Bitcoin as Currency and Catalyst

John Merriman Sholar
Stanford University

Abstract
The past five years have seen the rise of the Bitcoin digital currency and, as a result, increased discussion of the idea of a digital currency. This paper seeks to address Bitcoin in several contexts, viewing it as representative of the broader state of the digital currency debate. Through an analysis of several of the most important factors shaping Bitcoin’s existence, this essay develops and defends the assertion that Bitcoin will not achieve widespread adoption in the United States, and in all likelihood will fail to do so throughout the rest of the world as well. In light of this hypothesized downfall, this paper discusses the considerably more viable potential for Bitcoin (and its underlying blockchain technology) to drive innovation in the financial sector and other industries.
Introduction

In October of 2008, Satoshi Nakamoto published a paper titled, “Bitcoin: A Peer-to-Peer Electronic Cash System,” which outlined a plan for a digital cryptocurrency which could exist without the regulation of a central authority. Three months later, he made his vision a reality when he released the Bitcoin source code, which would become the foundation of the Bitcoin network. The first bitcoins were mined and traded shortly thereafter, and over the course of the past six years the currency has expanded rapidly, garnering worldwide attention and debate (Barski, Conrad, & Wilmer, 2015, ch. 1). It’s clear that the currency will have far-reaching implications, but this begs the question: what are they? How does Bitcoin have the potential to change modern perceptions of what defines a currency, and how does the technology behind it have the potential to spark innovation in other fields? How will Bitcoin act as both currency and catalyst in the years to come?

Before we can explore the ramifications of Bitcoin for modern technology and economics, we must establish exactly what Bitcoin is and how it works. Bitcoin (capitalized when referring to the system and with a lowercase “b” when referencing units of the currency itself) is a decentralized digital currency, which means that it does not reside under the control of any governmental entity (Franco, 2014). All of Bitcoin’s regulation occurs in a distributed database called “the blockchain,” which acts as a ledger for every bitcoin transaction that has ever occurred. Every computer in the Bitcoin network maintains its own copy of the blockchain, which is updated every time a new transaction occurs—thus, every user individually verifies the blockchain to maintain its integrity, and the “official” blockchain is one that a majority of users agree upon.

Verification of the blockchain is completed in “blocks” (essentially large chunks of transactional data) and requires large amounts of computational power due to certain imposed constraints. Users are incentivized to complete this task with a bitcoin reward; the first user to verify the current block within these constraints collects a reward of (currently) 25 bitcoins. This reward will continue to halve every 4 years until the total number of bitcoins reaches an arbitrary cap of 21 million, at which point production of the currency ceases entirely. Additionally, the Bitcoin network adjusts the difficulty of verification by modifying a “proof of work” function, such that every block takes roughly 10 minutes to verify. These two regulations ensure that Bitcoin is released (or “mined”) at a continuous but ever-decreasing rate (Franco, 2014, ch. 7). The concept of the blockchain is a well-founded one: every user has an incentive to verify honestly (because the blockchain contains their transactions as well), and verify actively (because this increases their chances of collecting the bitcoin reward). Thus, the processes by which new bitcoins are produced and old bitcoins are tracked become one and the same in the process of mining, which perpetuates the cycle that drives the Bitcoin currency forward.
The relatively complex nature of Bitcoin produces a wide variety of reactions to the digital currency. Some contend that Bitcoin’s lack of regulation renders it wholly impractical, unable to thrive as a currency, and doomed to remain a curiosity of academics, economists, and cryptologists (Henwood, 2014). Others assert that the benefits engendered by this lack of regulation (among other features) outweigh the costs, and that with time, the currency can achieve widespread acceptance (Alstyne, n.d.). Still others say that Bitcoin can succeed, but not in its current form, which raises the question: if Bitcoin must adapt in order to succeed, has it really succeeded at all (Brito, 2014)? Finally, many are more fascinated by the technologies behind Bitcoin than by the currency itself, and hypothesize that while Bitcoin may be a passing trend, technologies such as the blockchain have lasting potential (Bradbury, 2015; Pagliery, n.d.; Howard, n.d.). This essay will explore the dialogue between these sources and others to develop an idea of how Bitcoin is viewed as both a groundbreaking currency and catalyst for technological innovation, as well as the ramifications of each of these two roles.

The assertions of this essay are threefold: firstly, Bitcoin will fail to achieve widespread adoption; secondly, Bitcoin’s eventual failure is irrelevant; lastly, while Bitcoin itself will impact economics and technology in the coming years, by far its most important contributions to these and other fields will come as a result of the technologies and ideas it has introduced. Bitcoin’s legacy will be one not of earthshattering revolution, but rather one of experimental genesis—the first primitive stage in an evolutionary process which will, in time, produce fitter adaptations. This paper will begin with an exploration of the relative merits and weaknesses of Bitcoin, both in theory and in practice, and examine how these competing traits will ultimately render Bitcoin inaccessible to the general public and relegate it to mere academic curiosity. Having examined the factors behind Bitcoin’s eventual downfall, this essay will explore the currency’s potential to act as an impetus for change in other fields (particularly finance and technology), which will persist regardless of Bitcoin’s success or failure and eventually form its legacy.

Bitcoin as Currency
Contention over Bitcoin’s role as a currency is fierce, and exists over even the most basic question: is Bitcoin a currency at all? Classically, economists define money as “a store of value, a unit of account, and a medium of exchange” (Henwood, 2014, p. 13); Bitcoin fails in some way to meet all three of these criteria. In 2013 and 2014, the average one-day change of the value of a bitcoin was 4.3 percent, compared to .3 percent for the US Dollar for the same period (p. 13); this amount of volatility renders the bitcoin impractical as a store of value. On one hand, it’s not unreasonable to believe that greater adoption of Bitcoin would stabilize its price, allowing further adoption and perpetuating a virtuous cycle of stable
growth leading towards what might be called success by our definition. On the other hand, for reasons explained later in this section (including negative public opinion, lack of regulation, and others), it’s unlikely that this critical threshold will be reached to begin with, and thus likely that Bitcoin will remain unstable and unusable for those who cannot afford extreme financial volatility. Furthermore, because a small minority of businesses accept Bitcoin, and because almost none “keep their books in [it],” Bitcoin is not an adequate unit of account or medium of exchange either (p. 13). In “The Bitcoin Fantasy,” economic analyst Doug Henwood takes the perspective of two Goldman Sachs economists cited in his article: “Bitcoin . . . [lies] somewhere on the boundary between currency, commodity, and financial asset that can be used as a medium of exchange” (p. 17). Other sources, even those who are generally supportive of Bitcoin, seem to tacitly acknowledge this by avoiding the issue (Alstyne, n.d.). Ultimately, this argument is nothing more than a debate over semantics, and as such this essay will not take a position on whether or not Bitcoin is a “currency” according to a stringent, classical definition. Such a distinction has little bearing on the real-world impact of Bitcoin and should not exclude it from contemporary economic dialogue. In fact, this unique status only adds to Bitcoin’s value as a point of discussion and debate, with its potential to revitalize conversation with new concepts and alter long-standing economic dogma.

As has been stated, much of the current discussion surrounding Bitcoin centers on whether or not the currency will succeed, and though this issue has been covered from seemingly every perspective, it nonetheless merits discussion here as a crucial component of the currency’s identity. This issue is actually best broken into two questions. The first asks if Bitcoin should succeed. That is, is the currency itself theoretically sound? Will its underlying concepts work in the favor of those who adopt it? The second question asks not if Bitcoin should succeed, but rather if it will succeed. Where the first question is based in opinion and political ideology, the second is based more real-world analysis. Both questions address the idea of Bitcoin’s success, and in order to respond to either of them, some definition of “success” is needed. This is understandably an arbitrary and vague concept, and as such we can choose any definition of “success” which suits our purposes, with the understanding that other discussions may define the term differently. For the purposes of this essay, we will define the “success” of Bitcoin as widespread acceptance, adoption, and use by the general public, noting that this definition does not require that Bitcoin replace preexisting currencies, only that it coexist with them. Finally, we note that success is not a binary quality, but a gradient, and must be treated as such. Our predicted outcome will not be one of simple “success” or “failure,” but rather a qualified, complex position between the two; the nuanced nature of success necessitates a nuanced answer.
Controversy
The debate which rages over if Bitcoin should succeed as a currency is complicated by a vast array of economic and political philosophies (and often biases), all of which play into a given individual’s perspective. Due to the intensely political nature of the debate, the same characteristic of Bitcoin is often used as an argument in favor of two conflicting viewpoints (though contending opinions on the currency are far from binary); two particularly controversial traits are the currency’s anonymity and lack of regulation.

In a post-Snowden era of ever-increasing government surveillance, the ability to make transactions anonymously becomes ever more valuable for those who do not wish to disclose their commercial activities to potential observers. Every Bitcoin transaction ever made is confirmed and noted in the blockchain, but the parties in these transactions are identified only by a public key (a digital ID number)—never by any details that could reveal the person who manages the account. Barring instances in which certain public keys are traced to certain individuals or organizations (a feat which can only be accomplished through careful analysis of transactional data and even then is difficult if not impossible in some cases), users remain essentially anonymous. Bitcoin’s anonymity allows its users to engage in digital commerce without the need for (and free from the restrictions of) a third party, such as PayPal or a credit card company. In “Bitcoin: More than Money,” Jerry Brito cites the refusal of Visa, Paypal, and Mastercard to allow donations to Wikileaks (at the behest of the American government) in 2010 as an example of undesirable “censorship or control” by a third party (par. “Censorship and Resistance”). With Bitcoin, such restrictions no longer apply, and users are free to exchange goods and services as they please, for better and for worse. Unfortunately, included in “for worse” is massive potential for illegal activity, including drug dealing and human trafficking. The most prominent example of such activity is the infamous “Silk Road” website, dubbed “the black market Amazon,” through which users could (prior to its shutdown in November 2014) purchase all manner of illicit goods and services, shielded from the law by the anonymity of Bitcoin (Norrie & Moses, 2011). While the benefits and challenges posed by Bitcoin’s anonymous transactions seem to be new at first glance, a moment of insight reveals them to be reincarnations of problems that are hundreds of years old. Transactions through Bitcoin are anonymous, free from regulation, and preferable as a means of criminal commerce as a result of the first two reasons; taken together, these traits apply to a form of currency already in widespread use around the globe: cash. Bitcoin provides a digital analog to cash, and carries many of the same benefits and problems as a result. For this reason, though many point to Bitcoin’s anonymity as either a problem or a solution (depending on ideology), we cannot consider it to be either in deciding if the currency is economically
sound because these characteristics are not unique to Bitcoin, but rather digital analogs of characteristics that apply to all currencies.

Possibly the most prominent point of debate regarding Bitcoin is its lack of regulation. The decentralized nature of the currency means that no single entity can enact fiscal policy; Bitcoin rides entirely on the whims of the free market—for better or for worse. Debate over this aspect is especially polarizing because it calls into question the age-old conflict between Keynesian and Austrian economic schools of thought. In “Bitcoin: More than Money,” Jerry Brito takes a classically Libertarian view, praising the fact that Bitcoin’s lack of central authority “makes any artificial currency inflation impossible” (par. “The How of Bitcoin”). Interestingly, opposing sources (e.g. “The Bitcoin Fantasy”) cite the same point as a weakness of Bitcoin rather than a strength, harking back to the long-standing economic debate this dialogue builds upon. “The Bitcoin Fantasy” cites the fact that lack of regulation has allowed the value of the currency to fluctuate wildly (“Bitcoin Charts,” n.d.), and has in several cases cost users large sums of money due to technical glitches. The most famous of these cases was the collapse of the Mt. Gox exchange (the largest Bitcoin exchange at the time) due to “theft, fraud, and mismanagement,” which left anybody with bitcoins in the exchange with nothing (Henwood, 2014, p. 13). Henwood and other advocates of regulation cite the absence of an FDIC-esque program (or indeed, even the potential for existence of such a program) in the Bitcoin network as a large reason why the currency remains inaccessible to the general public. Where Bitcoin’s anonymity provides arguments both for and against the widespread adoption of the currency, the currency’s lack of regulation paints a much more one-sided picture. While the classic libertarian argument that Bitcoin is superior because it isn’t subject to central regulation may be of varying merit depending on one’s political perspective, it’s difficult to argue against the economic danger posed by such a high level of instability coupled with a total lack of insurance. These conditions create an especially high barrier to entry for low and middle-income individuals, who cannot afford to make high-risk investments. Without the backing of these demographics, Bitcoin cannot (by our definition) be successful, because it will have failed to gain widespread acceptance.

Bitcoin’s anonymity and lack of regulation are two of the most prominent points of contention in the debate over the currency’s viability. From a theoretical perspective, although anonymity supports arguments on both sides, lack of regulation provides a compelling case for the unviability of Bitcoin for widespread use by the general public.

Downfall
Bitcoin is, in theory, unlikely to succeed as a currency, and the situation only becomes bleaker when put into practice. Analysis of current affairs seems to suggest that central banks, government opposition, ideological
debate, and public response will all be obstacles to Bitcoin’s widespread adoption.

One hurdle that Bitcoin may face is the response it will garner from governments and central banks if it expands much beyond its current size. As of May 2014, Bitcoin’s net volume was around $11.5 Billion, or about .1% of the American Money Supply (Henwood, 2014). At these levels, its effects are miniscule, and most governments and central banks have been content to simply observe it as a curiosity. However, one of the roles of the Federal Reserve is “[to ensure] safety and soundness of the nation’s banking and financial system” (McWhinney, 2015), which encompasses all currency used within the country. If Bitcoin were to establish a larger presence in the American economy, the Federal Reserve could be forced to confront the unfortunate truth that it had forfeited some non-negligible amount of control. At this point, it seems likely that a central bank or government looking to regain control would step in to decrease Bitcoin’s influence. Doug Henwood, author of “The Bitcoin Fantasy,” hypothesizes that, “were Bitcoin to legitimate itself through regulation and become a serious money, it’s impossible to imagine that the states would tolerate it for long.” He adds that a central financial institution would respond by “enforcing a ban at the point of conversion from state money to cryptomoney without attempting to crack the coin’s infinitely complicated algorithm” (p. 17). In other words, the fact that a government cannot regulate Bitcoin itself does not prevent it from taking aggressive measures to eliminate the influence of the cryptocurrency.

Another obstacle in Bitcoin’s path to mainstream acceptance comes from within the Bitcoin community itself. Bitcoin is a defined system, but that definition changes over time as people interact with it; it is a product of the collective will of its users. In “Bitcoin: More than Money,” Jerry Brito describes a conflict between two groups within the Bitcoin community: “ideological backers” who view the currency as an avant-garde economic experiment and reject regulation (feeling that it would undermine the intellectual spirit of Bitcoin), and “entrepreneurs” who see regulation as a prerequisite to legitimization and profit. The debate is still ongoing. At this point there are several possible outcomes, but unfortunately, none of them end particularly well for Bitcoin. If the ideological backers succeed, Bitcoin will be reduced to an economic, cryptographic, and academic curiosity, and it will never attain the regulation it needs to achieve widespread acceptance. However, the outcome if the entrepreneurs succeed is no better. It’s entirely possible that the currency will achieve widespread acceptance in this case, but if Bitcoin is heavily modified and regulated in order to succeed, such that it might barely resemble the original concept, has it succeeded at all, or simply been bastardized into something else entirely? The final and least desirable outcome is where neither group wins, and Bitcoin continues to exist in a state of limbo between idealism and pragmatism, attempting to conform to each philosophy, and ultimately satisfying neither.
Bitcoin’s final and most difficult challenge will be its public perception and image. In order for the currency to succeed (that is, achieve widespread use by the general public), it needs to be legitimate, understandable, stable, safe, and useful, for the simple reason that most members of the general public will not invest in anything that doesn’t meet these criteria for fear of losing their investment. Unfortunately, Bitcoin fails to meet each of these criteria at present: its ties to illegal activity give it an air of illegitimacy; the complicated nature of the blockchain renders the currency largely incomprehensible to everybody but experts; the lack of any central regulation means the value of any holdings fluctuates wildly; and users have lost millions of dollars due to technical errors, with no possibility of recovery because no insurance exists. Finally, and most importantly, even if all of these problems (and numerous others) are solved, the general public has little incentive to start using Bitcoin when there are no significant problems with preexisting currencies. Ultimately, by the given definition, public perception and response determine the success or failure of Bitcoin, and because public perception and response are negatively impacted by all of the factors listed above and others, Bitcoin will likely not achieve widespread acceptance as a currency.

Bitcoin as Catalyst

The debate over Bitcoin’s future success or failure thus far has been excessive and misguided, fueled by enthusiasm from some sources and gross lack of understanding from others. Participants in this dialogue have not only discussed at length a fate which is for the most part already decided, but have, more importantly, largely ignored another very prominent side of the issue—Bitcoin’s role as a catalyst for innovation. Unsurprisingly, as the first digital cryptocurrency, Bitcoin’s presence is altering longstanding paradigms in the financial sector, particularly with regard to security and privacy. Less obvious and possibly more important impacts are the potential applications of the blockchain technology to ledger-based challenges (i.e. the maintenance and verification of data). While this initially seems to be a narrow subset of problems, further exploration reveals the resulting applications to be quite diverse. The remainder of this paper will explore Bitcoin’s role as a catalyst, with particular focus on the two aforementioned topics: innovation within the financial sector driven by Bitcoin itself and more diverse innovation driven by the blockchain ledger technology upon which Bitcoin is built.

Financial Innovation

Though the debate over the merits and weaknesses of Bitcoin rages on, several points of consensus have been reached, among them that Bitcoin sets a new standard for security in online transactions. The currency has eliminated the need for a trusted third party in digital commerce, allowing for an unprecedented level of privacy and security. And though Bitcoin
has certainly made enemies in the financial sector (merely by virtue of the fact that its existence is a challenge to the foundations upon which many financial institutions stand), it’s beginning to paradoxically gain acceptance as well. Key players in major markets are beginning to recognize not only that Bitcoin’s threat to them is minimal, but also that the technologies behind it can be harnessed for their gain. The first major example of this acknowledgement of Bitcoin’s legitimacy and utility by the financial community came in early May 2015, when NASDAQ announced that it would begin using a blockchain system to keep track of its NASDAQ private market, which handles trading of shares in the pre-IPO phase (Pagliery, n.d.). The experiment is, admittedly, a limited one; the pre-IPO market is small. However, the NASDAQ, encompassing 2975 listings with a combined market cap of 8.5 trillion dollars (“NASDAQ Companies”), is most certainly not. Such action by one of America’s most prominent financial institutions could signal Bitcoin’s emergence as a catalyst for financial innovation.

Bitcoin has made truly private online transactions possible for the first time in history, and though this level of security and privacy isn’t yet possible with other currencies, it may nonetheless prompt people to consider who has the ability to view and exercise control over their transactions. Credit cards have been just one medium of exchange to come under fire as a result. In most credit card transactions, credit card and personal information is shared between buyer, vendor, credit card company, and bank. On the other hand, in a Bitcoin transaction, no potentially compromising personal or financial information is shared. In recent years, Bitcoin’s new gold standard of security has prompted some to turn a more critical eye towards the required release of information that accompanies a credit card transaction. This, in turn, has resulted in a wave of “digital wallet” products, most notably Google Wallet and Apple Pay, which attempt to combine the convenience of a credit card with the anonymity and security of Bitcoin. In a digital wallet transaction, personal information is kept totally private, and financial information is shared only between buyer, credit card company, and bank (not with the vendor) (Turner, 2014). These advances represent a considerable improvement over the intrinsic issues of credit cards, and have one additional significant advantage over Bitcoin: credibility. Ironically, while Bitcoin may be driving the shift towards greater commercial security, its competitors are utilizing their considerably greater resources and star power to capitalize on it. Though the trending success of digital wallets doesn’t bode well for Bitcoin (indeed, little does), the demand for increased security and privacy in mainstream personal transactions nonetheless illustrates the currency’s role as a catalyst for innovation within the financial sector.

Diversified Innovation through the Blockchain
It’s unsurprising that much of the innovation that stems from Bitcoin comes in commercial and financial sectors. It is, after all, a currency.
However, the blockchain technology upon which Bitcoin is based is by no means finance-specific, and has served as the basis for a series of ledger-based applications, which have arisen across different fields in the last few years and which range from tracking intellectual property in the music industry to tracking land rights in Honduras.

The ledger-based nature of the blockchain means that it is capable of recording and verifying the existence of a given piece of data at a given time. One only has to consider the forms this data could take (text, music, video, images, and many more) to arrive at what could become the most popular non-financial application of the blockchain: intellectual property. George Howard discusses the potential applications of the blockchain technology to the recording industry in his article “The Bitcoin Blockchain Just Might Save the Music Industry If Only We Could Understand It.” Howard and others assert many of the problems currently facing the music industry today (centered around legal disputes over usage rights) could be mitigated through the introduction of a blockchain ledger which would track the status of intellectual property rights across the industry. This would eliminate much of the ambiguity surrounding intellectual property that currently mires the music industry in aggressive litigation. It’s not unreasonable to imagine that a similar model could be applied to other industries centered primarily around intellectual property, including film, publishing, and others, illustrating the versatility of this application of the blockchain.

The immutable nature of the blockchain allows it to act as a perfect record of any data that users wish to record, free of any malicious interference. This quality lends itself to a surprising application of the blockchain for social good: mitigating bureaucratic corruption. The government of Honduras recently announced plans to implement a blockchain-based system for its Land Registry, in order to provide accurate verification of land ownership (Naughton, 2015). Previously, the Land Registry was notoriously vulnerable to manipulation, allowing corrupt officials to seize control of desirable property. It is hoped that the introduction of this system will mitigate the land title fraud, low registration, and corruption that have plagued Honduras in the past (Riley, 2015). In theory, the blockchain is totally resistant to any unauthorized modification; in practice, the efficacy of this solution is debatable. While the blockchain implementation should prevent direct interference with the land ownership registry, corruption is a persistent beast. It’s entirely possible that landowners could simply be forced to relinquish land against their will (under some form of threat). Nonetheless, the new approach should at least mitigate existing problems, even if it will likely not eliminate them.

Both of these examples illustrate the wide range of applications of the blockchain technology, but it remains important to consider the limitations of such approaches. Many have criticized the recent “Blockchain not Bitcoin” trend that has permeated the Bitcoin community with the same
level of infectious (and often shortsighted) enthusiasm that accompanied the currency’s initial release. The fact remains that a large portion of blockchain applications are still Bitcoin-specific (Torpey, n.d.). This comes as the result of an inconvenient truth: the applications of the blockchain are fundamentally limited by its nature. Issues arise even with ledger-based systems—the bread and butter of the blockchain model. Because the blockchain model relies on the fact that users are incentivized to continue verifying data, it’s not always relevant to non-financial applications where no such incentive exists. Furthermore, for non-ledger based applications, the utility often disappears almost entirely. Unfortunately, some systems are simply better implemented in a centralized (i.e. nondistributed) form—a fact often lost on some of the more overzealous advocates of the “Blockchain not Bitcoin” movement. However, these challenges have more recently been addressed by the emergence of Smart Contracts, implemented through platforms such as Ethereum (which is not a cryptocurrency itself, but rather a public blockchain platform which allows for the extension of the blockchain model to new applications by independent developers). With the collective force of the open-source development community behind it, the blockchain model, when applied appropriately, has the potential to significantly bolster security, clarity, and efficiency in the applications to which it is extended—three traits of which modern applications have no small need.

Conclusion

Bitcoin’s future success or failure is a relevant topic of discussion for modern finance which has unfortunately fallen into a stasis of media frenzy populated by pundits only speaking to hear themselves talk. The facts are these: while Bitcoin’s anonymity is a somewhat neutral trait, its lack of regulation contributes to a negative public image which will ultimately draw opposition from governments and individuals alike, thwarting any widespread adoption of the currency. The question is largely decided: Bitcoin cannot, should not, and will not succeed. The debate, however, persists in a state of artificial controversy which draws attention away from subtler but no less interesting or applicable aspects of the currency, chief among them Bitcoin’s role as a catalyst for innovation. In the coming years, even as the currency settles into its final state as an economic curiosity, its primary role will be as an impetus for other innovation, particularly in the financial sector, but also in a broad range of fields in which the blockchain technology can be applied to previously unsolved problems. The blockchain is not a panacea for every technological problem we face, but it can and will drive much-needed innovation in the fields that suit its particular traits. Together, these factors and others will converge to solidify Bitcoin’s dual legacy as currency and catalyst.
References
