eCoin System

Project Proposal

by

Geoffrey Byron Paul Glass, J.D.
paulglass@ecoinproject.org

eCoin Ltd. DBA eCoin Project
https://ecoinproject.org

[DRAFT PAPER – REVISION DATE: 2016-11-10]

[Latest revision may be found here.]

ABSTRACT

Many enthusiasts view Bitcoin and other cryptocurrencies as an alternative form of money, free from the weaknesses of fiat currency and the current state of our monetary, banking, and financial system. However, cryptocurrencies have weaknesses of their own.

We posit that Bitcoin and cryptocurrencies currently suffer from the following: (1) high price volatility, (2) a lack of transactional privacy, (3) and a lack of proper governance. We surmise that these weaknesses are of such significance that they greatly diminish the use, value, utility, and sustainability of Bitcoin and other cryptocurrencies.

To rectify these weaknesses, we propose the creation of a new cryptocurrency system called the eCoin-eShares Cryptocurrency System ("eCoin System"). The undertaking of this proposal is known as the eCoin Project. Inspired by Bitcoin and other cryptocurrencies, the eCoin Project's goal is to develop a cryptocurrency designed to have the following: (1) price stability, (2) transactional privacy, (3) and democratic governance.

TABLE OF CONTENTS

1. INTRODUCTION

The 2007-2009 global financial crisis, along with the subsequent response by governments and central banks around the world, highlights the fact that our current monetary, banking, and financial system is significantly flawed. Satoshi Nakamoto, the inventor of Bitcoin, was aware of this long before many. Realizing the need for an alternative system, Nakamoto released Bitcoin to the world during the height of the crisis on Halloween 2008.

Described as "cash for the Internet"[1] or a form of "digital currency"[2], Bitcoin enables the transfer of electronic money (in the form of bitcoin) without the need of an intermediate third party (e.g. bank or payment processor). In other words, with the advent of Bitcoin, financial transactions became possible outside the paradigm of centrally-controlled fiat currency and bank-intermediated financial exchange. This is an extraordinary achievement.

Free from the grips of central-banks and financial institutions, Bitcoin appeared to provide a possible solution to the inherent flaws of fiat-currency and the monetary, banking, and financial system. Not surprisingly, many critics of the current system became ardent Bitcoin and cryptocurrency enthusiasts (ourselves included). However, Bitcoin and other cryptocurrencies ("cryptos") have not turned out as hoped.

As time has gone on, it has become apparent that Bitcoin and cryptos suffer from the following fundamental weaknesses: (1) huge price volatility, (2) a lack of transactional privacy, (3) and a lack of proper governance. We surmise that these weaknesses are of such significance that they greatly diminish the value, utility, and sustainability of cryptos, as well as being their primary hindrance to widespread adoption.

---

[1] Bitcoin.org, *FAQ: What is Bitcoin?*, https://bitcoin.org/en/faq#what-is-bitcoin, *archived at* https://perma.cc/443Y-2DT7 (explaining that "from a user perspective, Bitcoin is pretty much like cash for the Internet").

[2] Robert McMillan & Cade Metz, *Bitcoin Survival Guide: Everything You Need to Know About the Future of Money*, Wired (Nov. 25, 2013), https://www.wired.com/2013/11/bitcoin-survival-guide, *archived at* https://perma.cc/HJE2-2WDW (describing Bitcoin as "a digital currency").

We are not the only ones to recognize these issues. Many within the so-called "crypto-community" are also aware of Bitcoin and cryptos' weaknesses, and a small number of "specialized cryptos" have been developed as a result. For example:

- In response to cryptos' massive price volatility, BitShares[3] (along with the corresponding bitUSD asset), Nu from NuBits[4], and Tether are designed with the goal of providing a crypto pegged to the value of fiat.
- In response to cryptos' lack of transactional privacy, the CryptoNote[5] protocol (with its most popular offshoot Monero[6]), CoinJoin[7] implementations such as Dash[8] (previously known as Darkcoin), and Zcash (still in development) are designed with the goal of providing anonymous transactions.
- In response to cryptos' lack of proper governance, BitShares, Nu, NXT, and Dash are each trying different governance models aimed at achieving various levels of stakeholder control.

While these cryptos provide (in our opinion) ingenious solutions and are important steps toward resolving the weaknesses facing Bitcoin and cryptos, they are not without their flaws.

All of the previously mentioned "specialized cryptos" may be categorically described as the having the following problems: First, many of them provide only "half solutions", meaning that while they may fix certain aspects of a particular weakness within

---

[3] *See generally*, Fabian Schuh & Daniel Larimer, *BitShares 2.0: General Overview* (Dec. 18, 2015), http://docs.bitshares.eu/_downloads/bitshares-general.pdf, *archived at* https://perma.cc/P9PG-KT33. *See also* Fabian Schuh & Daniel Larimer, *BitShares 2.0: Financial Smart Contract Platform* (Nov. 12, 2015), http://docs.bitshares.eu/_downloads/bitshares-financial-platform.pdf, *archived at* https://perma.cc/56R7-LBUT.

[4] *See generally*, Jordan Lee, *Nu* (Sept. 23, 2014), https://www.nubits.com/assets/nu-whitepaper-23_sept_2014-en.pdf, *archived at* https://perma.cc/NU9T-69XA.

[5] *See generally*, Nicolas van Saberhagen, *CryptoNote v 2.0* (Oct. 17, 2013), https://cryptonote.org/whitepaper.pdf, *archived at* https://perma.cc/EVZ2-3YWD.

[6] *See* The Monero Project, *About Monero*, https://getmonero.org/knowledge-base/about, *archived at* https://perma.cc/TX7N-73AR (noting that Monero was developed because "with Bitcoin, as well as with the vast majority of cryptocurrencies that have been established since, any and all transactions are entirely traceable.")

[7] *See generally*, Gregory Maxwell, *CoinJoin: Bitcoin privacy for the real world*, Post # 1 (Aug. 22, 2013, 02:32 AM), https://bitcointalk.org/index.php?topic=279249.msg2983902#msg2983902, *archived at* https://perma.cc/MGX6-M7P6 (proposing CoinJoin as a solution to Bitcoin's lack of transactional privacy).

[8] *See generally*, Evan Duffield & Kyle Hagan, *Darkcoin: Peer-to-Peer Crypto-Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System* (Mar. 18, 2014), https://www.dash.org/wp-content/uploads/2014/09/DarkcoinWhitepaper.pdf, *archived at* https://perma.cc/42U5-7W3S.

Bitcoin and cryptos, the underlying problem is not completely resolved. Second, in many instances the solutions provided by these cryptos are either inadequate or actually bring about new problems of their own. Third, none of these cryptos provide a comprehensive solution, meaning that none of them are aimed at resolving all of the aforementioned weaknesses. In short, what we need is a new cryptocurrency that provides a comprehensive solution to all three of cryptos' fundamental weaknesses.

With the aim of achieving that goal, we propose the development of a new cryptocurrency called the eCoin-eShares Cryptocurrency System ("eCoin System"). Upon release, the eCoin System will be the first and only crypto specifically designed to provide a comprehensive solution to the weaknesses currently found in Bitcoin and other cryptos. Inspired by the dream of creating a currency that exists for the benefit of all people and is truly free of the monetary, banking, and financial system, the eCoin System will be designed to have the following: (1) price stability, (2) transactional privacy, and (3) democratic governance.

2. THE RISE OF BITCOIN

2.1. The 2007-2009 Financial Crisis

> *This is an extraordinary period for America's economy . . . We've seen triple-digit swings in the stock market. Major financial institutions have teetered on the edge of collapse, and some have failed. As uncertainty has grown, many banks have restricted lending. Credit markets have frozen . . . We're in the midst of a serious financial crisis . . . [a]s a result, our entire economy is in danger.*[9]
>
> – President George W. Bush, Address to the Nation on the Financial Crisis, September 24, 2008

Between 2007 and 2009 the world experienced a global financial crisis, the likes of which had not been seen since the days of the Great Depression in the 1930's. Decades of lax government regulation – coupled with the advent of new complex derivatives – had led to an opaque credit environment, enabling investment banks to take on hidden leverage to excessive proportions.[10] By early-2007, this excess hidden leverage was proving to be a "powder keg" to the stability of the financial system.[11]

Ripples of the crisis first began when the "housing bubble" burst in mid-2006[12] and home values started to decline for the first time in decades.[13] As home values declined, many homeowners found themselves "upside-down", where the underlying debt of their mortgage surpassed the market value of their home, and therefore either unable or

---

[9] President George W. Bush, *Address to the Nation on the Financial Crisis* (Sept. 24, 2008), Selected Speeches of President George W. Bush 2001–2008, 575, http://georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Selected_Speeches_George_W_Bush.pdf, *archived at* http://perma.cc/JPB4-6UG6; video *available at* https://www.youtube.com/watch?v=YsDmPEeurfA [hereinafter *Bush Speech*].

[10] *See generally* Michael Simkovic, *Secret Liens and the Financial Crisis of 2008*, 83 Am. Bankr. L.J. 253 (2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1323190, *archived at* https://perma.cc/XJ84-LWDN.

[11] *Id.* at 254.

[12] *See e.g.*, Shawn Tully, *Welcome to the dead zone: The great housing bubble has finally started to deflate, and the fall will be harder in some markets than others* (May 5, 2006), CNN Money, http://money.cnn.com/2006/05/03/news/economy/realestateguide_fortune/, *archived at* http://perma.cc/7M8K-CJGP.

[13] *See e.g.*, The Economist Data Team, *American house prices: reality check* (Nov 3, 2005), The Economist, http://www.economist.com/blogs/graphicdetail/2015/11/daily-chart-0, *archived at* https://perma.cc/2HBF-KU5Z.

unwilling to pay their mortgages.[14] This lead to disastrous consequences for financial institutions.

As the number of mortgage defaults rose, over-leveraged investment banks holding these mortgages in the form of mortgage backed securities ("MBSs") and collateralized debt obligations ("CDOs") suffered unprecedented losses. The massive drop in MBSs and CDOs created a cascading effect on credit default swaps ("CDSs"), which acted as a form of "insurance" that financial institutions used to hedge their positions in the event of a drop in MBSs or CDOs.[15] In summation, within a very short period of time, the world's largest and most powerful financial institutions had been brought to their knees.

By late-2007 the unravelling of the housing derivatives market was having such a detrimental impact on the solvency of financial institutions that Treasury Secretary Henry Paulson called it "the most significant . . . risk to our economy."[16] The stock market was in a panic, and the whole system appeared on the verge of collapse.[17] Fearing destruction of the entire global monetary, banking, and financial system, U.S. officials and heads of major financial institutions met in a series of crash meetings over a period of eights days.[18] Within those meetings the United States government began discussions on what would essentially become bailout packages for the very institutions that had created the crisis.[19] It was a foreshadowing of more to come.

---

[14] *See generally* William R. Emmons, *The Mortgage Crisis: Let Markets Work, But Compensate the Truly Needy* at 13 (July 2008), Fed'l. Reserve Bank of St. Louis, *available at* https://www.stlouisfed.org/~/media/Files/PDFs/publications/pub_assets/pdf/re/2008/c/mortgage.pdf, *archived at* https://perma.cc/8757-YXTR (explaining that declining home prices, coupled with increased risky subprime mortgages, were the catalysts for the financial crisis).

[15] *See Bush* Speech, *supra* note 9 at 576-77.

[16] Edmund L. Andrews, *Housing Slump 'Unfolding,' Treasury Chief Says* (Oct. 16, 2007), N.Y. Times, http://www.nytimes.com/2007/10/16/business/16cnd-paulson.html, *archived at* http://perma.cc/TX2P-YX9B.

[17] *See, e.g.*, *Bush Speech*, *supra* note 9 at 575-80.

[18] *See generally*, James B. Stewart, *Eight Days: The battle to save the American financial system* (Sept. 21, 2009), The New Yorker, http://www.newyorker.com/magazine/2009/09/21/eight-days, *archived at* http://perma.cc/AP82-WCNS.

[19] *See generally*, Damian Paletta, Susanne Craig, & Deborah Solomon, *New York Fed Holds Emergency Meeting On Lehman's Future* (Sept. 13, 2008), Wall St. Journal, http://www.wsj.com/articles/SB122126724103330909, *archived at* https://perma.cc/37JW-XYZD?type=pdf (reporting on a Sept. 12, 2008 meeting between top U.S. gov't officials and CEOs of America's largest financial institutions, discussing government assistance in light of the growing financial crisis).

2.2. Governments & Central Banks Respond

Facing the unacceptable alternative of what appeared to be complete economic catastrophe, the United States and governments around the world went on an unprecedented spree of institutional bailouts, fiscal stimuli, and expansionary monetary policies.[20] In the United States, federal bailouts of the very institutions that had precipitated the crisis helped the national debt soar from pre-crisis levels of approximately 64% of the nation's GDP to 99% of GDP by the end of 2011.[21] In less than five years the national debt had nearly doubled, going from $8.4 trillion in June 2006[22] to $15.2 trillion by December 2011.[23]

In an effort to stabilize markets and provide liquidity to the global banking system, the Federal Reserve ("Fed") also took drastic action. Through its policy of "quantitative easing", the Fed effectively quintupled the money supply.[24] Furthermore, results of a successful Freedom of Information Act lawsuit[25] have revealed that the Fed also secretly provided trillions of dollars in loans to other central banks and financial institutions around the world, with various estimates placing the total figure at $7.77 Trillion (Bloomberg),[26]

---

[20] *See*, *e.g.*, Kavaljit Singh, *Fixing Global Finance: A Developing Country Perspective on Global Financial Reforms*, Stichting Onderzoek Multinationale Ondernemingen: Centre for Research on Multinational Corporations 14, *available at* http://somo.nl/publications-en/Publication_3588/at_download/fullfile, *archived at* https://perma.cc/T8KN-KS8X?type=pdf.

[21] *See*, *e.g.*, Trading Economics, *United States Government Debt to GDP 1940 – 2015*, http://www.tradingeconomics.com/united-states/government-debt-to-gdp, *archived at* https://perma.cc/9KPV-V3YR, *chart set to 2006-2012*.

[22] U.S. Dep't of Treasury, *Monthly Statement of the Public Debt of the United States: June 30, 2006*, ftp://ftp.publicdebt.treas.gov/opd/opds062006.pdf, *archived at* https://perma.cc/WZ3Q-HE65.

[23] U.S. Dep't of Treasury, *Monthly Statement of the Public Debt of the United States: December 31, 2011*, https://www.treasurydirect.gov/govt/reports/pd/mspd/2011/opds122011.pdf, *archived at* https://perma.cc/7ZHM-MUZW.

[24] *See*, *e.g.*, Congressional Research Service, Marc Labonte, *Monetary Policy and the Federal Reserve: Current Policy and Conditions* at 13 (Jan. 28, 2016) https://www.fas.org/sgp/crs/misc/RL30354.pdf, *archived at* https://perma.cc/2DF8-FDJV (noting that after three rounds of QE between 2009 and 2014, "the Fed's balance sheet increased by more than $2.5 trillion . . . making it about five times larger than it was before the crisis").

[25] *See* Bloomberg, L.P. v. Board of Governors of the Federal Reserve System, 601 F.3d 143 (2d Cir. 2010), *archived at* https://perma.cc/VE5C-AFFG.

[26] *See generally*, Bob Ivry, Bradley Keoun & Phil Kuntz, *Secret Fed Loans Gave Banks $13 Billion Undisclosed to Congress* (Nov. 27, 2011), Bloomberg Markets,

$16.115 Trillion (GAO),[27] and $29 Trillion (Levy Economics Institute).[28] As researcher James Felkerson put it, "in an attempt to stabilize financial markets . . . the Fed engaged in loans, guarantees, and outright purchases of financial assets that were not only unprecedented (and of questionable legality), but cumulatively amounted to over twice [the] current U.S. gross domestic product."[29]

Sadly, this unprecedented level of U.S. government and central bank intervention has not improved economic conditions as much as policymakers hoped. Nearly seven years into the "recovery" and economic data for 2016 continues to indicate lackluster growth in the U.S. economy.[30] Couple this with the extraordinary amount of U.S. national debt totaling over $19.5 Trillion as of September 2016,[31] and things are not looking so bright in a time where the Great Recession is supposedly behind us. To make matters worse, the structural integrity of our monetary, banking, and financial system has actually become more precarious since the 2007-2009 crisis[32] and there is talk of another crisis looming.[33]

---

http://www.bloomberg.com/news/articles/2011-11-28/secret-fed-loans-undisclosed-to-congress-gave-banks-13-billion-in-income, *archived at* https://perma.cc/ADQ7-FHZD.

[27] U.S. Gov't Accountability Office, *Federal Reserve System: Opportunities Exist to Strengthen Policies and Processes for Managing Emergency Assistance* (July 2011), http://www.gao.gov/new.items/d11696.pdf, *archived at* https://perma.cc/5Y72-JT6M at 131 (showing that the largest financial institutions borrowed over $16 trillion from the Fed between Dec. 2007 and July 2010).

[28] *See generally*, James Felkerson, *$29,000,000,000,000: A Detailed Look at the Fed's Bailout by Funding Facility and Recipient* (Dec. 2011), Levy Economics Institute, *available at* http://www.levyinstitute.org/publications/29000000000000-a-detailed-look-at-the-feds-bailout-by-funding-facility-and-recipient, *archived at* https://perma.cc/PB8V-QDNH.

[29] *Id*. at 2.

[30] *See*, *e.g.*, Jeffrey Sparshott, *U.S. Growth Starts Year in Familiar Rut* (April 28, 2016), Wall St. Journal, http://www.wsj.com/articles/u-s-first-quarter-gdp-advances-at-0-5-pace-1461846715, *archived at* https://perma.cc/53TP-D3ZQ.

[31] U.S. Dep't of Treasury, *Monthly Statement of the Public Debt of the United States* (Sept. 30, 2016), http://www.treasurydirect.gov/govt/reports/pd/mspd/2016/opds092016.pdf.

[32] See Int'l Monetary Fund, *Stengthening the International Monetary System – A Stocktaking* at 1 (March 2016), https://www.imf.org/external/np/pp/eng/2016/022216b.pdf, *archived at* https://perma.cc/SF85-4ZNV (noting that since the 2007-2008 crisis, "financial cycles [have been] growing in amplitude and duration, capital flows have become more volatile, and nonbanks have gained importance, [which are further] altering [and increasing] the nature of systemic risk").

[33] *See*, *e.g.*, Larry Elliot, *IMF warns of fresh financial crisis* (April 13, 2016), The Guardian, *https://www.theguardian.com/business/2016/apr/13/imf-warns-fresh-financial-crisis-global-stability-report-eurozone-banks*, *archived at* https://perma.cc/3UXD-FNU2.

Naturally, such extraordinary action by governments and central banks has had its fair share of critics.[34] The rapidly increasing national debt, coupled with the Federal Reserve's continued monetary expansion, has lead some to predict that hyperinflation is just around the corner.[35] Correspondingly, some have advocated for an end of the current fiat monetary system and a return to the gold standard; still others have called for a complete use of only gold and silver as legal tender.[36] While such critics have advocated varying and sometimes conflicting views, most have come to recognize at least two things: (1) that our current system is broken, and (2) that we need a new form of currency.

2.3. The System is Broken

> *The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.*[37]
>
> – Satoshi Nakamoto, Inventor of Bitcoin, February 11, 2009.

---

[34] Concerns over "moral hazard" notwithstanding, opposition to any bailout was widespread. For example, it was not until the stock market plunged after Congress' initial rejection of the rescue package that it would get passed a mere five days later. *See generally*, Carl Hulse & David M. Herszenhorn, *House Rejects Bailout Package, 228-205; Stocks Plunge* (Sept. 29, 2008), N.Y. Times, http://www.nytimes.com/2008/09/30/business/30bailout.html, *archived at* http://perma.cc/QS7D-MLEH. *See also*, David M. Herszenhorn, *Congress approves $700 billion Wall Street bailout* (Oct. 3, 2008), N.Y. Times, http://www.nytimes.com/2008/10/03/business/worldbusiness/03iht-bailout.4.16679355.html, *archived at* http://perma.cc/83WN-SZQY.

[35] *See e.g.*, Mike Patton, *Is U.S. Hyperinflation Imminent?* (Apr. 28, 2014), Forbes, http://www.forbes.com/sites/mikepatton/2014/04/28/is-u-s-hyperinflation-imminent/, *archived at* https://perma.cc/C5N6-N57C?type=pdf (reporting that Marc Faber – renowned economist who accurately predicted, *inter alia*, the 1987 stock crash, rise of oil and precious metal in 2000's, and the market correction in 2007 – is now predicting "hyperinflation in the U.S. is a certainty within the next 10 years").

[36] Kelsey L. Penrose, *Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 N.C. Banking Inst. 529, 530 (2014), *available at* http://www.law.unc.edu/journals/ncbank/volumes/volume18/citation-18-nc-banking-inst-2014/banking-on-bitcoin-applying-antimoney-laundering-and-mon ey-transmitter-laws/, *archived at* https://perma.cc/P2QV-ZUWM?type=pdf.

[37] Satoshi Nakamoto, *Bitcoin open source implementation of P2P currency*, P2P Foundation: The Foundation for Peer to Peer Alternatives (Feb. 11, 2009, 22:27), http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source, *archived at* http://perma.cc/299Z-ZRSQ [hereinafter *Nakamoto P2P Post*].

If we have learned anything since the global financial crisis of 2007-2009, it is that the foundational underpinnings of our current banking and financial system are much more fragile than previously thought. Similarly, we have come to recognize the precarious nature of our fiat monetary system and the economic disarray that results from central-bank manipulation of currencies and interest rates.

We have witnessed the system enable institutions to take excessive risk via securitization and leverage. We have seen how this enablement results in market distortions and the creation of huge bubbles. Furthermore, we have seen the disastrous consequences of these bubbles and how, when things go wrong, the very institutions that cause them are often given legal protections and government bailouts.

In short, for those who look seriously into the matter, our monetary, banking, and financial system is, in many ways, fundamentally broken. We posit that this sad state of affairs flows from the following deficiencies:

1. Our use of fiat currency, in that it provides no inherent check on the ability of central-banks and governments to manipulate the value of the currency and debase it at will.
2. The extraordinary power given to banks in their ability to control access to money, credit, and financial exchange.
3. A regulatory and political environment that allows and encourages the centralization of power and enables banks and financial institutions to intermingle and exert undue control and influence over how the monetary, banking, and financial system is structured and operates (essentially, "the fox watching the hen house").[38]

Satoshi Nakamoto seems to have been aware of these deficiencies and can arguably be said to have created Bitcoin in response. Instead of fiat-currency – which is

[38] In the United States this can largely be traced to an erosion of the power and effect of the Glass-Steagall Act since its passage in 1933. *See generally*, Julia Maues, *Banking Act of 1933, commonly called Glass-Steagall*, Federal Reserve Bank of St. Louis, http://www.federalreservehistory.org/Events/DetailView/25, *archived at* https://perma.cc/RZB5-T78K (providing an overview and explaination for the purpose of Glass-Steagall). *See generally also*, Kathy Czyrnik, *The decline of Glass-Steagall: Deregulation and its impact on financial institutions* (Jan. 2001), *available at* http://digitalcommons.uconn.edu/dissertations/AAI3004839/, & https://www.researchgate.net/publication/27404995/, (examining how deregulation and the decline of Glass-Steagall has led to a greater concentration of financial power, whereby large institutional players are able to make exceeding profits in comparison to smaller counterparts).

often manipulated and debased – the rules governing bitcoin's supply would be deterministically hard-wired. Whereas the current system gives exorbitant power to banks to control how, when, and where we can access and transfer our money, Bitcoin provides a decentralized peer-to-peer solution via the blockchain that enables financial transactions to occur without a trusted intermediary. Instead of an oligopoly of central banks and financial institutions creating the rules of the system, Bitcoin would be an "anarcho-democratic" hybrid – no official Bitcoin organization would exist,[39] anyone could propose changes through Bitcoin's open-source development, and any proposed changes would take effect after receiving 51% of miner-approval (i.e. a majority of bitcoin miners installing the proposed code).

In late-2008, just when the American people and the rest of the world were beginning to come to grips with the sad state of affairs of our current monetary, banking, and financial system, Nakamoto had already been hard at work creating this alternative. It would be a monetary system for the 21st Century, using the Internet as its backbone to process transactions. It would be unveiled just one month after President Bush's Address to the Nation on the Financial Crisis, and the timing could not have been more perfect.

2.4. Bitcoin is Unveiled to the World[40]

> *Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments . . . [which] increases transaction costs . . . A certain percentage of fraud is accepted as unavoidable . . . What is needed is 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 for a trusted third party.*[41]
>
> – Shatoshi Nakamoto, Inventor of Bitcoin

[39] While taking note of the Bitcoin Foundation (more information available at http://bitcoinfoundation.org/about-us/), it is not an official organization, but a self-appointed body.

[40] To receive a deeper understanding of Bitcoin's development and history in the form of a user-friendly interactive timeline, visit http://historyofbitcoin.org.

[41] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 1 (2008), https://bitcoin.org/bitcoin.pdf, *archived at* https://perma.cc/2PJ3-8UN9?type=pdf [hereinafter *Bitcoin White Paper*].

As the global financial system deteriorated into a panic[42] and the American people's confidence in the banking system approached an all-time low,[43] Bitcoin was announced to the world on Halloween, 2008.[44] The inventor of Bitcoin, an unknown person (or persons) using the pseudonym Satoshi Nakamoto,[45] posted on the Cryptography Mailing List hosted by metzdowd.com, "I have been working on a new electronic cash system [since 2007][46] that's fully peer-to-peer, with no [need for an intermediate] trusted third party."[47] Nakamoto further described the invention as "a purely peer-to-peer version of electronic cash [which] would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution."[48] Nakamoto called it Bitcoin.[49]

Bitcoin is truly a revolutionary technology. With Bitcoin's arrival in late-2008, for the first time in history one could conduct financial transactions across the globe without the need of a trusted intermediate third party.[50] Bitcoin does this by solving what is referred to as the "double-spending problem".[51] The basic issue is that, unlike physical assets, data

---

[42] *See, e.g.*, Nick Mathiason, *Three weeks that changed the world: It started in a mood of eerie calm, but then 2008 exploded into a global financial earthquake* (Dec. 27, 2008), The Guardian, http://www.theguardian.com/business/2008/dec/28/markets-credit-crunch-banking-2008, *archived at* http://perma.cc/9QST-2Y2J.

[43] *See generally*, Dennis Jacobe, *Americans' Confidence in Banks Up for First Time in Years* (June 14, 2013), Gallup, http://www.gallup.com/poll/163073/americans-confidence-banks-first-time-years.aspx, *archived at* https://perma.cc/3G48-N3XF?type=pdf.

[44] Satoshi Nakamoto, *Bitcoin P2P e-cash paper*, The Cryptography and Cryptography Policy Mailing List (Oct. 31, 2008, 14:10 EDT), http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html, *archived at* https://perma.cc/PY3G-XUJP?type=source [hereinafter *Nakamoto Metzdowd Post*].

[45] Though there has been much speculation about who Satoshi Nakamoto is (or was), no definitive answers have been provided and Nakamoto's identity remains unknown. *See generally*, CoinDesk, *Who is Satoshi Nakamoto?* (Mar. 28, 2015), http://www.coindesk.com/information/who-is-satoshi-nakamoto/, *archived at* https://perma.cc/8BVE-G37T?type=source.

[46] Satoshi Nakamoto, *Bitcoin Forum Post #5* (June 18, 2010 04:17PM), bitcointalk.org, https://bitcointalk.org/index.php?topic=195.msg1617#msg1617 *archived at* https://perma.cc/3AKD-FRVM?type=source (Nakamoto, replying to the question, "How long have you been working on this [Bitcoin] design?", "Since 2007.")

[47] *Nakamoto Metzdowd Post*, *supra* note 44.

[48] *Id*.

[49] *Bitcoin White Paper*, *supra* note 41 at 1.

[50] Jerry Brito & Andrea Castillo, Mercatus Ctr. at George Mason Univ., *Bitcoin: A Primer for Policy Makers* 3 (2013), http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf, *archived at* https://perma.cc/8TJL-C5UD?type=pdf. *See also*, *Bitcoin White Paper*, *supra* note 41 at 8.

[51] *See Bitcoin White Paper*, *supra* note 41 at 2.

can be easily duplicated. Within the context of electronic financial transactions, this means that unless some mechanism exists to prevent it, a self-interested party can copy a digital token (representing a form of electronic money) and send it to multiple parties without the receiving parties knowing the token is being "double-spent". Before Bitcoin, the solution to this problem was to use what essentially equates to being a centralized ledger system, wherein a "bank" or financial intermediary controls the flow of transactions, verifying that digital tokens are not being double-spent before allowing them to go through.[52]

The ingenious solution that Bitcoin provides is the use of a decentralized electronic peer-to-peer network which timestamps and logs the transaction of digits ("bitcoin") on an open ledger system ("blockchain") via an algorithmically designed consensus mechanism using cryptographic proof-of-work. No longer requiring a financial intermediary to process transactions, the arrival of Bitcoin introduced two concepts: (1) the blockchain, which acts as a decentralized ledger, logging the flow of transactions from one account to another, and (2) the idea of bitcoin[53] (the digits being transacted), which provides a new form of digital money that is independent of existing governments and institutions. This is an astounding achievement.

Free from the grips of central-banks and financial institutions, Bitcoin appeared to provide a possible solution to the inherent flaws of fiat currency and the monetary, banking, and financial system. Not surprisingly, many critics of the current system became ardent Bitcoin and cryptocurrency enthusiasts (ourselves included). However, Bitcoin and other cryptocurrencies ("cryptos") have not turned out as hoped.

Ironically, the answers that Bitcoin provides to the weaknesses of our monetary, banking, and financial system have introduced new weaknesses of their own. In response to the problem of fiat-currency, which can be easily created and thereby debased, Bitcoin

---

[52] *See*, *e.g.*, Mark Dermot Ryan, *Digital Cash* (2006, *estimated date*), http://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/, *archived at* https://perma.cc/3XFH-UDYK.

[53] By convention, lower-case "b" (for bitcoin) is used to refer to the transactional unit of account, whereas upper-case "B" (for Bitcoin) is used to refer to the Bitcoin network or the Bitcoin system as a whole. *See e.g.*, *Correct use of the word Bitcoin?*, http://bitcoin.stackexchange.com/questions/20901/correct-use-of-the-word-bitcoin, *archived at* https://perma.cc/NDE2-EAFN.

has a limited and deterministic supply. However, this has resulted in high price volatility. Whereas the blockchain enables bitcoin to be transacted without an intermediary, it also makes every transaction publicly available, resulting in essentially no transactional privacy. Instead of an oligopoly of central banks and powerful financial institutions creating the rules of the system, Bitcoin's attempt at "anarcho-democracy" has led to an "oligopoly" of lead developers and control by an increasingly centralized mining industry. In short, Bitcoin and cryptos have a number of fundamental weaknesses: (1) high price volatility, (2) a lack of transactional privacy, (3) and a lack of proper governance.

3. CRYPTO WEAKNESS #1: HIGH VOLATILITY[54]

3.1. High Volatility Hinders User Adoption

Bitcoin and nearly every other crypto that exists suffers from extreme price fluctuations. A quick survey of coinmarkcap.com[55] shows this fact. While such high volatility may be beneficial to a very small minority of potential crypto users (namely speculators), it brings nothing but downsides for the great majority.

Volatility itself is a measure of uncertainty and an indicator of risk. The more volatile an asset is, the greater the amount of risk one accepts by holding on to it. In the same way, high volatility is an impediment to planning. When a currency is highly volatile it is impossible to determine the future cost of anything within a range of certainty. This means that when certain cash flows are needed, holding onto a volatile asset for a future date (versus transferring it into a more stable asset now) means a greater chance of shortfall. To make matters worse, the amount of risk this entails expands exponentially the further into the future one is planning.

For most, this kind of risk and uncertainty automatically creates psychological discomfort and stress. When compared to fiat, this puts cryptos in a peculiar disadvantage. In short, not only does cryptos' high volatility result in less utility by requiring more work and planning to mitigate potential shortfalls, it also turns away potential users.

Bitcoin and cryptos high volatility turns away the average user.

The average person is wary to use something as a monetary unit that rapidly changes in its marketable value, let alone something that fluctuates as wildly and unpredictably as cryptos. History and anecdotal evidence indicates this. When presented

[54] Some have advocated that Bitcoin's high volatility (speaking nothing of other cryptos) is just a temporary phenomenon to be worked out. *See e.g.*, Timothy B. Lee, *These four charts suggest that Bitcoin will stabilize in the future* (Feb. 3, 2014), Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2014/02/03/these-four-charts-suggest-that-bitcoin-will-stabilize-in-the-future/, *archived at* https://perma.cc/9XG3-XUAR. Essentially the theory is that as Bitcoin gains further acceptance, a certain level of price stability will be achieved. However, we argue that it is not a lack of acceptance that results in bitcoin and other cryptos volatility, but is in fact the opposite.

[55] *Crypto-Currency Market Capitalizations*, located at https://coinmarketcap.com/, is arguably the foremost website for finding aggregated data from the various crypto-exchanges.

with the opportunity, people will immediately exchange a risky asset (i.e. one with high volatility) for one that is less risky (all things being equal).[56] Not surprisingly, most people are unwilling to use bitcoin or other cryptos because the alternative provided by fiat currency is simply more stable and less risky. For the average person who may try cryptos, they are often only holding small amounts as a novelty item, or merely as a curiosity to be experimented with.

Bitcoin and cryptos high volatility turns away merchants.

The daily price swings of bitcoin and other cryptos make any merchant who uses them vulnerable to potentially huge losses. Rather than opening themselves to such risk, most merchants will simply not accept cryptos. However, for those few merchants who may be willing to accept them, the great majority will simply transfer their cryptos into fiat as quickly as they are received.

Most merchants are interested in operating their business and making a profit, not dabbling in the fields of speculative investment or currency exchange. As a result, those merchants who do accept cryptos are likely either: (a) crypto enthusiasts themselves, or (b) accepting cryptos merely as a way to gain potential customers. Other than (b), cryptos are essentially disadvantageous for a merchant, in that they simply add an additional layer of transaction costs and complexity in processing orders.

In short, most merchants do not want to deal with the additional level of risk, transaction cost, and complexity, that accepting cryptos entails. The end result is that few merchants are willing to accept bitcoin or other cryptos as a form of payment. This only acts as a further hindrance to general user adoption of cryptos, as they are accepted in only a limited number of places.[57]

---

[56] This is similar to the economic principle known as Gresham's law. *See generally* Wikipedia, *Gresham's law*, https://en.wikipedia.org/wiki/Gresham%27s_law, *archived at* https://perma.cc/835N-FUNH.

[57] While we are aware of the existence of third-party processors (such as BitPay) that enable one to spend bitcoin more or less like using a credit card through integrating the infrastructure of credit card systems with bitcoin debit accounts, this still requires trusting a third party, which is contrary to the purpose of Bitcoin.

Bitcoin and cryptos high volatility turns away investors.

By investor (as opposed to “speculator”, or “speculative investor”), we are referring to someone seeking a moderate return on their investment based upon a reasonable expectation it will rise in value, or at least maintain its purchasing power, over the long term. Such a person is willing to accept some reasonable and moderate risk, but is generally wishing to avoid the potential of sizeable losses on their principle investment. Naturally, the high volatility we see in bitcoin and other cryptos is contrarian to these goals, causing potential investors to stay away. This only further hinders cryptos’ adoption as investable vehicles and thereby their overall marketable value.

Bitcoin and cryptos high volatility is only good for speculators.

High volatility is really only beneficial for one particular type of crypto user – speculators. With high volatility, there is the potential for high profits. This gives speculators (who are willing and able to stomach the greater risk) the opportunity to make larger profits by buying and selling at the right time within the gyrations of the market. Nevertheless, while high volatility may be beneficial for this type of crypto user, this hardly makes cryptos congenial to mass adoption. In short, unless cryptos are able to reach price stability, they will never reach the normal user and instead continue to be held by mainly niche enthusiasts, novelty collectors, and speculative investors.

3.2. High Volatility is Contrary to Cryptos Purpose

In the end, the true purpose of money is to act as a medium of exchange for the purchase of goods and services. While bitcoin and cryptos inherently have this ability, in that they represent some kind of value and can be readily transferred, the fact is that their high volatility effectively results in nearly every purchase using some sort of third-party payment processor. This is true for both the merchant who accepts cryptos and then exchanges them immediately into fiat (to avoid the risk that cryptos’ high volatility entails), and also for the user who converts their cryptos into fiat to make a purchase at places that

do not accept cryptos (in part because of their high volatility). This is hardly an ideal situation.

One of the primary goals of Bitcoin is to enable financial transactions without the need of an intermediary. Technically, Bitcoin succeeds in this goal. However, because bitcoin and other cryptos experience such high volatility, the end result is that nearly every purchase of a good or service that involves a crypto includes a third-party payment processor at some point in the transaction. In a system designed for the purpose of avoiding such financial intermediaries – as is Bitcoin (and presumably most cryptos) – this represents a problem.

In short, while one may technically transfer bitcoin and other cryptos to another without the need of a financial intermediary, normal use is quite the contrary. In fact, because bitcoin and other cryptos are so highly volatile (and therefore risky to hold onto), most purchases include the involvement of a third-party payment processor at some level of the transaction. In such a scenario, cryptos do nothing more than add an additional layer of cost and complexity to transactions, while also arguably negating their very reason for existence in the first place.

3.3. High Volatility is Inherent to Cryptos Current Design

> *Cryptocurrencies like Bitcoin govern the supply of coin through simple and deterministic coin supply rules . . . This is a significant departure from even pure commodity money systems, as the supply of a precious metal is responsive to price changes that cross the marginal cost of pulling the stuff out of the ground. If a cryptocurrency system aims to be a general medium-of-exchange, deterministic coin supply is a bug rather than a feature.*
>
> – Robert Sams [58]

Ironically enough, Nakamoto recognized how important it is for money to maintain its value. Indeed, this was one of the chief criticisms Nakamoto expressed over the

[58] Robert Sams, *A Note on Cryptocurrency Stabilisation: Seignorage Shares* at 1 (Apr. 28, 2015), *available at* https://github.com/rmsams/stablecoins *archived at* https://perma.cc/9NAE-XKDS.

fiat-monetary system around the time Bitcoin was released.[59] When it comes to maintaining value (a.k.a. purchasing power), our fiat monetary system has two major weaknesses: (1) the arbitrary power wielded by central banks in their ability to manipulate money and interest rates, and (2) the inherent problem of fiat currency, in that it provides no hard-set rules to prevent its debasement and resulting inflation. In these regards, the alternative offered by Bitcoin seemed to make sense.

Instead of the arbitrary power wielded by central banks and the inherent weakness of fiat to be easily debased, Bitcoin would have a deterministic supply and the total number of bitcoins to ever be created would be hard-wired into the Bitcoin system.[60] In doing so, Bitcoin provided the following structure:

- All newly created bitcoins are distributed to miners as remuneration for processing bitcoin transactions.
- Bitcoin transactions are processed using proof-of-work ("PoW"), requiring miners to compete using computational power to determine who processes a particular transaction on the Bitcoin network, and thereby who receives bitcoin.
- Newly created bitcoins are released approximately every 10 minutes (during each block) and distributed to the "winning" miner.
- The amount of newly created bitcoin (and thereby the amount disbursed to miners) decreases over time, halving roughly every four years, with the total supply of bitcoins capped at 21 million.[61]

This system appeared to provide two major advantages. First, Bitcoin's use of PoW mining, along with the internal mechanism of varying difficulty (which makes it harder to "win" bitcoin as the total network hashrate increases), assures that any newly created bitcoin does not come about freely, but at a cost. Second, the deterministic supply of bitcoin (while being slightly inflationary at current) guarantees that there are only a limited number of available bitcoins.[62] The theoretical result of these two mechanisms is that

---

[59] *See Nakamoto P2P Post*, *supra* note 37.

[60] It is important to note that, other than a few exceptions (addressed in Sections 3.4 and 3.5), every single crypto that currently exists works in this manner.

[61] Bitcoin.org, *FAQ: How are bitcoins created?*, https://bitcoin.org/en/faq#how-are-bitcoins-created, *archived at* https://perma.cc/RVZ4-CVYG.

[62] *See*, *e.g.*, *Projected Bitcoins Long Term*, https://en.bitcoin.it/wiki/Controlled_supply#Projected_Bitcoins_Long_Term, *archived at* https://perma.cc/SCA6-74H8 (showing the estimated release schedule of bitcoin over time).

bitcoin maintains value, based largely upon the unspoken premise that miners will not sell bitcoins for less than it actually costs to produce them.[63]

At first, this seemed to make sense. The value of bitcoin would be based upon the amount of work put into the system and the supply of bitcoin could not be expanded upon on a whim (as appears to be the case with fiat). However, as it turns out, this does nothing to help bitcoin maintain a certain price point. In other words, while Bitcoin's PoW distribution system and deterministic supply schedule encourages bitcoin to maintain some kind of value (whether that value be equivalent to one cent or a thousand dollars is left for the market to continuously find out), it fails to encourage bitcoin's price to remain stable. In fact, the deterministic supply of bitcoin (and similar cryptos) is instrumental in creating the very volatility we are witnessing.

In any normally functioning market, the traditional rules of supply and demand apply. In short, (all things being equal) at any point when the price for a good or service rises, demand for that good or service will go down and supply will go up, and vice-versa. This can be explained to occur for the following reasons:

First, on the demand side, as the price for a good or service rises, certain participants will be unable to afford the higher price and thereby be forced out of the market. This has the effect of decreasing demand. When price decreases, the opposite happens and new market participants are now able to afford the good or service, thereby increasing demand.

Second, on the supply side, when the price of a good or service rises, those who provide the good or service are incentivized to produce more, thereby increasing supply. If price decreases, those providing the good or service are incentivized to produce less (or not as much), leading to a decrease in supply through normal consumption.

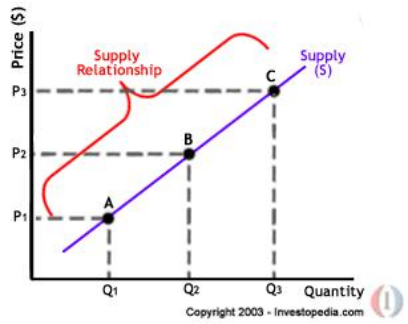
---

[63] In many respects, this premise is similar to the disreputed *labor theory of value*, which erroneously argues that the price for a good or service is determined by the amount of labor put into producing it, rather than the actual utility that the good or service provides. For a general understanding of why this theory and its modern proponents are incorrect in describing price formation (the goal of any economic theory of value), *see generally*, Robert P. Murphy, *The Labor Theory of Value: A Critique of Carson's Studies in Mutualist Political Economy*, Vol. 20 No. 1 Journal of Libertarian Studies, 17-33 (Winter 2006) *available at* https://www.mises.org/library/labor-theory-value-critique-carsons-studies-mutualist-political-economy, *archived at* https://perma.cc/BF3V-B2KW.

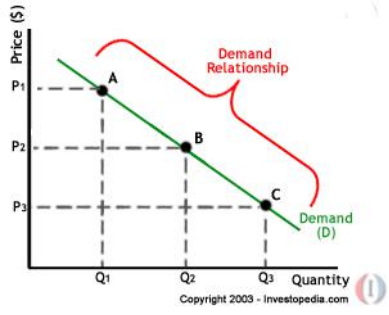
Third, for both those on the demand side and those on the supply side, every purchase or provision of a good or service brings with it a certain opportunity cost. For those making a purchase, this would be the loss of what one could otherwise have spent their money on. For those providing a good or service, this would be what they could have otherwise invested their money, labors, and time on. Resultantly, as the price for a particular good or service rises, demand decreases because people would rather spend their money on something else they value more. Similarly, supply will increase because the opportunity cost is now less (i.e. a better investment of time and resources) for those providing the good or service.

This effect that price has upon supply and demand is illustrated in the following two charts:

Example of an increasing supply relationship[64]

	Points A, B, and C represent the quantity of a good or service supplied at any given price point. As price goes up, so does supply (Point C); as price goes down, supply also goes down (Point A).

Example of a decreasing demand relationship[65]

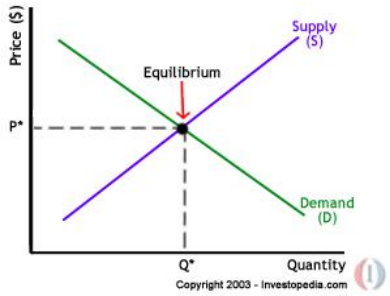
	Points A, B, and C represent the quantity of a good or service demanded at any given price point. As price goes up, demand goes down (Point C); as price goes down, demand goes up (Point A).

[64] Reem Heakal, *Economics Basics: Supply and Demand*, Investopedia, http://www.investopedia.com/university/economics/economics3.asp, *archived at* https://perma.cc/AJS4-MQ5E.

[65] *Id.*

Similar to how price affects the overall supply and demand for a good or service, supply and demand also have an influence on price. If supply is low (another way of saying that demand is high) for a good or service, this has the effect of bringing the price up as those who demand the good or service compete with each other to receive it. Similarly, if demand for a given good for service is low (another way of saying that there is too much supply), this has the effect of bringing the price down as those who provide the good or service sell off at a lower price points to maintain cash flow (or sell for other reasons). The idea of modern economics is that these competing forces of supply and demand tend to reach towards a point of equilibrium, where both meet at an agreed upon price.

Example of where demand and supply reach equilibrium[66]

	At this point, the market has reached equilibrium, where the forces of supply and demand have come to an agreeable quantity (Q*) and price (P*) for a particular good or service.

In most markets these competing forces of supply and demand tend to encourage a level of price stability (where a long-term equilibrium price is met for a particular good or service). This is because in most markets, the quantity of a good or service is able to adjust with changes in demand. For example, when demand for a product goes up (reflected by a temporary increase in price), suppliers are incentivized to ramp up manufacturing (to realize the greater profits that comes with this increase in price), thereby increasing supply. Correspondingly, when demand goes down, suppliers will respond by decreasing the quantity they produce, which eventually leads to a decrease in supply through normal consumption.

In normally functioning markets, this has a tendency to bring about a natural "leveling" of price. When demand for a product goes up (as reflected by a temporary

[66] *Id.*

increase in price), supply will also go up, which tends to bring the price back down. Similarly, when demand goes down (as reflected by a temporary decrease in price), supply will go down, leading the price to go back up. In this way, the forces of supply and demand act as a sort of "yin-and-yang", continuously countervailing each other to reach the most efficient price point, resulting in a tendency to keep the price of the underlying good or service stable.

Nearly every market that exists operates in this fashion,[67] where the supply of a goods or services adjusts in some way to changes in demand. This even occurs in the gold market (which Bitcoin is often erroneously compared to),[68] where the marginal increase in the supply of gold is responsive to changes in its demand (as reflected by changes in price). However, unlike nearly every other market, the supply Bitcoin (while currently inflationary in the order of around 10%)[69] is inelastic and deterministic. In other words, unlike normal markets, where supply is able to adjust in response to demand (thereby encouraging some level of price stability), the supply of bitcoin is unable to do so.

In the chart copied below, Robert Sams shows that the deterministic supply model currently utilized by Bitcoin and other cryptos is the primary reason for why they are so highly volatile. To summarize, because the supply of bitcoin and other cryptos is inelastic and cannot adjust according to fluctuations in demand, any change in demand directly reflects upon the cryptos' price. This is the root cause of bitcoin and cryptos' high volatility, indicating a fundamental weakness and one of the primary reasons that Bitcoin and cryptos have yet to receive mass adoption.

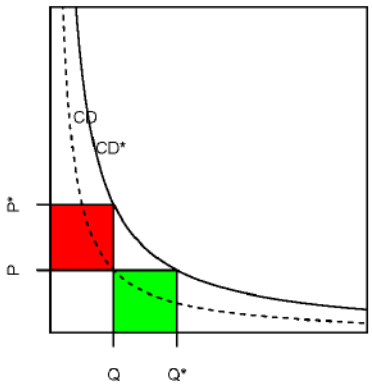
---

[67] In fact, the only exception we can think of are items such as rare collectibles.

[68] *See*, *e.g.*, Ari Levi, *Bitcoin gains validity as digital gold after Brexit vote* (June 27, 2016), CNBC, http://www.cnbc.com/2016/06/27/bitcoin-gains-validity-as-digital-gold-after-brexit-vote.html, *archived at* https://perma.cc/XT34-SBNE (quoting a venture capitalist that "Bitcoin is effectively becoming digital gold").

[69] Chart of Bitcoin inherent inflation rate, https://www.reddit.com/r/Bitcoin/comments/1s3buc/chart_of_bitcoin_inherent_inflation_rate_til_it/, *archived at* https://perma.cc/N23W-CJKE (indicating that bitcoin's inflation rate as of 2016 is around 10%)

Crypto Supply and Demand[70]

	Crypto demand ("CD", dashed line) represents demand for a crypto at a given time at price ("P") with quantity ("Q") being supplied. In deterministic supply cryptos, such as bitcoin, when CD shifts to CD*, P shifts to P* (because Q is "fixed" and unable to adjust relative to price). In such a system, price is simply a proxy for demand, indicating that bitcoin and other cryptos' deterministic supply inherently leads to high volatility. In normally functioning markets, when CD shifts to CD*, Q has a tendency to shift relative to CD* towards Q*. In this way, price stability may be achieved.

If a crypto is going to be adopted by the masses, its price must remain stable. As shown, this necessitates the ability of a crypto to adjust its supply according to changes in demand. In other words, if demand goes up (as reflected by a temporary increase in price), then the supply of that crypto should rise proportional to meeting demand, thereby causing the price to correct back to what it was before. Similarly for vice-versa. The problem is that the current design of Bitcoin and cryptos inherently makes this impossible.

Instead, what is needed is a new crypto that uses a built-in elastic supply model that utilizes automated mechanisms to adjust the supply of the crypto according to changes in demand. While no such crypto yet exists, there are a few cryptos attempting to achieve price stability in different ways. In the next two sections we review the current models those few cryptos use and problems with the solutions they offer.

3.4. Cryptos Current Attempts at Price Stability

[THIS SECTION IS CURRENTLY BEING WORKED ON]

3.5. Problems with Current Price Stabilizing Cryptos

[THIS SECTION IS CURRENTLY BEING WORKED ON]

[70] Chart taken from Robert Sams, *supra* note 58 at 2.

4. CRYPTO WEAKNESS #2: LACK OF PRIVACY[71]

4.1. Cryptos Open Blockchain Hinders Privacy

> *Bitcoin is often perceived as an anonymous payment network. But in reality, Bitcoin is probably the most transparent payment network in the world.*[72]
>
> – Bitcoin.org

Contrary to popular opinion,[73] bitcoin transactions are not anonymous, nor are they private.[74] At best, these transactions may be described as pseudonymous. However, pseudonymity hardly means privacy. Ironically, it is the open blockchain – the very system that enables Bitcoin and other cryptos to act as decentralized payment systems – which creates this unique problem.

As explained in Section 2.4, when miners are processing bitcoin transactions they are recording them via an algorithmically designed consensus mechanism (called hashing) onto a distributed public ledger (the blockchain). The blockchain acts much like an accountant's logbook, where one can to trace the flow of transactions going from one account to another throughout different periods in time. This is how Bitcoin and other cryptos are able to achieve decentralized consensus in how much coin each account has, simply by adding the credits and debits for each user's crypto address.

The weakness of Bitcoin and other cryptos is that, unlike the accountant's logbook whose information is typically private and confidential, the blockchain is completely public and available for all to see. Similarly, where it is reasonable to assume that at some point

---

[71] We take it as axiomatic that privacy, in general, and financial privacy, in particular, are important and necessary. For an interesting discussion on why privacy matters, *see generally* Julie E. Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904 (2013), *available at* http://harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf, *archived at* https://perma.cc/68W3-GVCF.

[72] Bitcoin.org, *Protect your privacy*, https://bitcoin.org/en/protect-your-privacy, *archived at* https://perma.cc/PFV9-BEV4.

[73] *See*, *e.g.*, WikiLeaks, *Donate to WikiLeaks*, https://shop.wikileaks.org/donate, *archived at* https://perma.cc/CU5S-4R9P, (*stating* "Bitcoin is a secure and anonymous digital currency.").

[74] While this section mainly discusses Bitcoin, please note that besides the few exceptions discussed in Sections 4.4 and 4.5, the same applies for every other crypto that currently exists.

an accountant's logbook and its contents will be destroyed or lost in time (which is good for privacy), this will never occur with the blockchain.[75] In short, every transaction that takes place within Bitcoin is logged forever on the blockchain and available for any member of the public to review.

By having an open blockchain, Bitcoin and other cryptos make available a host of information that can be easily data mined. For example, within every bitcoin or crypto transaction, one can easily locate the sender's and receiver's crypto addresses, the amount transacted, and the approximate time of when the transaction took place.[76] This poses a significant threat to transactional privacy.

4.2. Cryptos Pseudonymity Provides Little Privacy

The open blockchain, as utilized by Bitcoin and other cryptos, makes every transaction that occurs on these networks publicly available. This means that, if any level of transactional privacy is to be achieved on these systems, users' crypto addresses must remain pseudonymous. Crypto addresses (in themselves) do not contain any personally identifying information and comprise of nothing more than a unique string of randomly generated letters and numbers, used for sending and receiving payments.[77] The problem is that once a user's identity is linked to a particular crypto address, then every transaction associated with that address, including the user's entire balance, payment, and receipt history are fully known. In other words, compared to the traditional banking system, using bitcoin or other cryptos is like having the entirety of one's bank records publicly posted on the Internet with every transaction updated in real-time. In such a scenario, the only way of maintaining financial privacy is the hope that no one is ever able to link one's bank account number to the owner's identity (information divulged nearly every time a transaction occurs). This is hardly privacy.

The whole point of a currency is to act as as a medium of exchange (i.e. to be transacted). One cannot do this with Bitcoin or any other crypto unless their is a known

[75] Given the distributed nature of the blockchain, it would be practically impossible to do so.
[76] See, e.g., http://www.blockchain.info (showing the blockchain for Bitcoin).
[77] Example of a bitcoin crypto address: 1BSrAt2esgwmqKe9RiK3a89bCg9RuDpT3r

recipient crypto address to send a transaction to. Naturally, those who accept Bitcoin and other cryptos as a form of payment post their crypto addresses on public forums and websites. The problem is that, once this occurs, pseudonymity may be already broken. The posted crypto address is now obviously associated with that person's username, and "passive analysis of multi-input transaction can possibly reveal other keys [crypto addresses] associated with that user. Even if users do not publish their keys [crypto addresses] in this way, some association may be released if a user takes advantage of services or stores that accept bitcoins" or other cryptos.[78]

Once a user interacts with a store or service that accepts cryptos, those transactions are easily identifiable on the blockchain. For an adversary wishing to identify the user, this information provided by the open blockchain now provides an attack vector for obtaining that user's information. For example, "one can imagine a scenario where some law enforcement agency might want to investigate a user . . . [where] we can determine a group of addresses that belong to the user, and if any of those addresses interacted with a Bitcoin exchange or service, the law enforcement agency could seize the personal information of the user from such a service. Even further, we can see all the addresses with which a user interacted, which could implicated other users."[79]

Those within the Bitcoin community are aware of these issues and provide two general recommendations for uses attempting to maintain pseudonymity and therefore transactional privacy.[80] The first recommendation is that "Bitcoin addresses should only be used once and users must be careful not to disclose their addresses."[81] The hope is that doing this will prevent traceability – the practice of tracing the linkage of transactions within the blockchain, enabling one to identify owners of crypto addresses, their interactions with others on the blockchain, and a host of other information. The second recommendation is

[78] Liam Morris, *Anonymity Analysis of Cryptocurrencies*, Rochester Institute of Technology, 21 (April 20, 2015), *available at* http://scholarworks.rit.edu/theses/8616/, *archived at* https://perma.cc/W5EP-G8AS.

[79] *Id*. at 23.

[80] *See generally*, Bitcoin.org, *Protect your privacy*, *supra* note 72.

[81] *Id*. Nakamoto was also aware of this problem and provided similar advice. *See Bitcoin Whitepaper*, *supra* note 45 at 6.

to use the anonymizing Tor service[82] because Bitcoin is "a peer-to-peer network [and] it is possible to listen for [user's] transactions' relays and log their IP addresses."[83] The hope is that using Tor will obfuscate users true IP addresses (which can otherwise be used to reveal a user's identity). Sadly, as shown in the next section, these recommendations are neither practical nor useful.

4.3. Cryptos Privacy is Broken

> *Bitcoin is often promoted as a tool for privacy but the only privacy that exists in Bitcoin comes from pseudonymous addresses which are fragile and easily compromised through reuse, "taint" analysis, tracking payments, IP address monitoring nodes, web-spidering, and many other mechanisms. Once broken this privacy is difficult and sometimes costly to recover.*[84]
>
> – Gregory Maxwell, Inventor of CoinJoin

One of the primary ways that Bitcoin and crypto users attempt to maintain transactional privacy is by using a new crypto address for every transaction. The idea is that doing so will obfuscate ownership of crypto addresses and aid in maintaining pseudonymity by having one's financial transactions spread out over a web of multiple, seemingly unrelated, accounts. However, an increasing body of research is accumulating where, despite such attempts, investigators are able to apply data heuristics and statistical modeling to blockchain analysis, enabling them to identify common ownership of these addresses.[85] Researchers Koshy, Koshy, and McDaniel also show that by using similar techniques, along with direct monitoring of Bitcoin network traffic, one can readily identify

[82] *f*, note 72 (recommending to Bitcoin users "you might want to consider hiding your computer's IP address with a tool like Tor so that it cannot be logged"). For more information about Tor and a basic overview of how it works, *see* https://www.torproject.org/about/overview.html.en.

[83] Bitcoin.org, *Protect your privacy*, *supra* note 72.

[84] Gregory Maxwell, *supra* note 7.

[85] *See*, *e.g.*, Sarah Meiklejohn *et al*., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names* (Dec. 2013), http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf, *archived at* https://perma.cc/9H6F-GG39 ("using heuristic clustering to group Bitcoin wallets based on evidence of shared authority, and then using re-identification attacks (i.e., empirical purchasing of goods and services) to classify the operators of those clusters)" *quote* at 1).

owners of multiple bitcoin addresses all the way down to their IP addresses.[86] Similarly, Researchers Biryukov, Khovratovich, and Pustogarov present "an efficient method to deanonymize Bitcoin users . . . [by] link[ing] user pseudonyms [bitcoin addresses] to the IP addresses where the transactions are generated."[87] Alarmingly, they show that if fully deployed at an estimated cost of less than 1500 EUR per month, such methods would produce "deanonymization rates up to 60%" of the entire Bitcoin network.[88]

To thwart being identified in such a manner, more privacy conscious crypto users use Tor for the purpose of hiding their IP address. However, using a real-life attack, Biryukov and Pustogarov show that "combining Tor and Bitcoin creates an attack vector for the [use of] deterministic and stealthy man-in-the-middle attacks" in which "using Bitcoin through Tor not only provides limited level[s] of anonymity but also exposes the user" to significant security risks.[89] They show that, at an estimated cost of less than 2500 USD a month,[90] "a low-resource attacker can gain full control of [the] information flows between all users who chose to use Bitcoin over Tor . . . [enabling them to] link together user's transactions regardless of pseudonyms [crypto addresses] used . . . and [to create] a totally virtual Bitcoin reality . . . for such set of users. Moreover . . . an attacker can fingerprint users and then recognize them and learn their IP address when they decide to connect to the Bitcoin network directly" outside of Tor.[91] In short, combining Bitcoin and Tor not only arguably provides less privacy, but also puts users at greater risk.

A third way that crypto users attempt to maintain privacy is by using third party mixing services. These services presumably provide additional privacy protections by

---

[86] *See generally*, Koshy, Koshy, & McDaniel, *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic* (2014), *available at* https://www.semanticscholar.org/paper/An-Analysis-of-Anonymity-in-Bitcoin-Using-P2P-Koshy-Koshy/c27762257f068fdbb2ad34e8f787d8af13fac7d1, *archived at* https://perma.cc/7X4U-VZ9K (showing that by reviewing the open blockchain and monitoring live Bitcoin traffic, "heuristics for identifying ownership relationships between Bitcoin addresses and IP addresses" can be deployed, in which "addresses can be mapped to their likely owner IPs", *quote* at 1).

[87] Biryukov, Khovratovich, & Pustogarov, *Deanonymisation of clients in Bitcoin P2P network*, 1 (July 5, 2014), *available at* http://arxiv.org/abs/1405.7418, *archived at* https://perma.cc/J27R-GZ8F.

[88] *Id*. at 2.

[89] Alex Biryukov & Ivan Pustogarov, *Bitcoin over Tor isn't a good idea*, 1 (Jan. 8, 2015), *available at* http://arxiv.org/abs/1410.6079, *archived at* https://perma.cc/CL7K-QCM8.

[90] *Id*. at 2.

[91] *Id*. at 1.

mixing cryptos with multiple parties. The premise is somewhat similar to that of the idea of using a new crypto address for every transaction, in that mixing cryptos across multiple parties will make it more difficult to trace the linkage of transactions and identify the true ownership of individual crypto addresses. However, this itself presents two problems. First, this is not ideal, as it requires trusting a third party to presumably maintain privacy (something that is arguably antithetical to the purpose of Bitcoin and cryptos). Second, independent analyses indicate that these services are ineffective in providing the very privacy they purport to deliver.[92]

In summary, the open blockchain of Bitcoin and other cryptos creates a severe weakness in that every single transaction is logged and available for anyone to see. This means that the only privacy Bitcoin and other cryptos currently provide is based on pseudonymous crypto addresses, coupled with the hope that someone will never be able to link a user's crypto addresses with that person's identity. However, as researchers have shown, this is already feasible.

As time goes on and cryptos presumably become more prevalent as a means of financial exchange, the methodologies already used for successfully breaking the pseudonymity of crypto addresses and enabling one to identify and trace individual users via the open blockchain will only become more prevalent, easier to deploy, and increasingly effective. Just as how companies such as Google and Facebook are able to deduce increasingly large amounts of revealing and extremely accurate information about their users simply by analyzing multiple pieces of seemingly innocuous data,[93] one could

---

[92] *See*, *generally*, Möser, Böhme, & Breuker, *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem* (Sept. 17, 2013), https://maltemoeser.de/paper/money-laundering.pdf, *archived at* https://perma.cc/E6E3-3WWK (showing through taint analysis that the popular mixing service "BitLaundry cannot be considered to reliably increase anonymity" *quote at* 10). *See also*, *generally*, Kristov Atlas, *Advisory: Weak Privacy Guarantees for SharedCoin Mixing Service* (June 9, 2014), http://www.coinjoinsudoku.com/advisory/, *archived at* https://perma.cc/P3KT-TFDC (showing through custom-built software that conducts relationship analysis by examining "all possible combinations of inputs and outputs" that, despite being able to overcome taint analysis, the popular SharedCoin mixing service provided by Blockchain.info (essentially a CoinJoin variant) still fails to prevent identification of bitcoin owners).

[93] *See*, *e.g.*, Scott Allan Morrison, *Scary New Ways the Internet Profiles You – Facebook, Google, and the other Internet titans have ever more sophisticated and intrusive methods of mining your data, and that's just the tip of the iceberg* (Feb. 8, 2016), The Daily Beast, http://www.thedailybeast.com/articles/2016/02/08/scary-new-ways-the-internet-profiles-you.html, *archived at* https://perma.cc/7Y7P-RVV4.

do similarly with the blockchain. Many of us have heard the cautionary statement that "data never dies." There is no form of technology this saying could not apply more to than the blockchain. Within the context of the open blockchain, this means it is only a matter of time that any limited transactional privacy that may currently exist in bitcoin and cryptos is completely broken.[94]

4.4. Cryptos Attempts at Privacy Through Anonymity

[THIS SECTION IS CURRENTLY BEING WORKED ON]

4.5. Problems with Current Anonymity-Based Cryptos

[THIS SECTION IS CURRENTLY BEING WORKED ON]

[94] *See* Bitcoin.org, *Protect your privacy*, *supra* note 72 (recognizing that in regards to Bitcoin and similar cryptos, even the limited privacy they currently provide is unsustainable, "as the block chain is permanent, it's important to note that something not [easily] traceable currently may become trivial to trace in the future").

5. CRYPTO WEAKNESS #3: LACK OF GOVERNANCE

5.1. Bitcoin & Other Cryptos Lack Proper Governance

[THIS SECTION IS CURRENTLY BEING WORKED ON]

5.2. Cryptos Various Attempts at Governance

[THIS SECTION IS CURRENTLY BEING WORKED ON]

5.3. Problems with Current Alt-Governance Cryptos

[THIS SECTION IS CURRENTLY BEING WORKED ON]

6. eCOIN-eSHARES CRYPTOCURRENCY SYSTEM

The following pages provide a basic overview for the eCoin-eShares Cryptocurrency System ("eCoin System") and how it is intended to function.

6.1. Summary of eCoin System Main Features

Price Stability

- Two assets – eCoin and eShares. eCoin will be the intended currency, while eShares will be the investible asset that enables the creation of new eCoins and their removal from the system.
- Elastic supply model – the supply of eCoin will be able to adjust automatically with demand. As demand increases, so will the supply of eCoin and vice-versa, thereby enabling eCoin to maintain a stable price.
- Internal exchange market – the eCoin System will consist of a decentralized internal exchange market ("eCoin DEX") that enables users to exchange eCoin and eShares. These transactions will be logged on the blockchain. The eCoin DEX will also play a prominent role in providing price stability to eCoin.
- Independence from fiat currency – with the use of decentralized external price feeds, the price of eCoin will be pegged to the average residential consumer price of one kilowatt-hour of electricity in the United States. This will provide price stability, while also ensuring eCoin maintains purchasing power better than fiat.

Transactional Privacy

- Encrypted blockchain – eCoin transactions will be uniquely encrypted end-to-end.
- Independent payment verification – transactions may be independently verified via a unique transaction token id (only divulged by sender or receiver).
- Speed – private transactions take place in a matter of seconds (instead of minutes to hours as found with other cryptos).
- Tor integration – the eCoin System will have full integration and support for the anonymizing Tor service.

Democratic Governance

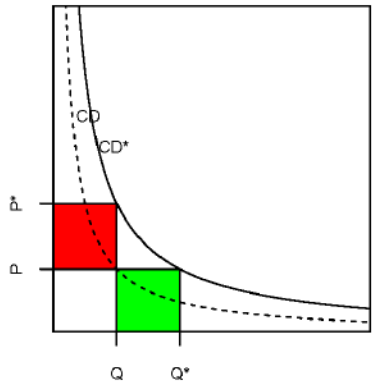
- Democratic blockchain – eShares holders will vote via the Internal Voting System ("IVS") directly on the blockchain

- Stakeholder control – eShares holders will be able to create proposals for changes to the eCoin System and any changes to the system will require eShares holder approval via a democratic process on the IVS.
- eShares Foundation – eShares holders will vote via the IVS on a continuous basis for members of the eShares Foundation board of directors (the nonprofit representative organization of eCoin), through a form of *negative voting*.[95]
- Separation of duties – after release of the eCoin System, the Coin Project shall no longer make decisions for the eCoin System but shall assume the role of being solely a developer, working under the eShares Foundation.

6.2. Achieving Price Stability within the eCoin System

One of the main goals of the eCoin Project is to offer a price stable crypto that also maintains independence from fiat currency. As explained in Section 3.3, the primary reason why bitcoin and other cryptos experience such high volatility is because they use deterministic supply models, wherein the supply of the crypto is unable to adjust with changes in demand. This was illustrated in the crypto supply and demand chart, reproduced below.

Crypto Supply and Demand[96]



Crypto demand ("CD", dashed line) represents demand for a crypto at a given time at price ("P") with quantity ("Q") being supplied.

Robert Sams has shown that in deterministic supply cryptos, such as bitcoin, when CD shifts to CD*, P shifts to P* (because Q is "fixed" and unable to adjust relative to price). In such a system, price is simply a proxy for demand, indicating that bitcoin and other cryptos' deterministic supply inherently leads to high volatility.

If the goal of a crypto is to maintain price stability (as is the case with eCoin), then the supply of that crypto must be able to meet demand. As illustrated in the figure above, when crypto demand ("CD") goes up and shifts to CD*, a stable price may be achieved by

[95] For specifics on how a negative voting system basically operations, *see* https://en.wikipedia.org/wiki/Voting#Negative_voting.

[96] Chart taken from Robert Sams *supra* note 58 at 2.

increasing the quantity ("Q") of the crypto to Q*. Similarly, if demand goes down (represented in the chart as a shift from CD* to CD), then decreasing the supply of the crypto in response to that change in demand (going from Q* to Q) will maintain a stable price. In other words, in order to maintain price stability, eCoin's supply must be elastic and able to adjust in response to changes in demand. However, in order to do that, we first need to establish a baseline, or peg, value for eCoin.

Independence from fiat - eCoin pegged to 1 kWh

Other cryptos that currently have price stabilizing features are pegged to fiat currency (typically USD). While this provides more price stability than the gluttony of cryptos that float freely with the market, it still makes those underlying systems dependent upon fiat currency, central banks, and all the risks and flaws inherent to our monetary, banking, and financial system. In short, what is needed is a peg to some other instrument or measure of value that is not directly linked to fiat currency and that will maintain its purchasing power.

Different ideas have come to mind. One is to peg eCoin to a precious commodity such as gold or silver (somewhat representing the gold standard that existed in the past). While this would make eCoin independent of fiat, gold and silver can be just as volatile as cryptos, which would essentially defeat the purpose of attempting to provide price stability to eCoin. Additionally, the commodity markets (particularly gold and silver) are arguably manipulated,[97] not reflecting their "true" price.[98] Another option is to peg eCoin to some form of inflationary index, such as the urban consumer price index ("CPI-U") used within the United States. However, the CPI-U is hardly an ideal candidate. The computations and data used to calculate the CPI-U are highly complicated, based upon subjective criteria

[97] *See*, *e.g.*, David McLaughlin & Tom Schoenberg, *Banks Face U.S. Manipulation Probe Over Metals Pricing* (Feb. 23, 2015), https://www.bloomberg.com/news/articles/2015-02-24/banks-said-to-face-u-s-manipulation-probe-over-metals-pricing, *archived at* https://perma.cc/FGQ5-W38Z (reporting that "the U.S. Justice Department is investigating whether [at least ten of] the world's biggest banks manipulated prices of precious metals such as silver and gold").

[98] Admittedly, one can say the same for the price of electricity in the U.S. (or any market, for that matter). Nevertheless, a peg to 1 kWh appears to provide the features we need (read further).

that change with time, and arguably fails to accurately follow the true inflationary effect of fiat.[99]

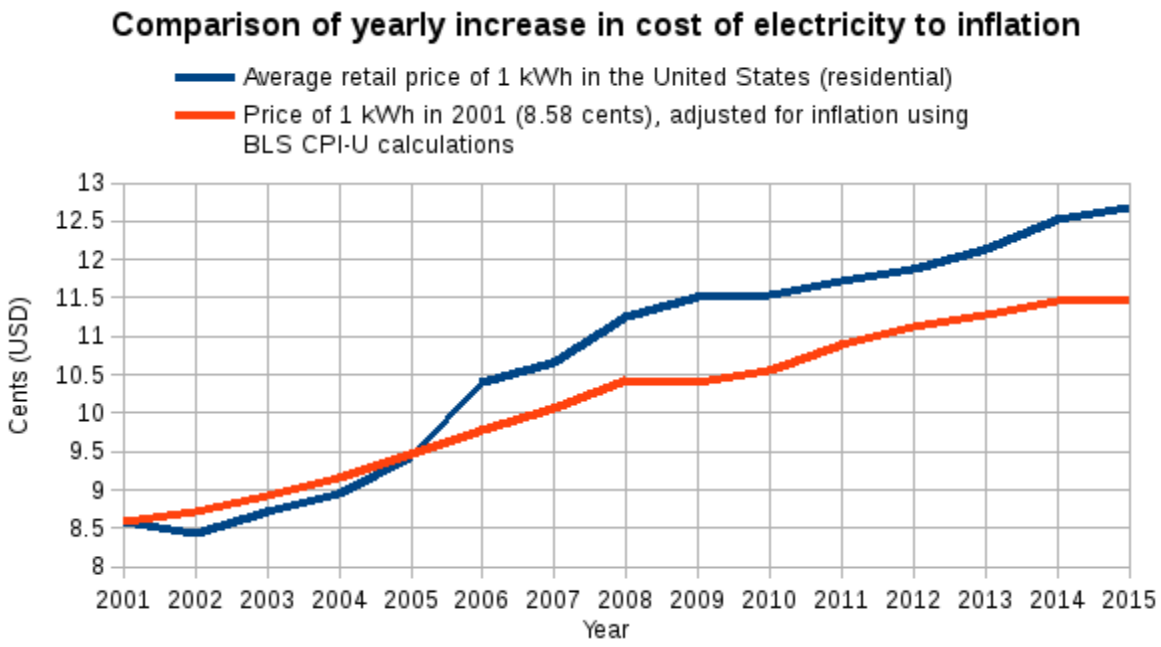
Instead of the previous options, the peg for eCoin will be to the average retail price of one kilowatt-hour of electricity for residential consumers within the United States (the "price of 1 kWh").[100] The eCoin System will use this data as it is published monthly by the U.S. Energy Information Administration and incorporate it into the calculations used for providing price stability for eCoin. Some of the advantages to pegging eCoin to the price of 1 kWh of electricity are that it is: (1) stable, (2) not easily manipulated, (3) objective, in that the criteria for calculating the price of 1 kWh do not change, the variables are known, and the mathematics are simple, (4) provides independence from fiat, and (5) offers protection against price inflation. Furthermore, a peg to the price of 1 kWh of electricity represents a utility that all of modern society depends upon and is built – arguably an important basis for establishing any type of long term monetary peg.

As seen in the comparison chart below, the price of 1 kWh of electricity has historically increased in step with the rate of inflation. In fact, it appears that since 2005, the price of 1 kWh has risen faster than the the generally accepted (though questionable) index for price inflation in the United States (the CPI-U). This means that pegging eCoin to the price of 1 kWh would not only provide price stability, but also seems it would effectively make eCoin inflation-proof.

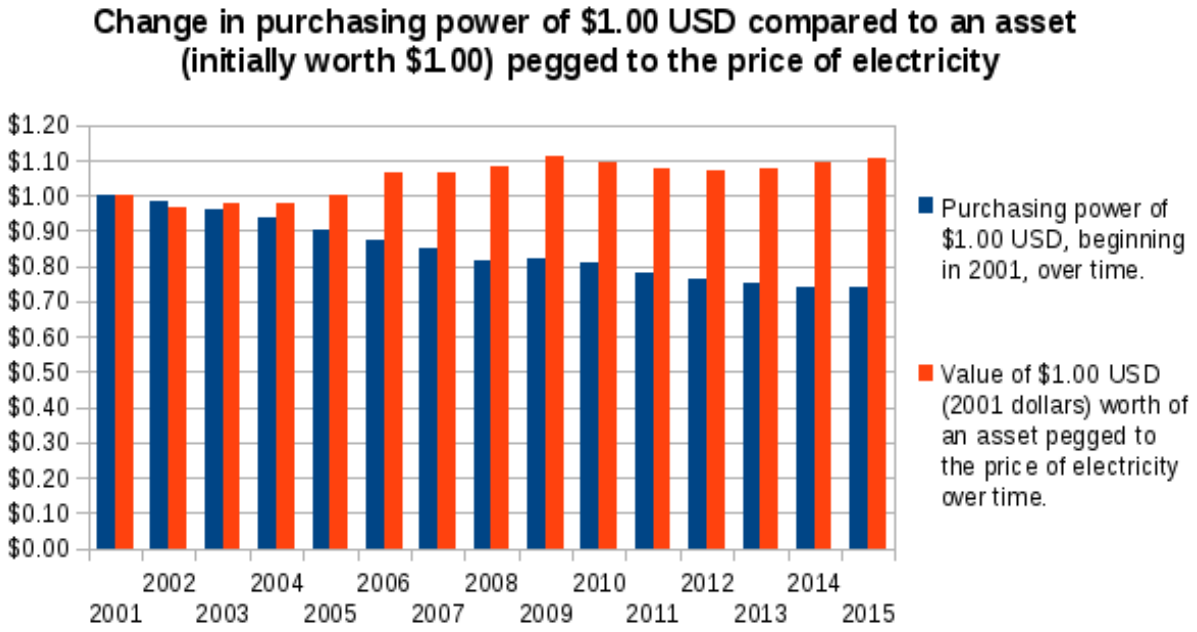
---

[99] *See*, *e.g.*, Dick Morris, *How the Fed Hides Inflation: The Economic Tricks Every American Should Know About* (Apr. 28, 2011), http://www.frontpagemag.com/fpm/91796/how-feds-hide-inflation-dick-morris, *archived at* https://perma.cc/PS8Q-NZ4P (noting how the way the CPI-U has been measured has changed over time in ways to hide inflation). *See* also, John Williams, *No. 515 - Public Comment on Inflation Measurement and the Chained-CPI* (April 3, 2013), http://www.shadowstats.com/article/no-438-public-comment-on-inflation-measurement, *archived at* https://perma.cc/AN22-XEYA.

[100] U.S. Energy Information Administration, *Average Retail Price of Electricity (Monthly, Residential)* 2001-2016, http://www.eia.gov/electricity/data/browser/#/topic/7?agg=0,1&geo=g&endsec=vg&linechart=~ELEC.PRICE.US-RES.A, *archived at* https://perma.cc/Y4DV-TMU2 (showing average monthly price data for the cost of 1 kWh for U.S. residential consumers from 2001 to present).



One of the problems with fiat currency is that it loses value over time (purchasing power) as result of inflation. However, as seen in the comparison chart above, an asset pegged to the price of electricity (as eCoin is intended to be) increases in value along with the rate of inflation. In other words, an asset pegged to 1 kWh maintains its purchasing power over time.



As seen in the chart above,[101] a hypothetical asset pegged to the price of electricity maintains its purchasing power over time. Such an asset, valued at $1.00 in 2001, would be worth around $1.10 (in 2001 dollars) by 2015. This represents a cumulative increase in purchasing power of 10% over that time period. On the other hand, fiat currencies such as USD lose their purchasing power. As the chart shows, USD lost approximately 24% of its purchasing power (using CPI-U data), going from being able to purchase $1.00 worth of goods and services in 2001 to being only worth 76 cents (in 2001 dollars) by 2015.

In summation, by maintaining a peg to the price of 1 kWh of electricity, eCoin will not only have independence from fiat, but also be more stable and far better at maintaining its purchasing power. This is something existing cryptos (or any other system) has yet to achieve. In the next few pages, we provide a basic description of the eCoin System's price stabilizing mechanisms and how they will ensure that eCoin maintains its peg to the price of 1 kWh of electricity.

eShares & eCoin[102]

In order to provide price stability, the eCoin System will have two assets: eShares and eCoin. eCoin is the intended currency that will be pegged to the price of 1 kWh of electricity. eShares will float freely with the market and act as the investible asset that enables the creation of new eCoins and their removal from the system. The supply of eCoin will be elastic and able to adjust in response to changes in demand according to internally controlled rules (explained later). The total supply of eShares will be fixed and distributed to those who contribute to the eCoin Project (see Section 7, below). When the eCoin System is first released, eShares will be the only asset within the eCoin System (i.e. no eCoins will exist).

[101] Chart created using data on yearly residential electricity prices compiled by the U.S. Energy Information Administration (*see supra* note 100), and calculations of decreasing USD purchasing power using the U.S. Department of Labor Bureau of Labor Statistics *CPI Inflation Calculator* (*see id.*).

[102] In addition to the features explained in this section, eCoin and eShares will have all the normal functions and features of existing cryptos (e.g. transactability, divisibility, etc.)

Investing eShares

When contributors to the eCoin Project first receive their eShares, one of the options they will have is to *invest*[103] them. Once an eShares holder invests a chosen amount of eShares, the invested eShares will be internally removed from the eShares holder's account for a period of time (tentatively determined to be 21 days) and added to a *collective pool* that comprises all *invested* eShares at any given time. This collective pool will provide the basis for establishing a price support for eCoin within the eCoin-eShares internal exchange market and thereby a mechanism for ensuring that the price of eCoin does not go below a certain level. If the price of eCoin goes above a certain level, new eCoin will be automatically created and randomly distributed to those investing eShares.

At any time after the required investment period ends (tentatively determined to be 21 days), applicable eShares holders may then *uninvest* their remaining amount of eShares, at which point the amount of eShares they choose to uninvest are removed from the collective pool and returned to the control of the user. Alternatively, the user may choose to keep his or her eShares invested by doing nothing.

eCoin-eShares Internal Exchange Market

The eCoin System will have an internal decentralized exchange market ("eCoin DEX"), enabling one to exchange eShares for eCoin, and vice-versa. These transactions will be trustless, using smart contracts built into the blockchain. Internalized within the eCoin DEX will be a price support for eCoin, created from the collective pool. This, along with the use of decentralized external price feeds, will provide the eCoin System with the necessary structure for increasing and decreasing the supply of eCoin according to changes in its demand.

[103] In the context of eShares, the words "invest, investing, etc." have a specific meaning. For those familiar with PoS cryptos, "investing" will appear to be somewhat similar to "staking" or "minting", in that a certain proportion of one's total wallet balance is set aside and unspendable. However, this where the similarities end. Unlike "minting," which provides the mechanism for processing transactions in PoS cryptos, *investing* eShares will provide the basis for providing price stability in eCoin.

Decentralized External Price Feeds

The eCoin System will incorporate the use of decentralized external price feeds. Naturally, this necessitates the existence of external exchange markets to provide price data. At this point we shall assume that such markets will exist for both eCoin and eShares when the eCoin System is released.

There are two distinct possibilities for how external price feeds will achieve decentralized consensus. One possibility is to use delegates who will provide the price feed data, democratically chosen by an ongoing vote of eShares holders. Another is to have eShares holders provide the data themselves through the use of some sort of "Schelling Point" system.[104] Alternatively, the eCoin System could use a combination of both.

Regardless of the model ultimately chosen, decentralized external price feeds will provide trading data from external exchange markets for eCoin and eShares. Any change in the price of eCoin price can be used as a proxy for determining its level of demand. This will aid the eCoin System, along with eCoin's peg to 1 kWh of electricity, to determine where the collective pool should place the price support for eCoin within the eCoin DEX.

Guaranteeing a minimum price for eCoin

As previously stated, when the eCoin System is first released there will only exist eShares. These eShares will be distributed on a predetermined basis according to those who have contributed to the eCoin Project. Those who receive eShares may *invest* them or trade them on the eCoin DEX (in addition any other normal things with a crypto). When eShares are invested for the first time, this immediately creates new eCoin on a one-to-one basis for the number of eShares invested, which will immediately appear in the invested eShares holders' account.[105] These newly created eCoins may then be immediately spent or transferred as any normal crypto, as well as be traded on the eCoin DEX.

---

[104] *See, generally*, Robert Sams, *supra* note 58 at 6.

[105] Again, this will only occur on a one-time basis and provide the initial supply of eCoins.

When eShares are invested, they are removed from the eShares holder's control, meaning that (while there is an accounting of them) the eShares holder may not transfer or exchange these eShares while they are being invested. These invested eShares are sent to the collective pool, which consists of all invested eShares at any given time in the eCoin System. Using external price feeds, the eCoin System will internally calculate the going market price for eShares and eCoins. With this information, the eCoin System will then automatically place a moving buy order on the eCoin DEX for eCoins, using eShares from the collective pool.

When placed on the eCoin DEX, this automated buy order from the collective pool will be a few percentage points (tentatively determined to be 3%) below the going price for 1 kWh of electricity. This will enable the price of eCoin to float by some small amount (anticipated to be five or six percent) and thereby adjust in the short term, as may necessary, while also enabling price stability over the long term. The amount/volume of the buy order will be a randomized, but relatively small, percentage of the total amount of eShares held by the collective pool at any given time.

The idea is that these buy orders, placed on the collective pool, will continuously provide an adequate level of price support thereby guaranteeing the price of eCoin does not go below a certain level. If someone sells eCoin and fills a buy order placed by the collective pool, this person will receive eShares that are withdrawn from the pool. The eCoin that would otherwise be received by the collective pool is destroyed. In this way, the supply of eCoin will be elastic able to be reduced to meet demand, further ensuring eCoin maintains a stable price.

Creating new eCoin when demand increases

When the collective pool sells eShares on the eCoin DEX, these eShares have been randomly taken from those who invested their eShares. Naturally, one may be wondering why a user would invest their eShares given that whenever the collective pool's buy order is completed, an invested user is at risk of a potential loss. The reason is that investing one's eShares brings the potential of receiving newly created eCoins.

In the event that demand for eCoin rises, as a reflected by an increase in price via external price feeds, new eCoin will be created and distributed to those investing their eShares. For example, if the price of eCoin goes a certain level above the price of 1 kwH as monitored by the external price feeds (perhaps by 3%), then new eCoin will be created and randomly dispersed to those investing eShares (tentatively based upon the amount of eShares invested and perhaps time invested). In this way, if eCoin's price reaches too high, then the supply of eCoin may be increased in response, resulting in eCoin's price bring brought back down to an acceptable level.

In determining how much new eCoin to create, the eCoin System will base the amount on the volume of existing buy orders. In other words, new eCoin will be created based upon the total number of eCoins that external markets are willing to purchase at a certain level above the price of 1 kWh of electricity (perhaps by 3%). For example, if external markets show existing buy orders respectively for 1000 eCoins at 3.1% and 500 eCoins at 3.2%, above the price of 1 kWh, then 1500 eCoins will be newly created and dispersed to those investing eShares. If those existing buy orders remain unchanged after a certain period of time (perhaps by 30 minutes), then the eCoin System will again randomly disperse 1500 eCoins to investing eShares holders, and continue disbursing in this fashion until external markets no longer reflect a price for eCoin (i.e. existing buy orders) at more than 3% above the price of 1 kWh. In such a way, the supply of eCoin will be elastic and able to increase if need be, thereby meeting demand and ensuring that the long term price of eCoin remains stable.

Improving stability by increasing market depth

In addition to having elasticity of supply, another important element for maintaining price stability is having enough market depth. In other words, eCoin needs to have enough tradeable volume to offset the effect of buy and sell orders being able to move its price in the markets. The price support established in the eCoin DEX via the collective pool, coupled with the ability to decrease the supply of eCoins when sold to the collective pool, should provide ample support depth to offset this effect on the selling side. The real question is how to prevent buy orders from moving the price of eCoin too high.

As stated before, the eCoin System will already have a built-in mechanism for increasing the supply of eCoin, thereby causing downward pressure on buy orders if eCoin's price rises too far above the price of 1 kWh of electricity. While this helps to provide long-term price stability, it does nothing to prevent the price of eCoin from skyrocketing in the short-term. In other words, similar to how the collective pool provides constant and immediate price support on the eCoin DEX, the eCoin System needs a way of providing price resistance.

To ensure the price of eCoin does not rise too far above the price of 1 kWh of electricity in the short-term, the eCoin System will provide an automated sell feature. This feature will enable eShares holders to have newly created eCoin they receive from investing their eShares to be automatically sold on the eCoin DEX. In addition, eShares holders will be able to input a specific percentage above the price of 1 kWh of electricity that they would like to have their eCoin sold at. For example, an investing eShares holder could choose that any newly created eCoin they receive will be automatically placed on the eCoin DEX to always be sold at 3.42% above the price of 1 kWh. Once these options are chosen, any eCoins that the eShares holder receives from investing will be automatically placed on the eCoin DEX in moving orders to always be sold at 3.42% above the price of 1 kWh.

Any transactions completed using this automated sell feature will operate just like any normal order on the eCoin DEX. The eShares holder would receive eShares in return for the eCoin sold; the counterparty would receive eCoin in return for his/her eShares. The idea is that such a mechanism would provide an easy and automated process for those wishing to invest their eShares and make a profit by selling any newly created eCoin. Along with the eCoin System's ability to increase the supply of eCoin as needed, this automated sell mechanism should ensure there exists sufficient price resistance and sell depth to ensure the price of eCoin does not rise too high.

Providing stability in a black swan event[106]

So long as eShares maintain some amount of value and they are being invested into the collective pool, there will always be automated price support for eCoin. However, it is plausible that at some point in time the eCoin System will have a black swan event, where there are not enough invested eShares to provide sufficient price support for eCoin and the system begins to crash. To provide a safety buffer for such an event, a backup price support mechanism could be built into the eShares System.[107]

Such a system could work in the following manner: Imagine the price of eCoin drops to a certain level (perhaps 15% below the price of 1 kWh) and maintains a price at or below that level for a certain period time (for example 180 minutes). A backup mechanism can be built into the eCoin System so that after 180 minutes, the eCoin System will automatically place buy orders on the eCoin DEX and purchase all eCoins being sold at less than 3% below the price of 1 kWh (which is the intended price support of the collective pool). In order to complete these purchase, the eCoin System would use newly created eShares, and any eCoins received in exchange would be destroyed.

The downside of this type of mechanism is that it increases the supply of eShares, which would presumably decrease their overall value in the long-term. However, the benefits of such a strategy may outweigh its downsides. If the price of eCoin is precipitously falling, such a mechanism may be necessary to save the system. Additionally, this strategy has the benefit of providing an additional level of price support to the eCoin System while also being able to lower the supply of eCoin when drastically needed. Furthermore, such a mechanism may bring peripheral benefits, in that knowing that such a mechanism exists may take away some psychological angst for potential eCoin holders, further encouraging its use and adoption.

---

[106] "A black swan is an event or occurrence that deviates beyond what is normally expected of a situation and is extremely difficult to predict." In the case of eCoin, this most likely would be an event where the price of eShares suddenly plummets due to an extraordinary amount of temporary sell pressure. *Quote from* Investopedia, *Black Swan*, http://www.investopedia.com/terms/b/blackswan.asp, *archived at* https://perma.cc/NB3T-72PH.

[107] While we suggest that such a mechanism should be included within the eCoin System, it is not necessary to eCoin's functionality. As such, this matter will be looked into further as development progresses.

6.3. Achieving Transactional Privacy with eCoin

[THIS SECTION IS CURRENTLY BEING WORKED ON]

6.4. Achieving Democratic Governance with eCoin

[THIS SECTION IS CURRENTLY BEING WORKED ON]

7. PROJECT FUNDING & eSHARES DISTRIBUTION

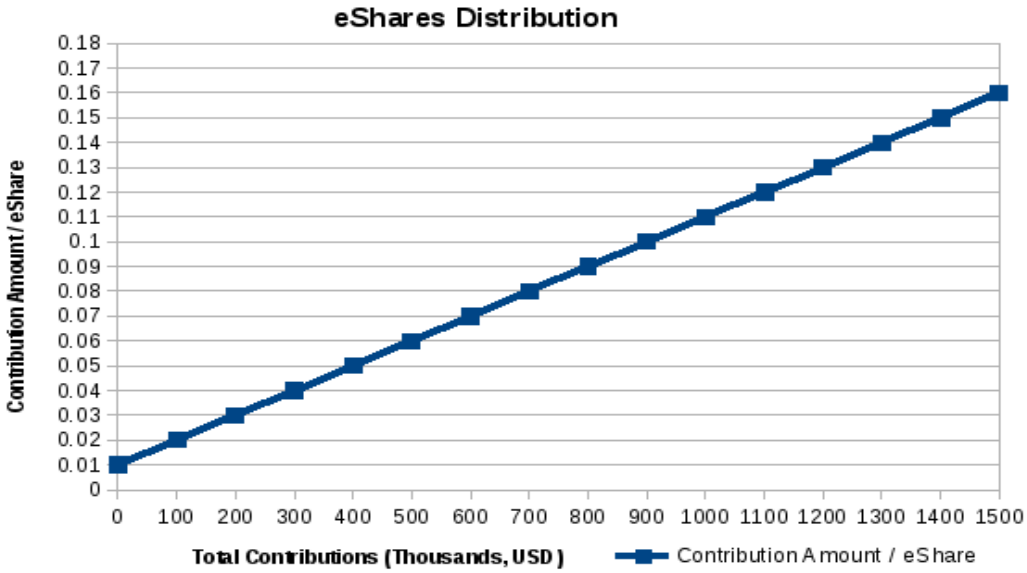
7.1. eCoin Project Funding Model

In order to develop the eCoin System in a timely manner, we conservatively estimate that the eCoin Project will cost somewhere around $1.5 million USD. To reach this funding target, the eCoin Project will have a contribution campaign. The campaign will take place in two phases – a "soft-launch" and a "hard-launch". The total number of eShares to exist will be determined by the contributions received during both phases of this campaign.[108]

When the eCoin System is released, those who contributed to the eCoin Project will receive eShares. The amount of eShares that will be released for a given contribution will be based upon two factors: (1) the amount of the contribution (in USD or its equivalent), and (2) when the contribution was made. During the campaign's soft-launch, the contribution amount for each eShare will be fixed at $0.01 (one cent USD, or its equivalent). Soft-launch will take place throughout the end of 2016 as the eCoin Project Proposal and website are updated. At the start of 2017, the contribution campaign's hard-launch will begin, during which the contribution amount for each eShare will rise incrementally as each contribution is received. The rate of this increase will be equivalent to that of one cent for every $100,000 raised, as represented in the eShares Hard-Launch Distribution Chart below.

[108] The total number of eShares will include those eShares reserved for contributors to the eCoin Project plus an additional 10% set aside for the eCoin Project and eShares Foundation (to be divided between the two on a 50/50 basis).

eShares Hard-Launch Distribution Chart



Hard-launch will be ongoing until an amount equivalent to the cost of 10 GWh of electricity for the average U.S. residential consumer (currently 1.29 million dollars)[109] is raised. Once this amount has been reached, a countdown will begin, where the eCoin Project will continue taking contributions and preallocating eShares for thirty more days. At the closing of that thirty day period, the eCoin Project will no longer be taking contributions and the total amount of eShares will be fixed. Afterwards, the eCoin Project will continue developing the eCoin System and will distribute eShares to contributors upon its release.

The 10 GWh figure is established for a number of reasons. First, it is close to the amount of funds needed to fully develop the eCoin System (representing around $1.29 million of the estimated $1.5 million needed). Second, this amount will hopefully provide the eCoin System with a sufficient amount of market depth and diversity of eShares ownership to ensure that the eCoin System is not controlled by any one person or group. Third, once this amount of funds have been raised, this will mark the point at which the

[109] Figure arrived at by multiplying the current price of 1 kWh of electricity for U.S. residential consumers (12.9 cents) by one million (the number of kWhs per GWh) by ten (for the number of GWh). *See* U.S. Energy Information Administration, *Table 5.6.A. Average Price of Electricity to Ultimate Customers by End-Use Sector*, Electronic Power Monthly (Aug. 2016), http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_6_a (showing the latest price data of 1 kWh of electricity for the month of August, 2016).

contribution amount per eShare is equal that of the intended peg for eCoin (i.e. the price of 1 kWh of electricity, currently at 12.9 cents). This will hopefully signal to the market a future minimum (or absolute baseline) value for eShares so that there will be sufficient price support when eCoin System is released and eShares holders invest their eShares for the first time to receive eCoin on a one-to-one basis.

7.2 Contributing to the eCoin Project[110]

The eCoin Project's contribution campaign is designed with three purposes in mind. First, by providing everyone with the same opportunity to get eShares at the lowest contribution amount during soft-launch, the distribution of eShares is intended to be fair and equitable. Second, by having a two-phase campaign, the eCoin Project hopes to reward those who believe in the project and contribute early compared to those who contribute later on as the fundraising campaign's success (and thereby development of the eCoin System) becomes more of a certainty. Third, raising the contribution amount per eShare during hard-launch will encourage early contributions, so that the eCoin Project may be quickly funded and the project may then focus on development rather than raising money.

It suffices to say that funding is a large factor in determining the success of any project. This is no different for eCoin. In the interest of promoting contributions so that the eCoin System may be developed, we wish to highlight the interest an individual would have in contributing to the eCoin Project in order to receive eShares.

If the eCoin System succeeds in functioning as intended, those who contribute to the eCoin Project have the potential of making a windfall. As stated in the earlier section, when the eCoin Project begins taking contributions, the contribution amount for each eShare will start at $0.01 (one cent USD) and after hard-launch will rise incrementally as each additional contribution is received. Say a hypothetical contributor gives to the eCoin

[110] Please note: nothing presented within this section, or this entire paper, is to be regarded as investment, financial, or any other form of advice. We cannot guarantee that the eCoin Project's fundraising campaign will be successful, nor can we guarantee that the eCoin System will be developed or function as intended. As such, eShares and eCoins are not an investment, nor do they have any cash value. Similarly, contributions are to be given without consideration, subject to the eCoin Project's Terms and Conditions.

Project relatively early on in the campaign and ends up receiving eShares at an average contribution amount of three cents per eShare. Then, when the eCoin System is released, this contributor *invests* these eShares, entitling him/her to receive eCoin on a one-to-one basis for the number of eShares invested.

As outlined earlier, the eCoin System is intended to provide price stability for eCoin by pegging it to the price of 1 kWh of electricity. Using current figures for the price of electricity, this means that our hypothetical contributor could sell these eCoins received from investing eShares at 12.9 cents each, thereby netting a profit of 9.9 cents for every three cents contributed (representing a return of 330%). Furthermore, when the eShares investment period ends, this contributor may then sell off his/her remaining eShares at whatever price the market gives, only furthering returns. For example, even if the price for eShares reaches as low as the previously mentioned baseline value (12.9 cents), this would represent a total return of 860%. In short, in addition to providing the humanitarian benefit of helping bring about a better crypto, those who contribute to the eCoin Project could also be greatly benefiting themselves.

8. CONCLUSION

Bitcoin was intended to be a solution to the problems of fiat currency and the weaknesses inherent to our monetary, banking, and financial system. However, as time has shown, Bitcoin and cryptos have weaknesses of their own. We identified these weaknesses as the following: (1) huge price volatility, (2) a lack of transactional privacy, (3) and a lack of proper governance.

To rectify these weaknesses, we have proposed the creation of a new cryptocurrency system called the eCoin-eShares Cryptocurrency System ("eCoin System"). Inspired by the dream of an alternative currency that is free from deficiencies of fiat currency and the centralized banking system, the eCoin Project aims to create a new crypto with the following features: (1) price stability, (2) transactional privacy, and (3) democratic governance. With your help, we can make this dream, and the first steps toward a new monetary revolution, a reality.

