

The Return of Private Money:
Building Private Money in the Fiat Age

William Smith
Dr. Herbener
ECON 401
5 February 2019

Money is not what it used to be. Government, which is prone to market intervention already, monopolizes the money market. Yet, where future profits exist, entrepreneurs will move. Like any other commodity, money can change to the market's preferences, opening up new avenues to outstepping government outreach. In accordance with Carl Menger's and F.A. Hayek's theoretical framework for money adoption, it is found that Bitcoin is a better medium of exchange than fiat alternatives because of its higher salability.

To examine the evolution of money and why cryptocurrencies are an economic response to government interventionism, Menger's *The Origins of Money* and Hayek's *The Denationalization of Money* will be examined. Afterward, an investigation into the monetary theory of cryptocurrencies will be conducted with particular reference to Ludwig von Mises' *The Theory of Money and Credit* and frequent recall to Hayek.

The Genesis of Money

Carl Menger's *The Origins of Money* shows how money is created through a process of choice among individuals. The selection of money is analogous to a whittling: commodities are exchanged until one or a few commodities becomes the media of exchange. Menger dispelled the myth of government money appointment by starting with the genesis of money. In a world void of prices, exchange is conducted by barter which severely limits the amount of trades available. The lack of coincidence of wants, when direct exchange is not possible, initiates the money creation process. In indirect exchange, a common medium of exchange facilitates trade. Commodities, through the whittling process, are selected by individuals based on selective features to become a common medium of exchange. Menger describes this whittling process as *salability*, a good's ability to exchange against other goods.

Salability is a measurement of degrees: goods that have more tradable features are more saleable: “[the] greater or less facility with which they can be disposed of at a market at any convenient time at current purchasing prices, or with less or more diminution of the same.”¹ The economic price and the time of listing versus time of sale, furthermore, are the best metrics of salability.² In other words, the more saleable good will be cost more and be purchased quicker than other goods.

Menger breaks down salability into three categories: 1) at the economic price at any given market, 2) by its spatial limits, and 3) by time. A list for each sub-point will be given as a means of simplification:

The Market ³

1. Demand, its extent, intensity, and longevity.
2. The purchasing power of persons.
3. Available quantity of the commodity in relation to the unsupplied want.
4. The divisibility of the commodity and ways it can be adjusted to the needs of the individual consumer.
5. Development of the market and the extent of speculation.
6. The political or social limitations imposed.

Spatial Limits ⁴

1. The distribution of goods in space.
2. Transportability and cost of transportability in proportion to value.
3. Extent to which infrastructure develops around the commodities.
4. The local extension of organized markets and their inter-communicated by arbitrage.
5. Restrictions to trade both locally and internationally.

Time ⁵

1. Permanence of the need of a commodity.
2. The durability and suitability for preservation.
3. The cost of storing and preserving them.
4. The rate of interest.
5. The periodicity of a market for the same.

¹ Carl Menger, *The Origins of Money*, (Auburn: The Ludwig von Mises Institute, 2009), 25.

² *Ibid.*, 26-27.

³ *Ibid.*, 29-30.

⁴ *Ibid.*, 30-31.

⁵ *Ibid.*, 31-32.

6. The development of speculation.
7. The political or social restrictions on movement of goods over time.

To the degree a commodity holds these features in superiority to other goods, it becomes a more saleable good and, therefore, a better medium of exchange.

The market economy tends towards one media of exchange, implying that a goods salability becomes absolute against other goods. In the barter economy, it is preferable to have a more saleable good than a less: the higher degree of salability, the higher potential for exchange.⁶ The medium of exchange is chosen, therefore, by the choices of individuals within singular exchanges. Overtime, social consensus forms around one commodity which all individuals prefer against other goods. This commodity is called sound money. The value of the entrepreneur should not be overlooked: those who discover, market, and implement saleable features become the most successful traders and play a fundamental role in the whittling process.⁷ Practice and habit, Menger concludes, turn a saleable commodity into the medium of exchange.⁸

A core feature of this whittling process is the absolute nature of a chosen medium of exchange. The very fact that a good is preferred for trade over other goods increases its salability. As this preference grows, salability grows exponentially into the absolute medium of exchange.⁹ Money begins as a commodity, but its absolute salability separates it from all other commodities.

Yet this separation does not go so far as to lose its jurisdiction to individual valuations.¹⁰ In other words, money is not totally disconnected from being a commodity valuation once it gains absoluteness. While a simple observation, it bears significance in that a commodity can

⁶ Ibid., 33-34.

⁷ Ibid., 36.

⁸ Ibid., 36.

⁹ Ibid., 39.

¹⁰ Mises, *The Theory*, 117.

become a money only to later lose this status to another commodity. As technology, tastes and preferences, and other factors that determine the value of goods change, so will the medium of exchange.¹¹

When a commodity becomes absolutely salable, a fork occurs between commodities that become money and those that do not. At this juncture, the true investigation into the value of money starts: “the real problem of the value of money only begins where it leaves off in the case of commodity values, [sic] at the point of tracing the objective determinants of its subjective value, for there is no subjective value of money without objective exchange value.”¹²

The process of money selection results in one medium of exchange. Historically, this has been gold. Often termed money maximalism, the whittling down to one medium of exchange is the consequence of market demand for one media. The use cases for money; such as accounting, transportation, and storage, are optimized under one media.¹³ The government money monopoly has artificially set one medium of exchange, fiat money. This fiat money has huge problems, however, as observed in leakage out of the system.

Looking at the greater money market, the recent emergence of financial technology, or fintech, and more specifically cryptocurrencies, indicates a change in society’s preferences. Indeed, one can even view the various and wide array of alternative stores of value, also known as ‘safe havens,’ as an unnatural event. If fiat money were truly sound, alternative stores of value would not exist on such scales.¹⁴ An implication of coercion derived money is instability: as

¹¹ Ibid., 59.

¹² Ludwig von Mises, *The Theory of Money and Credit*, trans. H.E. Batson (Indianapolis: Liberty Fund, 1980), 119.

¹³ Hans-Hermann Hoppe, “How is Fiat Money Possible? –or, the Devolution of Money and Credit,” *The Review of Austrian Economics* 7, no. 2 (1994): 51.

¹⁴ Alternative stores of value for sound money do exist, but they exist as other producer goods. In today’s fiat system, capital flight to different currencies are often the recourse for a failing fiat currency. Under a sound money system, the money would never depreciated to cause capital flight.

politics change, so does the money. On the other hand, sound money holds value through time. This is evident in the *Belle Époque*, a period of almost uninterrupted growth in Europe between the Franco-Prussian War and World War I. During this period, the gold standard secured wealth.¹⁵ In the United States, the only interruptions, the financial panics of the latter 19th and early 20th centuries, largely occurred because of government monetary inflation.¹⁶

The driving values of historically good money have bearing on future good money. To repeat, sound money is that commodity which holds its salability absolutely against other commodities. The best medium of exchange is that which is fungible, durable, and transportable; these three features are the common reduction of Menger's list. The more a money possess these characteristics, the better money it is.

Fungibility, durability, and transportability boil down to stability. To be stable is to lack volatility in value over time. These features allow for more transactions over space and time because they hold up over space and time. So, the less a good fluctuates on the market against other goods, the superior money it is. As Menger writes, key factors determining stability include the method of production, consumption, and exchange of money.¹⁷ For emerging currencies like Bitcoin, these key factors are consequential to its success as money.

As a commodity, and even more so as the absolute commodity, the medium of exchange takes on two important descriptors: unit of account and store of value. Typically, these features are bundled and inseparable, as Mises writes.¹⁸ However Hayek is more stresses nuance with

¹⁵ Governments coined money during this period, but the market was extremely wary of monetary inflation. Paper bills, furthermore, were backed by gold bullion unlike today's fiat.

¹⁶ Murray Rothbard, *The History of Money and Banking*, Auburn: The Ludwig von Mises Institute, 2002, 167.

¹⁷ Menger, *The Origins*, 49: Due to the limited scope of this paper, money production receives scant review. It is, however, an important factor and would make an excellent addition to this topics research.

¹⁸ Mises, *The Theory*, 47.

consequence. While these two features do flow from a money's foundation as the medium of exchange, they vary by degree when a new currency is being established.

Questions of stability raise questions of value: can the value of money be described in an empirical sense? Yet this question, often posed by governments, misunderstands the nature of money as a value relationship. To define money empirically is a snake eating its own tail: to value a dollar as one dollar brings one back to the original question. Since money is a value relationship, the closest one can approach an empirical definition of money is to call it a price index.¹⁹ As the common medium of exchange, all goods are compared to money. This comparison allows for individuals to forgo knowledge of all commodities and know valuations between money and certain commodities.²⁰ When money is defined properly, essentially ratios to all marketable goods, one can perceive the benefits of stability. A stable money, then, is one that holds its value constant against all commodities.²¹

Government Money

Historically, the government money monopoly was built upon the "seal of approval." The stamping of a head of state or image on metal coins goes back past memory; it stands as a marker of trust and fairness in exchange. If the coin was stamped, it could be trusted more than non-stamped coins. This sign of fairness in exchange, however, is soon exposed for its malicious intent: debasement.

In *What Has Government Done to Our Money*, Murray Rothbard argues that government control of the money supply, under the excuse of mediating exchange, has three immediate implications: government can choose which coins operate on the market and, overtime,

¹⁹ Ibid., 62.

²⁰ Mises, *The Theory*, 62.

²¹ Hayek, *The Denationalization*, 70.

government can choose the fineness of the monetary unit.²² Thirdly, government can intervene on exchanges under the justification of actual ownership of the media of exchange. In the modern fiat system, the debasement of currency is slightly different. For instance, the tool of choice is the interest rate and/or printing paper money. Regardless, the principles of government interventionism, particularly in reference to inflationism, remain the same.

By picking what money operates on the market, Government disrupts the natural process of individual valuation and money selection. Historically, government chose which coins were acceptable on the market. Today, government uses legal tender laws. Legal tender laws do not exclude other monies from being used explicitly, but rather force acceptance of government money for the settling of debt.²³ Herein lies the basis of government fiat money: it is a media of payment and not of exchange.²⁴ Yet, as F.A. Hayek writes in *The Denationalization of Money*, legal tender laws spring up from a misunderstanding of the origins of money.²⁵ The process of exchange created money, not government; a media of payment precludes a medium of exchange. Not only does government misunderstand the origin of money, its mistake inhibits the creditor/debtor relationship. As Hayek writes, “legal tender is simply a legal device to force people to accept in fulfillment of a contract something they never intended when they made the contract.”²⁶ If government truly wished to protect the relationship, they would not enforce legal tender laws that subscribe to one sort of money. Instead, they would allow judgment for repayment on a case by case basis.²⁷

²² Murray Rothbard, *What Has Government Done to Our Money?* (Auburn: Ludwig von Mises Institute, 2010), 57.

²³ Anthony M. Endres, “Currency Competition: A Hayekian Perspective on International Monetary Integration,” *Journal of Money, Credit Banking* 41, no. 6 (Sep. 2009): 10.

²⁴ Mises, *The Theory*, 84.

²⁵ Hayek, *The Denationalization*, 37.

²⁶ *Ibid.*, 39-40.

²⁷ *Ibid.*, 38.

Although the evolution of the market is towards one money, this will not be the total case until a certain point of market integration. A certain currency can work for some people better than others depending on their tastes and preferences relating to their environment. Some may prefer a highly liquid money. Others may prefer a stable money. And yet others may prefer a good store of value. While all these features tend to back one another up, it is not necessarily the case in all instances. As F.A. Hayek writes, currency is an adjective to describe the degree to which a money fulfills certain features of a good money:

By referring to different kinds of money we have in mind units of different denomination whose relative values may fluctuate against one another. These fluctuating values must be emphasized because they are not the only way in which media of exchange may differ from one another. They may also, even when expressed in terms of the same unit, differ widely in their degree of acceptability (or liquidity, i.e. in the very quality which makes them money), or the groups of people that readily accept them. This means that different kinds of money can differ from one another in more than one dimension.²⁸

A simple observation of this fact is found in the different prices of monies on exchanges. People value different monies differently. As will be discussed, the value fluctuations expressed in price fluctuations is integral for the selection of new private currency emerging from government fiat.

Secondly, government separates money from its commodity basis by choosing the fineness of the money, i.e. inflation. This separation is the prerogative for unrestrained government spending. By legally maintaining the value of money at its commodity strength only to separate it from its commodity basis is to steal real wealth from society. As a result, three points occur. First, prices go up to the extent the inflationism is realized. Second, the relationship between creditors and debtors is skewed in favor of debtors. Inflation destroys savings. Lastly, this debasement results in the boom bust cycle. Market recognition of debasement must occur and has been the reason for the collapse of businesses, governments, and even empires.²⁹ The capital structure is twisted through inflation, creating unpayable debt bubbles: “The past

²⁸ Ibid., 55-56.

²⁹ Ammous, *The Bitcoin*, 25-27.

instability of the market economy is the consequence of the exclusion of the most important regulator of the market mechanism, money, from itself being regulated by the market process.”³⁰ A collapse ensues because of the burdensome government spending on the economy, the lack of real savings against entrepreneurial activities, or a combination of both.

Exchange surveillance is the third main manifestation of the government money monopoly. As a third party with political interest, any exchange using the government system comes under bureaucratic scrutiny. From a purely economic point of view, all exchanges are perceived as beneficial in the moment. An exchange would not take place if one did not value the other object greater than one gave up. So, any exchange government interrupts is by definition an economic negative, also called dead weight loss. The government money monopoly allows for a justification of exchange seizure. As will be discussed later, the ability to survey exchange and the subsequent risk for participants is a key reason for the genesis of non-fiat monies in the 20th and 21st centuries.

The Reintroduction of Private Money

The detrimental effects of the government money monopoly are strong enough problems to launch private money once again. More succinctly, the issuing of a private money stems from four conclusions: 1) the most desired feature of money is stability, 2) competition creates more stability than monopoly, 3) issuing institutions would regulate according to market demand, and 4) the market is the best method of regulation.³¹ Any private money would face significant pressure not only getting off the ground on the market, but from the state. The remainder of this paper will outline these pressures and possible responses. The first section will survey Hayek’s

³⁰ Hayek, *The Denationalization*, 103.

³¹ Hayek, *The Denationalization*, 51.

argument in *The Denationalization of Money* and the second section will provide a descriptive economic analysis of the burgeoning cryptocurrency scene.

To Hayek, the reintroduction of private money would come through enterprise.³² A business would issue a limited supply of notes backed by different fiat deposits and baskets of goods.³³ Initially, these notes would be issued through auction at a premium and then via short term loans.³⁴ To the firm, the notes are derivative assets. The firm gains capital from both the initial sale and subsequent appreciation of their own holdings of the money. For purchasers of the notes, they are quasi-investments. Both the issuer and buyer can only expect the notes to rise in value and never fall below the initial sale price.³⁵ This expected rise is because the private fiat is competing against public fiat: public fiat consistently inflates versus all other goods. The comparative strength of private fiat would only increase adoption.³⁶

It is important to note that the business would make no legal claims tying the goods to baskets of commodities. Rather, market competition, particularly the reputation of the business, would decide the fate of the purchasers. While the private fiat could always be exchanged for public fiat at the bench mark, the business has no incentive to keep the relationship between baskets of commodities and the private fiat parallel.³⁷ So, the purchasers take the risk equivalent to the rise in value of the private fiat versus the public fiat. There is a need for competition, therefore, to determine the fate of one's investment.

³² Any attack against the government money monopoly would be detrimental to the state. Violent or coercive retaliation, then, is a real possibility. Although not explicitly discussed, Hayek's use of money stemming from a business initiative possibly sidesteps this threat.

³³ Robert P. Murphy, "Hayek's Plan for Private Money," The Ludwig von Mises Institute, July 2005. Accessed November 12, 2018. <https://mises.org/library/hayeks-plan-private-money>

³⁴ Hayek, *The Denationalization* 47.

³⁵ Murphy, "Hayek's Plan."

³⁶ Hayek, *The Denationalization*, 47.

³⁷ *Ibid.*, 48.

The maintenance of a private fiat system would fall under the question of competition: can the issuing institution match the market demand for money? Three obstacles must be overcome: the company's survival itself, the inevitable fracture between initial reserves and appreciating money, and the ability to predict consumer money preferences. First, the health of this business itself will play into the volatility of the money. The perceived health of the business; as demonstrated via stocks, cash flows, or other mainstream methods, will necessarily move the value of the money. Knowing that the most stable money is the best, the most stable businesses should have the best money. When looking at business failures and fluctuations overtime, it may seem foolish to entrust private enterprise with currency production. Institutional arrangements, however, would take place, mitigating the volatile effects of business performance. One such arrangement, for example, would be a joint money. Multiple companies could band forces and issue a more stable money. The institutional nature of knowledge development is perfectly compatible with the nature of competition, moreover.³⁸ In fact, it will result in the optimum outcome: those money producers who fulfill the consumers' needs best will survive. In more direct language, those who are able to maintain money stability against business fluctuations will compete best.

Second, as the private fiat appreciates in value against the public fiat, a fracture will develop between the actual reserves and outstanding notes. Yes, the issuers pledge to redeem the notes to goods is nonbinding and the notes would only be equivalent to the initial level of fiat. Yet, the issuing company has a continuing monetary incentive to keep their money alive: as the money appreciates, the issuing institution's stake appreciates. For the money to depreciate so rapidly as to cause a re-exchange of public for private fiat represents a significant loss of capital

³⁸ F.A. Hayek, "The Meaning of Competition," *Econ Journal Watch* 13, no. 2 (May 2016): 363.

for the issuing firm. So, the firm must mind the fracture. The fracture, like modern day fractional reserve banking, can be maintained to a degree of certainty. Moreover, as more issuing institutions participate and are weeded out, the weaker private fiat will collapse—time tells all. Issuing bodies must be mindful of the extent of the fracture.³⁹

In the private money market, the degree to which an issuer is able to perceive the consumer demands is the degree to which the issuer will be successful. Indeed, the outcome of this entrepreneurial process is the nexus of the issue:

The question we have to consider is whether competition between the issuers of clearly distinguishable kinds of currency consisting of different units would not give us a better than we have had, far outweighing the inconvenience of encountering more than one kind.⁴⁰

Once private money is reintroduced on the market, the question of the private money's performance is a question of knowledge: how is the knowledge dispersed, to what degree, and what are the implications?

The return of private money is not dissimilar to the genesis of money: both utilize the dispersal of knowledge by economizing individuals. In *The Use of Knowledge in Society*, Hayek contends that it is the very nature of knowledge to reside across space and time. In other words, knowledge is dispersed in localities: “the dispersed bits of incomplete and frequently contradictory knowledge which all the separate individual's possess.”⁴¹ By implication, a decentralized system is superior to centralized one. Centralized knowledge, or scientific knowledge, excludes entire bodies of knowledge because of the contradiction between knowledge and centralization: not everything can be known or catalogued. The return of private money, therefore, must start from this understanding. Only through decentralizing money can the

³⁹ Hayek, *The Denationalization*, 49.

⁴⁰ *Ibid.*, 51.

⁴¹ F.A. Hayek, “The Use of Knowledge in Society,” *The American Economic Review* 35, no. 4 (Sep 1945): 519.

best features of it come forth. For ease of analysis, the question of knowledge dispersal will be divided into consumer knowledge and issuer knowledge.

To the consumer, prices relate knowledge. Prices are the summation of the ideas, ends, and means for attaining an action.⁴² To the economizing individual, the money that best suits his purposes, often stability, will be selected. Yet, will the money the individual select align with the rest of the market?⁴³ The issue of public adoption, then, is a chief concern of issuing institutions. Consumer adoption of private monies is dependent on the rate of knowledge dispersal throughout society. Like all other market activities, the best money—dependent on its real and behavioral features—will be selected by individual valuations that turn into group consensus.⁴⁴ Worse alternatives will die off.

In currency competition, consumer money valuation comes not only in the real features of money, but also based on its behavior. Behavioral descriptors of money as applies to consumer valuations comes in two forms: acceptability/liquidity and expected behavior/stability.⁴⁵ Liquidity and stability can be described as behaviors because they are non-permanent features of the money: they change depending on the supply of and demand for money. These two behaviors, furthermore, are interdependent to a degree: as variable features, they are not locked in stride. Consumers, then, can choose to use a money with higher liquidity than stability or vice versa. For instance, one could pay with a checking account over gold bullion. As the market closes in on one medium, however, these features tend to become totally

⁴² Ibid., 525.

⁴³ Hayek, *The Denationalization*, 54.

⁴⁴ By real, it is meant the money's durability, fungibility, and transportability. By behavioral, it is meant a money's reaction to supply of and demand for it on the market.

⁴⁵ Hayek, *The Denationalization*, 57.

compatible. Consumer choice of money is dependent on knowledge dispersal of real and behavioral factors.

Free floating bits of societal knowledge coalesce in the price of money. Competing currencies show their relative strengths and weakness via their price. The price of a money is a comparison to the most stable money. Wrapped up in this money price is the consumer valuations of the different features of that money.

Just like the consumer, the issuing institution must act according to its grasp of the knowledge at hand. As stated, the issuing institution is in a uniquely difficult spot: determining market demand for its money. This determination is similar to regular market production, yet dissimilar in that it involves effective regulation of its product. The goal may still be profit, but not through typical means.

The issuing institution has two methods for altering the volume of currency in circulation: sell or buy the currency against others or expand or contract its lending activities.⁴⁶ To control the currency, Hayek writes, the issuing institution would have to employ short term loans. Hayek describes institution maintenance the following way:

To assure the constancy of the value of its currency the main consideration would have to be never to increase it beyond the total the public is prepared to hold without increasing expenditure in it so as to drive up prices of commodities in terms of it; it must also never reduce its supply below the total the public is prepared to hold without reducing expenditure in it and driving prices down.⁴⁷

The demand to hold money and the demand for purchases are indicators of consumer demand for money. For the issuing institution, circulation rates are a useful indicator of consumer demand for money. Circulation rates can be broken down via the interest rate, the price against

⁴⁶ Ibid., 59.

⁴⁷ Ibid., 60.

commodities, and the price against other currencies.⁴⁸ In other words, the current and future price of a private money indicates the performance of the money.

A counter point to private money creation would be the glaring information asymmetry that exists between money consumers and money producers. At any point, particularly when the money has appreciated considerably, an entrepreneur could find it more personally expedient to exchange his personal stake of currency for another, and then abandon the maintenance of his private money. To call this money dumping a market failure, however, is shortsighted. The process of creative destruction weeds out entrepreneurs who would choose such a strategy. Institutional features, it is certain, would also provide a bulwark against such actions. Lastly, currency dumping like this could only occur early on as reputations are being established. If an issuing institution has any perceived weaknesses in the short run, it will fail to make it in the long run. Currency dumping could only be short run phenomenon.

Cryptocurrencies

Cryptocurrencies are the societal response to the government money monopoly. While government has intervened in money ostensibly since its genesis, a complete fiat money is relatively new. Ever since the United States officially left the gold standard in 1971 under President Richard Nixon, the U.S.D. has been completely severed from its commodity basis, gold. Cryptocurrencies may have several additional features that improve upon U.S.D., but the rise of cryptocurrencies can only be viewed in light of this separation. Indeed, the introduction of total fiat money was an unheralded event in economic history.

In vain with Hayek's argument, the remainder of this paper will focus on Bitcoin, minus some observations of the cryptocurrency market in general, because of its dominance to date.

⁴⁸ Ibid., 60.

Not only is it the first successful cryptocurrency, but all other alternative cryptocurrencies (altcoins) are based on it. It is the most competitive cryptocurrency and, therefore, the best for analysis.

Before moving on the economic analysis of cryptocurrencies, a quick glance at the relationship of gold and cryptocurrencies is needed. It is commonly posed that if gold was free of government coercion, cryptocurrencies would never exist. While perhaps an interesting question, it can only be answered through competition and not speculation. Both currencies hold features the others do not and only individual valuations of salability could determine the outcome.⁴⁹ In fact, it is possible to foresee a coupling of gold and cryptocurrencies, like the early 2000s BitGold, or a system of multiple currencies. To pursue this question further is to misunderstand the competitive process entirely.

A cryptocurrency is form of digital money backed by public key encryption that allows peer-to-peer transactions via a decentralized, open-source financial network. Bitcoin is a digital currency that mimics, and arguably expands upon, the gold standard. Lastly, Bitcoin is a philosophically rich monetary scheme purposefully built to strip away government monetary power.⁵⁰

Bitcoins are earned through hash mining. Instead of mining the earth's crust for gold, one's computer solves complex math equations. In return for computational power, a digital coin is dispersed from the program. These coins can then be transferred to a digital "wallet" on a phone or computer which acts as an encrypted folder holding the private "key" to your coins.

⁴⁹ Saifdean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, (Hoboken: Wiley, 2018), 205-212: For a thorough discussion of the benefits of cryptocurrencies, particularly Bitcoin, over gold, see Ammous discussion of "International and Online Settlement." In essence, Ammous argues that cryptocurrencies have superior settlement services due to the physical limitations of gold. Cryptocurrencies have low transactions cost relative to gold and bypass political boundaries with comparative ease.

⁵⁰ Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *The Satoshi Nakamoto Institute*, accessed December 12, 2018. <https://nakamotoinstitute.org/bitcoin/>: 1.

These digital coins can be spent through commercial enterprises that adopt Bitcoin. When a good is bought with Bitcoin, the exchange is recorded on an open digital ledger, the blockchain. The blockchain is a permanent ledger of all bitcoin transactions ever, stored on an open access network. When a Bitcoin is exchanged for a good or service, the privacy key is exchanged between the two parties while the public key records the transaction on the blockchain. In this way, all transactions are available to the public but the actors remain private. The exchange of keys initiates the transaction and the recording on the blockchain signifies closes it.

The crucial innovation of Bitcoin, and therefore all cryptocurrencies, is blockchain's open source ledger. Among other things, the ledger's public proof of purchase stamp is a main source of value to Bitcoin. Just like an accountant's book, the blockchain holds the record of all financial ins and outs. Since it is public, no custodian is necessary, but all can see a transaction took place. Yet, since it is encrypted, the transaction remains private.⁵¹ Consequently, for the first time in human history, peer-to-peer exchanges can take place over great distances among total strangers with total confidence.

Cryptocurrencies in the Hayekian Framework

Hayek's *The Denationalization of Money* is a powerful framework for return of private money, but it is no way completely authoritative. Hayek even admits as much: "I am inclined to think that, by [private enterprise] habitual procedure of selecting the most successful [money], it would in time throw up better solutions to these problems than anyone can foresee today [sic]."⁵²

Hayek's argument was merely a proposal for returning private money to the market. His

⁵¹ See Eric Hughs' *The Cypherpunk Manifesto*: A distinction between private and anonymous must be made. Privacy concerns selectively dispersing one's information to different parties. Anonymity is total secrecy where private information is not shared at all. Bitcoin allows for both types of transactions depending on one's commitment to covering one's tracks.

⁵² Hayek, *The Denationalization*, 102.

observations and predictions are helpful and should not be dismissed, however. The examination of profit incentive, competition, knowledge, and stability are fundamental to the analysis of the burgeoning cryptocurrency market. For the purposes of this paper, two of the most salable features of Bitcoin have been selected for examination.

Before jumping into these features, though, it is necessary to make a distinction between Hayek's fiat money and cryptocurrencies, a commodity money. Bitcoin's basis as a commodity makes it a stronger money than Hayek's fiat or government fiat money. As Mises writes, commodity money is "that sort of money that is at the same time a commercial commodity; and the name fiat money to money that compromises things with a special legal qualification."⁵³ A fiat money lacks a commodity basis: its value is found in its acceptance for payment via threat of government violence.⁵⁴ As stated, Hayek's private fiat is backed by a pegged claim to different fiats and a non-binding pledge to basket of goods. The pegging to government fiat makes it a fiat currency.

Cryptocurrencies, on the other hand, and particularly stronger cryptocurrencies such as Bitcoin, have no legal backing. The value is entirely wrapped up in consumers demand for its functions. It is true that both Hayek's private money and cryptocurrencies are born from commercial transactions—the only true way money can be created—but there does exist a real difference between the backings of the currencies.⁵⁵

Critics of Bitcoin, particularly gold enthusiasts, point out that Bitcoin lacks physical features which would give it commodity value. Indeed, Mises describes a commodity money as one with physical properties.⁵⁶ The precious metals, for instance, are often touted as the best

⁵³ Mises, *The Theory*, 74.

⁵⁴ Rothbard, *What Has*, 49-50.

⁵⁵ Mises, *The Theory*, 74.

⁵⁶ *Ibid.*, 74.

mediums of exchange because of the industrial demand for gold, silver, and other metals. This observation, however, is a misunderstanding of use-value and objective-exchange value. The value of money is thoroughly subjective according to the objective-exchange value: what properties of a medium of exchange make it a better medium?⁵⁷ Initially, the medium of exchange's value is found in its use as a commodity. Yet, Bitcoin steps into the competitive money market mid-scene: there is no need for regressing the value backwards through time. Additionally, to mistake use-value and objective-exchange value is to misunderstand the nature of money. The salability of a media give it its value, not its objective exchange value as a commodity and certainly not the fact it is tangible. This is proven historically: the South Sea Islanders of Yap used Rai stones—often larger than a man—as a mediums of exchange. While the stones could not be moved with ease, and therefore lacked commodity value, they had objective-exchange value as means of payment.⁵⁸ When a purchase was made, the owner of the Rai would merely announce to the community the stones new owner. The value of the stone lay in their ability to conduct exchanges. So, is the case with all money: the objective-exchange value supersedes its use-value. The value of money is found in objective-exchange value stemming from its salability.

Bitcoin's value operates in a similar manner: it has no physical presence, but high salability. Amongst many other features, the Bitcoin's unique governance protocol embedded in its very code raises its salability higher than any alternative. Other engineered features of Bitcoin exist, such as its scalability or use as a global unit of account, but the breath of this paper necessarily limits the scope of investigation. As discussed, Menger's key factors determining the stability of money include the method of production, consumption, and exchange of money. The

⁵⁷ Ibid., 118-119.

⁵⁸ Ammous, *The Bitcoin*, 12.

engrained features of Bitcoin fulfill these factors better than any money to date: the method of exchange is enhanced by sidestepping third party intrusions; Bitcoin is scalable over time for consumer needs; and Bitcoin production is mathematically set.

The anti-state features of Bitcoin can most easily be divided into anti-surveillance and anti-inflationary measures. First, Bitcoin is anti-surveillance because of cryptography. Satoshi Nakamoto, the anonymous creator of Bitcoin, built Bitcoin on public key cryptography. Public key cryptography is a mathematical method of sending and receiving related numbers. The exchange of public keys, private keys, and blind signatures, allows for the transmission of information with total privacy. In turn, the network can verify transactions by matching the address points and public key.⁵⁹ The implications of this technology are 1) the total privacy of parties exchanging goods, such as Bitcoins, 2) a reliable financial network independent of a third party, and 3) the ability to send money across space—particularly political boundaries—with relative ease.⁶⁰ Cryptographic privacy is a highly salable feature of Bitcoin because it sidesteps third parties.

Second, Bitcoin's engrained hard cap ensures low volatility upon widespread public adoption. Nakamoto programmed mining to stop at about 21 million bitcoins. This number, however, will not be met till around 2140.⁶¹ Mining, furthermore, is tied to a difficulty algorithm

⁵⁹ Ammous, *The Bitcoin*, 192.

⁶⁰ Nakamoto, "Bitcoin," 1; Hayek, *The Denationalization*, 125: "The extent of the control over all life that economic control confers is nowhere better illustrated than in the field of foreign exchanges. Nothing would at first seem to affect private life less than a state control of the dealings in foreign exchange, and most people will regard its introduction with complete indifference. Yet the experience of most continental countries has taught thoughtful people to regard this step as the decisive advance on the path to totalitarianism and the suppression of individual liberty. It is in fact the complete delivery of the individual to the tyranny of the state, the final suppression of all means of escape—not merely for the rich, but for everybody. Once the individual is no longer free to travel, no longer free to buy foreign books or journals, once all means of foreign contact can be restricted to those whom official opinion approves or for whom it is regarded as necessary, the effective control of opinion is much greater than that ever exercised by any of the absolutist governments of the seventeenth and eighteenth centuries."

⁶¹ Ammous, *The Bitcoin*, 179.

that calibrates coin dispersal according to the price.⁶² The result is absolute, mathematical scarcity. Scarcity, in turn, breeds stability: “Bitcoin has the supply restrictions that could make it have considerable demand as a store of value; in other words, it can have salability across time.”⁶³ Bitcoin’s encoded scarcity gives it superior stability over other cryptocurrencies.

Lastly, Bitcoin is also divisible to the 100,000,000th unit, called a Satoshi, making it “salable in scale.”⁶⁴ As deflationary pressures increase the price of Bitcoin, the Bitcoin-based economy can grow through its high divisibility. Already, applications such as the Lightning Network are building on top of this feature to increase Bitcoin’s use as a common means of payment. As the capital structure grows and Bitcoin’s inflationary rate decreases, Bitcoin can adapt to consumer needs for divisible units of exchange.

For the time being, Bitcoin does remain volatile. Since the supply schedule of Bitcoin is essentially set, it is particularly prone to market movements. Bitcoin only makes up one percent of the world’s supply of money and large transactions or small movements in demand have tremendous effect on its price.⁶⁵ This volatility, though, is a necessary stage of competition. Just as described by Hayek, individual valuation grows according to knowledge dispersal. As Bitcoin is adopted, it will become more stable. Indexes of Bitcoin’s volatility since its launch in 2009 show a substantial decrease in volatility: volatility spikes of Bitcoin against the U.S.D. above 15 percent were once quite common, but now only make sensational headlines.

Cryptocurrencies are a response to the government money monopoly. The embedded features were designed by entrepreneurs to mimic the best and improve upon features of other currencies. Chief amongst these are anti-surveillance and anti-inflationary measures. The

⁶² Ibid., 179.

⁶³ Ibid., 181.

⁶⁴ Ibid., 181.

⁶⁵ Ibid., 213.

adoption of cryptocurrencies is dependent on the rate of knowledge dispersal: if a currency is better than the alternatives, it will succeed and become the new medium of exchange.

Bibliography

- Ammous, Saifdean. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Hoboken: Wiley, 2018.
- Endres, Anthony M. "Currency Competition: A Hayekian Perspective on International Monetary Integration." *Journal of Money, Credit Banking* 41, no. 6 (Sep. 2009): 1251-1263.
- Hayek, F.A. *The Denationalization of Money: The Argument Refined*. London: The Institute of Economic Affairs, 1990.
- _____. "The Meaning of Competition." *Econ Journal Watch* 13, no. 2 (May 2016): 359-372.
- _____. "The Use of Knowledge in Society." *The American Economic Review* 35, no. 4 (Sep. 1945): 519-530.
- Hoppe, Hans-Hermann. "How is Fiat Money Possible? –or, the Devolution of Money and Credit." *The Review of Austrian Economics* 7, no. 2 (1994): 49-74.
- Menger, Carl. *The Origins of Money*. Auburn: The Ludwig von Mises Institute, 2009.
- Murphy, Robert P. "Hayek's Plan for Private Money." The Ludwig von Mises Institute, July 2005. Accessed November 12, 2018. <https://mises.org/library/hayeks-plan-private-money>
- Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." *The Satoshi Nakamoto Institute*. Accessed December 12, 2018. <https://nakamotoinstitute.org/bitcoin/>
- Rothbard, Murray. *The History of Money and Banking*. Auburn: Ludwig von Mises Institute, 2002.
- _____. *What Has Government Done to Our Money?* Auburn: Ludwig von Mises Institute, 2010.
- Von Mises, Ludwig. *The Theory of Money and Credit*. Trans. H.E. Batson. Indianapolis: Liberty Fund, 1980.