Danny Nguyen

BCUSP 135D

Katherine Voyles

10 March 2014

Future of Bitcoin and the History of Economies

With the rising concern over the financial future of the global economy, confidence of the average consumer and the most dedicated of investors have fallen significantly. Many are turning to Bitcoin, a purely digital currency where instability unlike anything the global economy has ever seen is just part of doing business with it. With its decentralized network putting it mostly out of the reach of regulators making financial institutions unnecessary, bitcoins have the potential to come out as the dominant global currency. Today's economy has moved a long way from its roots in the systems of barter that once drove it. From trading goods and services that both parties desired, all the way to placing value economic models that guess at the future of the economy. People have moved from the exchange of commodities that both party desired to the use of common currency, representing the value of a commodity that only one of the trading party needs to desire. Then value was abstracted further by systems of credit and investment. Where once value was represented by currency, trust and confidence of repayment and financial growth have taken its place. After layers upon layers of abstractions that is the modern economy comes Bitcoin, an open source peer-to-peer network and digital currency where value is determined by everybody agreeing that bitcoins have value.

Like every evolution in economic activity, they all find their roots in the system of barter. Barter itself is the direct exchange of goods or services by at least two parties, where both parties must be interested in what the other has to offer. This served well enough as transportation in

early history did not make long distance travel viable, meaning any form of economy would have been localized to neighboring villages. However barter had its limitations. As described by English economist and logician William Stanley Jevons, a doctor of law, a master of arts, and a fellow of the Royal Society, who wrote in his book *Money and the Mechanism of Exchange* the biggest limitation is the need for a "double coincident of wants" (Jevons 4) which requires both parties to want what the other has for barter to occur. This becomes a problem because of the improbability of the wants, the needs, or the events that cause or motivate a transaction happening at the same time and the same place. Another is the lack of a common measure of value. One cow may be worth two sheep between two farmers, but that may not be true to another pair of farmers or that same cow may be worth three sheep with another farmer. This becomes a larger hindrance when trading for commodities such as spices or precious stones as they have no practical or intrinsic value to begin with. Then there is the problem of storing wealth. If a society relies exclusively on perishable goods, such as crops, storing that wealth for the future quickly becomes impractical (Jevons 6). These limitations and others are part of what kept early economies from growing. The solution that rose to deal with these limitations was currency.

The emergence of currency allowed commerce to extend throughout the years and expand further beyond community boundaries. Adam Smith, a pioneer of political economy, described the origin and use of money in his book *An Inquiry into the Nature and Causes of the Wealth of Nations*. The earliest modes of trading with currency were the things with the greatest utility or reliability in terms of re-use and re-trading, which was determined the nature of the object or thing chosen to exchange. Some of the earliest currencies being barley or copper.

Commodities where what many societies used to measure value for any other goods or

services. However, since crops where perishables, or when some other commodity is simply not in demand, many traders used an intermediate commodity which could be in demand all year round such as copper, silver, or gold (Smith 26). Metals where commonly used for this function because they can be kept with little loss for hardly any substance is less perishable, and likewise can be divided and combined without loss. This created a standard of value that many people could easily recognize and advance commerce to allow not only easier trading but also easier borrowing and lending. Every person who makes a contract and expects to receive something at a future day, will prefer to have the security of a commodity that will likely to be as valuable then as now rather than one which its value fluctuates with the seasons (Jevons 6). What this creates is an item that embodies value in a convenient form. Money tends to circulates backwards and forwards around the same area a multitude of times, and may sometimes return to the same hands over and over. But at times a person may want to condense their property into a smaller form so that they may store it away, or carry it with them on a long journey, or transmit it to a friend in a distant country. A form of money becomes necessary that is very valuable, with of little bulk and weight, and which will be recognized as very valuable in every part of the world (Jevons 6). Now trading can occur well beyond not only community boundaries, but also beyond states and nations.

To this same end, promissory notes grew in popularity as technological advances allowed for broader use. A promissory note is a legal instrument in which one party promises in writing to pay a determinate sum of money to the other, either at a fixed or determinable future time or on demand of the other party. Most promissory notes usually take the form of banknotes or pawn tickets. Promissory notes are similar to coins as they where created to represent value in a form with minimal bulk and weight. The differences between the two are where they represent and

abstract their value from. Where coins derive their value by the metal they are stamped from, promissory notes (bank notes in particular) are receipts which the party issuing the notes is promising that they hold a commodity equal to the value written on the note which gives the note value. The commodities may vary between specific parcels or packages to general commodities of the same brand (Jevons). While this makes promissory notes very versatile, this has also created confusion at the point of trade. As Jevons states:

> He who has made a special promise to give definite parcels of goods in return for particular individual papers, cannot issue any such promissory papers without holding corresponding goods. If he does so, he will be continually liable to be convicted of fraud or default by the presentation of a particular document. (Jevons 20)

This works well enough whenever money is being exchanged for exact quantities of a particular commodity. The issue arises when a promissory note is issued on general terms allowing any promissory document to be met by any portion of commodity of the proper quality or quantity (Jevons 20). This has given promissory notes a speculative issue as the value of the commodities the notes are suppose to represent are unclear, making the value of the notes being backed by an abstracted promise.

The speculative value of promissory notes exemplifies the next layer of abstraction in the history of economic activity, which is the use of credit. As commerce continues to prog[1]resses, people will begin to borrow and lend money with those they trust, giving rise to credit[1]. Credit is the trust which allows one party to provide resources to another to be reimbursed later, in place of immediate payment upon completing the transaction and deferring it till later. Usually the

---

1. Information regarding credit gathered from the article "Credit" in the *Encyclopedia of World Poverty* and the article "Money." from the *International Encyclopedia of the Social Sciences*

reimbursement is made with interest which is usually determined as a percentage of the initial payment and computed annually, which makes the future payments greater than an immediate payment would have been. As Julian Schuster describes “Credit enables producers to close the gap between production and sales of goods and services, and it allows consumers to purchase goods and services at the present time and pay for those services from their future income.” (Schuster 215). Common forms of credit includes credit cards, installment loans, retail loans, pawns, and mortgages.

Many lenders in today's economic world use a formula known as the six C's of credit when evaluating a credit worthiness. The first is character which is essentially a summary of the individual. Creditors look for people who appear to be trustworthy and reliable, and who are willing and able to meet their financial obligations. The second is capacity. This is the individual's ability to repay the loan; it is based on present and anticipated earnings balanced against any existing debts. The third is collateral or an item pledged by the borrower as security for the loan, which may be real state, stocks, savings, or mortgage. The fourth is the regulatory and economic conditions. Regulatory conditions apply to the lenders individual circumstances; for example, when banks are not lending in specific areas. Economic conditions determine the lender's general policy towards loan. Both are affected by the current economic cycle. Fifth is the borrower's credit history. As record keeping becomes more and more prevalent, a lender who does not know enough about a borrower's character can always refer to the borrower's past history of borrowing and repayment. Finally there is capital which is the net worth of the borrower. These are many of the guidelines that are used in lieu of personal economic interactions to determine trustworthiness and therefore credit worthiness. This formula combined with a multitude of factors that can influence these areas are then calculated into a credit score, a

numerical value representing credit worthiness. In the United States, a credit score is primarily based on credit report information, a record of borrowing and repayment, typically from one of the major credit bureaus, to calculate a three digit score, generally from three hundred to eight hundred fifty for a generic FICO score. While usually applied to individuals, any entity can have a credit score be it businesses, individuals, corporations, or whole countries. With credit effectively being what modern promissory notes are being backed by this allows for the possibility as Jevons states "...to create a fictitious supply of a commodity which does not exist..." (Jevons 20). This flaw has allowed large sums of money to be moved around and markets to be rigged which exploits the supply and demand of both commodity and currency.

With more and more traders trading in assets and promises, along with the introduction of the internet, a new practice has become a powerful force in modern economics which is the practice of high frequency trading (HFT). While we have been abstracting from value throughout the history of economics, now we have abstracted the process in which we have determined value. As described by Jacob Loveless, Sasha Stoikov, and Rolf Waeber, researchers at Cornell Financial Engineering Manhattan and Lucera HQ and authors of Online Algorithms in High-Frequency Trading, instead of trading occurring at exchanges such as the New York Stock Exchange where people gather to get their trade intentions heard, much of trading today happen on electronic servers in data centers where computers have replaced humans in communicating their trade intentions (50). This has led to the rise of traders and firms dedicated to this new electronic environment. While the intentions are the same, to buy an asset from one location or trader then sell it to another location or trader for a higher price, the difference as stated by the authors "The defining difference between a human trader and an HFT is that the latter can react faster, more frequently, and has very short portfolio holding periods" (50). Within a blink of a

human eye a HFT algorithm can complete multiple trades, a feat of which a human trader can not come close to competing with. Not only are these computer programs fast, they are competing with one another. There are many algorithms active in the market today, all trying to net as much money as possible for the company using them, and many more programmers designing and optimizing new algorithms to out perform each other. In today's highly technological society, more and more value is being placed on the means in which value is determined rather than the end commodity that is or is not valuable.

Economics as we know it is layers upon layers of abstractions, each furthering this story from the last, then comes the introduction of Bitcoins in 2008. Bitcoin is an open-source, peer-to-peer digital currency which first appeared in an academic paper published online by someone called Satoshi Nakamoto (actual identity is still unknown). Until the creation of Bitcoin, online transactions always required a trusted third-party as an intermediary. As Jerry Brito, a Senior Research Fellow at the Mercatus Center at George Mason University and Director of its Technology Policy Program, described in his overview “Bitcoin: A Primer for Policymakers” he states that “Without such intermediaries, digital money could be spent twice” (3). This is known as the “double-spending problem” which meant that a financial institution or a private company was needed to keep track of money as it is moved from one party to another across the internet. What makes Bitcoins revolutionary is that it does not require a third party to solve the issue of double spending. Bitcoin does this by distributing the necessary ledger among all the users of the system via a peer-to-peer network called the block-chain (3). Money transferred on this Bitcoin network is denominated in bitcoins, making this system a currency as well as a payment network.

It is to be noted that Bitcoin refers to the peer-to-peer network and the protocol that

dictates it while bitcoins are the currency denomination. Each individual bitcoin has a unique identification and every transaction is time-stamped on each bitcoin, and new transactions are checked against the block chain to ensure that the same bitcoins haven't been previously spent by the same user, thus eliminating the double-spending problem (3). Now thousands of users on a global network are the intermediaries. The bitcoins themselves used in these transactions are really chains of digital signatures of every former owner of the bitcoin. As Nakamoto describes the process in the original essay, *Bitcoin: A Peer-to-Peer Electronic Cash System, "Each owner transfers the coin to the* next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership" (Nakamoto 2). With this as the backbone of the blockchain, each user confirms each transaction and every transaction is announced to the entire network, keeping this public ledger constantly updated and verified (2).

To keep this infrastructure healthy, individuals known as miners contribute their computer's processing power to solve a cryptographic problem which authenticates the network. As a reward for contributing time and electricity they are given newly created bitcoins and transaction fees (Brito 5). However bitcoins were designed to mimic the mining of gold and other precious metals so this process of mining bitcoins will not last forever (Nakamoto 4). The arbitrary number chosen to be the cap is 21 million bitcoins, with the last hundred millionth bitcoin expected to be mined in 2140 (Brito 5) after which the only incentive will be transaction fees. And as more processing power is dedicated to mining, the protocol will increase the difficulty of the cryptographic problem to ensure that bitcoins are always mined at a predictable and limited rate.

After establishing that Bitcoin is a global network of users along with being a

decentralized currency, the question becomes what makes this different than any other forms of money. The first and most obvious is its decentralized nature. Because it is the users who each contribute to maintaining the network, no authority is ever directly in control of bitcoins, making regulations on bitcoins both difficult and unreasonable. This also means that there is no central infrastructure that can be attacked which eliminates that potential of complete system shutdown. This also means that issues of transaction and fraud cannot be solved administratively and is left to the user.

The second difference is that bitcoins are pseudonymous. As Brito covers in his primer, bitcoins fall between two extremes, on one hand bitcoins are handled similar to promissory notes as bitcoins exchanged between two users without any oversight, on the other hand every bitcoin transaction is recorded between the two keys, the time, and the amount transferred (5). What this means is that while those public keys are publicly viewable, a person's actual identity is not directly linked to that public key, and in fact one user can have multiple public keys if he or she so chooses (5). This is also what makes creating regulations for bitcoins so difficult since it is not readily known who any two users are or what country they are even from, which makes bitcoins also an attractive option for crime as Bitcoin does not easily fall under the jurisdiction of any law or law enforcement in the world. The psuedonymity of bitcoins can even lead to a potential solution to poverty and oppression by allowing access to financial services (7). This furthers the story of economic abstraction because now even the two parties in a transaction are unknown behind an alpha-numeric key.

The third major difference between bitcoins and more tradition commodity and fiat money is its sheer volatility. The bitcoin market has already gone through at least six major price adjustment in the last two years. Prices of single bitcoins have swung upwards of three thousand

percent increase within a month only to drop right back down. One of the most recent example is the shutdown of Mt. Gox, at the time the largest bitcoin exchange around. At the beginning of writing this paper, the price per bitcoin at Mt. Gox averaged around nine hundred and eighty dollars. Then Mt. Gox stopped all bitcoin trading due to reports of a critical bug found within the Bitcoin protocol, which later changed to a massive security breach by hackers stealing over one hundred million dollars worth of bitcoins. Within two weeks of this news, the price of bitcoins at Mt. Gox plummeted down to just above one hundred dollars along with the exchange going into bankruptcy. These are some of the challenges that Bitcoin faces as it moves forward, however it is to be noted that many of these challenges are similar to what more traditional money faces.

What does this truly mean for Bitcoin in the larger economic world and this story of abstractions? First of all, Bitcoin provides an innovative solution to digital currency and online transacting. At its core, it is a digital ledger system that the general populace maintains to allow money to be moved digitally. In terms of the history of currency, this is a natural evolution as technological progress is being made. Its peer-to-peer network has open the gates to those who wish for an alternative that sidesteps regulations whether for ease of use or just having open access to a source of finance. However none of this is too dissimilar to how we use traditional money. Where it begins really branch away from mainstream economics is how value is determined. Nowhere in the Bitcoin protocol says how the price of bitcoins is determined. So the value is set by an unspoken agreement between all users that bitcoins have value. That is it. There are no commodities that bitcoins are based upon. The conversion between bitcoin and fiat money is just a tool to illustrate a bitcoin's value, it does not set its value. There is no system of trust between any party. The fundamentals of credit simply does not apply in the Bitcoin protocol. GDP, interest rates, inflation, unemployment and every other macroeconomic variables

do not apply to bitcoins as they do not exist within the system. We are not just abstracting value into bitcoins, we are making it up on the spot without the historic baggage of past monies.

Whats more, as bitcoin is only exists digitally, it's not just money but smart money. As one of the core Bitcoin developer, Jeff Garzik, says “Ultimately Bitcoins are data, and you can use a data transit protocol to transit information other than just 'I'm sending you Bitcoins.” which makes Bitcoin a technological innovation akin to the internet. So far we are just using bitcoins for its obvious use, money. But what makes this really interesting are the applications of Bitcoin beyond economics. One use for the Bitcoin network as suggested by Brito in his article “Bitcoin: More than Money” is that it can be used as a decentralized notary service, allowing anyone to verify that a particular document existed at a certain point in time (Brito). His example is of a movie screenplay which before it makes its rounds through Hollywood, the author registers with the Bitcoin network proclaiming that the author had the screenplay first. This is a major boon towards copyright as now ownership can be tracked every step of the way. Another application is being developed by Joe Cascio, a semi-retired software engineer, to address the issue of anonymity on the internet. Because signing up for online services is often free and easy, an individual user can repeatedly create accounts to harass, spam, or otherwise be a nuisance to other users, combating this without comprising the original service for other users was impossible without constant administration, especially for services that caters to a community in the several millions. What Cascio is developing is based on the fact that bitcoins are all uniquely identified to remove these malicious users. An example is a website may require you to have a bitcoin wallet balance of one hundred dollars, if you do then you may register for the website. Because bitcoins and wallet ID is not directly linked to your real identity your anonymity is preserved and if an administrator decides to ban you from the website, the administrator can ban

the bitcoins you used to register. You never paid any bitcoins to register for the website and if banned you still keep your bitcoins, however if a malicious user wants to register a new account that user must register with a different set of bitcoins worth one hundred dollars making it an expensive proposition fast. "The fact that you can observe the history of a Bitcoin address is important because it means that you can't play Three Card Monte with IDs," says Cascio. These are just two examples of Bitcoins moving beyond money and, much like the internet before it, Bitcoin can have just as a large social impact as the internet.

Money has had a long history of abstracting value with each new advance in commerce. This is why so many people are paying attention to Bitcoin as it is not just the next evolution but also a new revolution. Bitcoin was created with all the lessons learned from the history of economics. The creators of Bitcoin drew from that history but made something the scope of which could expand far beyond just economics. The technology that the Bitcoin network uses can be applied to solve many issues in the world today or in totally new applications. Chances are that something else will come along that is far superior to bitcoins as a currency, but the Bitcoin network has the potential to become one of the greatest technological revolutions since the internet.

Works Cited

Brito, Jerry, and Andrea Castillo. "Bitcoin: A Primer For Policymakers." Policy 29.4 (2013): 3-12. Academic Search Complete. Web. 23 Feb. 2014.

Brito, Jerry. "Bitcoin: More Than Money." Reason 45.7 (2013): 34-42. Academic Search Complete. Web. 23 Feb. 2014.

Jevons, William Stanley, Money and the Mechanism of Exchange. 1876. Library of Economics and Liberty. 23 February 2014. <http://www.econlib.org/library/YPDBooks/Jevons/jvnMME.html>.

Kristoufek, L. BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. Sci. Rep. 3, 3415; DOI:10.1038/srep03415 (2013)

LOVELESS, JACOB, SASHA STOIKOV, and ROLF WAEBER. "Online Algorithms In High-Frequency Trading." Communications Of The ACM 56.10 (2013): 50-56. Academic Search Complete. Web. 23 Feb. 2014.

"Money." International Encyclopedia of the Social Sciences. Ed. William A. Darity, Jr. 2nd ed. Vol. 5. Detroit: Macmillan Reference USA, 2008. 249-253. Gale Virtual Reference Library. Web. 23 Feb. 2014.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." bitcoin.org. N.p., n.d. Web. 23 Feb 2014. <https://bitcoin.org/bitcoin.pdf>.

Schuster, Julian. "Credit." Encyclopedia of World Poverty. Ed. M. Odekon. Vol. 1. Thousand Oaks, CA: SAGE Reference, 2006. 215-216. Gale Virtual Reference Library. Web. 23 Feb. 2014.

Smith, Adam, An Inquiry into the Nature and Causes of the Wealth of Nations. Edwin Cannan,

ed. 1904. Library of Economics and Liberty. 8 March 2014.

<http://www.econlib.org/library/Smith/smWN.html>.