth and permissible investment requirements to help ensure that they are operating in a safe and sound manner. They, for example, need to have a large enough capital buffers on their balance sheets to absorb unexpected losses and financial shocks without going under. They are also limited in the types of investments they can hold – so they are not taking reckless risks with customer money in the search of windfall profits.

Virtual currency exchange firms should be required to abide by similar requirements. However, regulators need to restructure the rules in light of the fact that the virtual currencies these firms hold are not denominated in dollars or other forms of traditional currency. Coins held in trust, if lost, must be replaced by Coins held by the firm, not taken from the consumers' accounts. This much is obvious. But what if replacement Coins cannot be

found, or the theft bankrupts the company? What monetary replacements should be made, and how should the values be determined? If Coins are legally barred from being exchanged for cash, how will consumers be compensated for their losses? The issue is further complicated by the fact that the value of virtual currencies relative to traditional currencies can fluctuate significantly on a day-by-day or even hour-by-hour basis. The simple answer is that GodloveCoins, or any coins that are based upon a stable unit of value such as gold or corporate stock, will make such valuations trivially easy. Buyers and regulators will find themselves laboring to calculate the value of virtual currency that "floats". This is a strong reason that regulators should require virtual currency to be established upon some base value. If an exchange loses those Coins, the value can be easily calculated by determining the value of the base reserve that the Coins were created with at the time of the loss. Reserve capital requirements for exchanges can be easily calculated by state law: If virtual currency can easily be exchanged for cash by the exchange firm, it needs only to keep enough Coins in its own possession to satisfy existing state money transmission laws. These Coins must be held in offline wallets, safe from theft and "runs" by customers. End users who lose virtual currency held on their own would still be at a loss, however, but this will simply encourage them to save their virtual currency in secure exchanges.

Net worth, capital, and permissible investment requirements are among the most important consumer protection requirements we can put in place as regulators. Exchanges and other virtual currency firms that have frozen redemptions for extended periods of time damage to consumer confidence. The long-term strength of the virtual currency industry will require robust safety and soundness requirements – so customers have faith that their money won't get caught in a virtual black hole. These requirements can be met when exchanges are required to register as money transmission services, and undergo such safety and soundness requirements that this entails. The Silicon Valley company is handling this by becoming registered in each state as a certified money transmitter, which includes minimum amounts to be held. This new model of virtual business will need to be well-funded and will likely be regarded with suspicion by established banks for some time. This will lead to private arrangements dictated by the banks that do business with exchanges, on terms the banks set. Without burdensome restrictions, banks will likely dictate fairly robust soundness requirements on the exchanges that will become mainstream.

2. Should Exchanges Be Allowed to Invest on Virtual Currency

Should virtual currencies themselves be allowed as permissible investments? The maturing nature of virtual currency indicates that Bitcoins can be treated like investments more easily than as currency. For tax purposes, Bitcoins are treated as investment income. Purchasers and sellers who use Bitcoins are cash are relatively safe from the rise and fall of the market, and those who use future virtual currency should be aware that their value will be based on their ready-exchange rate into cash or traditional commodities. But institutional investors and those who seek to earn income with Bitcoin purchasers should not be regulated any more stringently than individual consumers.[190]

New York State regulators would like to make New York and the United States a magnet for legitimate, well-regarded exchanges and other virtual currency firms. They have already begun scrutinizing Bitcoin firms operating within their jurisdiction.[191] It should begin by mandating that all virtual currency bought and sold by institutions in the state be backed by some stable value. GodloveCoins and other virtual currency created with encrypted account codes that may be called upon at a later date, should be the only permitted medium of exchange in the state that money transmitters and institutional investors are permitted to use as investment vehicles. Investors should not be permitted to use virtual currency with no correlation to a fixed unit of value as speculative ventures; investing in such currencies is little different from gambling.

The basic soundness of these companies should be guaranteed by their abiding by current requirements for money transmitters. Regulators should avoid creating a separate set of requirements for different technologies that effectuate the same result. If my proposed development takes place, the safety and soundness of virtual currency will be brought up to a level that is tolerable and comparable to similar established technologies.

Currently, virtual currencies are at their most vulnerable when they are available on public offer. The password used by their owner needs only to be hacked before the Coins can be transferred out of the owner's possession without his authorization. Current exchanges that keep a majority of these

---

190. Marco Santori, *IRS Guidance Further Legitimizes Bitcoin and Provides Clarity, but Demands Unrealistic Reporting*, BITCOIN FOUND. BLOG (Mar. 26, 2014), https://bitcoinfoundation.org/blog/?p=600.

191. Greg Farrell, *N.Y. Subpoenas Bitcoin Firms in Probe on Criminal Risk*, BLOOMBERG (Aug. 12, 2013, 1:27 PM CT), http://www.bloomberg.com/news/2013-08-12/n-y-regulator-subpoenas-firms-over-bitcoin-crime-risks.html.

Coins out and available on the market and maintain poor accounting practices violate already-established federal law. The Foreign Corrupt Practices Act and state banking laws make such poor protection of property held in trust of another criminally negligent, and possibly federally felonious. As the market develops, standard practices will develop and such instances will become rare.

Future development of Coins of a limited duration, meant to be created, traded, and then cashed in in a relatively short period of time, should also increase the safety of virtual currency. When coins are automatically kept in offline holding and brought to online servers only to be used, then cashed in, the risk of theft will be low enough that the development of novel laws governing their safety would be counterproductive and duplicative.

D. The Use of Public Ledgers and Tumblers in Regulation

Law enforcement officials cite the importance of the public ledgers for Bitcoin and other types of crypto-currencies. It is conceivable that some virtual currencies could be created without the existence of a public ledger, but right now no cryptographically secure currencies exist or can be envisioned. Virtual currencies without an existing public ledger are simply single-point money transmission devises, similar in most ways to credit-card payment systems, and do not qualify as true virtual currency. Regulators need to require that newly created virtual currencies use public ledgers, both for definitional and public interest reasons. Currencies moving forward need to contain public ledgers, and these ledgers, as discussed above, can prove very helpful to law enforcement. These ledgers can accurately record essentially every single transaction that has occurred in a specific virtual currency since it came in the being. By seeing every transaction, law enforcement can institute a series of red flags for further investigation, similar to current banking laws that require disclosures of unusual transactions or large deposits. Banks and exchange firms must be regulated in the same manner, and through value-backed virtual securities, they can be held to relatively simple-to-follow standards for determining when large deposits or unusual exchanges have been made through them. Individual users and peer-to-peer transactions will be exempt, of course, but banks will be obligated to disclose unusual transactions when the GodloveCoins are redeemed, if the "cash out" terminating the Coins are unusual. This will satisfy law enforcement and still maintain the flexible spending of virtual currencies.

Appropriate know-your-customer requirements for virtual currency firms – public ledgers can help mitigate some of the documented concerns

related to money laundering and this new technology. Creators of Coins will be required to provide documentation to banks or other institutions on which they create the Coins, and users of exchanges will also need to provide accurate names and addresses, which will severely restrict the use of virtual currency in illicit markets while still maintaining the efficiency, secrecy and openness that day-to-day users crave.

A framework of institutions who cater to and facilitate the creation, transmission, and termination of virtual currency would obviate many of the associated questions about so-called "tumblers," which are of particular concern to law enforcement. Tumblers are a technology used to obscure the record and source of virtual currency transactions. By obscuring the public ledger, tumblers disguise the users within a block-chain, and could be used by criminal enterprises in the middle of a block-chain to launder money. This is less of a concern for Coins built to facilitate specific purchases and based upon a stable medium of cash because they have a designated bank or commodity at the terminal point.

Conclusion

This article has laid out the basic foundation of virtual currency. It paradoxically holds great promise for ease and safety in facilitating large international purchases, while the concept in its current nascent form is a useless and criminally mismanaged enterprise that has been flooded with the dishonest and foolish. However, it has become a viable and stabilized tool for transmission of money pseudo-anonymously over the Internet, and state and federal governments must respond. I have laid out the few simple laws that must be passed in order to bring virtual currency in line with other forms of standard currency transmission, and how such laws will eliminate many of the negative aspects of virtual currency while permitting their continued development and use. Future articles should respond to various government agencies' floundering first steps in this realm.