
NEW YORK UNIVERSITY
JOURNAL OF LAW & LIBERTY

THE INCOMPATIBILITY OF BITCOIN'S "STRONG" DECENTRALIZATION IDEOLOGY AND ITS GROWTH AS A SCALABLE CURRENCY

Yilu Zhang*

INTRODUCTION

Bitcoin[1] launched the digital currency revolution and remains the most successful of the cryptocurrency experiments to date.[2] Its reputation as a disruptor of the establishment tends to precede it:

* J.D., New York University School of Law, 2017; B.A., B.S., University of Pennsylvania, 2012. Thanks to Professor Mario Rizzo for his guidance on this note, and to Michael Lenoff and the rest of the *Journal of Law & Liberty* staff for their helpful comments and efforts throughout this process. Thanks also to Professor Alan Kors for starting me on this intellectual journey.

[1] A stylistic note—Bitcoin, "with capitalization, is used when describing the concept of Bitcoin, or the entire network itself;" bitcoin, "without capitalization, is used to describe bitcoins as a unit of account . . . ." For further explanation and a glossary of other common terms associated with Bitcoin, see *Some Bitcoin Words You Might Hear*, BITCOIN.ORG, https://bitcoin.org/en/vocabulary (last visited Jan. 21, 2017).

[2] For a list of about one hundred "failed attempts" at "cryptographic payment systems" preceding Bitcoin, see ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 3 (2016) (ebook).

"Bitcoin looks like it was designed as a weapon intended to damage central banking and money issuing banks, with a Libertarian political agenda in mind—to damage states [sic] ability to collect tax and monitor their citizens [sic] financial transactions." [3] Indeed, the original founding document behind the Bitcoin protocol called for the digital currency to achieve at least two fundamental goals: (1) financial transactions in a completely decentralized system, eliminating third-party institutions for either issuing the currency itself or facilitating its transfers; and (2) complete privacy and anonymity of transactions. Along with these deliberated aspirations for Bitcoin, another one of its inescapable characteristics is its intangibility, its lack of inherent value.

This note explores the idea that the widespread adoption of Bitcoin as a functioning currency is incompatible with its unique mix of decentralization, anonymity, and inherent valuelessness. Understanding the aptitudes of decentralized versus centralized orders through Randy Barnett's framework of First Order Knowledge Problems, this note argues that Bitcoin's lack of inherent value prevents it from conveying any meaningful localized knowledge to an operational, emergent price mechanism within a decentralized order. As a result, the prices that have emerged attaching to bitcoins have been conspicuously volatile, hindering it from serving as a reliable medium of exchange and store of value.

However, the persistent ideological gloss surrounding Bitcoin as an anti-authoritarian instrument belies the reality of how Bitcoin has actually spread across digital wallets around the globe. As if to acknowledge the incompatibility of Bitcoin's simultaneous characteristics of decentralization, anonymity, and inherent

---

[3] Charlie Stross, *Why I Want Bitcoin to Die in a Fire*, CHARLIE'S DIARY (Dec. 18, 2013, 1:53 PM), http://www.antipope.org/charlie/blog-static/2013/12/why-i-want-bitcoin-to-die-in-a.html.

valuelessness, the virtual currency's rise has in fact largely depended on private, third-party service providers to better serve existing customers and expand Bitcoin's reach to new ones. This note next explores how a few of these currency exchanges, digital wallets, and payment cards have fundamentally shaped the Bitcoin landscape. This note then examines how the Bitcoin community has inevitably collided with other centralized systems, such as conventional financial institutions and government regulators. Finally, this note concludes by comparing these two groups of middlemen and drawing a principled distinction between private, third-party intervention and governmental or regulatory intervention.

Bitcoin's success in continued expansion indicates that the algorithm powering this new cryptocurrency system is fundamentally working. Its reliance on third-party institutions and increasing cooperation with enforcement agencies, however, also indicates that some of its original ideologies must give way with an eye toward mainstream adoption.

I. INTRODUCTION TO BITCOIN

A. BITCOIN'S ASPIRATIONS OF DECENTRALIZATION

The concept of Bitcoin grew out of both ideological and practical frustrations. On the one hand, a small but impassioned minority sought an alternative to conventional monetary systems controlled by central banks, vulnerable to inflation, currency debasement, and other political manipulations beyond the consumers' control. [4] During the financial crisis of 2008, as anti-government critics pointed fingers at the Federal Reserve's role in the American real estate bubble, wariness of central banks escalated and continued to gain

[4] James Surowiecki, *Cryptocurrency*, MIT TECH. REV. (Aug. 23, 2011), https://www.technologyreview.com/s/425142/cryptocurrency/.

traction with Ron Paul's 2012 presidential campaign (complete with calls to "End the Fed").[5] Libertarians adopted the refrain that political power is better in the hands of many, rather than a single authority.

On the other hand was a practical annoyance with the ubiquity of bank transactions fees and the difficulty of transmitting money across international borders.[6] These activists wanted to cut out middleman institutions and establish a payment system worthy of the turn of the twenty-first century—a technologically-advanced time when it should not take three to five days to transfer money overseas. As early as 1996, Chairman of the Federal Reserve, Alan Greenspan, perhaps foreshadowed the Bitcoin movement when he remarked, "[w]e could envisage proposals in the near future for issuers of electronic payment obligations, such as stored-value cards or 'digital cash,' to set up specialized issuing corporations with strong balance sheets and public credit ratings."[7] Indeed, more than a decade later, the (still-unidentified) creator of Bitcoin, using the pseudonym Satoshi Nakamoto, published the Bitcoin "White Paper," which laid out both the technical mechanics and ideological features of his electronic cash payments system. Primary among these ideological goals was the need for "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need

---

[5] *See* Peter Ferrara, *How the Government Created a Financial Crisis*, FORBES (May 19, 2011, 1:50 PM), http://www.forbes.com/sites/peterferrara/2011/05/19/how-the-government-created-a-financial-crisis/#2eac2fcf4b69; Molly Ball, *Another Ron Paul Production*, THE ATLANTIC (Oct. 8, 2011), https://www.theatlantic.com/politics/archive/2011/10/another-ron-paul-production/246396/.

[6] NATHANIEL POPPER, DIGITAL GOLD 19 (2015).

[7] Alan Greenspan, Chairman, Fed. Reserve Bd., Regulation of Electronic Payment Systems, Remarks at the U.S. Treasury Conference on Electronic Money & Banking: The Role of Government (Sept. 19, 1996), http://www.federalreserve.gov/boarddocs/speeches/1996/19960919.htm.

for a trusted third party."[8] Thus, Nakamoto established a fairly radical decentralization baseline (i.e., the complete elimination of third parties) as one of Bitcoin's central purposes.

B. BRIEF OVERVIEW OF BITCOIN'S MECHANICS—THE "BLOCK CHAIN" TECHNOLOGY

To achieve this goal of Bitcoin's decentralization, Nakamoto turned to algorithms and cryptography in place of human central planners. Each electronic bitcoin consists of a "chain" of "digital signatures," and each transfer of a bitcoin generates two new pieces of information, appended to the coin's chain—(1) the cryptographic digital signature of the coin's sender and (2) the recipient's public key.[9] New transactions are broadcast across the Bitcoin network, and the "nodes," or computers supporting the network, collect them into a proposed "block."[10] Each proposed block is fed through a cryptographic "hash" function, transforming it into a unique string of digits.[11] Hashes await public confirmation by bitcoin "miners," or nodes connected to the Bitcoin network that perform the work of confirming Bitcoin transactions.[12] The confirmation process, or "proof-of-work," consists of these miners racing to solve the mathematical hash puzzle, achievable only by arduous trial-and-error.[13] When one miner stumbles upon the solution to the hash, other nodes can quickly check the work (it is easy to derive the hash from a given block value, but not vice-versa), and each confirming

---

[8] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG 1, https://bitcoin.org/bitcoin.pdf (last visited Jan. 21, 2017).
[9] *Id*. at 2.
[10] *Id*. at 1-3.
[11] Corin Faife, *Bitcoin Hash Functions Explained*, COINDESK (Feb. 19, 2017, 12:35 PM), http://www.coindesk.com/bitcoin-hash-functions-explained/.
[12] Nakamoto, *supra* note 8, at 4.
[13] *Id*. at 3.

node updates the universal "block chain" ledger accordingly. The winning miner is then rewarded with newly-mined bitcoins.

This block chain technology offers a single solution to the multifaceted goals of Bitcoin. It serves as a universal recordation mechanism that publicly tracks each bitcoin transfer, offering users security in their transactions. It allows these transactions to remain functionally anonymous, by requiring only digital signatures. This methodology is in stark contrast to existing payments systems, in which a bank or merchant is stuck covering the cost of a fraudulent charge on the protected customer's behalf. As a result, current players within the traditional financial system prefer to deal only with trusted, established players, who are "well-known and well-capitalized."[14] With Bitcoin, however, each cryptographic transfer is publicly authenticated on the block chain ledger and irreversible; the system tolerates direct transactions from completely anonymous strangers, as there are minimal transactions disputes ex post.[15]

Furthermore, the Bitcoin system runs entirely on a peer-to-peer, open-source protocol; any block chain confirmations and protocol changes require the distributed consensus of at least fifty-one percent of all computing power on the network.[16] As such, confirmations and protocol changes are independent of any single institution or authority otherwise necessary to regulate the digital cash system.[17]

---

[14] Timothy B. Lee, *Bitcoin is a Disruptive Technology*, FORBES (Apr. 9, 2013, 11:21 PM), http://www.forbes.com/sites/timothylee/2013/04/09/bitcoin-is-a-disruptive-technology/.

[15] Timothy B. Lee, *Lawsuit Illustrates Bitcoin's Chargeback Problem*, ARS TECHNICA (Mar. 7, 2012, 8:00 PM), http://arstechnica.com/tech-policy/2012/03/lawsuit-illustrates-bitcoins-chargeback-problem/.

[16] Nakamoto, *supra* note 8.

[17] While "[t]here have been times when pools of Bitcoin miners have controlled more than 51% of the hashing power in the network . . . they have not used it to carry out a majority attack. It is typically more profitable for a majority pool to use its hashing power honestly to generate new coins, than to use it to steal back payments made to

The algorithmic democracy of Bitcoin serves as a built-in, system-wide incentive to participate in and maintain the system—miners are rewarded with new coins, and the only way to ensure those holdings maintain value is to preserve the system's long-term integrity.

However, systematic decentralization comes with tradeoffs. While the fifty-one percent consensus threshold yields decisions that incorporate greater user input than a centrally-run system would, the prerequisite decision-making *process* takes longer to spread across enough nodes in order to attain that threshold (it can take up to an hour to gather multiple confirmations for a single transaction).[18] As a result, the transaction costs of transferring digital cash, at least in terms of time, may still have a lower bound under this approach.

C. BITCOIN AS COMMODITY VERSUS BITCOIN AS CURRENCY

Despite the success of its underlying algorithm, Bitcoin remains a commodity as opposed to a medium of exchange. In other words, users have not fully made the transition from buying and selling bitcoins to buying and selling *other things* with bitcoins. The distinction between Bitcoin as commodity and Bitcoin as currency is an important one, given the original aspiration of Bitcoin to serve as a private alternative to state-run currency systems. A successful currency freely and widely circulates as a medium of exchange for other things; the ideal for Bitcoin, therefore, is to serve as a means to those ends, those other traded goods. A successful medium of

---

other people." Fraida Fund, *Bitcoin: Reaching Consensus in Distributed Systems* (Mar. 7, 2016), https://witestlab.poly.edu/blog/get-rich-on-fake-bitcoins/.

[18] *See* Daniel Cawrey, *Green Address – The Solution to Slow Bitcoin Transactions?*, COINDESK (June 19, 2013, 3:40 PM), http://www.coindesk.com/green-address-the-solution-to-slow-bitcoin-transactions/; The Bitcoin algorithm is designed such that nodes generate about one confirmation every ten minutes, but "blocks aren't created in a fixed schedule . . . there's considerable variation in the time between successive blocks." NARAYANAN, *supra* note 2, at 17, 54.

exchange typically must be a consistent store of value and a unit of measure—which, in turn, requires that the medium itself maintain some sort of stability in value, in order to be a reliable store of value and unit of measure for other goods.[19]

At this stage, however, Bitcoin remains a commodity, or an end in itself. Users remain intrigued by it and desire it as a novelty item, for what it represents as a disruptive force amongst existing state-backed currency systems. Within this current framework, Bitcoin faces problems for broader adoption, precisely due to its decentralization. So long as users attach some exogenous value (whether political or emotional) to Bitcoin as a commodity, its pricing will, at least partially, reflect those psychic valuations and remain correspondingly volatile. Bitcoin's decentralization, coupled with its other features, unfortunately perpetuates its historic price volatility, which impedes the successful transition from Bitcoin as commodity to Bitcoin as currency.

II. FEATURES OF DECENTRALIZED ORDERS

Legal theorist Randy Barnett proposed a framework for understanding the decentralized orders as a valuable means of social ordering for certain contexts.[20] Barnett identified the "First Order Knowledge Problem," which poses the question of how individuals peacefully allocate and use resources, given resource scarcity and pervasive ignorance on two levels—(1) of each individuals' personal knowledge and (2) of disparate networks of local knowledge.[21] The First Order Knowledge Problem, therefore, ponders how scarce resources find allocations when those who desire those resources

---

[19] Irena Asmundson & Ceyda Oner, What Is Money?, Finance and Dev., Sept. 2012, at 52, http://www.imf.org/external/pubs/ft/fandd/2012/09/pdf/fd0912.pdf.
[20] RANDY E. BARNETT, THE STRUCTURE OF LIBERTY: JUSTICE AND THE RULE OF LAW (2000).
[21] *Id*. at 29-40.

face two levels of ignorance in coordinating and communicating desired resource use.

For Barnett, personal knowledge is the "knowledge unique to particular persons of their personal perception, of their personal preferences, needs, and desires, of their personal abilities, and of their personal opportunities." [22] Inherent in this First Order Knowledge Problem is the assumption that individuals have certain valuable "ends"—either the desire for certain scarce resources themselves, or other "ends" which those resources are a "means" of attaining.[23] However, to a certain degree, these personal ends are "inarticulate and inarticulable" as well as dynamic, subject to changing over time or by "conceptual evolution."[24] Local knowledge represents some degree of aggregation of personal knowledge—or, in other words, the "publicly accessible knowledge of resource use, the access to which is limited to certain associations of people."[25] Meanwhile, gaining access to networks of local knowledge is necessarily costly (for example, requiring the learning of some expert skillset or language).[26]

A centralized order is hardly capable of navigating the First Order Knowledge Problem for the whole of society. A centralized order delegates decision-making authority to some subset of persons within a society, while individuals and local networks comprising that society are unable to fully identify and communicate their own needs.[27]

Barnett suggests that a *decentralized* order offers an elegant solution to the First Order Knowledge Problem. Such a system

---

[22] *Id*. at 31.
[23] *Id*. at 35-36.
[24] *Id*. at 33-37.
[25] *Id*. at 34.
[26] *Id*. at 34-35.
[27] *Id*. at 46.

"orders the actions of diverse persons and associations by delegating to each person and association in society a defined authority to regulate their own conduct,"[28] primarily through the coordinating powers of the price mechanism.[29]

A functioning price mechanism reflects the voluntary transfers of resources among individuals and across local knowledge networks.[30] Control over resources are carved into what Barnett calls "jurisdictions."[31] The price mechanism collects and reveals individual and network preferences, or transfers of jurisdiction, on a transaction-by-transaction basis:

> The need of others to obtain the consent of a jurisdiction-holder means that anyone wishing to obtain a transfer of jurisdiction must offer the present jurisdiction-holder jurisdiction over other resources that the present holder believes he or she would *put to better use*. The types of offers, as well as the number of persons offering to make exchanges, educate the holder of the value that others place on the resources. When this value reaches a certain level, the holder is induced to make an exchange, thereby revealing that the value she placed on the resource was less than the value to her of the resources offered.[32]

As such, Barnett's decentralized order is premised upon comparing the use-values of the resources contemplated for exchange. The price mechanism works by revealing the price-point, as determined by

---

[28] *Id*. at 45.
[29] *Id*. at 54-57.
[30] *Id*. at 55-56.
[31] *Id*. at 47-48, 51.
[32] *Id*. at 56 (emphasis added).

comparing valuable uses, at which allocations of resources should change hands. Meanwhile, the fungible currency used to facilitate this exchange represents the exchange-value vehicle that compares the use-values of those traded resources, rendered into a common unit. Economist Friedrich Hayek corroborates this function of the price mechanism: it produces exchange-values from use-values, by "attaching to each kind of scarce resource a numerical index which cannot be derived from any *property possessed by that particular thing*, but which reflects, or in which is condensed, its significance in view of the whole means-end structure."[33]

Barnett's point about decentralized orders is that they are valuable for aggregating vast amounts of relevant personal and local knowledge (knowledge of individual "ends"), which centralized decision-makers, and indeed even these individuals themselves, are sometimes incapable of doing consciously. However, Barnett is careful to concede that centralized orders are conducive to *other types* of social ordering.[34] Particularly, centralized orders are "adept at pursuing almost any concrete objective or goal," or, in other words, situations which are not vulnerable to First Order Knowledge Problems.[35]

III. BITCOIN—CHARACTERISTICALLY UNSUITED FOR A DECENTRALIZED ORDER

Bitcoin's success as a decentralized system therefore depends in part on its susceptibility to First Order Knowledge Problems. As discussed above, a prerequisite for a successfully decentralized system for Bitcoin is a properly-functioning price mechanism for

---

[33] Friedrich A. Hayek, *The Use of Knowledge in Society*, The Use of Knowledge in Society, 35 AM. ECON. REV. 519, 525 (1945) (emphasis added).
[34] BARNETT, *supra* note 21, at 45-47.
[35] *Id*. at 46.

bitcoins. In a hypothetical market where the only commodity is Bitcoin, then, how *would* those coins be priced? Within a decentralized order, the price of Bitcoin ought to reflect the community's use-value for Bitcoin. In Barnett's words, the price of Bitcoin ought to emerge from individuals' and local networks' swapping of jurisdiction over their bitcoins, based on price points that reflect who would put those coins to "better use." Deriving use-value for Bitcoin, however, is problematic, given one of its inevitable features as an intrinsically useless thing, a currency manufactured essentially "out of thin air."[36] As Greenspan noted, "There is no fundamental issue of capabilities of repaying it in anything which is universally acceptable, which is either intrinsic value of the currency or the credit or trust of the individual who is issuing the money, whether it's a government or an individual."[37]

Bitcoin advocates who laud the technological breakthrough represented by block chain technology, and its potential for uses transcending Bitcoin itself,[38] suggest that "the intrinsic value of Bitcoin [is its functionality] as the conduit in a new global crowd-funded open-source payment network;" in essence, its technological potential is itself an intrinsic value for a new technological era.[39] Such attempts at defining "intrinsic value" try to capture the intangible properties embedded within Bitcoin, including its disposal of

---

[36] NARAYANAN, *supra* note 2, at 13.

[37] Jeff Kearns, *Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value*, BLOOMBERGTECH, (Dec. 4, 2013, 5:37 PM), http://www.bloomberg.com/news/articles/2013-12-04/greenspan-says-bitcoin-a-bubble-without-intrinsic-currency-value.

[38] For example, block chain technology has potential applications in facilitating asset transfers and sophisticated "smart contracts." *The Great Chain of Being Sure About Things*, THE ECONOMIST (Oct. 31, 2015), http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

[39] *PayPal Could Embrace Bitcoin*, BARRON'S (Dec. 2, 2013), http://www.barrons.com/articles/SB50001424053111903302604579234163250372446.

governments and regulations, its security and accessibility, its democratization—all of the initial, ideological goals that Nakamoto established for the digital currency in 2008.[40] Some insist that it was "the very virtual nature of Bitcoin that made it so valuable. Unlike gold, it could be easily and quickly transferred anywhere in the world, while still having the qualities of divisibility and verifiability that had made gold a successful currency for so many years."[41]

This conception of intrinsic value, however, remains uninstructive for determining Bitcoin's use-value. Here, it is helpful to distinguish between two nested layers of decentralized orders in the Bitcoin economy: (1) Bitcoin's true "use" is its ability to serve as a widespread currency, or medium of exchange, within a broader decentralized market order for other goods and resources; but, on the other hand, (2) strong Bitcoin decentralization advocates by definition insist that the pricing of bitcoins themselves occur within a subsumed decentralized order[42]—one which must first produce a stable, emergent price mechanism capable of giving Bitcoin stability as a medium of exchange, store of value, and unit of measure—all without any government backing or "bootstrapping" onto "some initial allocation of cash" or inherently valuable commodity (such as "gold or diamonds").[43]

These nested decentralized orders develop sequentially. Before Bitcoin can be both reliable and widespread as a currency, users must buy in to the system, which requires some display of faith in its stability as a means of exchange. One of the active members of an

---

[40] *See* Mark Rees, *You Say Bitcoin Has No Intrinsic Value? Twenty-two Reasons to Think Again*, BITCOIN MAG. (May 7, 2014, 5:14 AM), https://bitcoinmagazine.com/articles/you-say-bitcoin-has-no-intrinsic-value-twenty-two-reasons-to-think-again-1399454061.

[41] POPPER, *supra* note 6, at 109.

[42] *See* Brian Booker, *What Is Bitcoin Backed by?*, 99 BITCOINS (Aug. 25, 2016), https://99bitcoins.com/what-is-bitcoin-backed-by/.

[43] *See* NARAYANAN, *supra* note 2, at 4, 14.

early online Bitcoin forum attempted the first Bitcoin transaction by essentially applying the labor theory of value to his stash of coins: "[G]iven that no one had ever bought or sold [a bitcoin], NewLibertyStandard came up with his own method for determining its value—the rough cost of electricity needed to generate a coin, calculated using NewLibertyStandard's own electricity bill. By this measure, one dollar was worth around one thousand bitcoins for most of October and November 2009."[44] This metric of valuation quickly proved unreliable; NewLibertyStandard's online "Swap Variety Shop," where he hawked items for bitcoins, quickly stagnated.[45] This ending perhaps reflects the fundamental flaw of the labor theory of value itself—the reality that no amount of labor, or computer-powered mining activity, will spontaneously generate demand for bitcoins, absent the community's buy-in to the system in the first place.

Therefore, it is within this subsumed, decentralized order for the pricing of bitcoins themselves that some reference to the use-value of bitcoin is needed as a prerequisite to reliable pricing or stability of value emerging. However, at this level—again, a precedent to the broader decentralized market order that puts Bitcoin to use as a medium of exchange—use-value for Bitcoin does not yet exist. This discrepancy, an inescapable product of chronology, highlights the flaw of advocates who insist Bitcoin's block chain technology itself represents intrinsic value. The value of the algorithm's innovative technology is still tied to its use as a market-coordinating device (at least in the context of digital currencies), which is employed only in the outer decentralized order, subsequent to the nested decentralized order in which Bitcoin develops (or fails to develop) its use-value. In

---

[44] POPPER, *supra* note 6, at 38.

[45] This online shop offered postage stamps and Spongebob SquarePants stickers. *Id*. at 39.

other words, there is no intrinsically valuable use of the technology severable from the applied use of the technology.

Therefore, absent inherent use-value, *there is no personal or local knowledge regarding the use of Bitcoin for a decentralized order to aggregate, via an emergent price mechanism*. This is not to say that the pricing of bitcoins is an impossibility. On the contrary, the current market capitalization has exceeded $46,000,000,000 to date.[46] In spite of this growth, however, Bitcoin's lack of use-value within its existing decentralized order has yielded a volatile pricing trajectory.[47] Its commodity fetishization produces prices reflective of non-intrinsic values, or exogenous factors, characteristics and aspirations, which the community attaches to Bitcoin envisaged not as a pure currency. While these commodity-based valuations may arguably still reflect some sort of "use-value" as contemplated by Barnett's First Order Knowledge Problem, the fact that they are not rooted in some generally comparable inherent use makes it that much harder for these individual, preferential, speculative "uses" of Bitcoin as commodity to accurately convey meaningful personal and local knowledge as a stable, emergent price. Even today, the estimate is that "about 20 percent of the transactions on its network involve payments or other tasks where Bitcoin is used as a currency. The other 80 percent of those transactions are mere speculation, where Bitcoin is traded as a commodity in search of a profit."[48]

Actually, the first successful Bitcoin transaction took place in May 2010, when a software engineer named Laszlo Hancez offered

---

[46] *Crypto-Currency Market Capitalizations*, http://coinmarketcap.com/ (last visited June 8, 2017).

[47] *Bitcoin Price Index Chart*, COINDESK, http://www.coindesk.com/price/ (change time range on chart from "1d" to "All") (last visited Jan. 27, 2017).

[48] Cade Metz, *Coinbase Just Debuted the First Bitcoin Debit Card in the US*, WIRED (Nov. 11, 2015, 9:00 AM), http://www.wired.com/2015/11/coinbase-unveils-countrys-first-bitcoin-debit-card/.

to exchange 10,000 bitcoins for two pizzas—a transaction which required the "buyer" to accept the bitcoins and order Papa John's using a conventional credit card (so, at this stage, the vendor of the actual goods still had no contact with the digital currency). However, Bitcoin advocates cheered this successful maiden transaction as "a great milestone," recognizing it as proof of at least someone having faith in the value of Bitcoin (demonstrated by his willingness to accept the digital cash as payment).[49] Not surprisingly, this initial buy-in was hardly sufficient to establish any stable basis for Bitcoin as either a commodity or currency. As of this writing, the price paid for those pizzas amounts to about $28,325,700.[50] Nonetheless, Hancez's pizza transaction, in conjunction with his other communications on the Bitcoin forum, suggested that he was "more interested in ideas than in personal wealth or success. Indeed, as he mined coins, he was eager to show how Bitcoin could be used in the real world."[51] This initial alienation of bitcoins at a price point of 10,000 bitcoins for two pizzas was therefore not based on Hancez's use-value for Bitcoin or for Papa John's pizzas, per se; more arbitrarily, it reflected his desire to launch the technology off the ground. The latter goal does not need to consider at its core any meaningful comparisons of resource values (or, in other words, it does not face any First Order Knowledge Problems), which a decentralized order is aptly suited to coordinate.

Contrast the Bitcoin currency regime with statist currency regimes. State-run currencies arguably have no independent use-value either; the U.S. dollar ought to be worth no more than the paper on which it is printed. However, because the U.S. dollar operates within a centralized order, the need for emergent pricing as a

---

[49] POPPER, *supra* note 6, at 44.

[50] *Bitcoin Price – Bitcoin Charts*, COINBASE, https://www.coinbase.com/charts?locale=en (last visited June 8, 2017).

[51] POPPER, *supra* note 6, at 43.

coordinator of disparate knowledge problems surrounding the value of U.S. dollars is moot. Additionally, backed by government fiat, the U.S. dollar did not face an initial "buy-in" problem like a radically decentralized Bitcoin system does. Therefore, the sequential pricing problem for U.S. dollars is likewise moot—the Federal Reserve need not first prove that the U.S. dollar is a worthy store of value and unit of exchange before people transact in U.S. dollars, because the luxury of government backing allows the currency circulation and the buy-in to happen simultaneously.

In any event, the U.S. dollar had the benefit of having evolved from a commodity-based gold standard. In fact, economist Carl Menger has argued, in summary, that "all successful money arose from commodities that had some intrinsic value, even before they become money." [52] Austrian economist Ludwig von Mises' "regression theorem" elaborates on Menger's theory: the regression theorem explains why a currency's exchange-value is necessarily rooted in some antecedent use-value. [53] Consumers are willing to trade real goods and services for currency, because currency has future purchasing power, which allows consumers to obtain additional goods and services at some later time. [54] Consumers have faith in this future purchasing power, or exchange-value, of currency by reference to the currency's past purchasing power. This purchasing power regression continues across the history of the currency until its origin as a commodity. [55] Therefore, the base commodity that launches into a successful currency must have some antecedent, inherent use-value in order to avoid an infinite

---

[52] *Id*. at 109.
[53] For a deeper discussion of Mises' regression theorem, see Robert P. Murphy, *The Origin of Money and Its Value*, MISES DAILY (Sept. 29, 2003), https://mises.org/library/origin-money-and-its-value.
[54] *Id*.
[55] *Id*.

purchasing power regression. For Mises, then, a currency's origin as commodity is inevitable. He further claims that his approach is more than historically descriptive; it is theoretical, and "[i]t *must* happen this way. Nobody can ever succeed in constructing a hypothetical case in which things were to occur in a different way."[56] As Hayek's intuition corroborates,

> It is probably impossible for pieces of paper or other tokens of a material itself of no significant market value to come to be gradually accepted and held as money unless they represent a claim on some valuable object. To be accepted as money they must first derive their value from another source, such as their convertibility into another kind of money.[57]

It appears, therefore, that existing (successful) currencies have some components of *both* centralization and use-value backing—two traits that Bitcoin notably lacks. Nonetheless, some contemporary Austrian school economists attempt to reconcile Bitcoin's apparent lack of use-value with the regression theorem. Konrad Graf, Bitcoin monetary theorist, proposes that intangible commodities like Bitcoin can possess a different kind of use-value:

> [O]ne element to consider for intangible objects such as bitcoins are various "inherent" direct-consumption values that may be primarily psychological or sociological in character. Consider, for example, the geek value hackers find in creating and attempting to crack encryption codes of any kind: "Dude, look at this code; I bet you can't crack it," may

---

[56] LUDWIG VON MISES, HUMAN ACTION 407 (1998) (emphasis in original).
[57] FRIEDRICH A. HAYEK, DENATIONALISATION OF MONEY: THE ARGUMENT REFINED 31 (1990).

> indeed be more highly valued to some people in some contexts than certain "real" economic objects or specific quantities of fiat money. . . .
>
> Even now, well after their initial emergence, there appears to be a "mystique value" and a "curiosity value" attached to bitcoins among widening circles of newcomers who, compared with founders and earlier adopters, tend to understand the underlying mechanics of the system less and less, but have the impression that participation is a way to be proud and to send a message of being techno-savvy, up to date, in the know, etc.
>
> In other words, mere possession, knowledge, and use can carry social membership signaling functions in various sub-cultures, much as wearing certain styles of clothing does. These are also *direct-consumption values* to those concerned with such signaling. Direct-use values, whether psychological or sociological, do not have to be recognized by anyone other than those in a given sub-culture actually doing the valuing (according to methodological individualism and subjective value).[58]

Graf's formulation of Bitcoin's use-value, however, recalls Laszlo Hancez's Papa John's transaction better than it meaningfully reconciles Bitcoin's valuation with Mises' regression theorem. As explored previously, Hancez likely generated his 10,000 bitcoins-to-pizzas exchange rate largely based on "geek value," or his driving

---

[58] Konrad S. Graf, *In-Depth: Bitcoins, the Regression Theorem, and that Curious but Unthreatening Empirical World*, INVESTIGATIONS AND OBSERVATIONS (Feb. 27, 2013), http://konradsgraf.com/blog1/2013/2/27/in-depth-bitcoins-the-regression-theorem-and-that-curious-bu.html.

desire to see Bitcoin facilitate even just one transaction for real-world goods. "Geek value" and "psychological or sociological" values are inevitably subjective, more appropriately contained in the realm of commodity fetishization, and yield accordingly volatile price attributes; conflating such speculative valuations with true use-value disparages the economic function of the latter as a source and reference for subsequent, stable exchange-values.

IV. CURRENCY SYSTEMS AS NATURALLY CENTRALIZED ORDERS

It is not unreasonable to question whether any money system, which has the goal of widespread adoption as a pure currency with low transactions costs, *ought* to rely on some centralization. Anthropologist David Graeber asserts that, historically, currency regimes sprang from centralized orders—and furthermore, that some forms of decentralized "[m]arkets are brought into existence as a side effect" of these medieval states' systems of coinage and taxation.[59] In fact, the prevalence of such taxation systems serves as evidence against Adam Smith's claims that precious metals could successfully evolve into robust currencies absent state coordination:

> But if Smith was right, and gold and silver became money through the natural workings of the market completely independently of governments, then wouldn't the obvious thing be to just grab control of the gold and silver mines? Then the king would have all the money he could possibly need. In fact, this is what ancient kings would normally do. If there were gold and silver mines in their territory, they would usually take control of them. So what exactly was the point of extracting the gold, stamping one's picture on it,

[59] DAVID GRAEBER, DEBT: THE FIRST 5,000 YEARS 50 (2011).

> causing it to circulate among one's subjects—and then demanding that those same subjects give it back again?[60]

The answer, Graeber suggests, is that taxation was the best way to create markets where none previously existed—and imposing a coinage scheme was essential to a successful taxation system.[61] A medieval king relied on subjects across his domain to provision his standing army; otherwise, the king would incur great expense employing a separate fleet of servicemen solely for the purpose of following around and serving his troops. By doling out coins to his soldiers, and requiring that his subjects pay taxes only in that specific coinage, the king created kingdom-wide demand for his currency, turning his "entire national economy into a vast machine for the provisioning of soldiers, since now every family, in order to get their hands on the coins, must find some way to contribute to the general effort to provide soldiers with things they want."[62] If history serves as any reliable guide, then removing centralization from monetary systems is perhaps self-defeating in practice.

The prospect of centralization, however, is one which even anti-statists could be able to endure. In the Bitcoin context, centralization need not imply government intervention. Recalling the Nakamoto White Paper, the radical call for Bitcoin's decentralization insisted upon a peer-to-peer system of digital cash, completely devoid of any third-party interference, including banks, credit card companies, payments processors, digital wallet providers, and currency exchanges. This complete rejection of third parties can be seen as a "strong" form of decentralization. Strong decentralization, however, is only one manifestation of currency decentralization. In contrast, a

---

[60] *Id*. at 49.
[61] *Id*. at 49-50.
[62] *Id*. at 50.

"semi-strong" form of decentralization tolerates private third-party partners, but eschews state-backed participation.

Hayek's own proposal for the decentralization of money, laid out in his 1976 book *Denationalisation of Money: The Argument Refined*, relies crucially on a proliferation of private third parties to displace state-based currency regimes. Hayek attributed multiple ills to monopolistic, state-run currency systems, including unaccountable debasement and inflation,[63] abuses of the minting power (i.e., seignorage),[64] and expansions of other government powers "based on the assumption that government has the power to create and make people accept any amount of additional money it wishes."[65] Despite the persistent involvement of governments in the history of money, Hayek happily claims that the state is not a necessary element of successful currency systems. Governments started out with the limited task of quality control, "certifying the weight and fineness of a certain piece of metal," but eventually expanded to quantity control as well, making "deliberate determination[s] of the quantity of money to be issued."[66] The inertia of history produced the abiding "superstition that it is necessary for government . . . to declare what is to be money, as if it had created the money which could not exist without it."[67] However, Hayek is careful to distinguish this positive claim from a normative one: "We owe it to governments that within given national territories today in general only one kind of money is universally accepted. But whether this is desirable, or whether people could not, if they understood the

---

[63] HAYEK, *supra* note 57, at 33-34.
[64] *Id*. at 30.
[65] *Id*. at 32.
[66] *Id*. at 30.
[67] *Id*. at 37.

advantage, get a much better kind of money . . . is an open question."[68]

Hayek would propagate this "much better kind of money" by privatizing currency. The engine of this privatization would be "a number of institutions in various parts of the world which are free to issue notes in competition and similarly to carry cheque accounts in their individual denominations. I shall call these institutions simply 'banks,' or 'issue banks'. . . ."[69] These private banks serve as third-party aggregators and holders of individual consumers' capital. These banks also self-regulate the value of their private currencies, by, among other things, greater transparency and accountability through "alter[ing] the composition of the commodity standard as experience and the revealed preferences of the public suggested," and "announc[ing] precisely the collection of commodities in terms of which it would aim to keep the value of the [currency] constant."[70] The force of competition within the private marketplace provides the necessary incentive for such self-regulation: in order to attract demand for their services, these banks must preserve the purchasing power of their currencies; those that succeed engender public trust in private systems, retaining and further growing their customer base.[71] It is this competition mechanism that can address problems apparent in existing, dissimilarly unaccountable, monopolistic state-run regimes and can best safeguard the integrity of currencies. Concludes Hayek, "It would seem that in this situation sheer desire for gain would produce a better money than government has ever produced,"[72] a ringing endorsement for a currency regime formed under semi-strong decentralization.

---

[68] *Id*. at 38.
[69] *Id*. at 46.
[70] *Id*. at 46-48.
[71] *Id*. at 52.
[72] HAYEK, *supra* note 57, at 51.

The ideological impetuses behind Bitcoin, however, extend beyond Hayek's concerns about failures in government monetary policy. Even the introduction of third-party, non-state service providers will require Bitcoin users to sacrifice Nakamoto's original aspirations of complete anonymity and privacy of transacting. With Bitcoin debit cards for example, the consumer necessarily ties her identity to her Bitcoin card account, for the expediency of being able to swipe and pay merchants at points of sale.[73] At the end of the day, between competing goals of strong decentralization, privacy, and widespread adoption, something will have to give.

V. THE INEVITABLE CENTRALIZATION OF BITCOIN

In practice, the Bitcoin community appears to have in fact sacrificed both strong decentralization and privacy in favor of the goal of widespread adoption. Bitcoin has greatly depended on all types of third-party service providers in its growth process, including the infamous Mt. Gox exchange, to both success and great peril. When successful, the persistent reliance on third parties challenges the practical wisdom of the ideologues' insistence on a purely peer-to-peer system; but when third parties cause trouble, these ideologues' precise fears of concentrated authority are validated. Nonetheless, it is difficult to deny that Bitcoin's rise has depended on a whole host of these third parties—from currency exchanges, to digital wallets, to partnerships with conventional banking institutions, and even government entities, as both regulators *and* protectors.

The inherent technological complexity of Bitcoin explains in part why ordinary community participants have come to sacrifice the

---

[73] Joel Valenzuela, *8 Major Bitcoin Debit Cards: How Private and Anonymous Are They?*, THE COINTELEGRAPH (Aug. 20, 2016), https://cointelegraph.com/news/8-major-bitcoin-debit-cards-how-private-and-anonymous-are-they.

pure decentralization principle in favor of reliance on third-party providers. Regardless of how much faith Bitcoin users had in the open-source protocol, if they did not have faith in their own abilities to deal with the abstruse code, or to otherwise digitally hold their bitcoins securely, the alternative would be to outsource those responsibilities to an exchange account or a digital wallet. Even though an academic study found that as of early 2013, forty-five percent of Bitcoin exchanges had failed (taking their customers' money with them),[74] both unsophisticated Bitcoin buyers and savvy investors alike (such as Roger Ver, nicknamed the "Bitcoin Jesus"),[75] persist in handing their digital assets over to exchanges and online wallets for management purposes.[76] The desire for maintaining total personal control over their own money is, perhaps, not as strong for much of the Bitcoin community as it was for original ideologue Satoshi Nakamoto. Other developers more faithful to Nakamoto have actually turned their efforts to new cryptocurrency pursuits, like Darkcoin and Zerocoin, "starting with privacy as a first principle," and cutting out the middleman.[77] Meanwhile, Bitcoin continues its quest for mainstream adoption by embracing centralization mechanisms.

---

[74] Ian Steadman, *Study: 45 Percent of Bitcoin Exchanges End Up Closing*, ARS TECHNICA (Apr. 27, 2013, 9:23 AM), http://arstechnica.com/business/2013/04/study-45-percent-of-bitcoin-exchanges-end-up-closing/.

[75] Ansuya Harjani, *Meet "Bitcoin Jesus," a Virtual Currency Millionaire*, CNBC (Dec. 2, 2013, 5:28 PM), http://www.cnbc.com/2013/12/02/meet-bitcoin-jesus-a-virtual-currency-millionaire.html.

[76] POPPER, *supra* note 6, at 113.

[77] Andy Greenberg, *5 Bitcoin Projects That Could Make Payments Far More Anonymous*, WIRED (May 5 2014, 6:30 AM), http://www.wired.com/2014/05/bitcoin-anonymous-projects/.

A. MT. GOX BITCOIN EXCHANGE

Mt. Gox represents one of the most notorious players in the early history of Bitcoin. Detractors cite its failure as evidence that Bitcoin ought to remain independent from third-party players.[78] Other convenience-minded advocates portray Mt. Gox as an exception, a lesson for existing and future third-party service providers in how *not* to conduct themselves, while properly serving and enhancing the Bitcoin community.[79]

The Mt. Gox exchange launched in 2010, when a sudden increase in demand for bitcoins, following some favorable online press, highlighted a void within the existing system.[80] By design, mining by computing was the only way to initially acquire bitcoins, but plenty who lacked the hardware and the technological wherewithal to perform the mining now wanted to join the Bitcoin community as well. These consumers were certainly welcome, in theory—for Bitcoin to establish itself as a currency, it needed to be in as many different digital wallets as possible. As another byproduct of the publicity, more miners tapped into the network itself—and the Bitcoin algorithm responded, by design, by making it more difficult to solve future hash functions, thereby ensuring the rate of bitcoins released into the world stayed roughly constant, regardless of rate of mining activity.[81] With this growth in demand on two fronts, the only real way for most people to acquire bitcoins was to buy them.

However, before Mt. Gox, there was no open marketplace for buyers and sellers to connect with one another. Jed McCaleb, a

---

[78] POPPER, *supra* note 6, at 317.
[79] Sam Byford, *Mt. Gox Disappears as Bitcoin Community Goes into Damage Control Mode*, THE VERGE (Feb. 25, 2014, 12:50 AM), http://www.theerge.com/2014/2/25/5444866/mt-gox-goes-offline.
[80] POPPER, *supra* note 6, at 83.
[81] *How Bitcoin Mining Works*, COINDESK (Dec. 22, 2014), http://www.coindesk.com/information/how-bitcoin-mining-works/.

technology entrepreneur and early Bitcoin advocate, encountered this problem precisely—he was enamored with the ideas and concepts behind Bitcoin, but found he was unable to buy any during the nighttime.[82] He then set out to provide a platform allowing the community to buy and sell bitcoins at any time of day, resulting in the Mt. Gox Bitcoin exchange.[83] Mt. Gox functioned much like a traditional brokerage account—customers held both their dollars and bitcoins in Jed's PayPal account, and they could trade the currencies in both directions.

By offering the right service at the right time, Mt. Gox obtained the first-mover advantage in the Bitcoin exchange world. By McCaleb's own account, Mt. Gox beat out other nascent alternatives because of the confluence of convenience factors offered—"[i]t is always online, automated, the site is faster and on dedicated hosting, and . . . the interface is nicer."[84] What Mt. Gox offered in terms of convenience, however, came at the expense of undermining some of Bitcoin's fundamental ideologies. Nakamoto's "White Paper" called for his digital currency to eliminate "trusted third parties"—not to mention third parties that did not even have adequate security measures in place.[85] When McCaleb's original iteration of Mt. Gox launched, it lacked deposit insurance; while it aggregated its customers' private keys, it had no recovery protocol, in the event Mt. Gox happened to lose those keys (in which case, customers would lose access to their coins stored in Jed's account); and, of course, there were no regulators to force or suggest these measures upon or to Mt. Gox.[86]

---

[82] POPPER, *supra* note 6, at 51.
[83] *Id*.
[84] *Id*. at 53.
[85] Nakamoto, *supra* note 8, at 1.
[86] POPPER, *supra* note 6, at 52.

Eventually, Mt. Gox did suffer its first substantial security breach. A rogue user hacked into the accounts and stole around $45,000 worth of bitcoins, which McCaleb was fortunately able to recover when the hacker later deposited that sum back into Mt. Gox to buy more bitcoins (perhaps this return to the scene of the crime is evidence of how dominant Mt. Gox had become in the Bitcoin exchange business).[87] This incident, however, led McCaleb to realize he was in over his head with the exchange, lacking the security expertise requisite for such a position of power, and he sought to transfer management and control to someone else.[88] He eventually landed on an individual named Mark Karpeles, a native-French coder living in Japan, whom McCaleb had met online.[89] Now, the fate of Mt. Gox customers' Bitcoin investment rested in the capabilities of Karpeles—maintaining the violation of the Bitcoin principle of decentralization.

Unfortunately for Mt. Gox, Karpeles turned out not to be an adequately trustworthy third-party operator. Under his management, the leading Bitcoin exchange eventually filed for bankruptcy, threatening to set back what progress the digital currency had made.[90] The Mt. Gox disaster highlighted precisely the dangers of concentrating powers in the hands of one market player not otherwise subject to regulations, and there were red flags surrounding Karpeles' inadequacies as manager. In one instance, Karpeles chose to implement significant coding changes that impacted how his customers transferred their monies, without fully briefing those customers.[91] This lack of transparency, coupled with

---

[87] *Id*. at 67.
[88] *Id*.
[89] *Id*. at 67-68.
[90] Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014, 6:30 AM), https://www.wired.com/2014/03/bitcoin-exchange/.
[91] POPPER, *supra* note 6, at 205-06.

the trading lags the exchange suffered due to heavy traffic, impacted the Bitcoin market enough to cause about a $100 fluctuation in the price for bitcoins.[92]

In another instance, Karpeles had entered into an agreement with a separate entity that had an American bank account, in order to more easily serve Mt. Gox's American customers (since Karpeles operated out of Japan using Japanese bank accounts, he faced strict limits on the number of overseas wires he could perform daily).[93] However, when it actually came time to turn over the American customer files, Karpeles suffered from cold feet. Karpeles notoriously took days, or even weeks, to respond to customer inquiries.[94] In spite of these troublesome signs, customers managed to stay with Mt. Gox, which maintained its market lead purely due to the inertia of its first-mover advantage.

Eventually, the illiquidity of Mt. Gox's Japanese bank accounts resulted in bitcoins costing nearly $100 more than on other exchanges.[95] But this problem paled in comparison to the increasing number of complaints from customers who reported never receiving any coins at all, despite placing withdrawal requests.[96] Karpeles' initial response to the community did not assuage their concerns about either their assets or Karpeles' leadership—in a public statement, he chose to blame a fundamental flaw in the Bitcoin protocol, which could allow rogue users to alter transactions codes to request the same withdrawal multiple times.[97] While this flaw did exist, it seemed that other major Bitcoin companies had previously

---

[92] *Id*. at 204-06.
[93] *Id*. at 200.
[94] *Id*. at 201.
[95] *Id*. at 307.
[96] *Id*. at 308.
[97] *Id*. at 309.

identified the issue and were able to design around it entirely.[98] As Karpeles continued attempting to root out the withdrawals problem, Mt. Gox remained closed, and customers continued to be frozen out from their accounts.

What came to light eventually was that a hacker had in fact stolen from Mt. Gox's "hot," or online wallet by exploiting the multiple-withdrawals flaw that Karpeles had failed to preempt; and each time this hot wallet became empty, Mt. Gox refilled it with bitcoins from its customers' "cold," or offline wallets.[99] At one point, Karpeles drove across Tokyo, collecting from three storage sites individual pieces of paper on which he had recorded his customers' private keys (to keep them from the hands of hackers). Karpeles scanned them one at a time—and each indeed came up empty.[100]

Mt. Gox's loss this time—of nearly 800,000 bitcoins, or $460,000,000—was not reversible.[101] Failing to find viable investors to bail out the exchange,[102] it was forced to file for bankruptcy. Despite significant losses to some customers (including up to $12,000,000 in one reported instance), observers and many of the victims themselves tended to blame Mt. Gox, rather than the Bitcoin protocol itself.[103] From this perspective, in which "[t]he Mt Gox

---

[98] *Id*.

[99] *MtGox Situation: Crisis Strategy Draft*, SCRIBD, http://www.scribd.com/doc/209050732/MtGox-Situation-Crisis-Strategy-Draft (last visited Jan. 27, 2017).

[100] POPPER, *supra* note 6, at 311.

[101] McMillan, *supra* note 90.

[102] A Mt. Gox deputy reached out to the Winklevoss twins (famous previously for their litigation against Mark Zuckerberg over Facebook, now actively pursuing investment opportunities in Bitcoin) for a lifeline, but they declined. POPPER, *supra* note 6, at 312.

[103] Russell Brandom, *Mt. Gox was Bitcoin's Ugliest Success Story*, THE VERGE (Aug. 3, 2015, 1:20 PM), http://www.theverge.com/2015/8/3/9090191/mtgox-mark-karpeles-bitcoin-arrested-cryptocurrency.

Bitcoin scandal is the best thing to happen to Bitcoin in years,"[104] Mt. Gox and Karpeles' incompetency had been a liability to Bitcoin's legitimacy for too long, and it took nothing short of a $460,000,000 bankruptcy action to wipe out its scourge and finally get customers onto a more reliable third-party exchange. The centralization optimist's take on the fiasco is that Bitcoin's partnership or reliance on third parties need not inevitably go the way of Mt. Gox, if *better* third parties can take its place.

B. COINBASE DIGITAL WALLET AND EXCHANGE

Coinbase began in 2012 as an online wallet for Bitcoin storage and transactions. Third-party digital wallets appealed to Bitcoin customers who did not trust themselves to manage their own Bitcoin holdings—if they lost their private keys, access to any coins associated with those keys disappeared as well, with no recourse until those keys were recovered. One early Bitcoin investor, Wences Casares, presciently suspicious enough of Mt. Gox to avoid it entirely, therefore had to manage his own private keys. Realizing that storing them on his computer, phone, or any device attached to a network left those keys vulnerable to hackers, Casares brought together a small group of other Bitcoin holders, put their private keys on a laptop, and purchased a safe-deposit box in which they stored the offline computer.[105] It is unsurprising that a more casual Bitcoin consumer would be unwilling to go to such lengths to participate in the system.

Coinbase offers customers a more forgiving place to store their digital cash. Signing up for a Coinbase wallet gives the customer a

---

[104] Heidi Moore, *The Mt Gox Bitcoin Scandal is the Best Thing to Happen to Bitcoin in Years*, THE GUARDIAN (Feb. 26, 2014, 5:29 PM), http://www.theguardian.com/money/us-money-blog/2014/feb/25/bitcoin-mt-gox-scandal-reputation-crime.
[105] POPPER, *supra* note 6, at 201.

password, which is recoverable, like the password to other websites.[106] An added attraction of Coinbase is that it allows more laypersons access to the Bitcoin network as well—Coinbase customers can tap into the Bitcoin community without having to download the complicated Bitcoin software and the whole public block chain, further expanding the Bitcoin audience.[107] Of course, connecting private keys to a central management database like Coinbase squarely violated both of Bitcoin's original decentralization and anonymity ambitions:

> Consider CoinBase's internal policies—they resemble PayPal's, not the distributed utopia Bitcoiners imagine. Coinbase wants to know who you are. They want to know what you're doing with your money, and they'll block you if they disapprove. They spy on you and control you as much as any traditional financial institution (and to be fair, it's not really their fault—enforcers with guns will throw them in a cage if they don't do these things; it occurs under duress).[108]

Nonetheless, enough customers were happy to delegate storage responsibilities to this private company that in 2013, it garnered more than $5,000,000 in venture capital funding, the largest investment in a Bitcoin company up to that point.[109] A year later, Coinbase secured

---

[106] *Sign Up*, COINBASE, https://www.coinbase.com/signup (last visited Jan. 27, 2017).
[107] *How to Buy Bitcoin*, COINBASE, https://www.coinbase.com/buy-bitcoin?locale=en (last visited Feb. 8, 2017).
[108] Erik Voorhees, *Is Bitcoin Truly Decentralized? Yes – and Here Is Why It's Important*, BITCOIN MAG. (Jan. 22, 2015, 5:52 PM), https://bitcoinmagazine.com/articles/bitcoin-truly-decentralized-yes-important-1421967133.
[109] Sarah E. Needleman, *Coinbase Nabs $5M in Biggest Funding for Bitcoin Startup*, WALL ST. J.: VENTURE CAPITAL DISPATCH (May 7, 2013, 5:40 PM), http://blogs.wsj.com/venturecapital/2013/05/07/coinbase-nabs-5m-in-biggest-funding-for-bitcoin-startup/.

$25,000,000 from power-player investor Marc Andreessen and currently services 14,900,000 wallets around the world.[110]

By 2015, Coinbase had also expanded its services to include operation of the first "regulated" Bitcoin exchange, which boasts backing by the New York Stock Exchange.[111] Some, however, disputed the company's use of the term "regulated," noting, for example, that it did not actually have a license to operate as a Bitcoin exchange in New York.[112] New York's Department of Financial Services stated at that time that they were "working with several companies, including Coinbase, on licensing and will continue to move forward expeditiously."[113] It was not until January 2017 that Coinbase received its virtual currency license from the Department of Financial Services.[114] According to its press release, "DFS has conducted a comprehensive review of Coinbase's applications, including the company's anti-money laundering, capitalization, consumer protection, and cyber security policies. Coinbase, which is subject to ongoing supervision by DFS, offers services for buying, selling, sending, receiving, and storing bitcoin."[115] While some may parse the semantics of "regulation," even these efforts to bring watchdogs into the fold represent a vast departure from Mt. Gox's

---

[110] Alex Williams, *Coinbase Raises $25M Led by Andreessen Horowitz to Build its Bitcoin Wallet and Merchant Services*, TECHCRUNCH (Dec. 12, 2013), http://techcrunch.com/2013/12/12/coinbase-raises-25m-from-andreessen-horowitz-to-build-its-bitcoin-wallet-and-merchant-services/; *About Coinbase*, COINBASE, https://www.coinbase.com/about?locale=en-US (last visited Apr. 18, 2017).

[111] Daniel Roberts, *Yes, Regulation is Coming to Bitcoin*, FORTUNE (Mar. 24, 2015), http://fortune.com/2015/03/24/bitcoin-regulated-exchanges-winklevoss-coinbase/.

[112] Nathaniel Popper, *Coinbase, a Bitcoin Exchange, is Operating Without Licenses So Far*, N.Y. TIMES: DEALBOOK (Jan. 28, 2015, 10:15 AM), http://dealbook.nytimes.com/2015/01/28/coinbase-a-bitcoin-exchange-is-operating-without-licenses-so-far/.

[113] *Id.*

[114] *DFS Grants Virtual Currency License to Coinbase, INC.*, DEP'T OF FIN. SERVS. (Jan. 17, 2017), http://www.dfs.ny.gov/about/press/pr1701172.htm.

[115] *Id.*

failed modus operandi—that of dominating the Bitcoin exchange market while beholden only to Karpeles' own whimsical rules.

C. VISA SHIFT CARD

Until the Visa Shift Card, the Bitcoin community was mostly limited to spending its coins at businesses that affirmatively accept Bitcoin (which, while growing in number and including some major businesses, is still a fairly limited pool).[116] Shift Payments is a company whose aim is "to make it as easy to spend digital currencies, cryptocurrencies and loyalty points as it is to spend regular, fiat money."[117] By partnering with Coinbase, Shift Payments allows customers to connect their Coinbase wallets to a physical card, like a conventional debit card, and spend their bitcoins at any online or offline merchant that accepts VISA.[118]

In keeping with Coinbase's cautionary approach to regulation, the company "has shunned the shortcuts that have caused trouble for other services in the past."[119] Coinbase is careful to precede the Shift Card's rollout in each state by notifying the respective governments and ideally also obtaining licenses (so far, it has notified twenty-five states).[120] In addition, Coinbase requires Shift Card customers to verify their identities and pay a $10 insurance fee.[121] As the Shift Card

---

[116] *See* Ian Kar, *What Companies Accept Bitcoin?*, NASDAQ (Feb. 4, 2014, 10:05 AM), http://www.nasdaq.com/article/what-companies-accept-bitcoin-cm323438; Jonas Chokun, *Who Accepts Bitcoins As Payment? List of Companies, Stores, Shops*, 99 BITCOINS (Nov. 21, 2016), https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/.

[117] *Shift Payments*, CRUNCHBASE, https://www.crunchbase.com/organization/shift-payments#/entity (last visited Jan/ 27, 2017).

[118] Which, unsurprisingly, greatly expands the number of merchants available to Bitcoin users—VISA is, after all, everywhere you want to be. *See* Metz, *supra* note 48.

[119] *Id*.

[120] *Id*.

[121] *The Shift Card*, COINBASE (Jul. 8, 2016), https://support.coinbase.com/customer/portal/articles/2228646.

gets off the ground, domestic customers do not face transactions fees, but Coinbase has qualified that the luxury may exist only "for a limited time."[122] While some herald the Shift Card as the solution to one of Bitcoin's greatest obstacles to widespread adoption, by "cut[ting] merchant adoption from the technology,"[123] it brazenly transforms Bitcoin several shades closer to the very conventional banking and credit card companies—laden with paperwork, divulgence of personal information, and fees—that the digital currency initially aspired to extinguish.

D. BITCOIN'S RELIANCE ON CONVENTIONAL BANKS

Despite Bitcoin's ambitions as a "disruptive" technology,[124] it had to work *with* conventional banks before it could gain enough traction to disrupt them. In launching a virtual currency, or a company servicing virtual currency users, entrepreneurs have to first deal in dollars and cents, with established institutions like JPMorgan and Silicon Valley Banks, before their virtual currency infiltrates enough of the economy to stand on its own.[125] Inevitably, "[t]he ability of companies to get bank accounts is necessary so that they can take the next step in building out the core Bitcoin infrastructure."[126] The catch-22, however, is that these conventional institutions are wary of dealing with Bitcoin companies until the

---

[122] Romain Dillet, *Coinbase Partners with Shift Payments to Issue Bitcoin Card*, TECHCRUNCH (Nov. 20, 2015), http://techcrunch.com/2015/11/20/coinbase-partners-with-shift-payments-to-issue-bitcoin-debit-card/#.s5ahlyf:MZmx.
[123] Metz, *supra* note 48.
[124] Everett Rosenfeld, *Forget Currency, Bitcoin's Tech is the Revolution*, CNBC (Nov. 13, 2014, 10:22 AM), http://www.cnbc.com/2014/11/13/forget-currency-bitcoin-tech-could-disrupt-massively.html.
[125] Robin Sidel, *Banks Mostly Avoid Providing Bitcoin Services*, WALL ST. J. (Dec. 22, 2013, 4:32 PM), http://www.wsj.com/articles/SB10001424052702304202204579252850121034702.
[126] *Id*.

digital currency becomes more established, or until its legal status is clarified by the proper regulatory authorities. "This was like an anarchist commune that ran up against the unwillingness of local officials to continue delivering water and electricity. Such collisions with the recalcitrant real world are frequently where utopian schemes run into trouble."[127]

In 2013, following a Senate hearing on the digital currency, dubbed a "Bitcoin lovefest" by the *Washington Post*, such real world banks exhibited promising openness to Bitcoin.[128] This open-mindedness began to fizzle by 2014, however, with the collapse of Mt. Gox and the arrests of individuals linked to Silk Road, the underground online marketplace for illegal goods.[129] Aside from any reputational concerns attached to dealing in bitcoin, these banks were bound by their own strict set of regulations against money laundering. Unfortunately for Bitcoin, its built-in transaction-anonymity prevented existing banks from acquiring the records of accounts and transactions necessary to ensure they were not somehow involved in channeling funds to terrorists or organized criminals.

The stigma was so great that "some owners of fledgling virtual-currency businesses [were] trying to elude bank scrutiny by avoiding the words 'bitcoin' or 'bit' in their names."[130] Coinbase faced this problem acutely. It originally partnered with Silicon Valley Bank, one of the few willing to work with Bitcoin companies at all.[131] The bank

---

[127] POPPER, *supra* note 6, at 204.
[128] Timothy B. Lee, *This Senate Hearing is a Bitcoin Lovefest*, WASH. POST (Nov. 18, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/11/18/this-senate-hearing-is-a-bitcoin-lovefest/.
[129] Alec Liu, *"It's Hard to Put the Genie Back in the Bottle": Bitcoin's Top Cop Opens Up*, VICE: MOTHERBOARD (Feb. 21, 2014, 4:20 PM), https://motherboard.vice.com/en_us/article/the-best-of-bitcoin-regulator-ben-lawskys-reddit-ama.
[130] Sidel, *supra* note 125.
[131] POPPER, *supra* note 6, at 306.

still insisted on reviewing each Coinbase transaction that it facilitated. Even with Coinbase's heightened protocols in place for identifying their customers, these reviews cost Silicon Valley Bank more than Coinbase was generating in business; frequently, Coinbase ran into transactions limits imposed by Silicon Valley Bank and was forced to halt operations until the following day.[132] For Jamie Dimon, chief executive officer of JPMorgan Chase, Bitcoin could never simultaneously preserve its integrity and also succeed as a competing currency.[133] The Federal Reserve Bank of Chicago sees regulation as inevitably following on the heels of adoption: "Should [B]itcoin become widely accepted, it is unlikely that it will remain free of government intervention, if only because the governance of the [B]itcoin code and network is opaque and vulnerable."[134] Following this trajectory, Bitcoin would inevitably be subject to the same money laundering and compliance regulations as conventional banks, at which point, predicts Dimon, "[t]hat will probably be the end of them."[135]

Wences Casares, another Bitcoin advocate, technology entrepreneur (and owner of the offline laptop in a safe-deposit box), regularly turned to JPMorgan Chase for his previous startups.[136] When he launched his latest Bitcoin wallet company, Xapo, he once again turned to JPMorgan for a corporate account. This time, however, he was rejected, and rejected subsequently by another

---

[132] *Id*. at 203-04.
[133] Stephen Gandel, *Jamie Dimon: Virtual Currency Will be Stopped*, FORTUNE (Nov. 4, 2015), http://fortune.com/2015/11/04/jamie-dimon-virtual-currency-bitcoin/.
[134] François Velde, *Bitcoin: A Primer*, 317 CHI. FED LETTER (Dec. 2013), https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317 (follow "Download Entire Publication Link" to download document).
[135] Matthew J. Belvedere, *Lew: Dimon and I Share "Incredulity" on Bitcoin*, CNBC (Jan. 23, 2014, 8:03 AM), http://www.cnbc.com/2014/01/23/congress-needs-to-act-on-debt-ceiling-as-soon-as-possible-treasury-secretary-lew.html.
[136] POPPER, *supra* note 6, at 305.

bank, just as he received a $10,000,000 venture capital investment.[137] Casares eventually landed with Silicon Valley Bank as well, which seemed to be the only bank willing to partner with Bitcoin businesses at that point. Casares later brushed off his experience with JPMorgan and CEO Jamie Dimon by remarking, "I think whatever Jamie does or doesn't do will be as relevant as what the postmaster general did or didn't do about e-mail."[138]

E. GOVERNMENTS AS REGULATORS—AND PROTECTORS

Governments have the power to impact the price of bitcoin with simple statements and policy guidances, however speculative. Following the aforementioned favorable 2013 Senate hearing on Bitcoin, the price of bitcoin trading on Mt. Gox soared to over $900, from about $200 in the previous month.[139] Meanwhile, in China, the "force behind fluctuations in the global Bitcoin market in 2013,"[140] investors were anxiously awaiting their central bank's virtual currency regulations. While the People's Bank ultimately did not hold Bitcoin out to be per se illegal and did not call for the virtual-currency exchanges to outright close, it did classify Bitcoin as a digital commodity and required exchanges to register with the Ministry of Information.[141] The consequence of this official classification was to prohibit Chinese banks and payment processors from directly or indirectly dealing in bitcoin. In response to this (at-

---

[137] *Id*. at 305-06.
[138] *Id*. at 306.
[139] *"Legitimate" Bitcoin's Value Soars After Senate Hearing*, BBC (Nov.19, 2013), http://www.bbc.com/news/technology-24986264.
[140] Lauren Gouldeman, *Bitcoin's Uncertain Future in China*, USCC ECON. ISSUE BRIEF NO. 4, at 4 (May 12, 2014), https://www.uscc.gov/Research/bitcoins-uncertain-future-china (follow "USCC Economic Issue Brief - Bitcoin - 05 12 14.pdf" hyperlink).
[141] Gerry Mullany, *China Restricts Banks' Use of Bitcoin*, N.Y. TIMES (Dec. 5, 2013), http://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html.

best) lukewarm position, the price of bitcoin immediately plummeted nearly forty percent in Chinese markets.[142]

In the United States, a clear, coherent government position on Bitcoin has yet to emerge. Various regulatory agencies are only beginning to issue guidances, but optimism remains that Bitcoin is not flatly illegal. In 2013, the U.S. Treasury classified Bitcoin as a "convertible" and "decentralized" virtual currency.[143] The Federal Election Commission, in weighing in on whether political committees can accept donations in bitcoin, issued an advisory opinion setting forth many contingencies surrounding its allowing committees to accept up to $100 worth of bitcoin per election—but stopped short of classifying Bitcoin as a currency, instead slotting it into the "anything of value" category.[144] The Internal Revenue Service issued guidance indicating it considers virtual currency to be "property" for federal taxation purposes, and those who "mine" bitcoin as a trade or business are subject to self-employment tax.[145] As recently as September of 2015, the Commodity Futures Trading Commission took its first action against an unregistered Bitcoin options trading platform, with the agency exerting its authority over

---

[142] *See* Neil Gough, *Bitcoin Value Sinks After Chinese Exchange Move*, N.Y. TIMES, (Dec. 18, 2013), http://www.nytimes.com/2013/12/19/business/international/china-bitcoin-exchange-ends-renminbi-deposits.html?_r=0; Vitalik Buterin, *China Releases First Regulatory Report on Bitcoin Businesses*, BITCOIN MAG. (Dec. 5, 2013, 5:53 PM), https://bitcoinmagazine.com/articles/china-releases-first-regulatory-report-on-bitcoin-businesses-1386283989.

[143] *Statement of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network*, FIN. CRIMES ENF'T NETWORK (Nov. 19, 2013), https://www.fincen.gov/sites/default/files/2016-08/20131119.pdf.

[144] Memorandum from Lisa J. Stevenson et al., Deputy General Counsel, Fed. Election Comm'n, 5 (May 7, 2014), *available at* http://saos.fec.gov/aodocs/201402_2.pdf; Dave Levinthal, *What the FEC's Bitcoin Ruling Means*, THE CTR, FOR PUB. INTEGRITY, (May 8, 2014), http://www.publicintegrity.org/2014/05/08/14739/what-fecs-bitcoin-ruling-means.

[145] INTERNAL REVENUE SERV., NOTICE 2014-21, at 2, 4 (2014), https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

virtual currencies as commodities covered by the Commodity Exchange Act.[146]

Perhaps surprisingly, some within the Bitcoin community have been enthusiastic about more regulators jumping into the fray—or, at least, they found a silver lining to such regulation. To these sanguine advocates, regulation is a tacit signal of much-needed legitimacy. When the Financial Crimes Enforcement Network (FinCen) division of the U.S. Treasury issued effectively the first government statement on Bitcoin's legality (subjecting anyone selling virtual currency for "real currency or its equivalent" to federal rules),[147] chatter on online Bitcoin forums quickly addressed anti-statist naysayers by retorting that "this solidifies Bitcoin [sic] status as legal to possess and use for normal people," and furthermore, that "[m]ore legal/regulatory certainty is definitely a good thing . . . even if we might not like the regulations." [148] Indeed, the market responded positively to the FinCen statement, as Bitcoin prices rallied in the days immediately following the statement.[149]

Once again, "[t]he great irony of excitement over regulation is that many of Bitcoin's biggest supporters got involved with Bitcoin specifically because of its lack of regulation." [150] These differing positions on regulation certainly highlight the cleavage between two camps within the Bitcoin community, though at this juncture

---

[146] Press Release, U.S. Commodity Futures Trading Comm'n, CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering (Sept. 17, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7231-15.

[147] Fin. Crimes Enf't Network, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013), https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

[148] POPPER, *supra* note 6, at 196-97.

[149] Alec Liu, *Why Bitcoin's Price is Skyrocketing*, VICE: MOTHERBOARD (Apr. 4, 2013, 2:00 PM), http://motherboard.vice.com/blog/why-bitcoins-price-is-skyrocketing.

[150] Roberts, *supra* note 111.

perhaps to an even greater degree, as embracing government involvement casts aside not just strong decentralization, but even semi-strong decentralization. But, just as the human limitations of the lay Bitcoin user explain why so many have been eager to entrust their holdings to third-party exchanges and wallets, the same limitations may explain why financial institutions are naturally subject to regulatory oversight. Financial services customers similarly lack the expertise or resources to police these institutions themselves, and instead turn to agencies like the Federal Deposit Insurance Corporation to perform those functions and protect customers against losses.[151] Furthermore, market mechanisms may simply be insufficient as a form of redress or deterrence, in contexts where real investments with large values are at stake:

> Many libertarians and anarchists argued that the good in humans, or in the market, could do the job of regulators, ensuring that bad companies did not survive. But the Bitcoin experience suggested that the penalties meted out by the market are often imposed only after the bad deeds were done and do not serve as a deterrent. When it came down to it, in each case of big theft, Bitcoin users eventually went to government authorities to seek redress—the same authorities that Bitcoin had been designed, at least partly, to obviate. Mark Karpeles reported the Mt. Gox hack to the Japanese police and MyBitcoin users went to the FBI's cybercrime unit.[152]

---

[151] E.g., John R. Walter, Depression-Era Bank Failures: The Great Contagion or the Great Shakeout?, 91 FRB RICHMOND ECON. Q. 39 (2005).
[152] POPPER, *supra* note 6, at 114.

VI. COERCIVE CENTRALIZATION VS. MARKET-BASED CENTRALIZATION

It may be difficult for Bitcoin advocates who embrace government regulators to square such approval with the movement's founding principles of strong decentralization. For others who fall in the middle and tolerate semi-strong decentralization, acknowledging the values added by well-run third-party exchanges, wallets, and card services like Coinbase, Xapo, and the Shift Card *can* be reconciled with Bitcoin's ideological origins. Erik Voorhees, Bitcoin entrepreneur and outspoken anti-government activist, makes the case that the community's reliance on private third parties does not undermine the digital currency's claim of decentralization in any meaningful way. Voorhees draws a material distinction between "coercive centralization" and "market-based centralization." On the one hand,

> Coercive centralization is what we all experience in the legacy financial industry. The world's monetary system, based upon national fiat currencies created and managed by government-sponsored central banks, is coercive. It is coercive because the entities with the power over money's creation, regulation, and transfer have the will and the power to hurt you if you disobey. Not only that, but you are coerced into it in the first place, being forced to pay taxes and settle debts using only your government's anointed currency.

On the other hand,

> Market-based centralization is fundamentally different. Its key feature is the ability to opt out. Yes, Coinbase is a centralized entity. But you needn't use Coinbase to use Bitcoin. Yes, a Bitcoin exchange or web wallet is centralized, but you can always trade coins with a friend directly over

> the blockchain, or store it in a local wallet, without the permission of any third party.[153]

For discerning Bitcoin enthusiasts, then, the system's natural tendency away from strongly decentralized orders and toward at least semi-strong decentralization is no credible betrayal of their principles (and, again, finds support in Hayek's own conception of currency decentralization). It remains to be seen how the frontier between private third parties and government authorities will be negotiated, as the former continue to innovate and expand and the latter ramp up regulatory efforts in kind.

CONCLUSION

For nearly a decade now, Bitcoin has piqued the interest of libertarians, privacy advocates, technologists, the financial industry, and government regulators around the globe. Its novelty as a form of alternative currency comes from its unique triad of traits: Bitcoin was designed to be entirely decentralized, practically anonymous, and inherently valueless. Interestingly, these precise characteristics have proven self-contradictory and stand to impede Bitcoin's widespread adoption unless some of these founding ideologies are compromised along the way.

Randy Barnett's framework for understanding the mechanism of decentralized orders demonstrates why Bitcoin is fundamentally ill-suited to founder Satoshi Nakamoto's dream of strong decentralization. Because Bitcoin has no inherent use-value, it lacks the capacity to organically emerge as a stable currency that measures the prices of other goods on the market. Bitcoin is distinguishable from modern-day fiat currencies, like the dollar, all of which stabilized under the same process: they were first pegged to

---

[153] Vorhees, *supra* note 108.

inherently useful commodities (such as gold or silver), and later transitioned to the security of government custodianship. Eschewing any such reliance on central planners or other third party intermediaries, Nakamoto's radical Bitcoin ideal cannot overcome Barnett's First Order Knowledge Problem and remains trapped in a cycle of commodity fetishization, unable to evolve from commodity to stable currency.

Bitcoin's reality, however, has strayed from its founding principle of strong decentralization. In fact, a whole industry of third parties and middlemen have sprouted up around the storage, transfer, and use of bitcoin. From Bitcoin wallets and cards (such as Coinbase and the VISA Shift Card) to Bitcoin exchanges (including the legendary failed Mt. Gox), these services facilitate broader acquisition and use of bitcoins for the community's more casual participants, who otherwise lack the infrastructure and know-how required to directly mine for and store bitcoin. These service providers, however, contaminate the pure peer-to-peer dream and can preclude anonymous transacting, as mainstream partners like VISA bring Bitcoin transactions in line with traditional banking practices.

This burgeoning Bitcoin industry represents a compromise philosophy that splits the difference between familiar, government-sponsored currencies and Nakamoto's crypto-anarchism. While dependent on private, third-party coordinators, this middle ground approach can be characterized as market-based centralization, distinguishable from the coercive centralization of governments and regulators. This natural progression toward market-based centralization, in defiance of Bitcoin's founding charter, demonstrates the tensions among the cryptocurrency's unique mix of traits. Bitcoin's immutable characteristic as an inherently valueless, free-floating currency at least requires that its other ideal characteristic, strong decentralization, yield along the way to Bitcoin's widespread adoption and success as a scalable currency.