Bitcoin: A $5.8 Million Valuation

Crypto-Currency and A New Era of Human Cooperation

Mr. Game & Watch
MrGameAndWatch@protonmail.com

July 25, 2017

Abstract

This paper tries to demystify Bitcoin's value proposition. First, we note that the word "Bitcoin" refers to both a digital collectible, as well as to a peer-to-peer computer network. The collectible is required to make use of the payment network – even for transactions denominated in USD[1] (not BTC). The payment network is of enormous general utility, particularly to criminals and victims of political oppression worldwide.

Bitcoin has the ability to maintain its useful properties, even under harassment by wealthy or violent adversaries. It can process more transactions than VISA, and can perfectly imitate the properties of rival crypto-currencies – eliminating competition. Bitcoin can be both scarce and digital, because coins are owned by cryptographic passwords, not by possession of a particular digital file.

Worldwide adoption of Bitcoin is not as unthinkable as it may first appear – historically, mankind has migrated to a new form of money whenever technological improvements make an older form obsolete. In the future, certain groups (criminals, international travelers, freelancers, the underbanked, welfare loafers, and the young) may prefer Bitcoin to their local fiat currency, and the remainder of society may be indifferent between the two (as most individuals have net currency investments which are microscopic in comparison to the value of their labor, real estate, and equity investments). Very little prevents Bitcoin from becoming the dominant form of money worldwide.

1 The Two "Bitcoin"

The word "Bitcoin" refers to two different things: a digital collectible, and a piece of technology. The collectible has a market price and individual owners, and in this way it is similar to physical collectibles such as gold, baseball cards, or oil. The technology, in contrast, is a software application that will attempt to connect to a peer-to-peer computer network over the Internet. If the connection is successful, the application will download messages, interpret them, and display them to the end user. Henceforth, we use "BTC" to refer to the collectible, and "the blockchain" to refer to the technology.

The blockchain technology itself produces a resource, comparable to bandwidth, which we refer to as "blockspace". BTC is required in order to rent blockspace. Blockspace is required in order to broadcast a message into the blockchain.

It is widely believed that "blockchain" is "the technology behind BTC", but in fact the two have a mutual relationship. BTC prevents the blockchain from malfunctioning. Blockspace (created by a healthy blockchain) gives BTC its intrinsic value.

BTC's intrinsic value is that it alone will allow the wielder to access the network's blockspace. In turn, the intrinsic value of blockspace is that it, together with BTC, enables special USD transactions – we will call these "Peer-to-Peer Digital USD Payments", or "PDUPs" (see Figure 1).

These PDUPs cannot be made without BTC. First, there is a fixed cost per transaction, which can only be paid in BTC. USD must therefore be paid to a BTC-owner, in order to purchase the BTC which the PDUP requires. Second, BTC must be briefly "rented" in proportion to the magnitude of the transaction. Since the lowest 'ask' price is always higher than the highest 'bid' price, BTC-landlords earn USD-dividends

[1]For readability, this paper uses the abbreviation "USD" to replace more cumbersome phrases such as "US Dollars", "traditional currencies", "fiat currencies around the world", "non-blockchain currencies", and so forth.

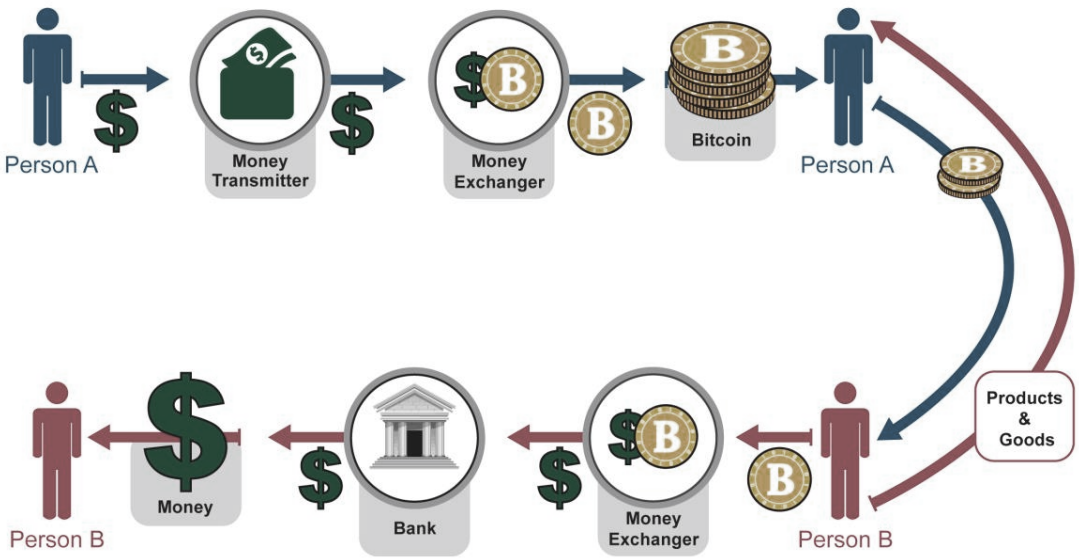

Figure 1: A USD payment that is made through the blockchain payment system [3]. Neither BTC nor the blockchain are used as money, they are instead used to facilitate a payment of USD. The BTC purchases in the upper "money exchanger" offset the BTC sales in the lower exchanger.

on each BTC rented for a PDUP, in an amount proportional to the current bid-ask spread. Therefore, BTC-owners are compensated, in USD, for the PDUPs which they enable.

Those who *invest* in BTC, may do so for innumerable reasons, but those who *consume* BTC do so in order to take advantage of the PDUP service.

2 The Utility of the Blockchain Payment Network

As explained above, BTC is required in order to make "Peer-to-Peer Digital USD Payments" (PDUPs).

2.1 PDUPs in Comparison to Traditional USD Payments

At first glance, PDUPs have a number of severe disadvantages. First, they require the user to learn a new technology and transaction process. Second, PDUPs (despite the name) require the user to interact with many new intermediaries, including at least one software provider and one exchange. Thus, PDUPs have a relative disadvantage on cost, speed, and convenience. PDUPs can also be unreliable, in that they can unexpectedly become more expensive during episodes of high exchange rate volatility.

On the other hand, PDUPs have a number of advantages. First, unlike mainstream digital payments (for example VISA, Venmo, and ApplePay), PDUPs protect the user's anonymity in all cases. Each PDUP user can instruct his computer to make any number of accounts (even tens of millions), and each account is defined only by a password, and has no identifying information whatsoever. He can then freely send his own money to and from these an unlimited number of times, obscuring his total account balance. Newer cryptographic methods [21] aim to emulate, and even surpass, the privacy of the traditional banking system.

Second, unlike historical digital cash schemes (for example Liberty Reserve and e-Gold), the payment service cannot be closed down or altered. This profound durability, and indifference to human action, is why the BTC can be tolerably regarded as a collectible – tokens which more-resemble physical gold than they do entries in a computer database.

Indeed, the name "Bit"coin is a clear reference to "Bit"torrent, a similar technology which enables (among other things) large-scale Internet copyright infringement. Despite ongoing pressure from major governments throughout the world [36], the Bittorrent protocol has operated continuously since its invention in 2001, and

during the 2004-2015 period was, at various times, estimated to be responsible for 29%-35% of all Internet traffic [35].

Bittorrent and Bitcoin are "protocols" – they exist only as *a set of rules*, and they therefore cannot be destroyed (even by their authors [41][40]). An endeavor to disable Bitcoin (or Bittorrent) would be as effective as an endeavor to disable "chess", or "the French language".[2]

2.2 Uses of PDUPs

Because PDUPs return financial sovereignty to the user, they are, for better or for worse, optimal for illegal transactions. PDUPs are often the cheapest (or only) way to engage in gambling, capital flight, tax evasion, and payments for ransomware[3]. PDUPs are often the only way to donate to criminals (for example, to those who leak copyrighted digital files) or to certain political groups (notably, WikiLeaks [25]). When combined with TOR (a technology for anonymous web browsing developed by the US Military), PDUPs enable online purchases of weapons, drugs[4], and prostitutes.

In these cases, PDUPs are more efficient by several orders of magnitude. The total effective cost of an illegal cash transaction, including travel, time spent, risk of bodily injury, entrapment, fraud, and/or embarrassment, is enormous. PDUPs let users accomplish as much, from the comfort and safety of their home computer or mobile phone.

Even in fully legal cases, PDUPs can often be more efficient. For example, many employees of Amazon.com are paid in Amazon store credit, which in some cases cannot easily be converted to the local currency. Instead, employees resort to purchasing marketable items (such as iPads), and pawning these off for cash [44]. Instead, a service called Purse.io allows employees to quickly liquidate their store credit for BTC. Employees are so desperate to take advantage of this service, that they tolerate salary reductions of 15% or more. Purse then liquidates this store credit by servicing a second set of customers: Amazon shoppers who want to pay with BTC. In this case, Bitcoin helps Amazon employees cash their paychecks, and helps Amazon shoppers get huge discounts. Purse is 3.5 years old and boasts over $10 million in conversions.

2.3 Intrinsic Value

As the enabler of the PDUP, Bitcoin is therefore intrinsically valuable. BTC helps its owner get paid, cheat on his taxes, shield his assets from a messy divorce, gamble, engage in underage drinking, defend his life and property, get stoned, and get laid.[5] For those suffering from ransomware or capital controls, PDUPs may be the only payment option. Victims of Venezuelan hyperinflation [9] (to say nothing of the entire slave population of North Korea, or the women of Saudi Arabia), may find these "illegal" blockchain payments to be the only dignified alternative to suicide.

In this way, the intrinsic value of BTC strongly exceeds that of gold (whose industrial, superficial, and cultural importance is at an all time low, and which the modern youth neither desires nor, in truth, can properly recognize) and perhaps even that of the USD (which is required to pay property taxes, on penalty of imprisonment). This intrinsic value is quite sustainable – it will persist wherever the local government is un-competitive. Most Western democracies feature immobile policies which are attractive to PDUPs: progressive income taxation, social welfare, large national debts, and fractional-reserve banking (whereby private banks create new money with each new loan). Individuals, of all dispositions, will be tempted to maximize their after-tax income by exploiting social programs (to extract USD), while pouring their work-ethic into a job (that pays in BTC).

[2] At first, it may appear that the Bitcoin infrastructure is most vulnerable at the exchange level, because exchanges must transmit traditional USD and they are therefore bound by the rules and limitations of legacy systems [16]. However, the big exchanges have private, over-the-counter rivals (such as "LocalBitcoins"), which are capable of running on the anonymous darknet – after all, if BTC can be used to buy a briefcase full of cocaine [26], it can be used to buy a briefcase full of $20 bills. The public today uses large, formal exchanges out of convenience, not out of necessity.

[3] Ransomware is a technology where hackers, or insiders, compromise a computer system and hold the victim's files hostage. According to an industry report [46], ransomware applications grew by 752% in the year 2016, during which attackers collected an estimated $1 billion from victims.

[4] Roughly 5.2% of the adult population (247 million) regularly uses drugs [48]. An estimated 9.3% of these reported a darknet drug purchase in 2016 (up from 4.5% in 2014). 5% of respondents stated that they did not consume drugs prior to accessing them through darknet markets [17].

[5] In short, everything that makes life worth living.

It can be shown that BTC will always be the *most* intrinsically-valuable of all the blockchain currencies. This is due to a technological breakthrough called the "sidechain" [45], which allows Bitcoin to imitate the properties of any rival blockchain technology. In this way, the blockchain technology behind BTC can only improve, and always at the fastest rate possible.

3 Scarcity

By design, only 21 million BTC can ever be created. This is similar to the way in which a game of chess only ever contains 64 board locations – the computer network is simply defined this way, and operates with complete transparency at all times.

It is true that "Bitcoin" –the software– can be easily copied, and that this copy can be used to build a new P2P network. This is analogous to creating a new game board, with 64 new squares and 32 new chesspieces. But this new board will contain a new game, with different opening moves, and the original chess players will not necessarily be aware of it. It is as if the new game were broadcast on a different radio frequency – by default, no one is listening.

Nor should they. A key benefit of the aforementioned sidechains technology is that it allows users to reuse the same board to play many simultaneous games. One board is all that is required.

Hence, while the supply of cryptocurrencies is unlimited, the supply of BTC is limited. BTC is scarce, but "cryptocurrencies" are not. And it is for this reason that only the former, and not the latter, can be considered to be money.

4 Bitcoin As Money

Bitcoin was designed to have optimal monetary properties:

Monetary Property	**Collectibles**	**Gold**	**Banknotes**	**Bitcoin**
Intrinsic Value (individual recourse if this monetary trade network collapses)	*low*	*medium*	**high**	**high**
Portability (transaction variable costs)$^{-1}$	*low*	*medium*	*very high*	**extreme**
Divisibility (ease of constructing fractional units, transaction fixed costs^{-1})	*very low*	*high*	**very high**	**very high**
Scarcity (ability to resist expansion of the money supply, inflation tax^{-1})	*medium*	*very high*	*low*	**extreme**
Recognizability (assay costs)$^{-1}$	*low*	*medium*	*high*	**very high**
Fungibility (user privacy, ease of value calculations, maintenance of recognizability)	*low*	**very high**	*low*	**very high**
Durability (total storage and maintenance costs, including security[6])$^{-1}$	*high*	*high*	*high*	**very high**

Table 1: Different types of money, and their properties.

Therefore, some PDUP-users may find it efficient to store some of their wealth in BTC. And we may therefore expect some speculators to purchase BTC as an investment, not only to speculate on its use in PDUPs, but also to speculate on its use as money.

[6]This concept of "securing one's money" is very context-specific – at any given time, a saver may decide that he most fears thieves, tax authorities, jealous family members, and/or his own carelessness.

The latter speculation is not ill-founded, as mankind has upgraded its money consistently throughout history. Nick Szabo [39] wrote a 2002 essay on the origin of money, expanding on Richard Dawkin's claim that money is "a formal token of delayed reciprocal altruism". Szabo generalizes the behavior of social mammals to that of pre-monetary humans. In this way, he describes a progression from reciprocal altruism, to collectibles, and ultimately to gold.

I will here extend the generalization to include the latest newcomers: banknotes and Bitcoin:

Time	Supporting Technologies	New Monetary Medium	Marginal Advantage	Characteristic "Waste" (cost of teamwork)
50-25 MYA	highly-folded brains, social instincts	status, favors, reciprocity	starvation insurance, specialization of labor	"unproductive" showing-off, zero-sum competition
c. 250 ka, BCE	craftsmanship, cognitive abstraction	collectibles (beads, shells)	fungibility, durability, portability	time spent making "useless" collectibles
c. 1.5 ka, c. 0.7 ka, BCE	scales, weights, forge, metallurgy	precious metals, bars, coins, gold	fungibility, divisibility, durability, scarcity	expenditures on gold mining, refinement, and vault storage
1960's	telephone[7], flight, international trade, international law	banknotes (1971)	portability, divisibility, recognizability (loss of scarcity, fungibility)	over-financialization lobbying/corruption, political polarization[8]
2000's	Internet, open source, smartphone	Bitcoin (2011)	intrinsic value, scarcity, fungibility, durability	energy "wasted" on double-sha256 mining

Table 2: The anthropological progression of "teamwork technology" (ie "money").

The generalizations are simple enough: as technology progresses, it enables new and superior "money" – in other words, new and superior ways of facilitating cooperation.

It is noteworthy to point out that mankind will also go in reverse, and downgrade its cooperative medium when the surrounding technological infrastructure deteriorates. During the relative anarchy of the USSR's 1917-1921 period, workers were unable to rely on banking infrastructure, and instead forged metal collectibles for use in trade [30]. During the European Medieval Period, serfs were forbidden to leave the farmland on which they worked, and most economic transactions were therefore among the same few individuals. In these relationships, gold fell into relative disuse – most peasants paid their taxes in food, military service, or labor. In prisons (throughout history), inmates avoided physical money and instead made investments in an appropriate reputation, religion, or gang affiliation. When tangible money does appear in prisons, it almost never takes the form of gold or banknotes – instead, they use whatever they have.

In addition to the properties outlined in Table 1 (above), money is said to perform three functions:

Label	Summary of the Function Served
medium of exchange	establishes a substrate upon which counterparties may express their transactions
store of value	allows an individual to transact, not only immediately but also in the future
unit of account	simplifies pricing calculations (from $O(n^2)$ complexity to $O(n)$) [39] and negotiations

Table 3: The functions of money.

As we have already seen, Bitcoin is so excellent a medium of exchange, that its intrinsic value is grounded in this property. Bitcoin is also a superb store of value, as it is both scarce and durable.[9] When Bitcoin is

[7] In 1960, 78% of households had a telephone [38], and 60% had a checking account [31]. By 1970, these percentages had risen to 91% and 75%, respectively.

[8] For an in depth exploration of these claims, see Appendix A.

[9] On this point, some will complain about BTC's exchange rate volatility. Firstly, the volatility lies on a consistent downward trend [8], and would be zero if Bitcoin were the unit of account. But more importantly, this volatility has been almost exclusively to the upside, which means that it represents the "risk" of earning too high a return. Since extra money can be freely ignored, evidence of unexpectedly greater wealth cannot be used *against* BTC's success in performing the store of value function. BTC has the highest Sortino ratio (which only measures the risk of loss, not gain) of any asset class in the recent century, [28] indicating, if anything, profoundly low volatility.

used as money (and not for PDUPs), it will be as good a unit of account as any (if such a function is still necessary, given that a common smartphone can recompute prices in realtime).

5 Adoption

5.1 Relative Intransigence

Nassim Taleb observed that nearly all of the drinks sold in the United States are Kosher, despite the fact that less than 0.3% of the American population is Kosher [43]. In explaining this asymmetry, two factors were at work: first, it was easier for the local store to carry one "type" of drink, instead of two. Second, there was a selective intolerance of non-Kosher drinks – Kosher customers couldn't tolerate non-Kosher drinks, but non-Kosher customers could easily tolerate Kosher drinks. Hence, it was costly to stock any mix of types, and costly to commit entirely to the non-Kosher type (thus losing the business of Kosher customers), leading to the all-Kosher outcome. Taleb generalized this principle to the spread of automatic gear-shifting in cars, fast-food chains in high transit areas, support for extremist political candidates, the prominence of various languages, and religious conversions.

The generalization also applies to Bitcoin, as both factors are strongly present. First, sellers of goods (or of labor) far prefer to use a single currency, over two. Second, there exists a selective intolerance of the USD – some USD-users are willing to become BTC-users, but many BTC-users are unable to become USD users.

The willingness to switch to BTC is strongest among criminals (including welfare loafers) and their victims and associates. For these groups, direct BTC payments are faster, cheaper, and more convenient than the circuitous PDUPs. Secondly, while many individuals find traditional banking to be expensive or inconvenient, Bitcoin is free to join and piggybacks on the existing telecommunications infrastructure. Thirdly, we have the privacy-conscious individuals who avoid using credit cards (either in general, or for especially sensitive purchases).

Interestingly, the selective intolerance of the USD is also present in a much simpler and more general way: each fiat currency is only tolerated within the borders of a single country – but in all others, the currency is useless. If a man wanders across the globe with USD in his pocket, the banknotes are, more often than not, completely worthless. They are not "tolerated" by local merchants in any sense. In stark contrast, BTC can be accepted everywhere, especially through the use of payment-processors such as "BitPay", which will accept a customer's BTC and deposit local fiat currency in the merchant's bank account. BitPay is much cheaper to use for transaction processing than credit cards (which expose merchants to losses resulting from fraud, identity theft, or chargebacks).

Therefore, the traditional USD is intolerable in many cases. But the reverse is not true – there is nothing that the USD does today that couldn't easily be done with BTC tomorrow (including even the collection of property taxes, and provision of public services). Relative to BTC, the USD is constrained as a medium of exchange.

5.2 Network Capacity

Commercial banks can trivially configure their existing computer systems to accommodate Bitcoin alongside the USD. Customers could then use the same banking services as always (checking accounts, credit cards, home equity loans), but with Bitcoin as the unit of account. In this model [12], the blockchain would only be used for large settlement transactions between banks.

However, such a model is only attractive if users have an alternative available to them in the form of the blockchain itself. Fortunately, in practice the blockchain network is likely to be quite scalable. As previously mentioned, Bitcoin can take advantage of sidechain technology [45] to access the blockspace of new blockchain networks. Since it can create an unlimited number of these, the effective blockspace of the network is also unlimited. In addition, a technology called the "lightning network" [33] enables Bitcoin to cache an arbitrarily unlimited number of transactions to a single blockchain ledger entry. Between these two technologies, the Bitcoin network can handle millions of transactions per second (in contrast, VISA could handle only 40,000 tps as of the year 2013 [47]).

5.3 Cultural Norms

In general, economic agents find the thought of abandoning their present currency to be quite daunting. Any attempt to switch from one currency to another is imperiled by the high likelihood of coordination failure and the disastrous outcome of wealth-loss.[10]

However, the loyalty to modern banknote money is probably not as insurmountable as it first appears, primarily because citizens avoid using their banknotes as a store of value. A recent banking survey [4] reported that 56% of American individuals had fewer than $1000 in their combined checking and savings accounts (this $1000 figure represents less than 2% of the household income of just that single year[11]). In fact, the US Federal Reserve [10] estimates that 20% of Americans have a negative net worth (and the Credit Suisse 2016 Global Wealth Report [6] finds similar results for the rest of the world). When net worth is positive, most of it is in equities (Vanguard [49] reports that the median equity-allocation among participants in their defined contribution plans is 83%, while only 8% is allocated to cash and a mere 5% is placed into bond funds). In short, most Americans own very few dollars, either because they are too poor to afford any, or so rich that they can afford to discard them by purchasing investments. A significant portion of the first world is in debt, and would directly benefit from the demise of their local fiat.

This especially applies to the modern youth, who are born with no loyalty to any particular asset (nor to any particular political or economic philosophy), and who are more willing to experiment with novel technology for their own advancement. Today's teenagers are, in fact, already using Bitcoin to gamble on e-sports (as of early 2016 at least), without their parent's knowledge or permission [7]. The BTC-phobic parent already resembles, or will very soon, the email-phobic grandparent.

A society which adopted Bitcoin as money would find that many of its previously-influential citizens were immediately worse off. However, as Daniel Krawisz points out [24], these natural opponents can individually hedge against this risk by purchasing BTC. Therefore, while Bitcoin may threaten the viability of many of today's organizations and institutions, it can still thrive among the *individuals* who make up those institutions. This is a unique function of Bitcoin's durability and longevity.

5.4 Self-Fulfilling Prophecies

Astute readers will have already noticed a positive feedback loop: As Bitcoin grows in dominance, it rewards its earliest adopters; and as new users adopt Bitcoin, they help Bitcoin become more dominant.

Bitcoin appears to proceed in adoption cycles. First, the exchange rate strengthens suddenly. The sudden appreciation triggers greater media attention (including social media), which, in turn, reminds bystanders of its objective significance. This ultimately motivates some of these bystanders to become adopters.[12]

The presence of such a self-fulfilling prophecy strongly increases the likelihood of worldwide adoption. Previous attempts at a world currency required explicit agreement from many uncooperative groups. Bitcoin, in contrast, does not require explicit cooperation of any kind – it can rise to prominence if world citizens acknowledge *only the mere possibility* that it will be found preferable *by a few wealthy individuals*. Even if prominent world leaders spoke out against Bitcoin adoption, it would only demonstrate that Bitcoin had become significant enough to attract their attention – after all, who can say that the critic is not himself stocking up on the currency behind the scenes, just in case?

[10] Of course, there is much more to it than the mere risk of some financial loss. If we consider the format of Table 2, and the assertion on which it relies (that money is a technological refinement of the instinct for reciprocity), then we reach a key insight: to abandon the monetary status quo is, really, to abandon all of one's current friends and allies.

Imagine a prison, where there is no tangible property and therefore the only money in use is reputational, and further imagine that one inmate proposes that they all delete all of their reputational memories from their minds, and start over with a blank slate. Such a proposal would be very distressing to the inmate's current friends and associates – they are immediately likely to abandon this careless, ungrateful ally. Simultaneously, the suggestion would threaten and offend the prison's most-reputable inmates – these powerful individuals are immediately likely to become the inmate's enemies.

Thus, even to *suggest* such a thing publicly would be both humiliating and treasonous. Few would tolerate even an open discussion along these lines, lest it mark the discussants as naive and unreliable – shameless and opportunistic. In sum, monetary revolution is a desire that is explicitly anti-social, and inescapably shameful. To express the desire aloud, is to out oneself as a defective person – someone unworthy of friendship or assistance.

[11] Moreover, only 66% of US households keep any assets in a checking account at all, and only 9.9% own bonds of any kind [10]. In contrast, 77% of US *individuals* own internet-enabled smartphones [37].

[12] It is likely that much of BTC's infamous exchange rate volatility as result of this circularity (and not the result of some mysterious flaw intrinsic to Bitcoin).

6 Valuation

This investment thesis asks the reader to consider BTC as the dominant world currency. If this is acceptable, the valuation is a comparatively simple matter of estimating the total value of all the world's money.

Economists define "broad money" as the sum of all currency, funds in bank accounts, and anything of value representing money.[13] We can use estimates from the World Bank [50] to estimate the value of all broad money, now and in the future.

Year	World GDP ($T)	Money Supply (% of GDP)	Broad Money ($T)	BTC Supply (M)	Price ($M/BTC)	NPV (at 15%) ($M/BTC)
1960	1.367	50.5	0.6899	–	–	–
2016	75.642	116.4	88.055	15.72	5.60	–
2017	81.262	118.2	96.016	16.42	5.85	5.85
2027	166.397	137.1	228.171	20.34	11.22	2.77
2037	340.722	159.1	542.222	20.90	25.94	1.56

Table 4: Macroeconomic factors determining the value of all broad money, in given years. Estimates for future WGDP and MS/WGDP values were estimated by assuming constant growth at their historical rates (of 7.43% and 1.5%, respectfully). All values are given in current year (nominal) terms, with the exception of the NPV calculation which is given in 2017 dollars.

The penultimate column gives the estimated USD price of one Bitcoin in each year, in those years where all broad money takes the form of Bitcoin. In other words, this column first determines what portion of GDP one could purchase with a given portion of the money supply, and then multiplies this portion against the future nominal value of GDP. For example, the 2027 figure notes that someone with all of the broad money in existence in 2027, could purchase goods and services which equaled 137.1% of everything produced in the year 2027.[14] The total produce of 2027 is estimated to be worth 166 trillion (measured in 2027 dollars), making the purchasing power of the entire 2027 money supply equal to 228 trillion 2027 dollars. Someone who owned 1/(20.34e6) of the total money supply of 2027 would own exactly one Bitcoin in an all-Bitcoin world, and about 11.22 million dollars in an all-dollar world.

The final column tries to account for the length of time it takes for Bitcoin to replace the world's broad money. Even if an investor is impatient to the degree of 15% per year, and must wait 20 years, Bitcoin is still an attractive purchase today at all prices less than 1.56 million USD.

7 Limitations, Assumptions, and Future Research

Most clearly, this paper assumes that the Bitcoin system will continue to have the properties that it has today. Therefore, researchers should investigate ways in which Bitcoin may be made to change its essential properties. Two properties of particular interest would be the the ability to make PDUPs ("fungibility") and the ability to audit one's account balance ("durability" and "recognizability").

A few of Bitcoin's most crucial scalability, fungibility, and anti-competitiveness technologies remain unfinished. The valuation assumes that these will be finished and deployed in a reasonable time, and without incident. The basis for this assumption is Bitcoin's (very impressive) track record of technological improvement.

This paper is not specific to Bitcoin – the results could apply to any digital asset with comparable monetary properties. However, Bitcoin is assumed to emerge as the prominent e-cash, by virtue of its superior historical precedence, robustness of properties, public awareness, PDUP transaction volume, and market capitalization. Nonetheless, society may come to adopt a different e-cash technology, especially if it makes an effort to respect previous account balances (precisely as the Banknote Era opened by respecting the terminal account balances of the Gold Era), or if the newer e-cash is overwhelmingly easier to use in PDUPs, or more effectively anti-competitive.

[13] In addition to broad money, Bitcoin may replace money substitutes, for example gold, US treasury bonds, valuable collectibles such as art, and personal favors.

[14] In other words, everything produced in that year, and some things that were produced in previous years.

Appendix A Waste in the Era of Banknotes

This appendix is an informal account of our current monetary era – the Age of Banknotes. We provide it for three reasons: to justify the format of Table 2, to provide the reader with a broader historical context, and to try to familiarize the reader with the nature of money.

A major suggestion of this Appendix is that, instead of pointlessly digging gold out of the ground, we instead pointlessly fight each other for control of a printing press located in Washington D.C. The allure of the press, and the limitless wealth it can provide, inspires a wide array of useless zero-sum behaviors – namely lobbying, campaigning, fundraising, advertising, election analysis, 'getting out the vote', and so forth.

A.1 The Incentive to Make Money

The temptation to "create" (ie, "counterfeit") a $20 bill must always be exactly equal to the temptation to earn a $20 bill through legitimate economic exchange. Thus, if money is to be valued at all, there will be a persistent incentive to engage in counterfeiting.

However, from the perspective of society at large, counterfeiting is quite harmful. Each activity of the counterfeiter consumes his scarce effort, and yet in return the only produce is a zero-sum inflation tax upon his trading partners. Hence the activity is on the whole negative-sum and might therefore be regarded as "wasteful".

For this very reason, societies tend to use forms of money which are very difficult to counterfeit. To date, however, no form of money has managed to completely resist the expansion of its supply and the associated "wasteful" activities. For Bitcoin and Gold, the waste is characterized by mining. For collectibles (shells, beads, art, and the like) the waste is characterized by labor. For social status, and other forms of money which are exclusively psychological, each organism is compelled to constantly present itself in the best light (what Holden Caulfield would describe as "phoniness") so as to maximize the respect and goodwill he receives from his fellow neighbors.

A.2 A Standard of Comparison

In a 1951 paper, Milton Friedman estimates the total annual cost of maintaining a 1900-1950 gold standard at **1.5 percent of national income** [13].[15] For the year 2016, that figure would amount to $279 billion for the United States. By comparison, this was less than half of the federal budget deficit ($587 bn), and more than twice the gross profits of the Walmart Corporation ($121 bn).

The sections which follow will attempt to set that $279 bn cost against new costs which may have been created or exacerbated by society's transition to banknote money.

A.3 Money Market Mutuals, Forex Futures, and Private Gold Hoards

Friedman, writing 35 years after the 1951 paper (above), suggests that paper money did not reduce the 'waste' of the Gold Era as much as he had initially expected (emphasis added) [14]:

> ...**I took it for granted that the real resource cost of producing irredeemable paper money was negligible**, consisting only of the cost of paper and printing. ...while [this] may be correct with respect to the direct cost to the government of issuing fiat outside money, is false for society as a whole..."

Friedman concluded that banknote money led to zero-sum behaviors which would otherwise have not been undertaken. In addition to the rise of money market mutuals, and of foreign exchange futures[16], Friedman cites (emphasis added):

[15] Friedman's analysis requires that enough new gold be stockpiled, each year, to maintain price stability (and ward off deflation). The historical gold standard had no such requirement, yet perhaps the assumption is realistic enough, give that price inflation from 1791-1933 *averaged* about 0% per year regardless [34].

[16] In 2016, the trading of forex futures and options reached an all-time high [1]. Based on third-party estimates in previous years, I estimate the total notional value of these [25.22 billion] contracts to be between 30-45 trillion USD. In comparison, the WTO reports 2015 international trade (the latest data) in *actual goods and services* as totaling only 20.7 trillion USD.

> "...a growth industry of "hard money" financial advisers...encouraging [the public] to prepare...by accumulating gold or silver bullion, coins, or other collectibles. ... **Since the end of Bretton Woods, even the direct resource cost of the gold and silver accumulated in private hoards may have been as great as or greater than it would have been under an effective gold standard.** That depends on whether gold production since 1971 has been greater or less than it would have been..."

Friedman rightly suggests that the answer to his question is not obvious from casual empiricism. Nonetheless, we may undertake some, given that this information is readily provided by the U.S. Department of the Interior [2]:

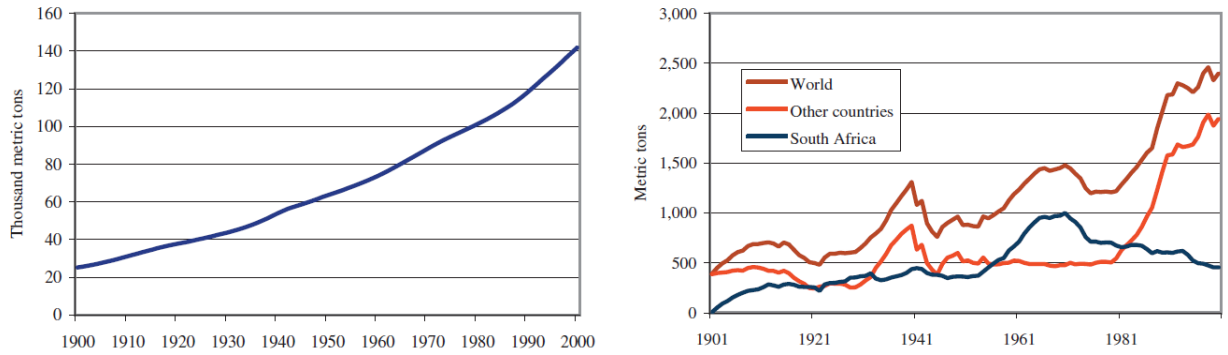

Figure 2: World gold production over time. Left, cumulative; right, annual.

The events of 1971 (or of 1933) seem to have had no significant long-run effect on global gold production. It is possible that production efforts would have climbed even higher under a strict gold standard, of course.

A.4 Mining for Banknotes

The previous section limited itself to merely discussing inconveniences that we endure under a system of floating exchange rates. In contrast, this section will try to describe how banknote money is created, and following sections will catalogue how individuals might "waste" resources fighting each other for control of this printing press.

A.4.1 How Banknotes Are Made

In the United States, there is actually only one bank[17], the Federal Reserve Bank (FED), of which all others are mere franchises. While these franchise banks (Bank of America, Chase, Citi, etc) compete with each other on location, customer service, marketing, and so forth, behind the scenes they share a common set of banknotes, common settlement systems, and common legal requirements (namely, to each store a percentage of every deposit at a Federal Reserve Bank).

The situation is further encumbered by the confusion that there are actually (at least) two types of banknote money: "high-powered money" (sometimes called the "monetary base") and "demand deposits" (which are most of the so-called "money supply"). The first can be freely altered by the FED at will. The second is always[18] equal to ten times the amount of the first, due to the voracious lending of the commercial banks which puts each always against the government-mandated 10% reserve requirement.

Any commercial bank can turn any HPM banknote into ten demand banknotes, and each bank has a strong incentive to convert as many as possible, as each conversion increase bank profitability directly. While

[17] Setting aside the investment banks, which are another matter.

[18] This described the state of affairs until late 2008, when the FED began intentionally flooding banks with excess reserves. We have no space here to fully unravel this complex topic, other than to say that the FED also began paying interest on all excess reserves, which turned these, somewhat, into bonds (as if these reserves were actually loans made back to the FED). Thus, it is still as if banks have taken every opportunity to lend out their reserves – some 'modern' reserves merely come 'pre-lent'.

the FED unilaterally creates (or destroys) HPM banknotes, the commercial banks all compete heavily with each other to convert them, and because of this competition the private commercial banks do not truly have the power to change the money supply. Despite the fact that nine out of every ten dollars in circulation was created by a private commercial bank[19], each individual bank can do nothing to actually alter the money supply's grand total – if one bank doesn't multiply a HPM note by ten, another bank will. Thus, control of the money supply –and the power of the printing press– lies with the FED.

Therefore, the counterfeit expansion of the money supply requires only that sufficient pretext, excuse, deception or corruption be supplied to the FED's board of directors. In practice this is most often achieved via an assertion that the FED must unconditionally ratify the budget deficits of the US Government, even if the budget is economically unjustifiable or otherwise preposterous.

While the process is quite complex and convoluted, the main conclusion is simple: if the government spends more in a given year than it collects in taxes, the difference is made up via counterfeiting.

A.4.2 The First Banknotes

The original set of banknotes was created by Executive Order 6102, signed by FDR in 1933. This act forced all citizens to sell their gold to the FED at a rate of 20.62 banknotes per troy ounce, and it also prevented citizens from converting the banknotes back into gold.

This event occurred near the end of the interwar period (1918-1939). Initially, this period was characterized by free trade and strong leadership under the victorious Allied Powers (for example, as in the Washington Naval Treaty), and therefore strong economic growth (as in the roaring 20's). However, it was later characterized by cultural and economic insecurity (in the form of globalization and the Great Depression), which led to strong policies of nationalism and in many cases total economic self-sufficiency. The regional autarky of this period echoed that of the medieval feudal period. Both periods saw a shift in the preferred monetary technology – trading partners felt that their stored-value would have greatest durability if it resided in the goodwill of their immediate neighbors, where it (and their lives) would be best protected from looters.

While citizens found direct conversion from USD to Gold to be impossible after 1933, it was made indirectly possible by the Bretton Woods system following WW2, if one were able to route the dollar through a foreign government. Initially, these conversions were very rare, as foreign nations were economically and militarily dependent on the US. However, by the 1960's most countries had recovered, and the US had become fiscally imprudent. The Gold Standard made its last stand in 1971, during which several foreign countries either redeemed their hoarded USD for Gold and/or left Bretton Woods, before Nixon suspended the gold peg in August. Thus a global gold standard reigned in America until 1971, interrupted only by WW2 and the autarkic economics of 'total war'. It was replaced by the modern era of floating exchange rates and quasi-nationalized banking.

A.5 Growth in Lobbying Post-1971

The US Political system progresses in multi-year election cycle: House members are elected every two years, Senators every six, and Presidents every four. And it may take many election cycles for political change to have impact, as the incumbent typically wins (rendering the election largely inconsequential).

Nonetheless, following the 1971 transition to the banknote era, Washington DC managed to change quite rapidly.

[19]This peculiarity allows bankers and borrowers to jointly levy an inflation tax on the public. Banks print new money, but this money can only be spent by borrowers, and only on bank-approved projects (for example, housing in the 2000's and higher education in the 2010's).

Robert G. Kaiser spent most of his 70 years living in Washington DC, and more than 50 years at The Washington Post, where he rose to the position of managing editor. In the table below, I have taken figures from Kaiser's book on the rise of US lobbying [22], and framed each in terms of compound annual growth rate (CAGR). I compare each of these to control rate (from the St. Louis FED) over the same time period.

page	Years	Item	Control	CAGR (Item)	CAGR (Control)
53	1969-1975	Congressional Staff – Senate	Civilian Labor Force	10.2%	2.5%
53	1970-1980	Congressional Staff – House	Civilian Labor Force	5.0%	2.6%
115	1974-1982	Combined Campaign Spending, all candidates	Nominal GDP	21.0%	10.1%
115	1970-1982	Cost of the average winning campaign in a contested race[20]– House	Nominal GDP	14.0%	9.91%
115	1978-1982	Cost of the average winning campaign in a contested race – Senate	Nominal GDP	66.4%[21]	9.2%
116	1974-1982	Political Action Committees ("PACs")	N/A	23.9%	0%
116	1974-1982	PAC Contributions	Nominal GDP	26.7%	10.1%
121	1968-1978	Trade Associations, including Unions, Headquartered in Washington D.C.	N/A	8.6%	0%
142	1978-1980	Money Raised by Both Parties	Nominal GDP	38.8%	10.2%
145	1980-1982	Money Raised by Both Parties	Nominal GDP	43.1%	8.1%
156	1982-1987	Revenues of Schlossberg-Cassidy	Nominal GDP	90.4%	7.8%

Table 5: Sustained, consecutive years of above-average growth would indicate that the economy is reorganizing to promote the underlying activity (over other activities).

Specific exerpts, concerning the Schlossberg-Cassidy lobbying firm's invention of the "earmark" in 1976, by getting Congress to pay for a new nutrition research facility at Tufts University (emphasis added):

> ...there were few precedents for what Mayer was seeking: a specific appropriation of federal funds to a single university for a particular facility... **In years to come this kind of legislative provision would become so common that it acquired a widely used nickname – an earmark**...But in 1976 this was an unusual idea. (p69)
>
> Schlossberg recounted a meeting with [Congressman] O'Neill [to discuss the Tufts earmark]: "[O'Neill] brought in his staff guy and said 'These two guys work for President Mayer at Tufts. We're going to try to help them out. I want you to work with these guys.' Manna from heaven. We now have what would turn out to be–you know, **like a prospector finding the first nugget with gold in it**." (p70)
>
> Daniel S. Greenberg [respected science writer] asked [in 1983] if the firm's clients get their money's worth "[Do] your customers' retainers come back many-fold?" **"In every case, many, many fold,"** Cassidy replied. [earlier] Cassidy added that the earmarks..."hurt...no one." They "represented money spent on science that would not have been spent". (p108)

The Schlossberg-Cassidy firm could deliver these "many-fold" returns because they had inadvertently rediscovered the gold mine of the Gold Era – not in the ground, but instead in the halls of Congress.

Cassidy's claim that these earmarks "hurt...no one" is of course irreconcilable with basic economics – if money is created and used to claim resources, then those resources are unavailable for use elsewhere. And not all of the earmark money was spent on "science" – Tufts would soon be paying Schlossberg-Cassidy $10,000 a month (p72).

[20]This refers to a scenario in which the winner of the election had less than sixty percent of the vote.

[21]The phrase "just a couple of hundred thousand dollars" was interpreted as $300,000.

A.6 Distraction and Hatred

A.6.1 The Trend Toward Greater Polarization

Suspiciously, political polarization has risen consistently in all the post-1971 years [32].

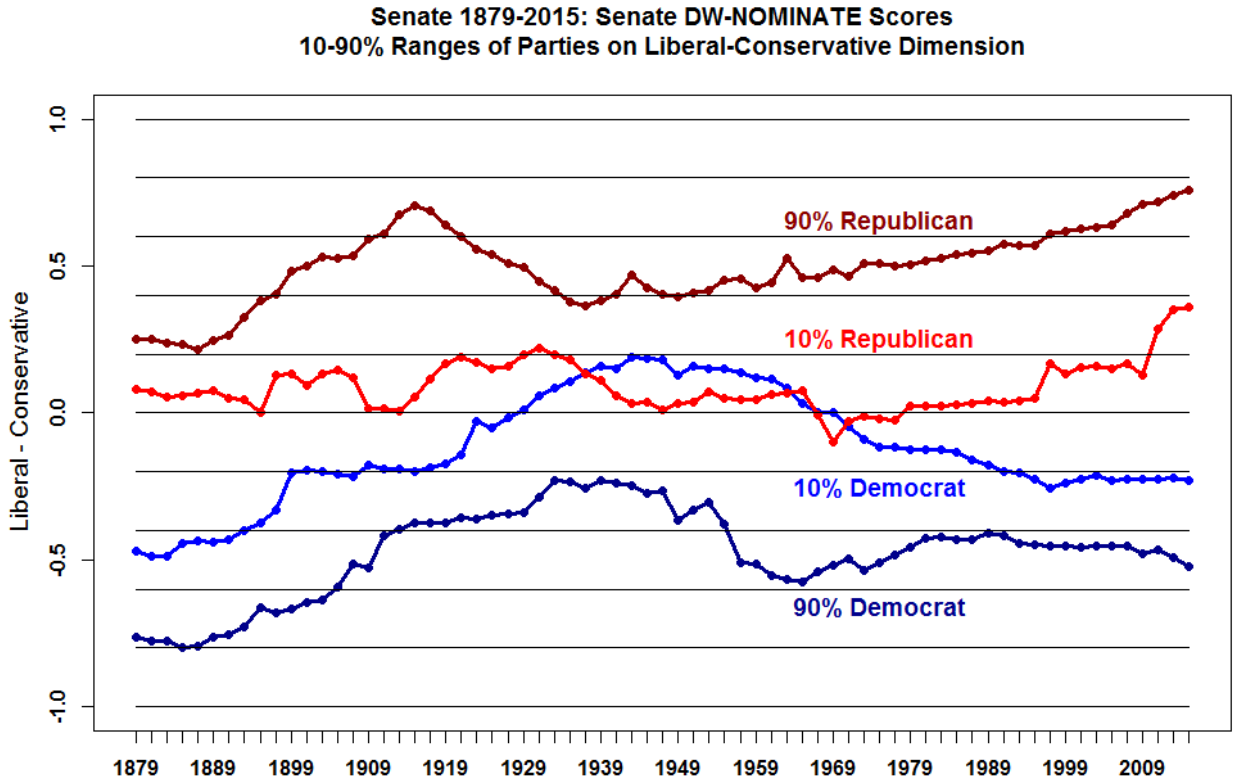

Figure 3: A metric of bipartisanship in the Senate. Polarization was very high during the post-Civil War Reconstruction Era (1865-77), and declined slightly during the Gilded and Progressive Eras (1977-1914) before falling sharply during and between the two World Wars (1914-71). However, the distance between moderate Republicans and moderate Democrats has widened consistently since their divergence in 1971.

Matthew Gentzkow published a report "Polarization in 2016" [15] surveying a wide array of polarization indicators most from 1960 onward (emphasis added):

> **We are less likely to find people holding liberal views on some issues and conservative views on others**, or to meet a liberal Republican or conservative Democrat. ... We don't see those on the other side as well-meaning people who happen to hold different opinions or to weight conflicting goals differently. We see them as unintelligent and selfish, with views so perverse that they can be explained only by unimaginable cluelessness, or a dark ulterior motive. Either way, they pose a grave threat to our nation.

The book *Polarized America* is summarized [27] as follows: "the authors find that polarization and income inequality fell in tandem from 1913 to 1957 and rose together dramatically from 1977 on".

Each year is the most polarizing of all. In the 2016 US presidential cycle, each of the *candidates themselves* asserted that their rival was an outright criminal and shouldn't even have been allowed to run. It was unknown if many of electorate even truly accepts the outcome ("Not my president!"), or would have accepted the alternate outcome ("This whole election is being rigged!").

In contrast, Senator George McGovern, Chairman of the Select Committee on Nutrition and Human Needs, is quoted [22] as saying "I think it's fair to say that we never had a partisan quarrel on that committee [1968-1977]" (p54) – something which is today almost unimaginable.

A.6.2 Polarization Helps to make Corruption Mandatory

There is certainly a connection between polarization and poor governing.

I will cite Ferguson [11] (p11, emphasis added):

> Politicians in both parties enrich themselves and betray the interests of the nation, including most of the people who vote for them. Yet both **parties are still able to mobilize support because they skillfully exploit America's cultural polarization**. ...Thus, the very intensity of the two parties' differences on 'values' issues enables them to collaborate when it comes to money.

And again Kaiser [22] (emphasis added):

> In an academic survey conducted as early as 1989, 44 percent of the consultants interviewed reported that their clients were uninvolved in deciding which issues would be emphasized in their own campaigns. Two-thirds said the candidates played no role in determining the tactics of their campaigns". (p347) What became known as 'wedge issues' remained effective from the 1980s through at least 2004. **If you could win voters' alliance with your opposition to gun control or gay marriage or flag burning, or by being tough on criminals and terrorists, who needed solutions to big national problems?** (p348) In the permanent campaign, public opinion is not the voice of the people, but something to be leveraged and massaged...(p349)

Polarization can shield politicians from the electoral consequences of their misconduct. In fact, any misconduct that is monetizable would now –paradoxically– help a politician *win* re-election. The offense need only be mixed with a dash of incremental extremism.

A.7 Academic Corruption

A.7.1 From the Private Sector

Charles H. Ferguson is hardly a member of the fringe – he has a B.A. in Mathematics from Berkeley and a PhD in Political Science from MIT, and has consulted for the federal government and for large corporations. In the 90's he founded a tech startup and then sold it to Microsoft for $133 million. This wealth presumably freed him to follow his lifelong passions of scholarship and film-making, as he then spent a decade at MIT, Berkeley, the Brookings Institute, and so forth before making the documentary Inside Job.

Keep that in mind, as you read these excerpts from his 2012 book Predator Nation [11] (emphasis added):

> The sale of academic "expertise" for the purpose of influencing government policy, the courts, and public opinion is now a multibillion dollar business. (p243) The problem of academic corruption is now so deeply entrenched that **these disciplines, and leading universities, are severely compromised**, and anyone considering bucking the trend would rationally be very scared. (p268). ...the committees that review grant proposals and the review panels that decide whether papers get published in academic journals are full of professors who consult for financial services companies. These people will have a major say in whether you get published, get a job, or get tenure. (p269)
>
> The release of the film *Inside Job* clearly touched a nerve with regard to these questions. I was contacted by a large number of students and faculty ... departments including the Wharton School and Columbia Business School, have adopted disclosure requirements for the first time. But **most universities still have no public disclosure requirements at all**, and few if any have any limitations on the *existence* of conflicts of interest or of income from such sources...Reporters at the *New York Times*, *Fortune*, and other major news publications are strictly prohibited from accepting money from any industry or organization they write about. Not so in academia. (p272)

Ferguson reveals that, at elite business schools and economics departments, many senior faculty can earn most (upwards of 80%) of their annual income by consulting for large banks. He names organizations such as the Brattle Group, Criterion, Compass Lexecon, and Charles River Associates, in which academics

make themselves available for hire, in order to testify as expert witnesses or produce research papers. In one example, an academic was paid $100,000 to write a paper that helped Icelandic banks become more profitable – for a time. However, the paper contained mistakes, and the author's negligence likely contributed to public losses of roughly $100 billion – six orders of magnitude larger than the payment to the author. The author did not indicate, anywhere in the paper, that he had been paid to write it (by anyone, let alone the Icelandic Chamber of Commerce).

A.7.2 From The Federal Reserve Itself

Excerpts from the Huffington Post article *Priceless: How The Federal Reserve Bought The Economics Profession* [18] (emphasis added):

> The Federal Reserve, through its extensive network of consultants, visiting scholars, alumni and staff economists, so thoroughly dominates the field of economics that **real criticism of the central bank has become a career liability** for members of the profession...
>
> One critical way the Fed exerts control on academic economists is through its relationships with the field's gatekeepers. For instance, at the Journal of Monetary Economics, a must-publish venue for rising economists, more than **half of the editorial board members are currently on the Fed payroll — and the rest have been** in the past.
>
> **"I would date it to maybe the mid-1970s,"** says University of Texas economics professor — and Fed critic — James Galbraith. "The generation that I grew up under, which included both Milton Friedman on the right and Jim Tobin on the left, were independent of the Fed."
>
> The Fed also doles out millions of dollars in contracts to economists for consulting assignments, papers, presentations, workshops, and that plum gig known as a "visiting scholarship." ... the Federal Reserve spent $389.2 million in 2008 on "monetary and economic policy," money spent on analysis, research, data gathering, and studies on market structure; $433 million is budgeted for 2009. ... **that's a lot of money for a relatively small number [est. 487] of economists**.
>
> "Try to publish an article critical of the Fed with an editor who works for the Fed," says Galbraith. And **the journals...determine which economists get tenure** and what ideas are considered respectable.
>
> Milton Friedman, in a 1993 letter to [Robert Auerbach, a former investigator with the House banking committee] argued that the Fed practice was harming objectivity: "...having something like 500 economists is extremely unhealthy. ... **You and I know there has been censorship of the material published**. Equally important, the location of the economists in the Federal Reserve has had a significant influence on the kind of research they do, biasing that research toward noncontroversial technical papers on method..."
>
> Paul Krugman, in fact, has gotten rough treatment. "I've been blackballed from the Fed summer conference at Jackson Hole, which I used to be a regular at, ever since I criticized [Alan Greenspan]," Krugman said [in 2007]. "**Nobody really wants to cross him.** ...[in 2005] the conference was devoted to a field, new economic geography, that I [Paul Krugman] invented, and I wasn't invited."

A.8 The Greenspan Put and The Financial Crisis

As everyone knows, there was a gigantic financial crisis in the late 2000's, the causes of which are numerous. But one clear problem was the so-called "Greenspan Put". Alan Greenspan famously promised that if the stock market went down, he would inject money into the economy and lower bank interest rates.[22]

Greenspan assumed that no one would be able to crash the stock market on purpose, or that no one would be inclined to do so, or that they wouldn't get away with it, or else Greenspan did not understand how anyone could uniquely benefit by doing so.

[22] This activity tends to stimulate money-creation by banks, and to drive money out of savings accounts and into investments or purchases. In this way, an unexpected decrease in interest rates causes asset prices to rise, which Greenspan used to give stockholders a free "do over" on bad stock market investments.

This perspective was quite flawed. Executives at large financial institutions trivially extracted money from Greenspan's put using what Nassim Taleb called a "blowup strategy".

From his congressional testimony [42] following the financial crisis (emphasis added):

> VaR encourages "low volatility, high blowup" risk-taking which can be gamed by the Wall Street bonus structure...**This is the profile for banks (losses in 1982, 1991, and 2008)** and many hedge funds. ...[this] consists in producing steady profits for a long time, collecting bonuses, then losing everything in a single blowup. Such trades pay extremely well for the trader—but not for society. For instance, a member of Citicorp's executive committee (and former government official) collected $120 million of bonuses over the years of hidden risks before the blowup; **regular taxpayers are financing him retrospectively**. (written submission, p14-15)
>
> This ["low volatility, high blowup"] is **a strategy that is pretty much pursued by the majority of people on Wall Street, by banks**. (p12)
>
> ...I am under oath and I will say exactly something that I want to be on the record. I was a trader for 21 years, and every time I said "What if we blowup?", [they] said, "Who cares? The government bails us out." **And I heard that so many times throughout my career**... "worry about down five percent, ten percent, don't worry about extreme risks, they are not your problem anymore, **it's not our problem**." I heard that so many times... (p72)
>
> ...don't give someone managing a nuclear plant a bonus based on cost savings, okay? (p74)

By pairing this loss event (the "blowup") with Greenspan's put, executives at large financial institutions had constructed a portfolio that couldn't lose. The taxpayer, correspondingly, inherited a portfolio that couldn't win.

A.9 The Public Good

Additional selections from Kaiser [22], indicating the changing nature of the job of Congressperson (emphasis added):

> "The Senate was a very different place then [1960's]: small staffs, members [of Congress] did so much of the work themselves...you did more of the work talking directly to members...**members knew what they were talking about**" –Gerry Cassidy (p55)
>
> Peter Hart, the Democratic pollster, was certain about it: "The quality of people that I started out with and **the quality of people today is just so vastly different**...[past Senators] appreciated the system and they appreciated the gravity of what they were doing and what their responsibilities were...all of these people where huge figures, not only within [the Senate], but within the country." (p316)
>
> Hart realized that [his] industry...had helped change the nature of the people who were attracted to politics. Polls and the political consultants who depended on them shaped what the clients should say, even what language they should use to say it...**The objective was not to govern effectively**, not to lead, but to win. (p317)
>
> Cassidy agreed [that] in the age of modern political technology, **the system did not value people who thought for themselves** or wrote their own speeches. (p317)
>
> ...it was a complicated system with many participants. The pollsters and consultants certainly did create demand for expensive services... To pay for these services, politicians had to raise ever-greater amounts of money... **The permanent campaign turned politics into a relentless struggle for power.** Dale Leibach – "The Hill [Congress] can't exist without downtown [the lobbyists], and downtown can't exist without the Hill. It's the largest, most democratic bazaar in the world. And **it's all about money**, going in both directions." (p318)
>
> The mess was created by ordinary people responding logically to powerful incentives. (p346)

The author moved to NYC in 2014, stating that, although he would miss his home town very much, "...for me, the fun has drained out of the game. So has the substance. ...The intellectual firepower in Congress declined sharply during my years in Washington [1974-2014]. Lawmakers who read books, have their own ideas, care about policy issues and believe in government have become rarer than Redskins victories." [23]

Unfortunately, the modern Congressperson is not a statesman serving the public good, but instead a professional fund-raiser and election-winner. Perhaps this is why we also experience *an opposite complaint* – that government is too small, or not doing enough. Despite reckless federal spending overall, when examined in specific the spending seems meagre and unsatisfying.

Until the 1970's, gross investment by the public sector [R&D plus investment in physical capital] averaged around 7% of GDP, but it fell below 6% in the 70's and 80's, below 4% in the 90's and 00's, and is now at 3.6% and falling. A government's most productive investment, after safety, is in infrastructure. Yet, despite undertaking the Eisenhower Interstate system in the 1950's, the US now (and since the mid-1970's) devotes less than 3% of its GDP to infrastructure spending (a figure which, by comparison, is lower than those of China [10%], India [10%], Europe [5%], or Mexico [3%]) [19].

Federal R&D spending, as a percentage of GDP, fell from 2% in 1966 to 0.7% in 2016 [19], resulting in less technological growth. The share of scientists with NIH grants in 2016 is half of what it was in 2010, reducing public defense against plague and disease. For primary and secondary public schools, real (inflation-adjusted) spending per student grew at an annual 4.90% during the years 1947-1970, but only at 1.77% during 1971-2013 [29]. Even an annual rate of 1.77% was enough to triple real spending per student from 1970-2009, but these funds appear to have been largely wasted – America's high school graduation rate rose until the 1970's but has been falling ever since (even after adjusting for increasing immigrant and minority populations) [20]. Today's *older* Americans are the most well-educated in the world, but today's younger Americans are not even close.

We might explain this paradox in two parts. First, by noting that two-thirds of the federal budget (excluding interest) is spent on entitlements such as Social Security (24.9%), Medicare (16.1%), Medicaid (10.1%), and Other (15.4%, a category containing unemployment benefits, federal retirement, EITC/SNAP, and so forth) [5]. These expenses take the form of checks that are written to specific individuals – they are not truly *public* goods at all.[23] In the past, the government provided goods that were legitimately public –such as roads, scientific research, containment of infectious disease, and the maintenance of the critical faculties of the electorate– but today it does not. Second, we note that the modern election can determine the fate of a theoretically unlimited amount of money. Because of this, elections warrant the recruitment of professional election-winners, and these professionals will exploit every advantage they can find – namely the use of public money for electoral bribes and kickbacks. For this 'modern' type of politician, advocating for the public good would be a distraction at best, and a severe handicap at worst.

A.10 Conclusion

Life is complex – if problems of corruption and financial crisis had simple causes, they would be easy to foresee and prevent. We certainly do not claim that there is a direct, unbroken line from the use of Banknote Money to the phenomena of excessive campaign spending or financial crisis. Instead we claim motive and opportunity: there is always an incentive to counterfeit, and –as an empirical matter– the public has allowed professional election managers to capture our governing institutions, and sell these to the highest bidder.

Banknote waste differs from other types of monetary waste in that it is much harder to perceive, by virtue of the complex nature of banknote creation. In contrast, Bitcoin mining directly consumes electricity, and gold mining obviously requires engineers, machinery, armed guards and so forth. At first glance, it seems incredible that impoverished hunter-gatherers would devote some of their precious time to the manufacture of silly beads and shells and other collectibles.[24] And, it seems wasteful indeed, that we humans use our powerful brains primarily to obsess over what other people think of us. All of these activities are wasteful, in a narrow sense, but in a broader sense they maintain the infrastructure required to promote and sustain cooperation. These are social activities – we engage in them because we are not alone.

[23] Certainly, the [Social Security and Medicare] payments to seniors are little more than bribes – and these payments total *forty-one percent* of the non-interest budget.

[24] Szabo notes that a single mammoth ivory bead "may have required one to two hours of labor to manufacture", during an era "when humans lived constantly on the brink of starvation" [39].

References

[1] Acworth, W. 2016 Annual Volume Survey, 2017. Available online at http://marketvoicemag.org/?q=content/2016-annual-volume-survey.

[2] Butterman, W., and Amey III, E. Mineral commodity profiles—gold, 2005. Available online at https://pubs.usgs.gov/of/2002/of02-303/OFR_02-303.pdf.

[3] Calvery, J. Statement before the united states senate committee on homeland security and government affairs, 2013. Available online at https://www.fincen.gov/news/testimony/statement-jennifer-shasky-calvery-director-financial-crimes-enforcement-network-0.

[4] Clements, N. Deeper into credit card debt with no regrets this holiday season, 2015. Available online at http://www.magnifymoney.com/blog/news/deeper-credit-card-debt-regrets-holiday.

[5] Congressional Budget Office. The Federal Budget in 2016: An Infographic, 2016. Available online at https://www.cbo.gov/publication/52408.

[6] Credit Suisse. Global Wealth Report 2016, 2016. Available online at https://www.credit-suisse.com/us/en/about-us/research/research-institute/publications.html, pages 28-30.

[7] DeRose, C., and Unseth, J. Kasper the gamer talks pro gaming, foregone conclusions, and sixteen year old remittance corridors, 2016. Available online at https://soundcloud.com/bitcoinuncensored/kasper-the-gamer-talks-pro-gaming-foregone-conclusions-and-sixteen-year-old-remittance-corridors#t=51:30, Timecode 51m30s.

[8] Dourado, E. The bitcoin volatility index, 2017. Available online at https://btcvol.info/.

[9] Epstein, J. The secret, dangerous world of venezuelan bitcoin mining, 2017. Available online at http://reason.com/archives/2016/11/28/the-secret-dangerous-world-of.

[10] Federal Reserve, T. Survey of Consumer Finances (SCF), 2013. Available online at https://www.federalreserve.gov/econres/scfindex.htm, specifically https://www.federalreserve.gov/econres/files/scf2013_tables_internal_nominal.xls, Tables 1,2,4.

[11] Ferguson, C. H. *Predator Nation*, 1 ed. Crown Business, Random House Inc., New York, NY, 2012.

[12] Finney, H. Bitcoin bank, 2010. Available online at https://bitcointalk.org/index.php?topic=2500.msg34211#msg34211.

[13] Friedman, M. Commodity-reserve currency. *Journal of Political Economy 59*, 3 (1951), 203–232. pages 207, 223.

[14] Friedman, M. The resource cost of irredeemable paper money. *Journal of Political Economy 94*, 3 (1986), 642–647.

[15] Gentzkow, M. Polarization in 2016, 2016. Available online at http://web.stanford.edu/ gentzkow/research/PolarizationIn2016.pdf.

[16] Gershman, J. Irs crackdown on bitcoin exchange fuels privacy worries, 2017. Available online at https://www.wsj.com/articles/irs-crackdown-on-bitcoin-exchange-fuels-privacy-worries-1490623200.

[17] Global Drug Survey. The global drug survey 2016 findings, 2017. Available online at https://www.globaldrugsurvey.com/past-findings/the-global-drug-survey-2016-findings/.

[18] Grim, R. Priceless: How the federal reserve bought the economics profession, 2009. Available online at http://www.huffingtonpost.com/2009/09/07/priceless-how-the-federal_n_278805.html.

[19] Hacker, J., and Pierson, P. *American amnesia : how the war on government led us to forget what made America prosper*, 1 ed. Simon & Shuster Paperbacks, 1230 Avenue of the Americas, New York, NY, 2016. pages 39-40, 33.

[20] Heckman, J., and LaFontaine, P. The american high school graduation rate: Trends and levels. *Review of Economics and Statistics 92*, 2 (may 2010), 244–262.

[21] Heilman, E., AlShenibr, L., Baldimtsi, F., Scafuro, A., and Goldberg, S. Tumblebit: An untrusted bitcoin-compatible anonymous payment hub, 2017. Available online at https://eprint.iacr.org/2016/575.pdf.

[22] Kaiser, R. G. *So damn much money : the triumph of lobbying and the corrosion of American government*, 1 ed. Alfred A. Knopf, Random House, Inc., New York, 2009.

[23] Kaiser, R. G. *How Republicans lost their mind, Democrats lost their soul and Washington lost its appeal.* The Washington Post, 2014. Available online at https://www.washingtonpost.com/opinions/how-republicans-lost-their-mind-democrats-lost-their-soul-and-washington-lost-its-appeal/2014/02/28/2ef5429c-9d89-11e3-9ba6-800d1192d08b_story.html.

[24] Krawisz, D. Bitcoin's shroud of subtlety and allure, 2014. Available online at http://nakamotoinstitute.org/mempool/bitcoins-shroud-of-subtlety-and-allure/.

[25] Matonis, J. Wikileaks bypasses financial blockade with bitcoin, 2012. Available online at http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin/.

[26] Max, M. Drop zone: An anonymous peer-to-peer local contraband marketplace, 2015. Available online at https://github.com/17Q4MX2hmktmpuUKHFuoRmS5MfB5XPbhod/dropzone_ruby/blob/master/Drop%20Zone%20-%20Whitepaper.pdf.

[27] McCarty, N., and Poole, K. *Polarized America: The Dance of Ideology and Unequal Riches*, 1 ed. The MIT Press, 2006. Summary available online at https://mitpress.mit.edu/books/polarized-america.

[28] Middleton, R. Is bitcoin the undisputed best performing asset class of the decade?, 2017. Available online at http://www.zerohedge.com/news/2017-01-25/bitcoin-undisputed-best-performing-asset-class-decade.

[29] National Center for Education Statistics. Digest of Education Statistics, 2016. Available online at https://nces.ed.gov/programs/digest/2016menu_tables.asp, Year 2016, Table 236.55.

[30] Nove, A. *An Economic History of the USSR*, 1 ed. Penguin Books Ltd, 7110 Ambassador Road, Baltimore, MD, 21207, 1972.

[31] Park, J. W. Household checking accounts in the united states, 2012. Available online at http://www.tandfonline.com/doi/abs/10.1080/00219444.1973.10533100?journalCode=vjeb19.

[32] Poole, K., and Rosenthal, H. The polarization of the congressional parties, 2016. Available online at https://legacy.voteview.com/political_polarization_2015.htm.

[33] Poon, J., and Dryja, T. The bitcoin lightning network: Scalable off-chain instant payments, 2016. Available online at https://lightning.network/lightning-network-paper.pdf.

[34] Sahr, R. Inflation Calculator, 2017. Available online at http://www.in2013dollars.com/.

[35] Sar, E. Bittorrent still dominates internet's upstream traffic, 2015. Available online at https://torrentfreak.com/bittorrent-still-dominates-internets-upstream-traffic-151208/.

[36] Sirohi, T. Despite the government crackdown on torrents, these 6 websites are still working, 2016. Available online at http://www.indiatimes.com/news/india/despite-the-government-crackdown-on-torrents-these-6-websites-are-still-working-262274.html.

[37] Smith, A. Record shares of americans now own smartphones, have home broadband, 2017. Available online at http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/.

[38] Statista. Percentage of housing units with telephones in the united states from 1920 to 2008, 2017. Available online at https://www.statista.com/statistics/189959/housing-units-with-telephones-in-the-united-states-since-1920/.

[39] Szabo, N. Shelling out: The origins of money, 2002. Available online at http://nakamotoinstitute.org/shelling-out/.

[40] Sztorc, P. Measuring decentralization, 2015. Available online at http://www.truthcoin.info/blog/measuring-decentralization/, Section "Development".

[41] Taaki, A. Bip purpose and guidelines, 2011. Available online at https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki#What_belongs_in_a_successful_BIP/, bullet point "Backwards Compatibility".

[42] Taleb, N. The risks of financial modeling: Var and the economic meltdown, 2009. Available online at https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg51925/pdf/CHRG-111hhrg51925.pdf,.

[43] Taleb, N. The most intolerant wins: The dictatorship of the small minority, 2016. Available online at https://medium.com/incerto/the-most-intolerant-wins-the-dictatorship-of-the-small-minority-3f1f83ce4e15.

[44] Torpey, K. Purse.io co-founder explains how bitcoin enables their amazon discounts, 2016. Available online at http://insidebitcoins.com/news/purse-io-co-founder-explains-how-bitcoin-enables-their-amazon-discounts/36301.

[45] Torpey, K. Bitcoin sidechain with a bigger block size limit may soon be a reality, 2017. Available online at https://bravenewcoin.com/news/bitcoin-sidechain-with-a-bigger-block-size-limit-may-soon-be-a-reality/.

[46] Trend Micro. Ransomware – past, present and future, 2016. Available online at https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf.

[47] Trillo, M. Stress test prepares visanet for the most wonderful time of the year, 2013. Available online at http://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/index.html.

[48] United Nations Office on Drugs and Crime. World Drug Report, 2016. Available online at http://www.unodc.org/doc/wdr2016/WORLD_DRUG_REPORT_2016_web.pdf, Page 1.

[49] Vanguard. How America Saves, Vanguard 2015 defined contribution plan data, 2016. Available online at https://pressroom.vanguard.com/nonindexed/HAS2016_Final.pdf, pages 51-52.

[50] World Bank, T. "broad money (% of gdp)", "gdp (current us$)", and "gdp growth (annual %)", respectively, 2015. Available online at http://data.worldbank.org/indicator/FM.LBL.BMNY.GD.ZS, .../indicator/NY.GDP.MKTP.CD, and .../indicator/NY.GDP.MKTP.KD.ZG, respectively.