Bitcoin: A Theoretical Analysis of Money Choice

Darren N Chu

December 2014

Senior thesis submitted in partial fulfillment

of the requirements for a

Bachelor of Arts degree in Economics

at the University of Puget Sound

Abstract

Due to its popularity, the cryptocurrency known as Bitcoin has gained a lot of attention in both field of economics and computer science. Despite its popularity, Bitcoin has yet to establish a market of users, and has struggled to be considered as a legitimate form of money. Many economists have defined Bitcoin as either an asset or a form of digital currency, but a concrete definition has yet to be established. The goal of this paper is to analyze Bitcoin's status as money. Once we've established Bitcoin's status as money, we will compare Bitcoin with current forms of socially accepted money in order to evaluate Bitcoin's potential as a socially accepted means of payment. In the final portion of this paper, we will use a theoretical model to analyze the costs and benefits of Bitcoin and compare them with other forms of money.

1 Introduction

In the last five years, the value and interest in Bitcoins have been increasing due to a lack of confidence in the traditional banking system, and various fiscal issues. Fueled by the financial crisis, bank bailouts and the need for financial rescuing, the interest for this decentralized, peer-to-peer currency has increased. However, Bitcoins have fallen under much scrutiny because they have been defined by the IRS as a form of property rather than a source of money. This thesis will compare Bitcoin to currency and other forms of socially accepted money in order to determine whether Bitcoins can function as money.

2 What is Bitcoin?

In 2009, Satoshi Nakamoto, a pseudonym, released a cryptocurrency known as Bitcoins to the public. Cryptocurrencies are a new technological form of digital asset that is created through cryptographic algorithms. These cryptocurrencies are used to verify and authorize payments through the use of cell phones or computers. In most cases, cryptocurrencies attempt to avoid the inflation issues that most "fiat" monetary policies may pose by setting a ceiling or maximum quantity of currency that can be produced. The ceiling will provide security to make sure that the number of cryptocurrencies will never increase too much or devaluate the currency.

Bitcoins are undoubtedly the most popular form of cryptocurrency. With approximately 2.5 million users,[1] Bitcoin leads their competitor Ripple, 120 thousand users,[2] as the most used cryptocurrency by a substantial amount. A precise definition, provided by Ron and Shamir (2012) states:

> "Bitcoins are digital coins which are not issued by any government, bank, or organization and rely on cryptographic protocols and a distributed network of users to mint, store, and transfer."

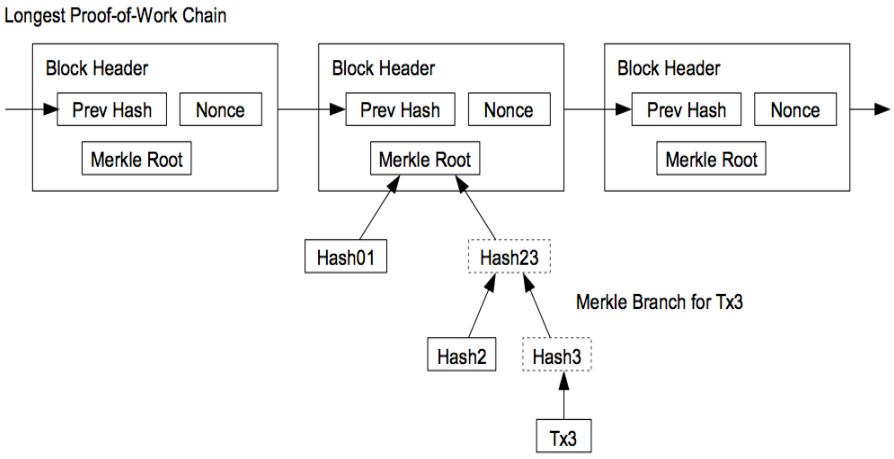
Bitcoins are a purely digital, highly-liquid asset that can be traded for speculative purposes or used as a means of payment. Although they are not sanctioned as legal tender or backed by any form of tangible asset, Bitcoins have found some success as a commodity.

Because Bitcoins are not fiat-money, they have been categorized as a digital version of gold or known as digital gold (Smith 2014). Bitcoin is a digital commodity that can be sent directly from one party to another through online payments. Bitcoin also allows one to exchange Bitcoins for traditional forms of currencies or used to purchase goods and services. The Bitcoin system is designed as a peer-to-peer source of trading that does not require a third party to hold, store or manage one's Bitcoin. Without this third party, Bitcoins can reduce their transaction fees and

[1] https://blockchain.info/charts/my-wallet-n-users
[2] https://www.ripplecharts.com/#/

provide very low transactions costs in comparison to current traditional electronic transfers and other means of payment.

The peer-to-peer source of trading allows for high ease of online payments. Transactions are made when a user transfers the coin by digitally signing both a hash of the previous transaction and the public key of the next owner. The hash and the public key are then added onto the end of the coin, thus allowing the payee to verify the chain of ownership and provide a proof of payment. Each proof of payment is labeled by a timestamp and then distributed into a timestamp server. A flow chart demonstrating the steps of the proof-of-work and utilization of the hashes is shown below.[3]



Source: Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System

[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (www.Bitcoin.org)

2.1 Proof-of-Work

The proof-of-work scheme above demonstrates the steps that are utilized to verify a transaction. Each of the block headers represents a verified transaction that has gone through all of the steps of the proof-of-work protocol. When users requests a transaction, they are required to show their proof-of-work or show the previous hash that they have associated in their Bitcoins.

Breaking it down even further, the hash is a container for an arbitrary-large amount of data. This data in the hash is used to create security in the form of verification. Each of the hashes is used in the proof-of-work scheme by requesting that the user send their most previous hash for the latest transaction. The path of transactions can show the chain of ownership for each of the previous transaction records that are shown by the previous hash. The previous transaction records demonstrate a cryptographic guarantee that the sender was the last recipient or user of the Bitcoins that are being sent. However in order to completely verify the chain of the proof-of-work through the hashes, the previous hash must be compared to the Merkle Root.

The Merkle Root works as a data tree graph that contains all of the transactions in the block. Therefore it is very easy to verify or catch a fraud in the Bitcoin system if the previous hashes provided in the transaction do not match the chain of transactions that are associated with the Merkle Root.

Finally, a cryptographic nonce is used in the transaction. A nonce is a random or pseudo-random number that is issued as an authentication protocol that will make sure that previous hashes or communications cannot be reused. Each of the transactions is stamped with a nonce. With a nonce, a transaction or the information in a transaction cannot be repeated or used multiple times. The use of a nonce, as Nakamoto has stated is used to solve the issue of double spending.

2.2 Verifying Transactions

Once a transaction has been activated between two parties, the transaction will be added into the timestamp server where miners approve the transactions. The timestamp server is essentially the public ledger where the miners can verify the transaction. Miners work as the third party member within the transaction. As mentioned earlier, these third party members are only monitoring the transaction between the two parties. Miners are rewarded with bitcoins for verifying the transactions between the two parties. In order to verify the transaction, the miners must solve math problems to approve the transactions. Once these transactions have been approved, the miners are rewarded with Bitcoins from the Bitcoin servers.

With each math problem that gets solved, the Bitcoin mining algorithm increases the difficulty based on the rate that the math problems are being solved. The math

algorithm allows for the production of Bitcoin to self-regulate and mathematically account for whenever a Bitcoin is minted into the Bitcoin market. When the Bitcoin system recognizes that the number of Bitcoins being added into the Bitcoin market is too fast, the mining algorithm's difficulty will increase until the production rate of Bitcoins stabilizes. By rewarding the miners for verifying the transactions, the Bitcoin system is self-regulatory. The nature of the Bitcoin system rewards those who verify the transactions while injecting more Bitcoins into the Bitcoin market at a stable rate.

Lastly, after transactions have been approved, the proof of payment is written in the final public ledger. The public ledger lists every transaction in real time and is available for access on https://blockchain.info/. The website allows for each transaction to be accountable and tracked. Bitcoins are also interpreted as a 'pseudo-anonymous' network. When a transaction occurs, both parties can hold their Bitcoin address without revealing anything about either party's identity. In theory one can hold multiple addresses and there would be no link between any of the addresses. However, if one publishes his or her Bitcoin address online, all of the transactions that were linked to the address will be open to the public. Thus, if their address is linked to their personal identity, every transaction will be linked to them.

As of today, there have been a total of 50 million transactions of Bitcoin (https://blockchain.info/charts/n-transactions-total). Despite the popularity of Bitcoin, Bitcoin still has many issues that most new means of payment face. Since

Bitcoin is not categorized as currency, consumers are hesitant to accept Bitcoins as currency or even as money. This thesis will compare Bitcoin to other forms of currency and means of payment in order to define whether or not Bitcoins can become a form of money through social acceptance.

3 What is Money?

Before one can determine whether Bitcoin can be considered as money, one must define what makes something money, and the different types of money. The concept of money is a difficult and abstract idea to deconstruct. As described by Rahmatian (2014), money is an abstract entity with no intrinsic value. Money is solely a representation of current and future value, created by social construct and by rule of law—fiat money. Rahmatian describes two states that money have, the 'res' or function of the abstraction 'property object' and the 'physical state' of the object.

The inherent difference between the 'res' and the 'physical state' is that physically, money does not have value. The object that one states is money does not come with a built-in monetary value. The 'physical state' category, refers to any form of tangible object. In fact, the object does not contain any value or ownership. Money is simply a social construct of value that we have put onto these 'physical state' objects. The idea of value is described within the 'res'.

The social perception of value or 'res,' is what gives money the idea of intrinsic value. However, the implied uses of money have been ingrained within the idea of the minds of the people. The fiat behaviors described by Rahmatian (2014) needed regulations, therefore governments and banks created fiat money. The need for a coherent money created the system of fiat currencies, and Government regulation of money that we know and use currently. Once fiat currency was developed, more means of payment, or socially accepted monies were created. Bitcoin is a digital asset and therefore cannot be categorized as fiat money. Bitcoin can only be defined as a means of payment or as a form of socially accepted money.

3.1 Does Bitcoin Fulfill the Definition of Money?

Money, in a traditional economic definition, must fulfill three main functions. These three functions are:

1. Mediums of exchange
2. Storage of value
3. Unit of account.

In theory, anything can potentially fulfill these three main functions and be used to extinguish debt.

Bitcoin is and can be defined as a form of money. In the Bitcoin Wiki,[4] Bitcoin is incorrectly labeled as a "digital currency." Digital currency is a very colloquial term for Bitcoin that is rather misleading. The term currency is defined as only state-approved money that includes "paper money and coins" (Mishkin, 2004; Campbell & Campbell, 1988). Therefore, the definition known as "digital" currency is essentially meaningless (Krohn-Grimberghe & Sorge, 2012).

Krohn-Grimberghe & Sorge both attempt to categorize Bitcoin as electronic money based on the European Union's definition of electronic money. In the second article of the E-Money Directive (2009/110/EC), electronic money "means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […], and which is accepted by natural or legal person other than the electronic money issuer". Based on this definition, Krohn-Grimberghe & Sorge state that the Bitcoin system would need to "electronically store monetary value" in order to be categorized as a form of electronic money. However, the Bitcoin system does not use account balances that correspond to a fixed value or currency amount. In fact, Bitcoins can be exchanged for currencies at varying exchange rates, but these exchange rates are "not a property of the system, but a feature offered by service providers" (Krohn-Grimberghe & Sorge, 2012).

[4] https://en.Bitcoin.it/w/index.php?title=Main_Page&oldid=35321

Although Bitcoin does not qualify as a type of currency or electronic currency, Bitcoin fulfills the functions of money that are defined by both (Mishkin, 2004) and the European Central Bank:

- Money serves as a medium of exchange. The medium of exchange aspect is used to move away from trading goods for other goods to extinguish debts. Bitcoin can be used as a medium of exchange for goods and services. Instead of using a direct exchange approach (e.g. goods for goods), Bitcoin can be used as a discharge of debt or payment for goods and services.
- Money serves as a storage of value. Bitcoins do not have to be spent right away. The address code and key pairs that one gets when they receive their Bitcoins can be held for years and can also retrieve the value when needed. The market value of Bitcoin does change over time, however most currencies also change in value due to fluctuating inflation rates. Despite these changes in inflation, the asset's market value can still be connected with Bitcoins in later periods of time. Like other sources of money, one may hold onto Bitcoin and use them for later periods of time because they serve as a storage of value.
- Money serves as unit of account. Bitcoin, as inherent in its design, is created as a unit of account. Bitcoin utilizes an exchange rate based on current currencies, but has an independent unit of account.

Just because Bitcoin can function as money does not mean that Bitcoin will be socially accepted. We will consider the criteria associated with the immediate funds transfers (IFT) payments and see if Bitcoin meets or improve on these attributes. The types of IFT payments are listed in Table 1. Since IFT payments are already socially accepted as a means of payment, we will look at the criteria for socially accepted monies to help us define our economic model.

3.3 Socially Accepted Money

In order to decide whether Bitcoins could be socially accepted money, one must look at the attributes of current socially accepted monies. The reason that new monies do not appear every day is that few of these monies become socially accepted. The most common forms of socially accepted monies are checks, e-cash, credit cards, and debit cards.

Monies such as checks, e-cash, credit cards, debit cards and wire transfers are forms of IFT payments. IFT payments allow for senders to pay the receiver electronically with high convenience, near certainty and in a secure manner with low costs, and nearly no delay for the receiver to receive and use these funds (Summers, and Wells, 2011).

Summers and Wells described the types and functionality of IFT payments in four different countries. The countries they analyzed in their case studies were Mexico,

South Africa, the United Kingdom and Switzerland. The authors illustrated the IFT banking systems and proposed the benefits of utilizing IFT payments. The authors also indicated several primary attributes associated with each form of IFT payments that influences a sender or receiver's choice of socially accepted monies:

- Certainty—assurance to the sender and receiver that funds are transferred as ordered;
- Speed—timeliness of funds transfer from sender to receiver;
- Security—assurance that payment is protected against fraud and completed as ordered;
- Control—the sender and receiver have good information about and are able to control the timing or payment;
- Universal Acceptance—the payment instrument is broadly accepted;
- Versatility—useful for a variety of personal and business transactions, including the ability to transmit remittance information; and
- Low Cost and Transparent Pricing—reasonable cost relative to value fees are clear to sender and receiver.[5]

These attributes are the main characteristics that separate things that can be considered as money, and money that is socially accepted. The criteria listed above will be known as the criteria for socially accepted monies. In general, socially

[5] Bruce J. Summers and Kirstin E. Wells, Emergence of immediate funds transfer as a general-purpose means of payment

accepted monies act as fiat-currency, but provide benefits that fiat-currency cannot provide.

The criteria for socially accepted money is a list of attributes used to measure the potential that a new type of money has to be used as a replacement for currency. The main goal for socially accepted money is to reduce the transactions cost of using currency for both the buyers and the sellers. Therefore, in order for Bitcoin to become a socially accepted form of money, it would need to meet the criteria for socially accepted money and have a transaction cost equal to or lower the current socially accepted monies.

4 Economic Model

As defined earlier, socially accepted monies are used and accepted when they work like fiat currencies, but have a lower transactions cost. These transactions costs influence a consumer's choice when purchasing goods and services, which in return will increase or decrease one's "happiness" or utility. Borrowing from Sproule (2009), the consumer choice problem can be represented as:

$$max_{x_i}\ U = f(x_1, x_2 \dots x_n) - \lambda\ (\sum_{i=1}^{n} p_i x_i - m)$$

Each consumer's maximum utility will be measured with the variable *U*. Utility will be measured as a function of the goods and services, *x*, and the prices, *p*, associated with the goods or service.

.

A consumer's utility is defined by the amount of goods and services that one is able to use or have. Therefore the utility function is a function of all possible goods and services that one can purchase, while being subject to the budget constraint. As a consumer, one's purchasing power is defined by their disposable income and the amount the prices of the goods.

The income variable, *m*, represents the income that each consumer possesses. Income can measure the number of goods or services one can purchase based on the price of each good.

$$m = p_1(x_1) + p_2(x_2) + \cdots + p_n(x_n)$$

The price above does not capture the value of the transactions costs that a consumer must take into account when choosing their means of payment. The use of Bitcoins, IFT payments and other socially accepted monies affect the transactions costs of purchasing goods & services. Therefore, the equation above needs to display both forms of costs, both implicit and explicit costs:

$$m = p_1(x_1) + p_2(x_2) + \cdots + p_n(x_n)$$

$$p_1 = p_{1m} + Tr_1(g)$$

$$p_2 = p_{2m} + Tr_2(g)$$

$$\vdots$$

$$p_n = p_{nm} + Tr_n(g)$$

$p_{xm} =$ market price of goods & service*s*

$Tr_x =$ transactions costs of the goods & services

g = all variables that affect the transaction costs

In order to determine whether Bitcoin can function as money, we will determine the transactions costs associated with Bitcoin and compare them to the transactions costs of current socially accepted monies. If Bitcoin's transactions costs are lower than the other forms of means of payment, consumers will have a higher amount of disposable income. Therefore, a consumer will have a higher purchasing power and overall utility by purchasing more goods & services. However, if Bitcoin's transactions costs are higher than the other forms of socially accepted monies, consumers will have the inverse affect towards Bitcoin.

We will propose three separate scenarios that the consumer can choose to utilize their income. With each proposal we will measure the transactions costs associated with each form of payment. The first proposal will be if the consumer is unwilling to accept any form of IFT or cryptocurrencies, and only uses fiat currency. The second proposal will be that the consumer is willing to accept Bitcoin and no other form of IFT. The third proposal will be that the consumer is willing to accept IFT and not Bitcoin. By measuring and comparing the implicit and explicit costs associated with

these three proposals, we will determine the transactions costs associated with each form of payment.

4.1 Transactions Costs

In this model, costs associated with fiat currency will be measured solely by the convenience of distance, while IFT payments and Bitcoin will measure the fees associated with them. Assuming that a consumer is purchasing a good *g,* the consumer's transactions costs will be measured with all three types of payments.

Starting with the simplest model, the consumer will purchase a good using only fiat currency at a price p_g that equals the market price and the transaction costs $p_{gm} + Tr(g)_f$.

The transactions costs of fiat currency is measured with the distance costs d_f for the consumer to travel to the seller of *g*, and the opportunity costs *o* where *o* is comprised of time *t* and wage *w*

$$o = (t \cdot \mathrm{w})$$

We will also need to incorporate the cost that it would take to exchange one fiat currency into another country's currency, ex_f. When added together we get

$$Tr(g)_f = d_f + o + ex_f$$

The d_f is positively associated with Tr_g, because when d_f is high, the convenience of fiat currency decreases and increases the cost of the consumer.

Next we are going to look at the transactions cost of IFT payments because IFT payments are socially accepted means of payments. The transactions costs for IFT payments $Tr(g)_{ift}$ also contain a distance cost of d_{ift}. However, unlike fiat-currency, d_{ift} is negatively associated with $Tr(g)_{ift}$.

The opportunity cost o_{ift} of IFT payments are much higher than fiat-currencies because time *t* will include the learning costs and the start-up costs.

Next, we will need to calculate the usage fees u_{ift}. For the usage fees, the transactions fees will be given as f_{ift}. IFT payments however, give back rewards to the consumer based on their usage. The rewards for IFT payments are given based on usage h_{ift}. This will give us

$$u_{ift} = f_{ift} - h_{ift}$$

Thus when added together

$$Tr(g)_{ift} = (-d_{ift}) + o_{ift} + u_{ift}$$

Next we will need to take into account whether the seller accepts the IFT payments or not. Acceptance will be measured by the dummy variable $a = \{0,1\}$ where $a = 0$ means the IFT payment is accepted and $a = 1$ means it is not accepted.

If $a = 1$, IFT payments will also include exchange costs ex_{ift}. The exchange cost will represent the cost of exchanging IFT payments into fiat currency. The exchange costs will be measured by the number of locations of exchange e_{ift} that are near the seller of g, and the exchange fees r_{ift}

$$ex_{ift} = r_{ift} - e_{ift}$$

With the dummy variable taken into account

$$Tr(g)_{ift} = \begin{cases} (-d_{ift}) + o_{ift} + u_{ift}, & \text{if } a = 0 \\ (-d_{ift}) + ex_{ift} + o_{ift} + u_{ift}, & \text{if } a = 1 \end{cases}$$

When comparing the $Tr(g)_{ift}$ with $Tr(g)_f$, the main difference between $Tr(g)_{ift}$ and $Tr(g)_f$ is the distance costs. In most cases, $Tr(g)_f \leq Tr(g)_{ift}$ if and only if $d_f \leq d_{ift}$. Also, if d_f passes the level of convenience for the consumer, it is much more convenient to use services that accept IFT payments and deliver the good or service to the consumer. Therefore, if d_{ift} for the consumer is high enough, the incentive to use IFT payments is much higher.

IFT payments are calculated based on the transactions costs that are associated with them. In most situations, $Tr(g)_f \leq Tr(g)_{ift}$, which allow IFT payments to become socially accepted as a means of payment. We will now compare the $Tr(g)_{ift}$ with the transactions cost for Bitcoin, $Tr(g)_b$. Since we are measuring the potential for Bitcoin to become a socially accepted means of payment, the transactions costs of Bitcoins, $Tr(g)_b$, will be measured with the same cost variables as $Tr(g)_{ift}$. The $Tr(g)_b$ is calculated as

$$Tr(g)_b = \begin{cases} (-d_b) + o_b + u_b, & \text{if } c = 0 \\ (-d_b) + ex_b + o_b + u_b, & \text{if } c = 1 \end{cases}$$

5 Analysis of the Model

Now that we have our economic model for both $Tr(g)_b$, $Tr(g)_{ift}$ we can analyze the necessary changes needed to lower the $Tr(g)_b$. As mentioned earlier, consumers will only choose to accept Bitcoin if the $Tr(g)_b$ is less than $Tr(g)_{ift}$. In comparison, the costs for IFT payments are lower than the costs for Bitcoin therefore more consumers prefer IFT payments. The main advantage that Bitcoin has is that $u_b < u_{ift}$ and $(-d_b) < (-d_f)$. The reason that some consumers prefer Bitcoin is because both transactions fees, u_b and $(-d_b)$ are very low.

However, most of the costs for Bitcoin are higher than IFT payments. Because Bitcoin is a new form of payment, both $o_b > o_{ift}$ and $ex_b > ex_{Ift}$. The main disadvantage for Bitcoin compared to IFT payments is because Bitcoin is currently not a highly-socially accepted means of payment while IFT payments in general are socially accepted. Therefore when compared between the two, $a = \{0\}$ and $c = \{1\}$

$$Tr(g)_{b,(c=1)} > Tr(g)_{ift,(a=0)}$$

Bitcoin can become socially accepted as a means of payment if it can become a cheaper means of payment than IFT payments.

$$Tr(g)_{b,(c=0)} < Tr(g)_{ift,(a=0)}$$

In order to do so, we would need to lower the o_b and the ex_b. We believe that the time spent learning costs associated with Bitcoin will lower over time. When the amount of technology and methods of learning how to use Bitcoin become more integrated and easier to understand. The Bitcoin technology and system are rather complicated to understand for most first-time users. When the Bitcoin system becomes easier to understand and much more integrated within society, o_b of switching from Bitcoins to IFT payments will be much lower. At the moment, o_b is much higher than o_{ift}, and consumers are unwilling to switch from IFT payments to Bitcoins. We believe that the o_b will lower in time if the technology of Bitcoin becomes more directed towards first-time users. If the time spent understanding

how to implement Bitcoin and the cost of switching from IFT payments to Bitcoin decreases, Bitcoin will become more appealing to a consumer, thus lowering o_b.

I also believe that as time continues, more and more developers will want to increase the technology of Bitcoin and cryptocurrencies. With the increase of technology, there will be an increase in the number of Bitcoin ATMs and other forms of exchange locations. Similar to IFT payments, consumers may need to be able to exchange Bitcoins into fiat-currency if the seller does not accept Bitcoins. Currently there are only Bitcoin ATMS and exchange locations in large cities. If more technology was invested into creating these ATM and exchange tools, ex_b will decrease as well. By decreasing both of these costs, consumers will begin to notice the advantages associated with Bitcoin. Even if the transactions costs of Bitcoin have been reduced, Bitcoins also need to overcome the issue of the Bitcoin price fluctuations.

The price fluctuations in Bitcoins have caused many consumers to be hesitant with whether or not they should choose to use Bitcoin as a means of payment. Because Bitcoin's price fluctuations are unaccountable and have been rather volatile, we must propose methods of regulating or securing the risk of volatile price fluctuations. The problem with Bitcoin's price fluctuations pose on consumers are that the consumers are incurring all of the risk of Bitcoins and their volatile prices. Therefore, we will propose two possible solutions that will either regulate or reduce the risk of these price fluctuations.

The first proposal that we will offer is the use of Government regulations. Similar to when gold was a main means of payment, the Government promised a constant price and value for gold. The Government had imposed a fixed price and value for gold, which effectively set a standard value and rate of exchange. In turn, gold had become a highly stable asset of exchange. This same form of Government regulations could solve the issue of price fluctuations in the Bitcoin market. With Government regulations, the risk of holding onto or using Bitcoins will lower due to the constant value imposed by the Government. However, the problem with Government regulations is that Bitcoins were created to be separate from any form of Government policy or regulations. As mentioned earlier, Bitcoin was made to be a decentralized form of money that only relied on those within the Bitcoin market. Bitcoin's peer-to-peer and self-regulatory market mechanisms were created in an attempt to remove the need for Government regulations. Although Government regulations may solve the issue of the price fluctuations, Bitcoin market may lose the consumers who were initially using Bitcoin as a decentralized form of money.

The second proposal that we will offer is the introduction of forward markets in the Bitcoin market. With forward markets, Bitcoin holders will give their Bitcoins to an insurance company or trusted exchange market. Both parties will make a contract that will ensure that the Bitcoin holder will have a stable conversion of Bitcoins set at the current price of Bitcoins. The entrusted company can lock in the current price and value of Bitcoins and nullify the price fluctuation over a chosen number of years

for this user. Basically, the entrusted company will hold onto the Bitcoin consumer's Bitcoins and regardless of what price fluctuations happen in the Bitcoin market, the entrusted company will return number of Bitcoins equal to the value that both parties agreed upon. With this system, the consumer of Bitcoin will only have a lose in returns if the value of Bitcoin increases during the years of the contract. However, the consumer of Bitcoin will not have to worry about the risks associated with a price drop in Bitcoins. Instead, the insurance company or trusted exchange market, will be incurring the risk and lose instead.

With both the proposed solutions to lower transactions cost and the implementation of either price fluctuation proposal, consumers will gain confidence with Bitcoin as a means of payment. Consumer confidence and acceptance of Bitcoin will allow Bitcoin to become a socially accepted means of payment and create a larger market for Bitcoins. As more and more consumers start to use Bitcoins, sellers of goods and services will be more wiling to accept Bitcoins. The sellers will adapt to the new means of payment because if they don't, the sellers will lose costumers within the Bitcoin market. Once Bitcoin has been added into the competitive market, both consumers and sellers will socially accept Bitcoin.

6 Conclusions

This paper has addressed the question of whether or not Bitcoin could be considered as a socially accepted means of payment by comparing Bitcoin to other,

current forms of socially accepted money. The first assertion that was examined in this paper is if Bitcoin, like any asset, can be described as money. This assertion was consistent with the criteria of money given from Krohn-Grimberghe & Sorge (2012), and Mishkin (2004). Based on the attributes and nature of Bitcoin, it was decided that Bitcoin couldn't be categorized as fiat-currency but rather as a potential type of socially accepted money.

We then took notice of many significant similarities between Bitcoin and the IFT payments described by Summers, and Wells (2011). IFT payments are the, most commonly used, form of socially accepted means of payments because the transactions cost of IFT payments are considered lower than fiat-currency. By building our theoretical model, we've proven that Bitcoin has the potential to become a means of payment if the transactions costs of Bitcoin is lower than that of the current most commonly used socially accepted means of payment. Despite the lower cost for Bitcoin, consumers will only accept Bitcoin if the value of Bitcoin is transparent. The price fluctuations are not a risk that consumers are willing to take with this new money. With price regulations in the form of Government price regulations on Bitcoin or the introduction of forwarding markets, Bitcoin has the potential to become a socially accepted means of payment.

TABLE 1

Attributes and examples of payment instruments

Attribute	Check	Direct debit	Direct credit	Wire transfer	General-purpose IFT[a]	Debit card
Certainty	Provisional payment to receiver	Provisional payment to receiver	Payment guaranteed to receiver	Payment guaranteed to receiver with immediate finality	Payment guaranteed to receiver	Payment guaranteed to receiver
Speed	Minimum one day	Minimum one day	Minimum one day	Real-time	Within minutes	Real-time authorization and guarantee; funds transferred end-of-day at the earliest
Security	Checks may be stolen and/or forged	Bank account and routing information from check can be used to originate debit transfer	Fraud is limited because payer directly sends funds from account	Fraud is limited because payer directly sends funds from account	Fraud is limited because payer directly sends funds from account	Card numbers may be stolen; use of PIN with certain cards limits unauthorized transactions
Control of timing	Payer controls instruction but cedes control of funds movement to payee	Payer controls instruction but cedes control of funds movement to payee	Payer controls transaction	Payer controls transaction	Payer controls transaction	Payer controls transaction
Universal acceptance	Yes	Sender and receiver must agree to use	Sender and receiver must agree to use	Yes	Closed system with limited number of users[b]	Limited by merchant acceptance
Versatility	Most types of payment transactions	Bill payments, business-to-business trade payments (with remittance information)	Recurring payments, business-to-business payments (with remittance information)	Financial market transactions (with limited remittance information)	Most types of transactions but limited POS	Point-of-sale (POS) and online only
Low cost and transparent pricing	Not transparent to individuals; per-transaction fee to businesses	Not transparent to individuals; per-transaction fee to businesses	Not transparent to individuals; per-transaction fee to businesses	High cost for sender and receiver (transaction fee)	Not transparent to individuals; ad valorem fee to merchant (PayPal)	Not transparent to individuals; ad valorem fee to merchant
Clearing & settlement	National check system	ACH system	ACH system	Accounts held with Reserve Banks or CHIPS	PayPal system	Card networks
Example	Business accounts payable	Utility payment	Payroll deposit	Purchase and sale of bank reserves	Purchase of goods and services	Grocery payment

[a]Information in this column is based on the features of PayPal, which is the nonbank IFT service most commonly used today by individuals (Shevlin, Fishman, and Bezard, 2010).
[b]As we discuss in the text, IFT in other countries links all or most transaction accounts held at banks.

[6]

[6] Bruce J. Summers and Kirstin E. Wells, Emergence of immediate funds transfer as a general-purpose means of payment

Works cited:

https://blockchain.info/charts/my-wallet-n-users

https://www.ripplecharts.com/#/

Campbell, C. D., & Campbell, R. G. “Money, Banking and Monetary Policy” 1988. Thomson Learning.

European Central Bank. “Virtual Currency Schemes” 2012. http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Krohn-Grimberghe, Artus, and Christoph Sorge. "The Practical Aspects Of The Commission's Findings." *The British Medical Journal* 2012. http://arxiv-web3.library.cornell.edu/pdf/1308.6760v1.pdf

Mishkin, F. S. “The Economics of Money, Banking and Financial Markets (7th ed.)” 2004.
Pearson International Edition.

Nakamoto, Satoshi. *Bitcoin*: “A Peer-to-Peer Electronic Cash System” 2008. www.Bitcoin.org

Rahmatian, Andreas. "Money as a Normative Text." Journal of International Business & Law, 2014
http://ssrn.com/abstract=2513286

Ron, Dorit, and Adi Shamir. “Quantitative Analysis of the Full Bitcoin Transaction Graph” 2012
https://eprint.iacr.org/2012/584.pdf

Smith, Jacob. "An Analysis of Bitcoin Exchange Rates" 2014.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2493797

Sproule, Robert. "A Note on the Endogeneity of the Price of Utility Within the Consumer's Static Profit Function." J Econ, 2010.
http://content.ebscohost.com.ezproxy.ups.edu/ContentServer.asp?T=P&P=AN&K=53781155&S=R&D=buh&EbscoContent=dGJyMNLr40Sep644xNvgOLCmr02epq9SsKa4TbKWxWXS&ContentCustomer=dGJyMPGusUqzqbZPuePfgeyx44Dt6fIA

Summers, Bruce J., and Kirstin E. Wells. "Emergence of Immediate Funds Transfer as a General-Purpose Means of Payment." 2011.
https://www.chicagofed.org/publications/economic-perspectives/2011/3q-summers-wells