The Bitcoin Revolution

The Digital Money Paradigm and the Financial Crisis

Tyler J. Kubik

4/22/2014

Introduction

Bitcoin has been the subject of countless sensationalist headlines in the United States for over two years. A typical headline one might read includes "Bitcoin['s] Future in Doubt,"[1] "Bitcoins: The Second Biggest Ponzi Scheme in History,"[2] or, conversely, "Bitcoin Price Skyrockets,"[3] all of which have appeared in headlines within the past six months. Sometimes, radically divergent headlines will be published in the *same day* leaving many Americans in a state of confusion and overall skepticism about Bitcoin. Although a recent poll suggested almost half of Americans now know what Bitcoin is, only 13 percent would choose it to invest in over gold.[4] Although Bitcoin has a relatively large group of dedicated followers,[5] few Americans recognize the significant potential Bitcoin has to revolutionize money and few recognize the revolution in digital currency Bitcoin has already affected.

This work will reinforce that before Bitcoin, there was a paradigm in digital money in which a central authority was often the method used to prevent double spending. It will present problems that resulted from various progressions in cryptography and manifestations of digital currencies as anomalies leading towards a crisis that would precipitate a paradigm shift, viz. Bitcoin. The introduction of Bitcoin will be shown to be interrelated to the 2007-2008 financial crisis, which exhibited the vulnerability of relying on government fiat currency as money and banks in facilitating transactions and acting as a central clearinghouse and holder of one's money. Although it can't be directly proven unless Satoshi Nakamoto, the inventor of Bitcoin,[6] unveils himself and explains his motivations, this work will suggest

---

[1] Jose Pagliery, "Mt. Gox Disappears, Bitcoin Future in Doubt," *CNNMoney,* February 25, 2014, http://money.cnn.com/2014/02/25/technology/security/mtgox-bitcoin/, accessed April 16, 2014.
[2] Douglas North, "Bitcoins: The Second Biggest Ponzi Scheme in History," *Gary North's Specific Answers*, November 29, 2013, http://www.garynorth.com/public/11828.cfm, accessed April 16, 2014.
[3] Jessica Roy, "Bitcoin Price Skyrockets," *Time Business,* November 7, 2013, http://business.time.com/2013/11/07/3-reasons-why-the-price-of-bitcoin-is-surging/, accessed March 1, 2014.
[4] Daniel Cawrey, "Poll: Vast Majority in US Would Rather Invest in Gold than Bitcoin," *Coindesk,* March 25, 2014*,* http://www.coindesk.com/poll-vast-majority-us-rather-invest-gold-bitcoin/, accessed March 28, 2014.
[5] As of March 28, 2014, Bitcoin's Reddit page has 115, 901 subscribers.
[6] The name Satoshi Nakamoto is thought to be a pseudonym; his explicit identity is not known and attempts to decipher who this mysterious founder is have been relatively fruitless, although it is generally accepted that his expertise lies in mathematics, engineering, and/or computer programming.

that the correlation between the crypto-anarchist concerns and what problems the housing and financial crisis illuminated are strong enough to suggest Nakamoto's Bitcoin paper and the implementation of Bitcoin were a response to the crisis. Corollary to this, the paper will examine ongoing anomalies, such as the Cypriot banking crisis of 2012-13, and conclude that these suggest the fiat government money system is heading towards a crisis that may result in a paradigm shift in which Bitcoin becomes more widely accepted than government currency.

I. The Double Spending Problem: An Introduction to Bitcoin

Since the advent of computers, individuals have been seeking to create digital money that could facilitate the transfer of money in cyberspace over long distances and in a fraction of the time it would take to transfer paper or commodity money over the same distance.[7] Further, payment processing services such as Western Union and PayPal charge excessively high fees to transfer money over long distances, which make small payments over long distances too costly to undertake.

To accomplish this feat, digital money would have to mirror the same characteristics that distinguish successful currencies; namely, it would need divisibility, durability, portability, scarcity, recognizability, and fungibility.[8] There have been multiple attempts at creating cyber currencies that have either been redeemable currencies denominated as a specific quantity of a commodity, such as gold, or fiat currencies that are entirely divorced from any commodity and are thus irredeemable and designed to stand on their own merits.[9] The problem in any scheme of digital currency has been in devising some form of clearing mechanism that will ensure someone cannot copy the currency's code—since after all digital currency is merely a string of code—and thus spend the same unit of money twice.

---

[7] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin.org* (October 2008): 1, https://bitcoin.org/bitcoin.pdf, accessed March 2, 2014.

[8] Gary North, *Honest Money: The Biblical Blueprint for Money and Banking* (Auburn, AL: Ludwig Von Mises Institute, 2011), 9.

[9] Government fiat currencies, of course *are not* designed to stand on their own merits, hence why they monopolize the production of money and implement legal tender laws. Some examples of centr4alized crypto currencies include e-gold, e-bullion, goldmoney, and arguably Ven and Linden Dollars.

Until recently, nearly all digital currency implementations have relied on a central clearing house that validates each unit of currency and keeps track of how it is spent and transferred between users similar to a bank's open book (checking) account or ledger.[10] The problem with using a system of centralized control is it is a trust-based system, meaning users must trust the central authority to be both competent in ensuring transactions are properly recorded and currency units are not double spent, as well as honest enough to not abuse their position of authority by defrauding their customers in some form or another. It is also a single point of failure that could result in the downfall of the entire system if the central authority becomes compromised.[11]

Bitcoin solved this problem theoretically in late 2008 with the publishing of the pseudonymous Satoshi Nakamoto's *Bitcoin: A Peer-to-Peer Electronic Cash System* and in practice with the introduction of the Bitcoin protocol to the world in early 2009.[12] What Nakamoto proposed was Bitcoin: A digital currency and payment processing network that relied on an open-source peer-to-peer system of transaction validation and money transfer, instead of a central authority, facilitated using public key cryptography and the basics of economic incentives and self-interest to promote users to devote computing power to supporting the network. Bitcoin solved the double-spending problem that had plagued digital currencies since their inception by publishing each transaction to the network in a ledger known as the Block Chain, in which users verify transactions and the order in which they occur by consensus. Individuals are incentivized to support the network because they can receive newly minted Bitcoins or transaction fees as a reward for "mining," that is successfully verifying transactions and

[10] As will be seen later, multiple theoretical models involved decentralized protocols but most of the implemented systems were more centralized.
[11] "Quoted: Marc Andreeson on What's Next For Bitcoin," *siliconbeat,* February 26, 2014, http://www.siliconbeat.com/2014/02/26/quoted-marc-andreessen-on-whats-next-for-bitcoin/, accessed April 10, 2014.
[12] Satoshi Nakamoto, "Bitcoin P2P E-Cash Paper," *GMANE* (October 2008), http://article.gmane.org/gmane.comp.encryption.general/12588/, accessed March 2, 2014. The paper was distributed using an obscure cryptography mailing list (cryptography@metzdowd.com) on October 31, 2008 and finally released on Bitcoin.org January 3, 2009.

solving cryptographically complex mathematical computations designed to mimic the costs and rewards of mining physical resources.[13]

Since its introduction in 2009, nearly all digital currency schemes have been either direct clones of Bitcoin or modified copies changing minor features, but preserving the substance of Bitcoin's solution to the double-spending problem.[14] Bitcoin has, to use the words of Thomas Kuhn, affected a *paradigm shift* in the world of digital currency that, barring any unforeseen events in the future, is the new basis from which digital currencies will operate moving forward.[15] At its peak in November 2013, Bitcoin had a total market capitalization of over $10 billion, an unprecedented valuation in the history of digital currency and a small step towards larger integration in the economy.[16]

II. The History of Cryptocurrency

It is evident from the history of digital currency that there had been themes—pervading the work of cryptographers and digital money advocates alike—involving the use of cryptographically-secure currency to deprive the government, whose control has done little more than devalue the currency,[17] from its paternalistic role in meddling with economic transactions.[18] While the history of the developments in cryptography is both extensive and technically sophisticated, a brief discussion of some particularly relevant developments in the history of cryptography can serve to illustrate how Bitcoin has incorporated these particular developments, or improved upon them, to create a radically divergent cryptocurrency that has revolutionized its field.

---

[13] Nakamoto, "Bitcoin," 2-5.
[14] Aside from a few examples, nearly all of the one hundred plus cryptocurrencies introduced since 2009 have been directly based off of Bitcoin's block chain novelty. This includes Namecoin, PeerCoin, Litecoin, Dogecoin, and numerous others. "Crypto-Currency Market Capitalizations," accessed March 28, 2014, http://coinmarketcap.com/.
[15] Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 2012), 66-76.
[16] See "Crypto-Currency Market Capitalizations".
[17] The U.S. dollar has been devalued by over 95% since the inception of the Federal Reserve in 1913.
[18] See Morgan Peck, "Bitcoin: The Cryptoanarchists' Answer to Cash," *IEEE Spectrum,* May 30, 2012, http://spectrum.ieee.org/bitcoin-the-cryptoanarchists-answer-to-cash, accessed March 28, 2014.

Given the advancements in computer technology from the 1960s through the early 1970s, including "such commercial applications as remote cash dispensers and computer terminals," there arose a need for complex cryptographic protocols that could secure digital information and "supply the equivalent of a written signature" in digital communications, which would come to include digital financial transactions.[19] In 1976, Whitfield Diffie and Martin Hellman fulfilled this need when they invented public-key cryptography. Public-key cryptography refers to a cryptographic algorithm involving two mathematically-linked keys—a public key and a private key—which can act as an encryption tool and verifier of electronic signatures (public key) as well as a decryption tool and creator of electronic signatures (private key). Each user has their own public and private key; when someone attempts to send a message to a particular user, the sender uses their private key to digitally sign a communication that can be verified by the recipient using the sender's public key. This ensures the message was sent by whom it was supposed to be sent by. Further, the message is encrypted using the *recipient's* public key, meaning only the recipient can decode the message since they are the only individual in possession of the private key capable of decrypting the message. The system is cryptographically secure such that it is computationally infeasible to attempt to employ a user's public key to calculate their private key and thus falsify the key and use it to decrypt the message. Public-key cryptography has been used since then in a variety of applications in which users desire private messages to remain secure while transmitted over unsecure networks.[20]

When retired Intel physicist Timothy May met with a group of friends and they dubbed themselves cypherpunks in 1992, their purpose was to use the tools of cryptography to create a system of privacy in digital transactions to help preserve one's anonymity in cyberspace. [21] The movement of

[19] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* 22, no. 6 (November 1976): 644–654.
[20] Wikipedia Contributors, "Public-key cryptography," *Wikipedia*, http://en.wikipedia.org/wiki/Public-key_cryptography, accessed April 7, 2014.
[21] Peck, "Bitcoin: The Cryptoanarchists' Answer to Cash".

these crypto-anarchists to create a digital currency really began here as they envisioned digital cash that could do everything from paying for goods to allowing citizens to anonymously pool their money and arrange to pay a hit-man to assassinate politicians who were purported to have violated the rights of his constituents.[22] These individuals were very conscious of the possibility for government to actively prevent privacy in digital communications by regulating e-mail and the Internet long before Edward Snowden exposed the NSA's massive indiscriminate spying program on American citizens. The American government recognized cryptography and an internet masked in privacy represented a grave threat[23] to its hegemonic dominance over the individual it has always been seeking to maintain and expand.[24] As Edward Snowden's revelations have demonstrated, fears of an Orwellian monitoring and filtering of communications were justified.

In 1997, British cryptographer Adam Back invented the first proof-of-work system that was designed to prevent Denial of Service (DoS) attacks such as massive spam emailing, which was rapidly becoming a dilemma at that time. The proof-of-work protocol, known as Hashcash, was designed to force users to expend a particular amount of CPU power and take a particular amount of time in creating e-mails and solving the cryptographic hash function that would then be affixed, comparable to a stamp, to the header of the e-mail. This protocol was designed to have a great enough threshold that would ensure that the sender of the email was not a spammer while at the same time maintaining a negligible cost for the receiver to verify the sender was not a spammer. As long as the sender could be

[22] Jim Bell, "Assassination Politics," *Outpost of Freedom*, April 3, 1997, http://www.outpost-of-freedom.com/jimbellap.htm, accessed March 28, 2014.
[23] Louis French, the Director of the FBI in 1996, delivered a speech in which he discussed the "the serious threat posed to public safety by the proliferation and use of robust encryption products." Louis J. French, Senate Committee on Commerce, Science, and Transportation, *Impact of Encryption on Law Enforcement and Safety: Hearing Before the Senate Committee on Commerce, Science, and Transportation*, July 25, 1996, https://www.fas.org/irp/congress/1996_hr/s960725f.htm, accessed April 16, 2014.
[24] For a concise understanding of the parasitic nature of the state, see Murray Rothbard, *The Anatomy of the State* (Auburn, AL: Ludwig von Mises Institute, 2009), available online at http://mises.org/pdf/anatomy.pdf.

shown to have satisfied the proof-of-work requirements, the receiver could be sure with a reasonable degree of certainty that the sender was likely not a spammer.[25]

Following this development, computer scientist Wei Dai invented the concept for b-money in 1998, which would incorporate a proof-of-work protocol similar to Back's Hashcash to create a digital money. It would involve each user creating a veil of anonymity using public-key cryptography and maintaining a database of every other pseudonymous user's account balance, each of which would later be incorporated in Bitcoin's protocol to varying extents. Further, these balances would be continually updated through broadcasting transactions to the secure network—a decentralized system of account verification—with each transaction requiring the solving of a complex cryptographical problem vis-à-vis the proof-of-work protocol.[26] Wei Dai's b-money proposal also involved various implementation and enforcement mechanisms for contracts that foreshadow today, as the "Ethereum" concept will attempt to allow for similar contract creation and enforcement mechanisms to create a distributed system of "smart property."[27]

In the same year,[28] computer scientist Nick Szabo came up with the idea for bit gold. Bit gold was Szabo's attempt to turn digital code into money. His goal was to create scarcity in a world of infinite replication using proof-of-work functions and their complex mathematical puzzles as a digital analogue to gold. If proof-of-work functions could parallel the costs and difficulty of mining gold, one could use time-stamped proof-of-work functions to distribute digital currency to users as a reward for solving the hash functions. Each hash function solution would be broadcast to the network creating a digital string of property ownership, in essence a registry. In this system, the value of the bit gold would be largely

[25] A spammer's business-model relies on their ability to send an abundance of messages at almost no-cost, so a proof-of-work function would be designed to raise the costs for spammers and make their model unviable. Adam Back, "Hashcash – A Denial of Service Counter-Measure," *Hashcash.org*, August 1, 2002, http://www.hashcash.org/papers/hashcash.pdf, accessed March 30, 2014.
[26] Wei Dai, "b-money," http://www.weidai.com/bmoney.txt, accessed March 30, 2014.
[27] Vitalik Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," *Github,* accessed March 29, 2014, https://www.ethereum.org/.
[28] Nick Szabo, "Bitcoin what took ye so long," *Unenumerated*, May 28, 2011, http://unenumerated.blogspot.com/2011/05/bitcoin-what-took-ye-so-long.html, accessed April 2, 2014.

dependent upon the computational difficulty involved in solving the cryptographic hash function. Unfortunately for bit gold, the idea suffered from certain vulnerabilities and uncertainties and failed to take hold.[29]

An alternative to these decentralized schemes of currency was DigiCash created in 1990 by David Chaum that used centralized authority, in this case banks, to handle oversight and keeping track of account balances and transactions. This was diametrically opposed to the crypto-anarchists' credo which was to create a system in which "government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations."[30] DigiCash was not a scheme innovators and crypto-anarchists such as Wei Dai or Timothy May could get behind and work to see implemented on a large scale; it would succumb to bankruptcy in 1998.[31] Other electronic cash pioneers such as First Virtual and CyberCash suffered similar fates, in no small part due to the inherent difficulty in maintaining trust in centralized systems of digital currency.[32]

As the history of digital currency attests, Bitcoin came onto the scene drawing together much of the innovation of these previous schemes while adding its own nuance in the form of the Block Chain. Instead of creating and broadcasting a chain of digital property ownership such as bit gold, Bitcoin would create a public chain of verified transactions. To summarize, Bitcoin:

---

[29] One of the vulnerabilities mentioned in Wikipedia was the Sybil attack in which a user in a peer-to-peer network could create large quantities of forged identities and thus control a large percentage of the number of network addresses, leaving it vulnerable to control by a user of small number of users. Also, it seems problematic because it would appear units of bit gold would not be seamlessly combined and divided (fungible) because each unit of bit gold is not identical, so it would have to function more closely to commodity market than an ideal market for money. Nick Szabo, "Bit gold," *Unenumerated*, December 27, 2008, http://unenumerated.blogspot.com/2005/12/bit-gold.html, accessed March 30, 2014.

[30] Dai, "b-money".

[31] Wikipedia Contributors, "DigiCash," *Wikipedia, http://en.wikipedia.org/wiki/Digicash* (accessed April 7, 2014).

[32] "Boom then Bust: How Electronic Cash Faltered," *ENT Mag,* March 1999, http://entmag.com/archives/article.asp?EditorialsID=6094, accessed April 7, 2014.

1. Eliminated the centralized clearinghouse mechanism, such as DigiCash had, in favor of a decentralized peer-to-peer system as has been theorized with bit gold or b-money.

2. Used proof-of-work functions comparable to Hashcash in order to distribute new currency, prevent any DoS-type attacks, and to verify transactions broadcast to the network.

In totality, Bitcoin is strongly drawn from the crypto-anarchist tradition of decentralized currency schemes that reject centralization and try to eliminate the role financial institutions play as "trusted third-parties to process electronic payments."[33]

III. The Financial Crisis

One of the most significant as well as one of the least discussed aspects of the Nakamoto's paper on Bitcoin was its release date in October of 2008 as America was in the throes of financial collapse and a few months away from the stock market's rock bottom in March of 2009. Nakamoto's paper does not explicitly name the financial crisis or his belief in the coming of a crisis as a motivation for his paper; in fact, without a date telling us when it was published, it would not look out of place at any time after 2003.[34] However, it is difficult not to make the connection between the financial crisis and the emergence of Nakamoto's paper, given that it is a direct assault on the trust-based system of central banking and fiat money that helped drive the crisis. What follows below will briefly present some of the most significant drivers of the housing bubble and financial crisis, how government was the root of the problem, and how Bitcoin might have emerged from the crisis due to the climate of fear it spawned.

To begin with, the Community Reinvestment Act (CRA) of 1977 was one of the significant government regulations leading to the housing bubble. The CRA was designed to aid lower income families in obtaining home loans and combat the practice known as redlining, whereby banks

[33] Nakamoto, "Bitcoin," 1.

[34] In his 2008 paper, the most recent paper cited was a 2002 paper pertaining to Hashcash written by Adam Back. Thus, there is little historical reference in his work to suggest recent events may have led to the publishing of his paper.

purportedly discriminated against lower income neighborhoods or minorities. Congress seemingly wanted to continue to promote the "American Dream" of homeownership for everyone, but they did so by intervening in the market and interfering with some sound as well as unsound lending practices, ending up with a much more significant problem than when it began. The key provision of the CRA pertaining to the housing bubble was the disparate impact provision which forbade banks from refusing to make loans if this practice resulted in a disproportionate impact on minority or low-income communities, the violation of which was grounds for a lawsuit by the Department of Justice or the Department of Housing and Urban Development.[35]

The CRA was problematic because it ignored some of the basic principles of economics, one of which maintains that individuals (or businesses) are risk-averse and seek to mitigate costs while maximizing their utility.[36] In certain cases, it may have been true that banks chose to lend to lower income whites rather than middle or upper income blacks and engaged in discriminatory lending towards blacks. However, to the extent that the CRA may have alleviated this discriminatory lending practice, it created new problems by forcing banks to lend to consumers they otherwise would not have lent to because they were too risky.[37] Common sense economics would tell us that higher risk individuals, such as those in poorer neighborhoods, require greater collateral, down payments, or interest rates to compensate for the fact that these individuals have higher rates of default than other consumers.[38] However, the CRA forced banks to lend to these high-risk individuals, many of whom they

[35] Howard Baetjer, "Let Market Forces Regulate – Mortgage Standards," *Free Our Markets*, January 3, 2014, http://www.freeourmarkets.com/let-market-forces-regulate-mortgage-standards/, accessed April 1, 2014.
[36] Wikipedia contributors, "Rational-Choice Theory,"*Wikipedia*, http://en.wikipedia.org/wiki/Rational_choice_theory (accessed April 2, 2014).
[37] Without doing more research, I'm not clear that it actually solved this problem, or to what extent this problem existed, but I think it is fair to say it probably eliminated many instances where low-risk loans to blacks were ignored in favor of higher risk loans to whites, given how many underqualified applicants of all races obtained home loans. Again, even if it did rectify this, it opened up a new and even bigger can of worms in the process.
[38] One of the problems in understanding "discrimination" is people fail to understand that discrimination is a necessary and even desirable practice under certain conditions. The term discrimination has acquired such a pejorative connotation it is difficult for anyone to actually seek to understand that there are various forms of discrimination, some more or less desirable that others. If, instead of seeing bank practices as discriminatory

would have outright rejected before the CRA, and also incentivized them to eliminate or reduce the severity of risk-mitigating protocols such as higher down payments or greater required collateral that would deter low-income applicants. Thus, high-risk individuals were approved for loans often without any information to support that they could pay back the loan; this happened not simply because banks were "greedy"[39] and wanted individuals to fail to pay back their loans so they could take possession of the house,[40] but because government regulation promoted and incentivized this behavior. These rules were directly antagonistic "with the core economic principle that in a world of scarce resources, loans should be made in keeping with borrowers' ability to meet their repayment obligations—to pay the money back—regardless of race and ethnicity patterns. Improvements in material well-being for everyone depend largely on how well we use scarce investment capital;"[41] incentivizing economically inefficient or deleterious behavior only creates more of this behavior.

Another factor that led to the financial crisis was the Basel Committee rules on banking supervision. The Basel committee is an international committee of ten central banks who coordinate efforts to "improve the quality of banking supervision worldwide" by establishing guidelines—although *de facto* they usually become law when the respective central banks implement these procedures—for banking regulation and supervisory procedures and rules.[42] Under the rules proclaimed by the second Basel accords (Basel II), the committee established distinct rules related to capital requirements for particular classes of assets, regulations which proved to be devastating in spilling over the consequences

---

against low-income individuals, one understands it as discrimination—or rather prudence—*against high-risk individuals*, which is undoubtedly the case *prima facie* with low-income individuals, it casts doubt on the whole purpose of the CRA and easily illuminates the problems it can, and did, cause.

[39] Thomas E. Woods, *Meltdown: A Free-Market Look at Why the Stock Market Collapsed, the Economy Tanked, and Government Bailouts Will Make Things Worse* (Washington, DC: Regnery Publishing, Inc, 2009), 13-18.

[40] A perfect example of this layman's perspective can be found in the lyrics of hip-hop artist Lupe Fiasco's song, "Words I Never Said." He says, "Crooked banks around the world would gladly give a loan today, so if you miss a payment they can take your home away."

[41] Baetjer, "Market Forces".

[42] Wikipedia Contributors, "Basel Committee on Banking Supervision," *Wikipedia* http://en.wikipedia.org/wiki/Basel_Committee_on_Banking_Supervision (accessed April 1, 2014).

of the housing collapse into financial markets.[43] The Basel II capital requirements ranged from 0% for low-risk assets such as government bonds and cash to 100% for unsecured debt.[44] Because of the AAA credit rating of mortgage-backed securities (MBS) among rating agencies, and the stamp of approval of numerous government regulatory agencies, mortgage-backed securities were placed in the 20% category, meaning they were considered low-risk and did not have to have large amounts of collateral held against them. From hindsight, it is almost nonsensical that MBSs were considered substantially less risky than business and home loans (100% and 50%, respectively); however, it was the regulatory rules and incentives that encouraged banks to hold MBSs on their balance sheet with little collateral because it was a convenient way to engage in regulatory capital arbitrage and give themselves a cushion against capital requirements while cutting their incomes very little.[45]

A final factor leading to the housing bubble and financial crisis, and arguably the most important, was the ability of the Government Sponsored Entities, Fannie Mae and Freddie Mac, to buy mortgage-backed securities with near impunity.[46] These organizations were tasked with buying billions of dollars of subprime mortgages from banks in order to subsidize home loans to high-risk buyers and concurrently lower the interest rates on home loans.[47] Although their purchasing of subprime mortgages largely failed to keep interest rates low, it did have the effect of encouraging banks to make more risky loans because they knew they would be purchased by Fannie and Freddie; thus banks did not have any fear of incurring the consequences for taking on increasingly risky home loans. Fannie and Freddie could

[43] Howard Baetjer, *Free our Markets: A Citizen's Guide to Essential Economics*, (New Hampshire: Jane Philip Publications, LLC, 2013), 270-71.
[44] U.S. Department of the Treasury, *Office of Thrift Supervision Examination Handbook*, September 2010, http://www.occ.gov/exam-handbook.pdf, Appendix B.
[45] Baetjer, *Free Our Markets,* 260-270. Although they were limited on how much MBS they could hold by the overall capital requirements.
[46] Woods, *Meltdown*, 2. Woods would argue that "the Fed's policy of intervening in the economy to push interest rates lower than the market would have set them was the single greatest contributor to the crisis." I am inclined to favor this viewpoint, but will not address this issue in the interest of focus.
[47] Charles W. Calomiris and Peter J. Wallison, "Blame Fannie Mae and Congress for the Credit Mess," *Wall Street Journal*, September 23, 2008, http://online.wsj.com/news/articles/SB122212948811465427, accessed April 1, 2014.

do this because they were known to be backed by the government with the implicit guarantee they would be bailed out if problems began arising.[48] Additionally, with no fear and a nearly inexhaustible ability to borrow money to pay for the loans, Fannie and Freddie were perversely incentivized to take on more risky assets that had higher yields because in the event of success, they would reap the benefits but in the event of failure, they would suffer none of the costs.[49] "[By] the eve of the federal government takeover in 2008 they had a hand in about half the country's mortgages, and nearly three-quarters of new mortgages." [50]

There were many more factors and nuances involved in creating the housing bubble and spreading its contagious effect onto the financial markets. But, the above analysis suffices to show that it was mostly—or at least significantly—government regulations which incentivized banks to lend to high-risk borrowers, invest in MBSs, and hold little capital against their MBSs without fear of the consequences facing these risks. Given the often contradictory nature of government regulation and the widespread misallocation of resources fostered by Congress and Fannie Mae and Freddie Mac, the security and stability of the American banking system is perilous indeed. In a country with a much more stable banking system free from the debilitating tentacles of government regulation and without central banks to inflate the money supply at the behest of the legislature, it is difficult to imagine a concept such as Bitcoin gaining much traction.[51] A stable banking system would mean the population could generally trust that their deposits will be secure and a stable currency could ensure the population would hold onto money without the fear of it depreciating in value due to the inflationary whims of central bankers. To the extent that one can recognize how Bitcoin can aid in removing the control of

[48] College loans today are being handled in nearly the same way by Sallie Mae. It is quickly becoming a higher education-loan bubble that could burst if the default rates on these loans continue to rise as they have been doing the past few years. Steven Horwitz, "An Open Letter to My Friends on the Left," September 28, 2008, http://myslu.stlawu.edu/open_letter.htm, accessed April 1, 2014; Woods, Meltdown, 14-15.
[49] Calomiris, "Blame Fannie."
[50] Woods, *Meltdown*, 15.
[51] Although, in a much more free banking system, it is entirely possible there would have been *more* or even *widespread entrepreneurial efforts* to move towards digital money.

currency from central bankers and exist free from government regulation that creates perverse incentives, one can identify how Bitcoin might emerge as a response to the banking crisis of 2007-2008. Crypto-anarchists had been seeking a way to ensure the government was forbidden from economic transactions in the digital world and they hoped to have found their golden goose in Bitcoin.

IV. Significance and Future

The significance of the Bitcoin revolution in digital money stems from its potential for widespread adoption, which could upset many institutions that have a vested interest in maintaining the status quo.[52] Until Bitcoin, virtual currencies were accepted only in exceedingly small, close-knit circles and were exchanged very infrequently and possibly never directly for any goods. Today, thousands of businesses and online merchants display "Bitcoin Accepted Here" posters in their windows and exchange Bitcoin for real goods and services as readily as if they were receiving a U.S. dollar. Solving the double spending problem allowed Bitcoin to be diffused to the masses, which was never before possible in the realm of virtual currency. It has created a situation where a digital currency has come very close to replicating the monetary characteristics of a physical currency without replicating some of the particular drawbacks associated with it.[53] While solving the double spending problem was a revolution within the small sphere of digital currency, which is what this paper has addressed, its true significance and revolutionary nature is an ongoing process as it attempts to achieve the status of general acceptance across the United States and eventually the world. As a financial crisis was likely the spark that led to the introduction of bitcoin to the population, so too could a future financial crisis lead to general acceptance of a digital currency by the population.

Following the U.S. financial recession in 2008, many other countries began feeling the ripple effects as a global financial crisis began hitting countries all around the world, including the small

[52] See Erik Voorhees, "Bitcoin – The Libertarian Introduction," *On Life and Liberty Blog*, April 13, 2012, http://evoorhees.blogspot.com/2012/04/bitcoin-libertarian-introduction.html, accessed February 2, 2014.
[53] Two examples of such drawbacks include the costs of physical transportation and the cost of storage, disadvantages which Bitcoin does not have.

Mediterranean nation of Greece. Despite being one of the fastest growing economies from 2000 to 2007, continuous and substantial deficit spending by the Greek government over a number of years accumulated vast debts to creditors around the world. The Greek government's debt-to-GDP ratio hovered around 100 percent for most of the 1990s, but in 2003, the ratio began climbing to an unprecedented level, exceeding 150 percent in 2009. This evoked fears among the holders of Greek debt who started questioning the government's ability to pay back the loans. Significantly, in January of 2010, "the European statistics agency, Eurostat…issued a damning report [on Greece] which contained accusations of falsified date and political interference." Government bond ratings began degrading at an exceeding rate due to fears of default, hitting junk bond status in late April of 2010.[54] Finally, on May 2, 2010, the International Monetary Fund agreed to bail out the Greek government to the tune of a $147 billion loan, conditional upon meeting conditions of austerity and privatization of government assets.[55]

As Greek bonds began plummeting and it was forced to be bailed out by the IMF, further anomalies began popping up as banks in Cyprus began to show signs of financial troubles. Cypriot banks had historically invested heavily in Greek bonds due to their close proximity and relationship, meaning their financial status took a heavy hit due to the Greek sovereign debt crisis and their large exposure to Greek debt.[56] Although the large exposure to Greek debt should have warned observers early on that there would be financial troubles brewing, "during the years 2011 and 2012, no less than nine awards for excellence were given to the Bank of Cyprus" by J.P. Morgan Chase and Citibank, listing the Cypriot Bank as "among the leading banks of the world."[57]

---

[54] Wikipedia Contributors, "Greek government-debt crisis," *Wikipedia*, http://en.wikipedia.org/wiki/Greek_government-debt_crisis (accessed April 7, 2014).
[55] Lefteris Papadimas and Jan Strupczewski, "EU, IMF agree $147 billion bailout for Greece," *Reuters*, May 2, 2010, http://www.reuters.com/article/2010/05/02/us-eurozone-idUSTRE6400PJ20100502, accessed April 7, 2014.
[56] Kurt Sansone, "Understanding the Cypriot bank crisis," *Times of Malta*, March 31, 2013, http://www.timesofmalta.com/Understanding-the-Cypriot-bank-crisis.463528, accessed April 7, 2014.
[57] Robert Wenzel, "Lessons from Cyprus," *Mises Daily*, April 5, 2013, https://mises.org/daily/6400/, accessed April 7, 2014.

However, tensions would build and on March 15, 2013, Cyprus's two largest banks, Laiki and the Bank of Cyprus closed indefinitely, prompting panic in the international community. Particularly ominous, the banks announced their closure on a Saturday when banks were closed leading to many fuming depositors who had no way to withdraw any of their funds.[58] The next day, on March 16, Eurozone members announced their intention to bailout these banks with a €10 billion loan conditional upon a tax on depositor's funds, 9.9% for deposits exceeding €100,000 and 6.7% for those deposits below that threshold in order to raise an additional €5.8 billion. Under European Union law, this tax would have been technically illegal due to deposit insurance guarantees on deposits up to €100,000. This agreement shocked Cypriot depositors and international observers who thought deposits were safeguarded through deposit insurance, viewing this proposal as little more than massive fraud and theft. Eventually, due to the widespread outrage over the preliminary agreement, the deal was changed, eliminating the 6.7% deposit tax altogether in favor of a closing down of the Laiki bank and selling off its assets to private interests. However, the new deal substantially raised the costs on depositors with balances greater than €100,000, as these depositors could lose up to 40 percent of their balance in the tax. [59] This episode spread fears around the world and particularly to the United States where yearly deficits had been and continue to be run year after year, piling up trillions of dollars of liabilities, which many believe a desperate federal government might try to snatch in the event of a financial crisis to fund its own excesses.

These instances[60] represent anomalies—albeit crises in their own right—in the economic system of fractional-reserve banking and Keynesian deficit-spending that has gripped the world since at least

[58] Wenzel, "Lessons from Cyprus".
[59] Theresa Papademetriou, "The Cyprus Banking Crisis and its Aftermath: Depositors Be Aware," *Library of Congress Blog,* April 4, 2013, http://blogs.loc.gov/law/2013/04/the-cyprus-banking-crisis-and-its-aftermath, accessed April 7, 2014.
[60] It is also worthy of note that in 2010, antecedent to the Greek and Cyprus anomalies, whistle-blowing website WikiLeaks was denied DNS (Domain Name Service), had Amazon drop its hosting services, and had PayPal, Visa, MasterCard, and Bank of America cut off the financial services from WikiLeaks to distance themselves from

the early Twentieth century.[61] These anomalies have parlayed the fundamental fear of bank failure and loss of deposits into concrete action for the hundreds of thousands of people who have adopted Bitcoin since 2009. If economic crises continue to accumulate, or if a large enough crisis comes to devastate the world economy,[62] Bitcoin, or some other non-governmental currency, could come to replace the systems of government control of money that have been around for thousands of years, finally freeing money from political interests and leaving it in the control of the invisible hand of the market. Indeed, if money is the most important driver of progress, one might surmise money is simply too important to trust to the arbitrary caprices of government.

whatever trouble WikiLeaks might be in due to its publishing of embarrassing government documents. In this instance, government pressure forced businesses to cave and do the state's political bidding to censor a website it found disruptive. This example of denial of services to organizations critical of the state is representative of these same concerns addressed throughout the paper. These themes involved shielding oneself from the state and seeking out innovative decentralized alternatives like Bitcoin that can facilitate commerce outside of the reach of the regulatory apparatus.

[61] While Keynes General Theory was published in 1936 and the Federal Reserve System—a symptom of the world-wide drive toward central banking—was established in 1913, the concepts and practices of central banking, fractional-reserve banking, and deficit spending had been around long before then. The Bank of England, for example, was established in 1694.

[62] Exogenous shock has tended to allow the most radical changes in entrenched institutions to occur and would be the most likely candidate for a change of this magnitude, in my humble opinion. It is difficult to see the government voluntarily relinquishing control of the money supply or not fighting to keep hold of this control, even if the effort would arguably be futile in the case of Bitcoin.