CYBER CURRENCY: LEGAL AND SOCIAL REQUIREMENTS FOR SUCCESSFUL ISSUANCE BITCOIN IN PERSPECTIVE

JASON S. SELIGMAN*

I. INTRODUCTION

The recent emergence of the private cyber currency *Bitcoin*[1] has reinvigorated a wholesale questioning of various aspects of design for fiduciary currency—currency without intrinsic value.[2] Who can issue fiduciary currency? How should it be issued? Why is it valued? What social role does it fill in facilitating trade and the creation of longstanding wealth among members of a society? What role does trust play in backing fiduciary currency and by what process is that trust manifest and preserved? To consider these questions, this Article will discuss various features of Bitcoin as a currency, highlighting aspects of greater and lesser merit for overall growth and acceptance. It will conclude by summarizing features of any cyber currency of merit for sustained issuance and use by society.

To be clear, none of the questions listed above are unique to the issuance of an electronic currency, nor to the issuance of a private currency, but may be particularly interesting to consider in these realms at this time. While private parties have previously issued currencies, both historically and in modern times, these efforts have met with greater or lesser success. In modern times, private and electronic issuance has been increasingly regulated by sovereign governments and associated international organizations created by groups of these governments such as the International Monetary Fund and the Bank of International Settlements. What is unique about *Bitcoin*'s emergence is its distinct distance from any of these entities. No sovereign government or international governmental organization stands behind *Bitcoin* as issuer.

---

* Assistant Professor, The Ohio State University John Glenn School of Public Affairs.

[1] The author uses the capitalized "Bitcoin" to discuss the concept of digital currency generally and lowercase "bitcoin" or "bitcoins" to describe the actual value of the currency.

[2] *Bitcoin – Open Source P2P Money*, BITCOIN FOUND., https://bitcoin.org/en/ (last visited Sept. 25, 2014) ("Bitcoin is an innovative payment network and a new kind of money.").

II. PRIVATE ISSUANCE AND TRUST

For those championing this independent currency, the lack of attachment to these entities is a virtue. Political policies ostensibly are not brought to bear on issuance and assets stored in bitcoin are harder to monitor and to freeze, so commerce is freed. Beyond the emotive excitement that some might experience from perceptions of freer markets, there is a valid and more general perspective. This perspective emphasizes that a lack of sovereign political discretion reduces motives for over issuance (debasement) and is seen to improve transparency and trust in the currency.

Facilitating trust in the case of Bitcoin appears to rely on more than just the intuition that sovereigns cannot manipulate it in wholesale or more targeted ways. Important aspects of the Bitcoin design with appeal for trust include: (1) an initial design and code proposal that, while short, is technical enough to be convincing,[3] (2) a distributed settlement system,[4] (3) a limit on total global issuance of Bitcoin in perpetuity, and (4) transaction anonymity. This duly noted, a careful read of the initial design proposal and recent history suggests that belief in these properties has been more than should be justified. Consider the fact, code, and recent administration of the Bitcoin currency.

Regarding administration, for example, the most successful publicly issued currencies come with an array of understood due process arrangements. For example, while the U.S. Treasury may freeze funds in transit in certain cases, private parties have the opportunity to hold the United States accountable in courts of law designed to consider and protect individuals' property rights. Thus, for those suspicious of the bitcoin currency, a lack of political attachment appears to make any due process less assured.

Consider one recent administrative failure, the hacking theft of roughly half-a-billion dollars in bitcoin (850,000 bitcoin) in February of 2014 from the leading bitcoin exchange, Mt. Gox, in Japan. This bankrupted the exchange. While 200,000 bitcoin were recovered over the following six months, the dollar value of these recoveries is lower than otherwise because the exchange rate of bitcoin declined in the wake of revelations of weak security. Most of the pain of loss was inflicted on exchange customers with little or no recourse.[5]

---

[3] *See generally* SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2014), *available at* https://bitcoin.org/bitcoin.pdf.

[4] See François R. Velde, *Bitcoin: A Primer*, CHICAGO FED LETTER (Fed. Reserve Bank of Chi.), Dec. 2013,for a coherent technical description of the distributed settlement system.

[5] Takashi Mochizuki & Eleanor Warnock, *Mt. Gox Head Believes No More Bitcoins Will Be Found: Mark Karpelès Describes Sleepless Nights in First*

Beyond direct property crimes, another concern regards the conduct of criminal activity. Given the due process arrangements for existing currencies, those that value bitcoin may be seen to value that due process less than those employing sovereign currencies. It follows that these Bitcoin users are more likely to hold illegitimate property claims, claims that could not be enforced anyway, as a result of their nefarious nature. Thus, on net, criminals may value Bitcoin's anonymity and opaque transaction structure while disregarding concerns regarding due process.

There is some evidence of this. The federal case against Ross Ulbricht, alleged creator of an billion-dollar "online drug bazaar," Silk Road,[6] charges Ulbricht with facilitating payment on the website through bitcoin due to these transactional features.[7] Tying both of these concerns together, following federal seizure, Silk Road was hit by independent hackers who stole roughly $2.7 million of bitcoin from the site's escrow account.[8]

Moving from day-to-day administration of Bitcoin transactions to matters of fact and code, both Silk Road and Mt. Gox were victims of a flaw in Bitcoin code that allowed hackers to manipulate transaction records and transfer currency without any exchange of value. What is more, the software design flaw has been understood to exist since 2011—that is, during a foundational period for the currency, several years before either event and before the currency exploded in value.

Interview Since Exchange's Demise, WALL ST. J., http://online.wsj.com/articles/mt-gox-head-believes-no-more-bitcoin-will-be-found-1403850830 (last updated June 29, 2014, 11:23 AM).

[6] Patricia Hurtado & Bob Van Voris, *Silk Road Online Drug Bazaar Accused Operator Indicted*, BLOOMBERG (Feb. 5, 2014, 12:01 AM), http://www.bloomberg.com/news/2014-02-04/accused-operator-of-silk-road-online-drug-bazaar-indicted.html.

[7] United States v. Ulbricht, No. 14-cr-68, 2014 WL 3362059, at *9 (S.D.N.Y. 2014):

> Count Four alleges that Ulbricht "designed Silk Road to include a Bitcoin-based payment system that served to facilitate the illegal commerce conducted on the site, including by concealing the identities and locations of the users transmitting and receiving funds through the site." ... "[K]nowing that the property involved in certain financial transactions represented proceeds of some form of unlawful activity," Ulbricht and others would and did conduct financial transactions with the proceeds of specified unlawful activity, "knowing that the transactions were designed . . . to conceal and disguise the nature, the location, the source, the ownership and the control of the proceeds." *Id.* (citations omitted).

[8] Jose Pagliery, *Drug Site Silk Road Wiped Out by Bitcoin Glitch*, CNN MONEY (Feb. 14, 2014, 11:16 AM), http://money.cnn.com/2014/02/14/technology/security/silk-road-bitcoin/.

To place the history of the design flaw in perspective, it was uncovered in a period when exchange rates (B:$) were roughly 3:1, well below a more recent 1:500.[9] Why, then, did the currency appreciate so tremendously following the revelation of the design flaw? It is quite possible that those aware of the risk underestimated the flaw's importance. It is also possible that a great number of folks were unaware of the flaw, focusing instead on other design aspects of the currency, but this is speculation and it would be difficult to know how these and other factors interacted. Thus, the interest and persistent popularity of Bitcoin can be said to be mysterious in several ways on first blush.

Indeed, for the uninitiated, the mystery surrounding the initial creator of Bitcoin's currency creation and payment network is more reminiscent of that surrounding L. Frank Baum's fictional *Wizard of Oz* than of modern currency and credit creation.[10] While banking was somewhat intentionally opaque a century or more ago, the modern model consists of visible and accountable teams of bankers, lawyers, and government officials, and this is true in both public and private spheres.[11]

In fact, the modern age of banking and finance has been defined by increasing transparency, and by and large this increase has been seen as improving private facilitation of commerce and lending.[12] Increases in transparency have been seen as positive by central bankers, as well.[13]

More broadly, the value of accountability across public and private financial parties is that it ensures that those who misrepresent the quality of collateral backing paper assets, such as Countrywide Financial Corp. co-founder Angelo Mozilo, can be prosecuted by the societies they harm.

---

[9] For a detailed chart of the exchange rates fluctuations of bitcoin, see *Bitcoin Price Index Chart*, COINDESK, http://www.coindesk.com/price/ (last visited Nov. 2, 2014).

[10] *See generally* L. FRANK BAUM, THE WONDERFUL WIZARD OF OZ (1900).

[11] *See* LIAQUAT AHAMED, LORDS OF FINANCE: THE BANKERS WHO BROKE THE WORLD (2009).

[12] *See generally* Eric T. Swanson, *Have Increases in Federal Reserve Transparency Improved Private Sector Interest Rate Forecasts?*, 38 J. MONEY, CREDIT, AND BANKING 791 (2006).

[13] *See* Ben S. Bernanke, Chairman, Fed. Reserve, Speech at the Cato Institute 25th Annual Monetary Conference, Washington, D.C. (Nov. 14, 2007) (transcript available at http://www.federalreserve.gov/newsevents/speech/bernanke20071114a.htm?inf_contact_key=5d17c9d1c1ee032d5aacc377ca6c88fd). Bernanke further quotes and cites the 1923 Federal Reserve Board as follows:

> The more fully the public understands what the function of the Federal [R]eserve [S]ystem is and on what grounds and on what indications its policies and actions are based, the simpler and easier will be the problems of credit administration in the United States. *Id.* (quoting 1923 FED. RES. BOARD ANN. REP. 38).

Mozilo paid a $67.5 million penalty to the SEC in 2010 "to settle SEC charges that he and two other former Countrywide executives misled investors as the subprime mortgage crisis emerged."[14]

While issues related to Countrywide Financial are perhaps sensational in terms of the magnitudes of ratio between systemic risk and one single entity's malfeasance in credit issuance, transparency in the area of credit creation supervision has been found to be of more general value, with authors finding that "enhanced disclosure can improve the allocation of resources in the banking system."[15]

Bitcoin, in its failures to be transparent, accountable, and secure, would appear to hold none of the advantages of modern publicly issued currency. Recently it has been argued that Bitcoin more resembles "a speculative investment than a currency."[16] In support of this thesis, consider that, in the three years from 2011 to 2013, its exchange rate versus the dollar increased from roughly 3:1 to 1:1,000, handily beating the lion's share of investment opportunities over that period. And, though it currently trades at a bit less than half its peak value (roughly 1:500) the four-year increase in its value is still well over 1,300%.[17] What about it makes it appealing, then? As a transactional asset, is it merely a "financial celebrity" in the sense of "being famous for being famous," and if so, is that alone enough to make it a valuable currency over the long run?

III. DEMAND AND SUPPLY FOR CRYPTOCURRENCY—THE CASE OF BITCOIN

Recognition is valuable for a currency. Recognition is perhaps particularly challenging for a currency that is not in tangible circulation to achieve. As one of an emerging class of cryptocurrencies, Bitcoin has a name-recognition status without peer. In this sense, Bitcoin, mysterious founder and all, is truly phenomenal. But name recognition is not necessarily the same as demand. A better measure of demand is found in terms of transaction frequencies. Here, Bitcoin is also relatively impressive.

---

[14] Press Release, U.S. Sec. Exch. Comm'n, Former Countrywide CEO Angelo Mozilo to Pay SEC's Largest-ever Financial Penalty Against a Public Company's Senior Executive (Oct. 15, 2010), *available at* http://www.sec.gov/news/press/2010/2010-197.htm (describing settlement that also permanently bars Mozilo from future officer or director roles in any publicly traded company).

[15] John S. Jordan, Joe Peek & Eric S. Rosengren, *The Market Reaction to the Disclosure of Supervisory Actions: Implications for Bank Transparency*, 9 J. FIN. INTERMEDIATION 298, 298 (2000).

[16] David Yermack, *Is Bitcoin A Real Currency? An Economic Appraisal* Abstract (Nat'l Bureau of Econ. Research, Working Paper 19747, Dec. 2013), *available at* http://www.nber.org/papers/w19747.pdf.

[17] *Bitcoin Price Index Chart*, *supra* note 9.

While having receded somewhat from a peak of over 100,000 transactions in a single day in late 2013, daily transaction volumes have varied around 60,000 or so for the first half of 2014, impressive in light of the security and exchange challenges over this period described earlier.[18]

Part of the persistence in use has to do with supplies of bitcoin and the established infrastructure. According to Haubrich and Orr, nearly fourteen million bitcoins have been "minted."[19] Holders of these naturally look for opportunities to use them. There are services online to help those holding the currency to purchase goods. This is helpful for those thinking about acquiring bitcoin as well.

For those looking to obtain bitcoins, there are two options: first, one can purchase them via an exchange at the exchange rate; or second, one can work to facilitate transactions in bitcoin, thereby earning some in the process. This second process is quite clever, from a systems perspective. The design distributes transaction processing, earns processors fees paid in bitcoin, and thereby manifests issuance of bitcoin (at least until the announced fixed upper limit of bitcoin supplies, twenty-one million,[20] is reached). This process is sometimes referred to as "mining" in as much as it generates new supplies of Bitcoin—in this way there is an analogue to older non-fiduciary mediums of exchange (such as precious and semi-precious metallic coinage).

While persistence may be explained by existing supplies and infrastructure, none of this explains why or how Bitcoin successfully scaled up to a position wherein it could be so resilient in the face of current challenges. Why did an initial group decide to transact and facilitate transactions in bitcoin?

To better understand the fundamentals for demand and supply of Bitcoin in the 2009–2011 period, it is advisable to revisit the three basic features of money. Money generally is agreed to serve three roles: (1) medium of exchange, (2) unit of account or measure of value, and (3) store of value.[21] In terms of the latter two as a unit of account and as a store of value, bitcoin has been seen to be volatile relative to other currencies.[22] In fact, the Bitcoin organization's page dedicated to things "you need to know" now states:

> The price of a bitcoin can unpredictably increase or decrease over a short period of time due to its young

---

[18] *See* Joseph G. Haubrich & Ashley Orr, Fed. Res. Bank of Cleveland, *Bitcoin Versus the Dollar*, ECON. TRENDS, Aug. 14, 2014, *available at* http://www.clevelandfed.org/research/trends/2014/0814/01banfin.cfm.

[19] *Id.*

[20] *Id.*

[21] Yermack, *supra* note 16, at 4.

[22] *Id.* at 11.

> economy, novel nature, and sometimes illiquid markets. Consequently, keeping your savings with Bitcoin is not recommended at this point. Bitcoin should be seen like a high-risk asset, and you should never store money that you cannot afford to lose with bitcoin. If you receive payments with bitcoin, many service providers can convert them to your local currency.[23]

However, over the initial startup period, both because the bitcoin payments for transactions facilitation were greater and because the exchange rate was quite low, holding bitcoin could be seen as both whimsical and speculative—and, in either case, with a relatively low downside and relatively high upside potential. Thus, consistent with the above guidance from the organization, bitcoin could be seen as something one could take a position in with relatively high opportunity for yield from a relatively low stake.

As well, the dynamics of the U.S. and global economy during this time period might have motivated interest in bitcoin. As a result of the Financial Crisis and Great Recession, broad equity indices like the S&P 500 remained below their spring 2007 levels until roughly the end of spring 2013. [24] Policy responses aggravated flight-to-quality dynamics for investors. In particular, over the 2008-2013 period, the U.S. and several other advanced economies lowered interest rates to nearly zero, and subsequently were involved in monetary base expansions, sometimes called "Quantitative Easing" (QE). These money supply expansions increased medium- and long-term inflation concerns among some investors and wealth managers, including some eminent thought leaders in the area of inflation.[25]

In this environment, the announced finite limit on bitcoin issuance coupled with promises of transaction anonymity for users might have motivated some to take an interest and position in bitcoin who normally would not have taken such an esoteric position. The fact that traditional commodity money hedges, such as gold, were pricing higher in this period may have further encouraged those looking for a substitute hedge to take on

---

[23] See *Some Things You Need to Know*, BITCOIN FOUND., https://bitcoin.org/en/you-need-to-know (last visited Nov. 2, 2014).

[24] As per the St. Louis Federal Reserve, FRED data tool for the S&P 500, Series – "SP500," the U.S. price of the index hit a high of $1,565 on October 9, 2007, and did not again achieve this level until April 23, 2013. Fed. Res. Bank of St. Louis, *S&P 500©*, FED. RES. BANK OF ST. LOUIS, http://research.stlouisfed.org/fred2/series/SP500 (last visited Nov. 2, 2014).

[25] *See* Shamim Adam & Lisa Tan, *Volcker Says Quantitative Easing May Create Inflation in Future,* BLOOMBERG (Nov. 2, 2010, 9:45 AM), http://www.bloomberg.com/news/2010-11-02/fed-s-quantitative-easing-program-may-create-inflation-surge-volcker-says.html (in the midst of early interest in bitcoin).

a position in bitcoin.[26] This line of thinking generally suggests that bitcoin was in the right place at the right time.

Moving to the first role of money, medium for exchange, historically cash, be it in a fiduciary or commodity money form, was an anonymous exchange medium. Anonymity has social value, and anonymity has been an issue for digital commerce. To consider anonymity's social value, consider two arguments below:

A. *Ability to Buy and Sell Without Being Known to Have Done So*

The lack of reputational effects is of more subtle value than is often considered. This issue is often associated with stigma—in particular, with the purchase of items that are of lesser social merit. However, because social norms are fluid, the full stigma costs of transactions may not be understood at the time of sale. For example, a person on record for purchasing alcohol for an event he or she hosts a year or two before the prohibition period in the U.S. may be concerned with stigma subsequently. So, there are potential effects related to timing.

Perhaps even more important for facilitating trade is the value of anonymity for reducing reputation-related monitoring and transaction costs for buyers. Lower transaction costs encourage market participation, maintaining trade equilibrium with larger volumes via the law of one price. By this notion, the value of anonymity for buyers is that it shields them from preference revelation and so offers protection against the exertion of market power by sellers. Anonymity protects buyers from sellers who might measure preferences and habits in repeat purchase environments. It thus protects buyers with strong preferences for particular products from prejudicial wealth extraction in the form of first-degree price discrimination (that is, being offered systematically higher prices than others for an otherwise equivalent good).

B. *Ability to Avoid Ex-post Negotiation or Fraud*

Users of credit and debit cards will likely be familiar with charge errors, like cases in which they are charged more than once for a single purchase. In the case of a credit card, the card issuer usually facilitates

---

[26] As per the St. Louis Federal Reserve, FRED data tool for the morning gold fixing price in London, Series – "GOLDAMGBD228NLBM," the U.S. price of gold increased from $869.75 on Jan 2, 2009 to a high of $1,896.50 on September 5, 2011, a period roughly consistent with the period of initial interest in bitcoin, when design flaws were not yet readily appreciable. Fed. Res. Bank of St. Louis, *Gold Fixing Price 10:30 A.M. (London time) in London Bullion Market, based in U.S. Dollars*, FED. RES. BANK OF ST. LOUIS, http://research.stlouisfed.org/fred2/series/GOLDAMGBD228NLBM (last visited Nov. 2, 2014).

restitution, but there are time and monitoring costs. Paper check purchases generally improve upon those risks a good deal, but because the Automated Clearing House (ACH) protocol employs a second magnetic rendering of the amount of the signed check (on the Magnetic Ink Character Recognition line) there is still a residual risk of fraud or error. Furthermore, the transaction costs of moving and analyzing these checks are much larger than for electronic forms of currency.

Cash historically has been unique in terms of its asymmetry. While cash trades cannot be unilaterally reversed, the general social convention has been to allow buyers paying with cash who obtain receipts for their purchases to return or renegotiate price and quality of goods over short time durations, even while avoiding any reputational, error, or fraud risk of the sort associated with credit cards and paper checks. This asymmetric feature of cash purchases makes them the gold standard of anonymity with maximum protection for purchasers' rights.

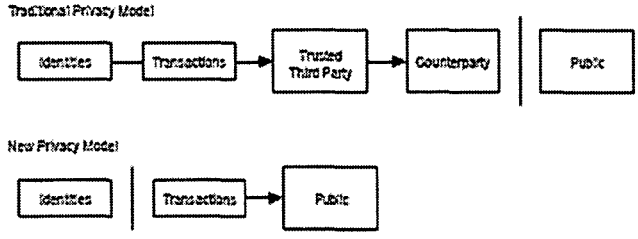
It should be noted that the anonymity features described above all speak to the social role a medium of exchange plays in facilitating trade. From the purchaser's perspective, there is an assurance in limiting the financial and other risks of engaging in transactions. In order to make credit and debit card use more appealing for transaction purposes relative to check or cash, card companies have often resorted to incentive programs to motivate use. Card companies can find these profitable even for customers who do not finance a balance on their cards because of the merchant transaction fees they charge. The lack of anonymity for consumers and, perhaps, sellers, as well as the merchant transaction costs and monitoring costs for consumers, naturally motivates interest in an immediate and anonymous electronic form of payment.

However, it should also be noted that Bitcoin is not anonymous. The particulars regarding privacy have been documented from the outset; here is the original language from Nakamoto:[27]

[27] Nakamoto, *supra* note 2, at 6.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

As the highlighting reveals, once one knows of a user's transaction, it is possible to link other transactions to the one and create a preference history. Thus, Bitcoin encryption is not designed to protect the user in this way. This point is now emphasized on the site's "you need to know" page as well, where it is stated directly "Bitcoin is not anonymous. Some effort is required to protect your privacy with Bitcoin. All Bitcoin transactions are stored publicly and permanently on the network, which means anyone can see the balance and transactions of any Bitcoin address."[28]

IV. HISTORIC PRECEDENTS FOR BITCOIN

While there were several electronic currencies ahead of Bitcoin, and banks have been wiring each other money since the age of the telegraph, a few stand out. Three recent historic examples of non-sovereign electronic currencies are instructive.

First, the International Monetary Fund's super-national currency, Special Drawing Rights (SDR), was created in 1969. This currency is backed by IMF capital contributed by sovereign nations from around the globe; it is not in wide circulation, and it is generally used to smooth out balance-of-payment issues that threaten the short-run stability of one or

[28] *Some Things You Need to Know*, *supra* note 23.

more countries. It has not evolved into a practical transactional currency outside of its sovereign audience.

Second, a relatively close precedent to Bitcoin was found in the private and unregulated DigiCash, which was manifest in 1990 and survived about eight years. This currency was notable in that it attempted to manifest a cryptographically anonymous form of electronic payment.[29]

Third, a private and perhaps best described as quasi-regulated electronic currency founded the year DigiCash went bankrupt is sometimes not thought of as a currency. It is PayPal. Founded in 1998, PayPal is an account-based transactional service owned by eBay since 2002. PayPal can be used to facilitate peer-to-peer and other electronic commerce. Recently the private investor Carl Icahn proposed splitting PayPal from eBay.[30] According to its most recent financial statistics, it has 152 million active registered accounts and facilitates trade in fifty-seven different sovereign currencies; total transactional volume for the second quarter of 2014 was over $55 billion, dwarfing bitcoin.[31]

To quickly sum the main points of this Article thus far, cyber currency has been shown to be of interest. People have been interested in creating and employing a non-sovereign electronic fiduciary currency that was stable and, ideally, anonymous. Bitcoin is not the first of these to have been developed. Bitcoin has not and does not currently fit this bill of objectives. The mystery of how and why bitcoin generated so much interest and a relatively strong user group (albeit small in comparison to sovereign or quasi-currencies like PayPal) may be due to: (1) the timing of its introduction, (2) the relative lack of trust in sovereign currencies based on QE policies, and (3) the contemporaneous concerns investors may have had with traditional financial market instruments in the aftermath of the Financial Crisis and Great Recession of 2007–2009.

One can still wonder whether a private cryptocurrency will exist in the long run and whether bitcoin might be that currency. This is a good place to conclude by revisiting trust in private fiduciary issuance while considering dynamics in the context of a cryptocurrency.

---

[29] What little history there is on DigiCash is fascinating. For more on DigiCash, see generally
Ian Grigg et al., *How DigiCash Blew Everything*, NEXT! MAG., Jan. 1999, *available at* http://cryptome.org/jya/digicrash.htm.

[30] Barbara Ortutay, *The Big Story: Ebay 4Q Earnings Up, Icahn Proposes PayPal Split*, ASSOCIATED PRESS, (Jan. 22, 2014, 7:32 PM), http://bigstory.ap.org/article/ebay-4q-earnings-revenue-13-percent.

[31] *See Q2 2014 Fast Facts*, PAYPAL, https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_Q2_2014_FastFacts_Final.pdf, (last visited Nov. 2, 2014).

V. TRUST REVISITED: LONG-RUN DYNAMICS FOR CRYPTOCURRENCY—CONCLUSIONS

There is clearly demand for a store of value that is not fiduciary and not sovereign (fiat), like gold. Much of the trust so-called "goldbugs" have in gold comes from: (1) its historic use as a currency, (2) established commodity market trade, (3) its use as a reserve asset by central banks, and (4) its current (albeit infrequent) minting by governments. Of these, the weakest link for those hoping to transact in gold has been the advantages that notional (paper) and fiduciary (not backed) currencies have over commodity money, which are portability and ease of use. This is a place where electronic currency shows even greater promise.[32]

The number of goods sold and purchased in bitcoin has grown and appears to be continuing to do so. For many pragmatic folks, the merit in a currency comes from the ability to transact in it—for both sundry and exotic items. Thus, trust in a cyber-currency may boil down to trust in your ability to use it at market, today and in the future. The popularity of a currency is more substantial than celebrity; it is of merit for users, generating positive network effects.

Over time, however, even given positive growth in network effects for transactions, the popularity of Bitcoin is subject to the hard politics of all three money properties. In particular, store of value dynamics may challenge a cyber currency, which is volatile and suffers systemic theft and exchange shocks. In light of this and consistent with improved administration of the Bitcoin environment, a group known as the Bitcoin Foundation states, "[a]s a non-political online money, [b]itcoin is backed exclusively by code. This means that – ultimately – it is only as good as its software design. By funding the [b]itcoin infrastructure, including a core development team, we can make [b]itcoin more respected, trusted, and useful to people worldwide."[33]

However, understanding the problem and addressing it are two separate matters. As such, challenges remain for validation, security, and

---

[32] *See* Fernando Alfonso III, *This 4chan User Bought a Lamborghini with $200K in Bitcoin*, DAILY DOT (Dec. 11, 2013), http://www.dailydot.com/business/4chan-bitcoin-lamborghini/. *See also Gold Fixing Price*, *supra* note 25. Consider the recent (2013) purchase of a Lamborghini for $209,995, paid in bitcoin. The purchaser transferred the bitcoin without even going to the dealership. At a then-current price of roughly $1,200 per ounce of gold, a purchaser would have been required to bring a bit over 10.4 pounds of gold to the dealership to complete a transaction, or to pay an agent to do so. *See id.* Such a transaction is feasible—most can carry this weight, but it is awkward, risky, and cumbersome in a number of ways.

[33] *About: Overview*, BITCOIN FOUND., (Aug. 20, 2014), https://bitcoinfoundation.org/about/overview/.

other challenges remain for crypto currency not backed by a traceable, reversible, and insured-loss system (as is the case with credit cards and travelers' checks, for example). The state of the art for private, non-regulated, fiduciary, cryptocurrency is less than sufficient.

While current Bitcoin users appear to be relying on good faith efforts associated parties to improve and repair security challenges, in the wake of the recent Silk Road and Mt. Gox swindles, there is less time for this work. Another such episode might well be enough to damage trust in the network inexorably. Thus, long-run dynamics can be said to be unstable at this point in time.

It is possible that the promise of anonymous, non-sovereign, fiduciary money may remain elusive. The early history of Bitcoin is not entirely unique. The currency DigiCash shared many objectives, and also had its foundation in a relatively short, yet thoughtful, scientific article.[34] The DigiCash environment grew for a while, and many serious financial organizations found its concept and design valuable to work with and grow.[35] Then DigiCash collapsed. In the aftermath of the DigiCash demise, some blamed the idiosyncratic behavior of its founder, David Chaum.[36] While Bitcoin's seemingly phantom creator, "Nakamoto," would by the nature of non-presence avoid such personality challenges, it is possible to see other parallels between these two cryptocurrencies in their quite fundamental cryptographic and leadership challenges.[37]

There is a range of possible scaled equilibria, so that in the end it does not have to be all or nothing for a viable cryptocurrency. It is possible that society will find that such currencies are of limited, but high, value in particular contexts and that bitcoin, as such a currency, with its current network will survive and grow—one potential area for targeted growth maybe peer-to-peer international asset transfer. Such a role might make bitcoin an international wire transfer service. But regulation will likely be part of any growth, targeted or broad. Taking the wire transfer case for example, without protections in place to keep bitcoin from attracting illicit international crime and terror clients, bitcoin will likely be less attractive to legitimate users.

Dynamics such as these are likely to play out in most transactional spaces, as they have in the Mt. Gox episode. They are likely to motivate Bitcoin to become subject to many of the regulatory protocols in place

---

[34] *See generally* Grigg et al., *supra* note 29.

[35] *Id.*

[36] *Id.*

[37] *See generally* David Chaum. *Blind Signatures for Untraceable Payments*, *in* ADVANCES IN CRYPTOLOGY 199–203 (David Chaum, Ronald L. Rivest & Alan T. Sherman eds., 1983), *available at* http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF.

across sovereign and regulated banking networks. In short, then, to exist in any form over the long run, will likely have to grow up a bit and earnestly address some of the fundamental challenges of its early history. Should Bitcoin fail, it is likely that another cyber currency will attempt to enter the space, though getting to a sufficient scale to be viable is and will continue to be a challenge. More likely, a nascent cyber-transaction facilitator like *PayPal* will eventually fill this space, albeit in a more legally regulated manner.