The Center on Capitalism and Society
Columbia University
Working Paper No. 82, April 2014

Economics beyond Financial Intermediation

Digital currencies' possibilities for growth, poverty alleviation, and international development

Dr. Saifedean Ammous[1]

Abstract

Bitcoin is the first technology for the final transfer of digital goods online, facilitating the groundbreaking innovation of instant global payments without intermediation. The operation of Bitcoin is based on a distributed, decentralized, and transparent asset ledger which acts as an ongoing chain record of all transactions, and is in turn divided into coins which can be traded on the network, and whose issuance goes to reward those who contribute processing power to the operation of the network. The possibilities created by this innovation are most significant for the world's poor—billions of people who remain to this day largely without access to financial services, and who could skip traditional financial services and move to digital currencies in the same way they have gone straight to using mobile phones and skipped telephone landlines. Billions the world over could prosper and escape poverty without having to wait for their governments to develop the financial, political, and economic institutions deemed necessary for economic development.

JEL Codes: F30, O31

Keywords: Bitcoin, innovation, finance, development.

[1] I thank Edmund Phelps, Ryan X. Charles, David Al-Achkar, and Lynn Chouman for helpful comments, as well as seminar participants in the Center for Capitalism and Society seminar series and the New York University Colloquium on Market Institutions and Economic Processes. Research on this topic was facilitated by a generous Seed Fund grant from the Lebanese American University.

I. Introduction

At the beginning of the twenty-first century, the telecommunication revolution has improved virtually all aspects of modern economic life. Email has vastly increased the ability to communicate information across the world, compared to paper mail and the telegram. Websites like Amazon and Ebay have given consumers an infinitely wider array of products and producers, while allowing producers to extend their reach to large numbers of consumers. Global Positioning Satellite systems have made driving and navigation safer and easier. Various fields of industry and agriculture have benefitted from the innovations that better communication and efficient production chain management have produced. Search engines have made information accessible worldwide in a manner heretofore unimaginable. Many more global transformative innovations can be listed, yet there remains one field where the internet has not made a large impact, and where business continues as it has done for decades, and that is finance and banking.

As the former chairman of the US Federal Reserve System Paul Volcker famously put it, the "single most important" innovation the financial industry has witnessed in the past 25 years was the introduction of Automated Teller Machines[2]. "I wish someone would give me one shred of neutral evidence that financial innovation has led to economic growth" (Hosking and Jagger, 2009). While banks have produced various new financial instruments and methods of hedging risk and maximizing their profitability, the banking experience for the consumer has not changed by much since the ATM allowed withdrawals outside bank branch locations and opening hours. Transferring money in any way other than in person continues to cost significant amounts of money and time for the majority of people. The most common method for payment today is still the credit card, which was invented in 1949, back when the vinyl record was the most prevalent method of listening to music recordings. Since 1949, the quaint vinyl records have evolved to tape cartridges, 4-tracks, compact cassettes, compact discs (CDs), and finally mass storage digital music players, while credit cards are still in use today, featuring glaring failures which modern technology could easily fix: Most notably, payment is still initiated by the recipient, meaning the payer must disclose their sensitive information to the recipient and risk compromising it every time they want to make a payment. Further, payment can only be received by people who own a credit card terminal, which involves significant set-up costs and high commissions.

These high payment transaction costs constitute a small problem for the populations of rich industrial nations, but they are an insurmountable obstacle for much of the world's poor, who do not present an attractive market for financial institutions, and thus remain largely unbanked and

[2] The Automated Teller Machine was actually invented in 1969.

unable to access financial services altogether. When they must use financial services for remittances, the fees they pay are exorbitantly high compared to the small amounts transferred.

Banking has not improved the speed and cost of transactions because of a dual logistical-political problem: Any transaction not carried out with cash in person has to rely on third-party intermediation to prevent double spending; i.e. to ensure that the payer does have the funds necessary for the payment, and that they are not making other payments that exceed these funds. Two parties cannot perform a financial transaction between their accounts without the custodian of the payer's account verifying that the sender has sufficient funds to perform the transaction. With the political and economic importance of financial intermediation, this role has been regulated by governments, limiting entry and exit, and isolating intermediaries from true free market competition that would weed out the inefficient and only allow the productive to survive. Capture of the regulatory agencies by the regulated parties has protected their rents by preventing market competition from more rapidly advancing the interests of the transacting parties. The result is that even as telecommunication technology has advanced, transaction costs have remained high, and modern financial innovation has not overcome this logistical and political obstacle. That changed in the year 2008, when a pseudonymously published 9-page paper contained the first workable design of a payment system technology that eliminates the need for trusted third-party intermediation: Bitcoin.

This paper discusses Bitcoin and the impact it can have on development. Section II explains Bitcoin in a functional manner—in terms of the technologies that constitute Bitcoin, outlining four main functional technologies: transfer of digital goods, the blockchain, the currency, and smart contracts. Section III outlines the main strengths and advantages of Bitcoin, while Section IV discusses other digital currencies and their importance and chances of success. Whereas this paper discusses Bitcoin in particular since Bitcoin is by far the largest and most important digital currency, the main thrust of the paper concerns the technology of digital currencies itself. Section V provides a preliminary brainstorming of the impact that digital currencies can have on developing countries and the world's poorest, illustrating ways in which it can help the world's poorest overcome the institutional drawbacks of their countries and participate in a growing global economy.

II. What is Bitcoin?

Bitcoin is a network that allows for digital payment between its members without third-party intermediation. Payment is irreversible, initiated by the payer, and virtually costless and

instantaneous. This paper will take a functional approach to the understanding of Bitcoin; its features and constituent parts can be expressed in terms of four distinct technologies: a technology for the transfer of digital goods, a common asset ledger (the Blockchain), a hyper-deflationary currency, and a technology for implementing 'Smart contracts'. This section overviews the basics of all four technologies.

1. Transfer of digital 'goods'

The groundbreaking innovation of Bitcoin is that it is the first technology for the transfer of digital "goods" from one network location to another. Since the inception of computer networks, it has been possible to send digital data and objects between computers, but such a 'transfer' actually only sends a copy of the data to the recipient, maintaining another copy with the sender—in other words, it's a method of copying and not sending. By using public-key cryptography on a decentralized asset ledger, Bitcoin allows for goods to be stored on the public asset ledger and for their ownership to be restricted to the person who has the requisite public key.

Before Bitcoin, all digital goods were non-rival and not scarce—they could be reproduced endlessly at virtually zero marginal cost and consumed simultaneously. For example, when an individual buys a song from a music website and stores it on their PC, they can then send it to other people while keeping a copy of it, and they could all listen to it at the same time. But the Bitcoin network allows the seller of the song to ensure that it can be accessed by only one PC. Should the owner of that PC choose to transfer the key to the song to someone else, they would immediately lose access to the song.

Through the use of cryptography, Bitcoin brings the scarcity, rivalness, finality, and irreversibility of physical transactions to the digital realm. A digital song can now be treated just like a physical cassette or CD, a rival good which cannot be played on two machines at the same time. This is not just true for music files, but for all kinds of digital data, goods, programs, and, most significantly, a currency. Before Bitcoin, any form of direct payment between two parties was unworkable, because there was no way to guarantee that the payer would reduce the currency balance in their account, or not use their balance for more than one payment, and so any form of payment had to rely on a trusted third party that maintains a balance for the payer and payee, and checks the transaction against the balance of the payer to ensure it is sufficient, and debits their account while crediting the account of the payee. By offering the possibility of reliable irreversible transfers of digital goods that leave no trace with the sender, Bitcoin solves the double-spending problem and makes payment without trusted third-party intermediation possible.

As such, Bitcoin is the world's first instance of digital cash, transferring the useful properties of paper cash to the digital realm[3]. Just like personal cash transactions, Bitcoin payments are irreversible and need no trusted third party intermediary. Unlike personal cash transactions, Bitcoin transactions are not restricted by limitations of space; the transacting parties need not meet in the same place at the same time for the transaction to happen, since payment can be made instantaneously across the world to any device with an internet connection. Instead of utilizing a trusted third-party intermediary, Bitcoin is based on cryptographic proof verified by the Central Processing Unit (CPU) power of the total network. As such, Bitcoin can be understood as being to currency what email is to paper mail: an infinitely faster and cheaper digital shortcut for a physical world activity that has been carried out for millennia.

Bitcoin allows for the transfer of digital goods without intermediation by maintaining the full record of ownership and transactions in a transparent distributed asset ledger shared by all computers on the decentralized peer-to-peer network. This record is named The Blockchain. The blockchain is not just a record of transactions, it can also be inscribed with text, data, and programming code, which can be made publically available or encrypted to restrict access.

2. The Blockchain

Technically, Bitcoin is an algorithm that records an ongoing chain of transactions between members of a decentralized peer-to-peer network, and broadcasts these records to all members of the network. There is no central intermediary to record transactions—all network members record them, and all members spend computer power verifying them and inscribing them into blocks. Processing power needs to be expended by these computers to perform mathematical operations to timestamp and validate the transactions.

New transactions continue to be written into new blocks, added to the previous blocks, forming The Blockchain: a common transparent, global, and openly-accessible asset ledger. The use of expended CPU as verification protects The Blockchain from manipulation by network members. The more members verify a transaction, the more CPU has been expended on it. The definitive and accurate record of transactions is the one on which most CPU power has been expended to verify transactions. Should a member of the network attempt to falsify the common record, they would need to marshal more than 50% of the total processing power of the network to validate

[3] Interestingly, the first discussion the author found of digital cash is from the late economist Milton Friedman in a video interview conducted in 1999 in which he states: "The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A… The way I can take a $20 bill, hand it over to you, and then there's no record of where it came from." (Cawrey, 2014)

their forgery. Without the majority of processing power, the transaction would simply be discarded by the network, ensuring only valid transactions are recorded onto The Blockchain.

When a member of the network expends processing power validating transactions, it groups them into a new block, which it transmits to all other members. As reward for expending this processing power on validating transactions, the network member receives new bitcoins—the currency unit in which transactions are recorded. This process is referred to as the mining of bitcoins, as it is the only way in which new coins come into circulation.

The Blockchain can be likened to a large conspicuous board in the center of a town square that acts as the monetary medium for the town, containing a transparent listing of each person's assets in non-physical tokens. Instead of transacting in paper currency, gold, or any other physical medium of exchange, transactions are performed by both parties going to the board when a majority of town residents are present, debiting the account of the buyer and crediting the account of the seller, and listing the transaction on it. No single entity is charged with maintaining the board, and no single individual can alter the record on it without the consent of a majority of town residents. The Blockchain is this large board, except it is visible to everyone around the world who has an internet connection, and needs the CPU of more than 50% of the total network to register a transaction.

The Blockchain obviates the need for a single third party to clear transactions, because honest transactions are inscribed on it and globally viewed and accessible. There is no single individual or institution who is necessary for the transaction to take place. And this record of transactions itself is then divided into blocks of coins that are traded on the network.

3. The Currency

The Bitcoin currency itself is made up of the chain of recorded transactions between members. A useful metaphor from the physical world is to imagine that a currency develops out of actual account books containing a record of transactions. The effort (CPU power) expended on verifying the online record of transactions ensures these records are accurate, which in turn makes the record book a valuable tool for any computer that would want to utilize the technology of payment without intermediation. The ownership of the record books is recorded, and the record books themselves become the currency. As more transactions are carried out, more CPU power is expended on verifying these transactions, creating blocks of transactions to be added onto the Blockchain, and with each new block, new coins are created. Thus, the supply of coins is increased to reward members who expend CPU power on validating and maintaining the

network. In economic terms, the network offers positive incentives for its own maintenance, as 'seniorage' goes to those who expend resources running and maintaining it.

The Bitcoin algorithm is programmed so that a new block of verified transactions is produced every ten minutes. At the inception of the currency, each new block contained 50 new bitcoins, and this rate continued through the first four years, until the end of 2012. The reward for each block was then halved to 25 bitcoins, and is programmed to continue at this rate for four years, after which it will be halved again. This process of 'halving' bitcoin rewards every four years will continue, and with it the bitcoin supply will grow, but at a steadily decreasing rate, asymptotically approaching 21 million bitcoins. By October 2014, more than 13.3 million bitcoins (63% of the total supply) have already been mined into circulation, leaving less than 8 million to be mined over the coming decades. Figure one calculates the theoretical supply and growth rate of Bitcoin from the above formula. The actual supply numbers have differed slightly from these idealized projections, as blocks are not issued exactly every ten minutes.

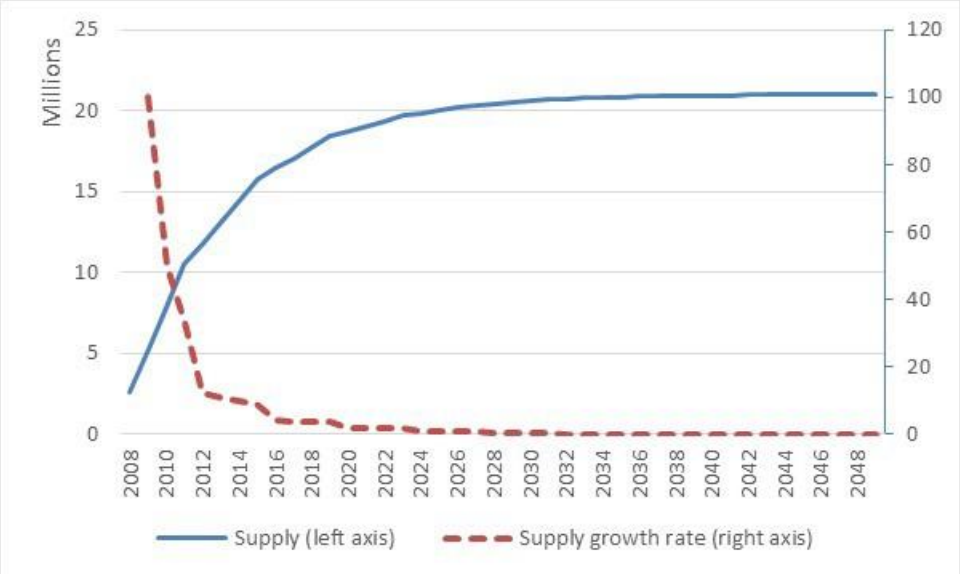

Figure 1: Projected Bitcoin supply and supply growth rate[4]

The bigger the network and the higher the number of transactions, the more mathematical work needs to be done to verify transactions, and the more CPU is needed to earn Bitcoin rewards. On the other hand, as the network size grows and the adoption of the currency increases, its real-world purchasing power also increases, thus ensuring that the block mining reward, while

[4] Source: Author's calculations based on Bitcoin algorithm generation frequency.

decreasing in terms of Bitcoin, and costing more in terms of CPU, is worth more in terms of real goods and services. This is the most strikingly ingenious facet of the design of Bitcoin: If the network grows, the rise in the purchasing power of the currency ensures that the reward to the computers that run the network is increased, thus incentivizing ever-more processing power to be dedicated to verifying the network. The programmed decreasing rate of increase of coin issuance, combined with the fast growth of the network ensures that miners who operate the network continue to be rewarded for running it as it grows. We can thus understand the Bitcoin currency as a currency with no central bank, where the traditional tasks of the central bank are controlled by a distributed mathematical set of rules.

First, currency issuance is not handled by a central bank and human discretion, but according to the pre-programmed distributed protocol, at a predetermined and entirely predictable rate of increase. This removes uncertainty in the currency supply, a major problem in modern fiat currencies whose supply can be routinely increased according to the whims of politics or the economic interests of the issuers; and whose supply can collapse as a result of deflationary recessions. Secondly, the intermediation of payments is also not handled by a central bank, but by the collective effort of the members of the network, who expend computer processing power on this task. Thirdly, the seniorage from the issuance of the currency does not go to the government or to institutions able to generate credit, but to the computers that spend processing power on maintaining the network and running transactions. A unique aspect of Bitcoin is that it uses the seniorage from currency issuance to reward the expenditure of CPU on validating transactions—or generating the blockchain. In other words, new coins are offered to those who maintain the Blockchain.

The more users adopt Bitcoin for purchases and payments, the higher the demand for the currency, the higher its real purchasing power in goods and services, the more valuable the reward for expending CPU on validating transactions, the larger the incentive to expend CPU on maintaining the network, ensuring it continues to run smoothly as the volume of transactions increases. There is also a very small transaction fee that rewards CPU expenditure on network maintenance and transaction verification.

The Bitcoin network grows as fast as Bitcoin adoption rises, or, in other words, as fast as the Bitcoin economy grows; the issuance of the currency, however, only rises at a predetermined rate, which is halving every four years. Though the supply of the currency is increasing, and will continue to do so for more than a century, the real purchasing power of the currency has increased drastically in the five years it has been circulating. The increase in adoption explains the rise in the purchasing power of bitcoins since circulation started in 2009. The first recorded

exchange rate of bitcoins for fiat currency was at a rate of 1,309.3BTC for 1USD, offered in October 2009 (Wallace, 2011). By October 2014, the exchange rate had risen to fluctuate around 0.0025BTC for 1USD, reflecting roughly a five-hundred-thousand-fold (0r 50,000,000%) increase in the price of a Bitcoin in US dollars in five years. The strictly limited amount of currency available means that the more the technology of Bitcoin catches on, the more the purchasing power of the currency rises. It is this rise in the value of Bitcoin that provides a very strong incentive for the maintenance of the network, and incentivizes more and more people to purchase bitcoins and accept them for payment.

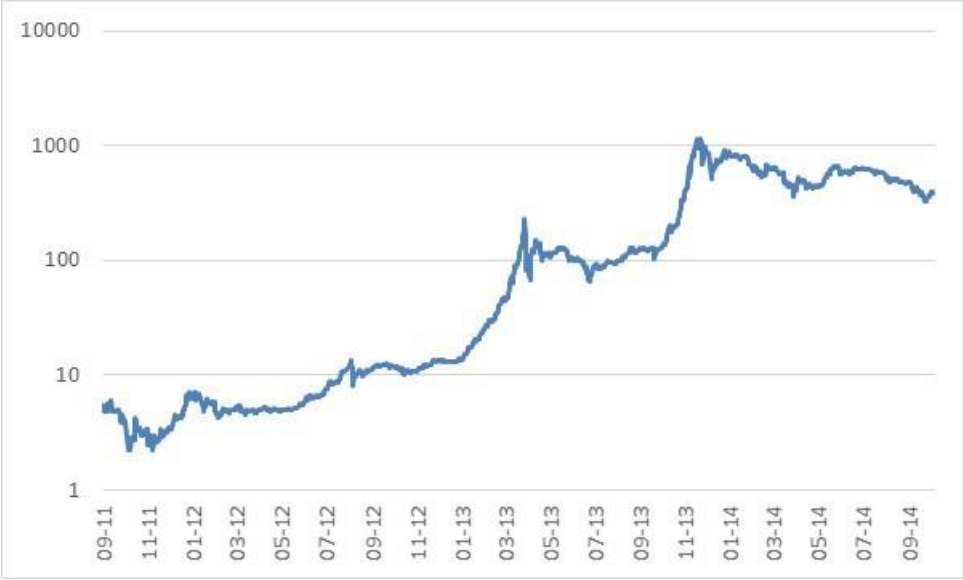

Figure 2: Bitcoin to USD exchange rate (log scale)[5]

Although the value of each Bitcoin has grown very quickly in terms of real purchasing power, Bitcoin as a currency is moderately inflationary, with the supply growing at 59% in 2011, 32% in 2012, and 15% in 2013. It is expected to grow at around 12.5% for the year 2014, and at around 10% and 9% respectively over the years 2015 and 2016. These numbers differ slightly in practice from the idealized projected numbers mentioned above, since block issuance is not done exactly every 10 minutes, but can vary slightly. But what is certain is that the growth rate of Bitcoin will continue to decline over the coming years, dropping to around 4% in 2017, 1.7% in 2021, and 0.8% in 2025, continuing to drop further after that until it becomes a negligible increase.

Here it is instructive to compare the growth in the stock of Bitcoin the currency to the growth rate of other major currencies. Table 1 shows the average, standard deviation, and the minimum and maximum annual growth rate of the (broadest measures) of the money supply for the major

[5] Source: Data from bitstamp exchange, downloaded from Bitcoincharts.com. Accessed October 16, 2014

fiat currencies and gold over the past 30 years. As it stands, all these currencies' broadest available measures (US Dollar's M2, Japanese Yen's M3, Swiss Franc's M3, Euro's M3 (and its constituent currencies pre-1992), and the British Pound's M3) are growing at a smaller average annual rate than Bitcoin's rate so far. Nonetheless, as Bitcoin's supply is programmed to grow at a continuously decreasing rate, it should start growing at a lower rate than all these currencies within the next decade or so.

Table 1: Average growth rate of monetary supply over the period 1984-2013[6]

	GOLD	USD M2	JPY M3	CHF M3	EUR M3	GBP M3
Average	1.71	5.53	3.47	4.70	6.19	8.80
Standard Deviation	0.15	2.58	3.67	2.88	3.34	5.52
Minimum	1.44	0.35	-5.10	-1.13	-0.65	-3.32
Maximum	1.89	10.30	11.14	10.92	12.03	19.14

Gold has been the most marketable and liquid commodity on the market across time and space. This is due primarily to it having the highest stock-to-flow ratio of all commodities and assets. By virtue of being indestructible, the stockpile of gold that humanity has accumulated over thousands of years dwarves the new annual production of gold every year, which is very small since gold is exceedingly rare and cannot be synthesized. This makes gold the least inflatable commodity on the market, with an annual growth rate averaging 1.7% per year over the past 30 years, with a standard deviation of only .15%. No other commodity comes even close, since other commodities are perishable and consumable, and are not as rare; hence new annual production is always significantly high compared to existing stockpiles. It is this property of gold which has guaranteed its monetary role virtually throughout human history and across civilizations. Should any other commodity or asset be used as a medium of exchange, it is very easy for its producers to inflate its supply very quickly over the existing stockpiles, thus depreciating its value. Only gold, with its rare occurrence in the earth's crust, and its indestructible stockpile, is immune from this inflationary pressure, and thus only gold has survived as a medium of exchange and store of value virtually throughout time and across civilizations.

Gold will continue to have a lower inflation rate than Bitcoin for the next decade or so, making it a theoretically more attractive store of value during this time, but Bitcoin's growth rate will drop below that of gold sometime around the year 2025, and will continue to be halved from then on.

[6] Source: Author's calculations based on money supply data sourced from websites of the US Federal Reserve Board (research.stlouisfed.org). Gold data obtained from World Gold Council (gold.org).

Around the year 2025, Bitcoin will be the one medium of exchange with the consistently and reliably lowest growth rate in the world.

The strictly limited supply of the Bitcoin currency is the most important way in which it differs from conventional currencies circulating today. In modern economies, central banks are tasked with ensuring the money supply expands at a controlled low pace, to allow economic growth without deflationary rise in the purchasing power of money (Bernanke, 2002). The standard economic textbook argues that this mild inflation is necessary to stimulate spending and investment and discourage hoarding. Should a central bank contract the money supply, or fail to expand it adequately, then a deflationary spiral can take place which would discourage people from spending their money and thus harm employment and cause an economic downturn (McConnell, Brue, and Flynn, 2009, p.535).

The designer of Bitcoin, on the other hand, is evidently influenced by the Austrian School of Economics, which argues that the quantity of money itself is irrelevant, that any supply of money is sufficient to run any economy of any size, since it is only the purchasing power of money in terms of real goods and services that matters, and not is numerical quantity. As Ludwig von Mises put it (Mises, 1949, p.421):

> "The services money renders are conditioned by the height of its purchasing power. Nobody wants to have in his cash holding a definite number of pieces of money or a definite weight of money; he wants to keep a cash holding of a definite amount of purchasing power. As the operation of the market tends to determine the final state of money's purchasing power at a height at which the supply of and the demand for money coincide, there can never be an excess or a deficiency of money. Each individual and all individuals together always enjoy fully the advantages which they can derive from indirect exchange and the use of money, no matter whether the total quantity of money is great or small … the services which money renders can be neither improved nor impaired by changing the supply of money.... The quantity of money available in the whole economy is always sufficient to secure for everybody all that money does and can do."

Murray Rothbard emphasizes Mises' point (Rothbard, 1997. p.311):

> "A world of constant money supply would be one similar to that of much of the eighteenth and nineteenth centuries, marked by the successful flowering of the Industrial Revolution with increased capital investment increasing the supply of goods and with falling prices for those goods as well as falling costs of production."

According to the Austrian view, if the money supply is fixed, then a growth in the economy will cause prices of real goods and services to drop, allowing people to purchase increasing quantities of goods and services with their money. Hence, according to Austrian theory of money, the limit on the supply of Bitcoin is not an impediment to its growth or adoption. If the currency continues to be adopted by more individuals, its purchasing power will continue to rise, making it even more attractive as a medium of exchange and store of value. This Austrian view on money explains Nakamoto's capping of the money supply, as well as the reduction in the rewards for miners, which reduces the currency's inflation quickly, while ensuring the rewards for miners increase in value in real terms if the network continues to grow.

The Austrian theory of money posits that money emerges in a market as the most marketable commodity and most saleable asset; the one asset whose holders can sell with the most ease, in favorable conditions (Menger, 1892). An asset that holds its value is preferable to an asset that loses value, and savers who want to choose a medium of exchange will naturally gravitate towards assets that hold value over time as monetary assets. Network effects mean that eventually only one, or a few, assets can emerge as media of exchange.

A money that appreciates in value incentivizes individuals to save for the future, as their savings gain purchasing power over time. Hence, it encourages deferred consumption, resulting in lower time preferences. A money that depreciates in value, on the other hand, leaves citizens constantly searching for returns to beat inflation, returns which must come with a risk, and so leads to an over-investment in risky projects and an increased tolerance of risk among investors, leading to increased losses.

Further, an economy with an appreciating currency would witness investment only in projects which offer a positive real return over the rate of appreciation of money; meaning that only projects expected to increase society's capital stock will tend to get funded. By contrast, an economy with a depreciating currency incentivizes individuals to invest in projects that offer positive returns in terms of the depreciating currency, but negative real returns. The projects that beat inflation but do not offer positive real returns effectively reduce society's capital stock, but are nonetheless a rational alternative for investors since they reduce their capital slower than the depreciating currency. These investments are what Ludwig von Mises terms *malinvestments*—unprofitable projects and investments that only appear profitable during the period of inflation and artificially low interest rates, and whose unprofitability will be exposed as soon as inflation rates drop and interest rates rise, causing the bust part of the boom-and-bust cycle. As Ludwig von Mises puts it: "The boom squanders through malinvestment scarce factors of production and

reduces the stock available through overconsumption; its alleged blessings are paid for by impoverishment." (Mises, 1949, p.575)

Bitcoin exists as a real-world experiment in this inflation/deflation debate. Whereas traditional currencies are continuously increasing in supply and decreasing in purchasing power, Bitcoin has so far witnessed a large increase in real purchasing power, in spite of a moderate (but decreasing, controlled, and capped) increase in its supply. If Bitcoin's depreciation rate is measured with respect to the US Dollar, it would be highly negative, as shown in the data below, averaging a -85% depreciation rate in the three years for which data is available.

Table 2: Bitcoin depreciation rate in USD[7]

DATE	BTC/USD	depreciation rate
DEC 31 2010	3.33	
DEC 31 2011	0.2118	-93.65
DEC 31 2012	0.074	-65.05
DEC 31 2013	0.0012	-98.32

If one were to perform the reverse experiment, and analyze the performance of the USD from the perspective of the Bitcoin economy, it would appear as a hyper-depreciating currency, depreciating at an average annual rate of 2,500% over the past three years.

Table 3: USD depreciation rate in Bitcoin[8]

DATE	USD/BTC	depreciation rate
DEC 31 2010	0.3	
DEC 31 2011	4.72	1474
DEC 31 2012	13.51	186.11
DEC 31 2013	806	5865.95

The growth of the Bitcoin network so far, in spite of the very sharp rise in the purchasing power of the Bitcoin currency, lends credence to the Austrian view that a rise in the purchasing power of money is not harmful, and in fact desirable. There seems to be no evidence so far to support the mainstream economic contention that a deflationary rise in the purchasing power of this currency would stall its growth, or the growth of the economy using it. As the value of the Bitcoin currency rises, people use smaller units for transactions. The first real-world purchase made with Bitcoin saw two pizzas exchange for 10,000 bitcoins on May 22, 2010 (Caffyn, 2014). These two pizzas would have exchanged for around 10 bitcoins in May 2011, and for

[7] Data Source: Bitcoincharts.com
[8] Data source: Bitcoincharts.com

around 0.2 bitcoins in May 2013, and around 0.05 bitcoins in May 2014. As the purchasing power of a bitcoin has soared, many exchanges and sellers have taken to stating their prices in milli-bitcoins (1/1000 of a bitcoin), and the bitcoin unit can be further divided into smaller units, all the way down to a satoshi, which is defined as $100{,}000{,}000^{th}$ of a bitcoin. There is no foreseeable practical reason why continued deflation would cause any problem for the growing Bitcoin economy, except in the trivial manner of readjusting prices, a task which is becoming increasingly trivial in the age of computers, where prices can be quoted in any other currency or gold, while transactions are settled in Bitcoin at the spot rate.

4. Smart Contracts

The Bitcoin blockchain allows for many applications beyond just Bitcoin the currency. Blocks can also contain text and computer code, which can be made publically accessible or encrypted, offering many potential applications which users have only just begun to explore. As a publicly accessible, transparent and open ledger, the blockchain can be transcribed with what Nick Szabo calls 'Smart Contracts'—contracts which are transcribed in actionable computer code that makes them self-enforcing or self-executing, obviating the need for third-party enforcement (Szabo, 1997). Such software can transparently and accurately assess compliance with contract terms, and based on it, carry out financial transactions in the Bitcoin currency, or control electronic devices, grant access to texts, execute wills, and so on.

It is currently possible to design such automated forms of contracts without the blockchain, but the stumbling block towards seeing them executed in the real world is ensuring that the code is not altered after the agreement. But if the code is implemented on a device belonging to one of the two transacting parties, that party will have an incentive to tamper with the code to their benefit, and this makes demand for such forms of contract virtually non-existent currently, and instead, all forms of contract currently must rely on a third party to oversee and enforce compliance with the terms of the contract. Such third-parties include, but are not limited to, lawyers, police, judiciary, government agencies, and private corporations.

But the invention of the blockchain introduces a new possibility to the idea of contracts: by placing the contract transparently on the blockchain, it can be assured that no party can tamper with the contract or alter it to their advantage. Only if one were able to amass more computer processing power than the 51% of the Bitcoin network could they alter the blockchain and change the terms of a contract inscribed therein.

At its heart, what the Bitcoin blockchain allows is the restructuring of various forms of human relationships based on transparent mutual consent, without the need for trust, or enforcement. Strangers could enter into binding agreements, trades and employment with one another knowing that the tamper-proof blockchain can reliably enforce the terms of the contract. This expands the possibilities for consensual agreements and curtails the need for coercion and the threat of coercion as enforcement and intermediation mechanisms.

III. The advantages and strengths of Bitcoin

In little more than five years in existence, Bitcoin has gone from being a computer program installed on two computers sending digital coins with no real purchasing power in the real world, to a global algorithm commanding the world's largest computer network, with the digital currency supply exceeding $5b in market value, and accepted by tens of thousands of merchants worldwide. All of this was achieved through voluntary cooperation of networks the world over. During this time, not a single attack or threat has succeeded in destroying the network. There are five main aspects of the design of Bitcoin that make it appealing to consumers and resilient to attack, and these are: elimination of trusted third-party intermediation, payer-initiated payments, the enormous processing power behind it, the absence of a single point of failure to the system, and the fact that participation in the network is entirely voluntary.

1. Eliminating the need for trusted third parties

The most appealing feature of Bitcoin is that eliminates the need for a trusted third party to a financial transaction that does not take place face to face. The payer in the transaction transfers the ownership of their coins on the blockchain to the recipient, and the validity of the transaction is verified by any one of the many computers working on verifying transactions. There is no need to trust any single individual or institution to carry out this transfer, miners compete among themselves to verify it in order to complete the verification of blocks of transactions and receive the newly minted coins. There is no need to trust any of these miners, as they are individually powerless to defraud transacting parties and would gain absolutely no benefit from doing so. The network is designed to offer significant reward for anyone who is willing to verify transactions honestly. This eliminates the need to trust any third party to carry out a transaction with anybody in the world. All other existing payment methods necessitate placing trust in various parties that are outside the transaction: a financial institution, possibly more than one, credit card companies, as well as the central banks that issue the currency in which the transaction is denominated. It is accurate to say that Bitcoin is built entirely on verification, and has no need, or use, for trust.

2. Payer-initiated payment

Bitcoin payments are initiated by the payer, and do not require that the payer reveal any sensitive information to the payee or to any other person or entity. By contrast, credit card transactions are initiated by the recipient of the payment, rather than the payer, and require the recipient to be privy to important information which can be easily compromised.

A credit card transaction necessarily involves the payer giving the recipient their credit card information to enter it into a credit card processing terminal. This is a major security problem with credit card payments, since a payer's credit card information can be compromised in any transaction. Many merchants maintain records of their customers' credit card information, which can be compromised later down the line. By having payment initiated by the recipient, and dependent on the recipient obtaining sensitive information from the payer, credit cards are rife with fraud problems. In the year 2012, credit and debit card fraud accounted for approximately 0.522% of all credit card transactions worldwide, which cost payment card issuers, merchants and banks $11.27 billion of losses (Nilson, 2013).

With Bitcoin, on the other hand, the recipient only receives the payment itself and the address of the payer, which is not information that can be compromised to defraud the payer, any more than knowing someone's email address leaves them vulnerable to being hacked. For the buyer, Bitcoin offers the peace of mind of knowing that their financial security is not dependent on the good behavior of the merchants and the third parties. For merchants, the finality of Bitcoin transactions offers the advantage of not having to worry about potential chargebacks and payments cancelled after the goods have been delivered.

3. Processing power

As a result of the lucrative rewards for maintaining it, the Bitcoin network has grown into what is by far the world's largest supercomputer. In October 2014, the processing power dedicated to Bitcoin was estimated at around 3,205,028.64 PetaFlops (source: Bitcoincharts.com). By contrast, the world's fastest supercomputer Tianhe-2, has a speed of 33.86 PetaFlops, as estimated by the Top500 List in June 2014 (Top500.org). The world's top 500 supercomputers combined have a processing power of 273.76 PetaFlops. In other words, the combined processing power of the global distributed network of computers validating Bitcoin transactions is 11,700 times larger than the processing power of the world's top 500 supercomputers combined. This system is perfectly incentive-compatible to ensure the continued smooth operation of the network: As more people demand bitcoins for financial transactions, the purchasing power of bitcoins increases, and with it increases the real value of the reward for

expending processing power on validating transactions, ensuring more processing power is dedicated to run the network.

4. No single point of failure

The lack of a centralized authority to issue bitcoins and monitor transactions is the chief strength of Bitcoin. Not having a central server that processes all transactions means that the system has no single point of failure, making it extremely resilient to attack or technical failure, if not impervious to them. A physical or digital attack that destroys any individual computers operating the network would not make a dent in the operation of the Bitcoin digital transfer technology, currency, or blockchain. Such an attack could destroy a fraction of the processing power behind Bitcoin, but would leave the Bitcoin blockchain intact as a ledger of assets and record of transactions. This might hurt the individual owners of these computers, but will have no impact on the integrity of the Bitcoin algorithm or the currency. No matter how many computers on the network are attacked and destroyed, the blockchain can continue to live on the remaining computers. So long as two computers can continue to communicate with one another anywhere in the world, the blockchain can survive as a record of all transactions and coin ownership.

Bitcoin is an embodiment of Friedrich Hayek's concept of distributed knowledge and complex spontaneous order emerging from simple individual actions (Hayek, 1945). Hayek's work was the inspiration behind Wikipedia (Mangu-Ward, June 2007), the online encyclopedia whose strength is that it does not rely on centralized authority, but on distributed knowledge. This makes Wikipedia resilient, specialized, up-to-date and immensely cheap to operate and access, in a way incomparable to any encyclopedia compiled by a centralized authority. Similarly, decentralizing the blockchain as a record of transactions, and verifying it with the distributed processing power of the network ensures a far cheaper, faster, and more resilient method of payment than any technology reliant on a centralized intermediary. Further, this simple algorithm designed by an anonymous programmer has evolved steadily over the past five years, been adapted into various other uses by individuals and groups that an entirely new ecosystem has emerged from it, and will likely continue to evolve. No single mind could have overseen the complexity of the ecosystem that is emerging, which is, as Adam Ferguson would put it: "the product of human action, not human design" (Ferguson, 1782).

5. Voluntary

The existence and operation of the Bitcoin network is entirely consensual: all the people who have traded bitcoins for goods, services, or other currencies, and all the people who have dedicated hardware processing power towards the maintenance of the network have done so out

of their own accord. Any person who does not like the idea, for whatever reason, can completely isolate themselves from it and suffer no adverse consequences from it. Any person who chooses to utilize the Bitcoin technology accepts the risks associated with it. In contrast, the legacy fiat currencies and financial system expose holders to risks in which they do not partake and for which they did not consent. Banking failures through contagion or liquidity shortages, as well as currency devaluation for political purposes, are prime examples of phenomena that cannot, by design, happen in Bitcoin. Good algorithm design combined with the transparency of open-source software and reliability of large decentralized networks can substitute for politicized and centralized institutions, and may prove more reliable.

This consensual and distributed nature of Bitcoin appears to make it immune to political pressure or sanction. Janet Yellen, the current chair of the US Federal Reserve Board has indicated that it is not possible for the FRB to regulate Bitcoin, stating:

> "Bitcoin is a payment innovation that's taking place outside the banking industry. To the best of my knowledge there's no intersection at all, in any way, between Bitcoin and banks that the Federal Reserve has the ability to supervise and regulate. So the Fed doesn't have authority to supervise or regulate Bitcoin in anyway." (Rushe, 2014)

While several central banks have issued warnings against its use, there is practically nothing that can be done to actually stop or ban its use. Any person with an internet connection can access any one of the many sites or services that utilize bitcoins. The only practicable way in which governments can stop Bitcoin adoption is by banning regulated financial institutions from using it, but that is largely immaterial to Bitcoin, which essentially eliminates intermediation and replaces the entirety of modern financial institutions with faster, cheaper, safer, and more efficient computer code. Such a ban is akin to a government banning the national postal service from using email; it might hamper the operation of the national postal service, but is unlikely to cause any serious problems for the technology of email. New York State is currently preparing rules to regulate New York businesses using bitcoins, yet these rules cannot be understood as affecting the Bitcoin network itself, but only affecting NY-based institutions dealing with bitcoins. Should they prove too onerous to Bitcoin businesses, that will be unlikely to hurt Bitcoin on the long-run, but to simply shift Bitcoin activity outside of New York.

At its heart, Bitcoin is a program running mathematical operations perfectly transparently. The notion of governmental regulation of mathematical operations is illogical; math only follows the rules of math and cannot be decreed to disobey them. The protocol and network will continue to operate mathematical algorithms and record the transactions regardless of what politics dictate.

It thus seems Bitcoin is extremely resilient to attack, whether by vandals, hackers, or government agencies. Bitcoin might even be termed anti-fragile to these attacks, since all such attacks so far have failed at killing it, and in fact seem to have only made it stronger, and more resilient to future attacks. Countless hacking attempts have failed, but many of them have exposed weaknesses in the code, and forced the operators of the network to revise it to make it more resilient. Government attacks, on the other hand, seem to have only succeeded in raising awareness of Bitcoin and exposing its idea to wider audiences, fueling the growth of the network.

IV. Other digital currencies: Altcoins

Bitcoin is the first decentralized digital currency, but it is not the only one. Hundreds of alternative digital currencies, commonly referred to as 'Altcoins' have been introduced since the inception of Bitcoin, copying the same basic design, with varying differences in features and implementation. Zerocoin, for instance, promises complete anonymity; Litecoin promises faster transaction processing, and Peercoin claims to distribute new coins according to usage of the coins, rather than processing power accumulation, supposedly allowing for less wealth accumulation among the early adopters. Peercoin is also programmed to continue to increase in supply at a rate of 1% a year indefinitely. These coins have coexisted next to Bitcoin so far, but have remained a tiny sliver of the size of the Bitcoin network in terms of market cap and processing power. It is not inconceivable that one of these coins could supplant Bitcoin as the leading digital currency, but there are three main impediments to this happening.

The first impediment is the first-mover advantage: As Bitcoin is the first digital currency, its reputation and name recognition is far greater than all altcoins, and it is likely to continue to grow faster than the others by attracting more of the new users of digital currencies. As it stands, the 'market cap' of Bitcoin is equal to 22.48 times the market cap of the 10 next largest altcoins combined[9]. A large infrastructure of services, such as exchanges, online wallets, and merchant facilitators, has developed around Bitcoin, and not around the other coins. Secondly, network effects mean that Bitcoin remains far more useful as an actual currency and medium of payment, since far more people are already using it as a medium of payment, while Altcoins are mainly a vehicle for speculation. Merchants and businesses which want to venture into digital currencies are far more likely to accept Bitcoin for payment since it opens up a far larger network of potential customers than any altcoin. Third, and perhaps most important, is the aforementioned

[9] Source: Author's calculations based on data obtained October 18, 2014 from Cryptocoinrank.com.

processing power behind Bitcoin, which is far larger than any other currency, making it far more resilient to attacks than the other altcoins. On October 18, 2014, the Bitcoin processing power was equal to 3,154 times the processing power of the next ten most powerful altcoins combined[10]. All three of these reasons make it likely that Bitcoin will remain the leading digital currency for the foreseeable future, though the opposite conclusion cannot be discounted. Altcoins will continue to be the testing ground for new innovations in the technology of digital currency, and it is impossible to foresee today how these innovations will play out. Given the aforementioned strength of Bitcoin, however, what is more likely than a new digital currency supplanting Bitcoin is the prospect of new innovation built on the Bitcoin network itself, with various types of currencies and financial instruments layered on top of the Bitcoin blockchain.

Yet such a question is not significant for this paper's purposes, as the technology behind Bitcoin is far more interesting than Bitcoin itself. Whether the current Bitcoin network is usurped by another digital currency with some superior features, or should it fail due to some unforeseen problem, we will still be left with the immensely useful and cost-effective technology of open-source distributed decentralized transparent asset ledgers allowing for financial transfers without trusted third-party intermediation. This technology cannot be uninvented, and can find more and wider applications across various economic, legal, technical and political avenues. It is this technology, more than Bitcoin itself, that is what is most interesting. After all, the technology behind search engines revolutionized the world, irrespective of the fate of the web's first search engine, Altavista, which has now gone out of business.

V. Bitcoin and development

The world's major developed economies have enjoyed the benefits of economic, financial, judicial, institutional, and monetary advancement for decades. Currency is largely stable in purchasing power, financial services are accessible to a majority of the population, the judicial system is responsive and relatively efficient, and the economic institutions are largely conducive to economic development; they broadly fall under the category of 'Private Property Institutions' or 'developmental institutions' as identified by Acemoglu, Johnson, and Robinson (2001). Bitcoin could facilitate improvements in financial services and institutional arrangements in these societies, but it stands to offer a qualitatively different, and potentially more transformative, impact on underdeveloped countries.

[10] Source: Author's calculations based on data obtained October 18, 2014 from coinwarz.com.

The world's poorest are citizens who live in countries with limited financial services, unaccountable governments, fast-depreciating currencies, corrupt judicial systems, and economic institutions that perpetuate the advantages of elites while excluding the majority of the population, with little incentive to reform—what Acemoglu, Johnson, and Robinson (2001) and Engerman and Sokoloff (1997) term 'Extractive Institutions'. These institutions do not seek to maximize economic growth and increase output, but rather to maximize the predation of the elites over the majority of the population.

A significant contribution to the survival of predatory and unproductive economic institutions is their ability to have a monopoly over their captive populations, who have no alternative to dealing with them. In the physical world of industry and trade, such monopolies are easy to enforce through brute bureaucratic force and controls on capital movement, information, and production. But the rise of the virtual economy introduces an escape hatch for these populations, who can now access information, trade, and transact while subverting the physical controls placed by predatory elites. But for as long as payment remains inextricably linked to centralized institutions easily controlled by elites, institutions in the developing world continue to be geared towards predation rather than production.

Bitcoin may provide populations living under predatory institutions with what Albert Hirschmann (1970) terms 'exit': to withdraw from the relationship with the institutions that ill-serve them. The mere threat of exit makes 'voice' more powerful: elites will feel more pressed to listen to the masses' problems and grievances if the masses have a credible fallback position that is harmful to the elites. This can have a twofold impact: it would allow these populations to deal with productive private property institutions, and it would threaten the elites of these societies with mass exit of their populations from their political and economic control, forcing them to reform their institutional arrangements. The Bitcoin network is the potential institutional competition to which the world's poor can defect. Elites and governments can rely far less on the safety of their territorial monopolies in a world where payment is virtual.

Bitcoin offers the most promise and potential to the billions of people who to this day remain unbanked and unable to access financial services. The high cost of financial intermediation makes the world's poor unattractive to financial institutions; the small market value of transactions means that the small fees charged on them cannot cover the costs of intermediation. Further, in developing countries where political instability is higher, financial institutions face difficulties in operating that reduce their services and reach. The developing world is well behind the developed world in terms of financial development, and would require extensive investment in infrastructure, education, training and capital accumulation to be able to catch up. But Bitcoin

offers the intriguing possibility that developing countries could sidestep the development of a traditional financial system and move to mass adoption of international online digital currency. Many developing countries also have underdeveloped telecommunication networks and very little telephone penetration, but the invention of the mobile phone has allowed for the spread of telecommunication without the need for large infrastructure spending or the prerequisite institutional and political reform (See Aker and Mbiti, 2010).

This section of the paper offers a preliminary exploration of how Bitcoin technology could impact six economic and political aspects of economic life in developing countries, and the institutional impact it can have.

1- Remittances

The market most ripe for disruption by digital currency is that of international remittances. The World Bank estimates global remittances in the year 2013 at $400b. At the end of 2013, the average cost of remittances is 8.58% of the amount of money transferred, with bank transfers costing an average of 12.33%, money transfer operators 7.01%, and post office transfers costing 4.12% (World Bank, 2014).

Sub-Saharan Africa is the region with the highest average cost of remittances, at 12.55% of remittance value (World Bank, 2014). After all the recent advances in communication and transportation technology, this is an anachronistically and astonishingly high ratio. The lack of penetration of traditional banking into Sub-Saharan Africa is arguably the culprit here, as is the inability of new players to enter the money transfer business due to heavy government regulation and entrenched elites.

Bitcoin can affect remittances in two manners: First, it can be used for direct person to person transfers, which would be virtually costless and instantaneous. The problem with this method, however, is that Bitcoin is not adopted widely enough for recipients to be able to spend it in place of their traditional currencies, at least for the time being. A Sub-Saharan African family receiving bitcoins today on a mobile device would find it hard to spend that money on meeting their actual expenditure needs.

The second entry point for Bitcoin into the remittances industry is through money transfer agencies adopting Bitcoin for their transfers, while paying recipients in cash. Kenya has already witnessed the emergence of the first such company, BitPesa[11], which currently charges only 3% and guarantees same-day delivery. BitPesa receives Bitcoin from expats all over the world and

[11] See Bitpesa.co

pays out their equivalent in local currency to Kenyans, in cash in person, via a domestic bank transfer, or through Kenyan mobile payment system M-Pesa.

If Bitcoin adoption continues to grow, that would likely be beneficial to services like BitPesa in the medium-run, as more expats would be willing to buy Bitcoin and send it to BitPesa. In the long-run, however, Bitcoin growth would likely undercut services like BitPesa by making it easier for individuals to transfer Bitcoin directly to each other at Bitcoin's very low fees.

2- Microfinance

Nowhere does the possibility of costless international cash transfers have more transformative promise than the area of microfinance, where transaction costs have the highest toll on the poor, and their elimination opens wide vistas of possibilities for international financing.

With Bitcoin, individuals in rich countries can make small transfers to individuals in poor countries and receive quick repayment. A quantity of money that would be trivial for an individual in a rich country could be life-altering to an individual in a developing country. This transfer today would not be a possibility since making the loan and each repayment would involve a large transaction fee, on the same order of scale as the payment itself. It is not feasible for an individual in a rich country to make a direct loan of $100 and get repayment in 12 installments if each of these 13 transactions would cost $20-40, as they do today. But if the transaction cost is eliminated, such loans become a distinct possibility, and a new world of international peer-to-peer microfinance could emerge.

Individuals in rich countries are likely to charge interest rates that are far lower than what the borrowers could get from local shark lenders or financial institutions. International zero-interest loans could become widely-available for individuals in poor countries. An online rating system for borrowers' repayment reliability could emerge, which would provide strong incentives for repayment.

As Bitcoin adoption spreads, such lending could be integrated into the business model of borrowers, who can receive their own payments in Bitcoin, making accounting completely transparent and repayment automatic. This reduction in informational asymmetry would lead to a reduction in the risk associated with lending, as well as the transaction costs, a the margin, this is likely to shift financing from lending to direct equity investment that shares in profits and losses.

3- Development aid

William Easterly has written extensively over the incentive problems faced by the foreign and development aid industry (Easterly, 2002). Aid agencies do not have proper market feedback on their actions like private market firms do. Their beneficiaries cannot take their business elsewhere; they do not have the credible threat of exit, and they have little ability to offer feedback. There are no mechanisms by which these agencies can suffer negative consequences from beneficiary dissatisfaction. Easterly further explains that foreign Aid agencies are generally monopoly providers of their services, and they function in a non-competitive industry structure. All of the limitations and problems of central planning elucidated by Ludwig von Mises, Friedrich Hayek, and others, apply even more forcefully in the context of economic development, as foreign agencies will have even more problems of insufficient knowledge in foreign contexts. As an alternative model, Easterly proposes the idea of "aid markets", whereby donors can give recipients aid vouchers, directly, and these recipients can then choose to spend their vouchers on the agencies which provide them with the services they want (Easterly, 2002, p.53). While highly original and promising, Easterly's proposal has not been enacted, nor does it seem likely that it will, due primarily to the large transaction costs and knowledge problems involved with distributing the vouchers and setting up voucher funds, as well as there being no incentive for aid agencies to give up their monopoly status in favor of a competitive solution. But with decentralized digital currency an even more direct manifestation of Easterly's idea can be enacted: donors can now make microdonations to recipients directly, allowing recipients to choose where to spend their aid money themselves, and forcing development agencies to be accountable to recipients themselves. Development agencies would then have to compete to get their funding from the recipients themselves, and donors can track directly how their funding is being spent.

Digital currency also makes possible direct microdonations from rich citizens in rich countries to the poorest citizens of the world. Whereas the transaction costs in the current banking system prohibit such transactions. The reduction of transaction costs on international transfers can have an impact on development aid similar to that in microfinance. Individual peer-to-peer donations can reduce overhead and waste significantly,

One particularly promising application of this is in the case of natural disasters, which can severely damage the financial infrastructure of an area, posing severe challenges to mobilization of resources for relief efforts. Digital currencies can transform disaster relief by allowing for donations from around the globe to go to the stricken areas immediately when they are most needed. Resources and relief efforts can be mobilized far faster when those afflicted by disaster have the financial ability to pay for them directly. Their local knowledge and their pressing need would direct their spending far better than a centralized solution from above would.

4- *International trade*

The biggest impediment to the globalization of trade is no longer shipping or information, but payment. Shipping and mail services are continuously getting cheaper and more widespread. The internet has made information on products accessible worldwide, and provides countless avenues for sellers to market their goods at very little cost. But payment remains more complicated, especially in developing countries. Merchants in poor countries find it prohibitively hard to access payment recipient solutions at financial institutions which can quickly and safely process payments from global buyers. Digital currency's potential is to be the great leveler of international trade, allowing producers and suppliers the world over to compete for a global marketplace, and to compete purely on the quality of their goods, rather than their access to finance.

5- *Capital accumulation*

The deflationary nature of the Bitcoin currency makes it appealing as an inflation haven. Currency devaluation, hyperinflation, banking failures, liquidity crises, and bank account confiscations are frequent events in many developing countries, as financial history books attest (See Reinhart & Rogoff, 2009). The rapid rise in the value of bitcoins over the past five years makes it a potential haven for citizens of countries whose currencies are devaluing, on top of the traditional havens of safe currencies and precious metals, which are easier to control by virtue of being physical. The appearance of an easier and more convenient inflation haven could increase the pressure on the value of the domestic currency. While this could theoretically lead to a hyperinflationary collapse, a more likely immediate consequence is that the threat of exit to Bitcoin could force governments to act with more monetary responsibility in the handling of their currencies.

The world's poorest are usually citizens of countries that continuously witness devaluation of the value of their currency. Should the world's poor begin to transact and accumulate savings in an appreciating currency, they would be able to accumulate capital far more effectively. Accruing higher levels of capital also leads to increases in marginal productivity of labor.

6- *International supra-legal contracts*

Security of property rights, enforcement of contracts, and efficiency of the judiciary system are three of the most significant institutional structures that are absent in many developing countries, hampering the emergence of an extended market order and a dynamic enterprise system. Bitcoin's Smart Contracts can be used to create self-enforcing contracts between strangers, offering citizens of developing countries a framework for transactions independent of the

domestic judicial and executive branch. Further, the blockchain can act as a global reputation mechanism for its users, thus incentivizing them to respect their contracts and abide by them in order to gain a reputation of trustworthiness. Instead of having to rely on third parties to enforce contracts and establish whether certain parties are worthy of contracts, the blockchain technology can let every individual and organization develop its own reputation and brand online, with complete transparency.

The institutional, governmental, and technological problems of developing countries form a formidable barrier for most their citizens partaking in a modern economy. Underdevelopment can be understood as both a cause and consequence of institutional impediments to individual opportunity. While still a technology in its infancy, Bitcoin offers a blueprint for how billions of the world's poor can partake in international modern capitalism without having to reside in countries with supportive modern institutions. This can be life-changing to those individuals, but can also pressure the governments and institutions of developing countries to reform properly or risk being left out. The nationalist monopolies in financial services, currency issuance, judicial systems, and credit provision will be challenged by the technology of distributed networks, and the old systems will have to improve their performance if they are to avoid being left behind.

VI. Conclusion

The technology of cryptographically secured decentralized distributed digital currencies is a nascent technology that suggests the possibility of digital transactions being carried out without intermediation. These currencies have so far been the focus of attention for their role as financial investments and currencies, but this paper argues that more significant than these considerations is the role that these currencies can play in the process of development and poverty alleviation. It is precisely in developing countries that the costs of intermediation are highest, and where the intermediation institutions are the most corrupt and least accountable. This paper attempted a preliminary brainstorming about the possibilities that these currencies could open in the developing world.

References

Acemoglu, D., Johnson, S., and Robinson, J.A. 2001. "The Colonial Origins of Comparative Development: An Empirical Investigation", *American Economic Review*, 91(5):1369-1401.

Aker, Jenny and Isaac Mbiti. 2010. "Mobile Phones and Economic Development in Africa". *Journal of Economic Perspectives*, 24(3):207-232.

Bernanke, Ben S. 2002. "Deflation: Making Sure "It" Doesn't Happen Here". Remarks before the National Economics Club, Washington, D.C. Accessed on federalreserve.gov in September 2014.

Caffyn, Grace. 2014. "Bitcoin Pizza Day: Celebrating the Pizzas Bought for 10,000 BTC". CoinDesk.com. May 22.

Cawrey, Daniel. 2014. "How Economist Milton Friedman Predicted Bitcoin". CoinDesk.com. March 15.

Engerman, Stanley L. and Kenneth L. Sokoloff. 1997. "Factor Endowments, Institutions, and Differential Growth Paths among New World Economies," in Stephen Haber ed. *How Latin America Fell Behind*, Stanford, CA: Stanford University Press.

Easterly, William. 2002. "The Cartel of Good Intentions: Bureaucracy versus markets in foreign aid." Center for Global Development Working Paper 4. March.

Ferguson, Adam. 1782. *An Essay on the History of Civil Society*. London: T. Cadell

Graf, Konrad. 2013. "On the origins of Bitcoin: stages of monetary evolution" konradsgraf.com

Hayek, FA. 1945. "The Use of Knowledge in Society." *American Economic Review*. XXXV, No. 4. pp. 519-30. American Economic Association. 1945

Hirschmann, Albert. 1970. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States.* Massachusetts: Harvard University Press.

Hosking, Patrick and Suzy Jagger. 2009. "'Wake up, gentlemen', world's top bankers warned by former Fed chairman Volcker." Timesonline.co.uk. December 9, 2009.

Mangu-Ward, Katherine. 2007. “Wikipedia and Beyond”. *Reason.* June 2007.

Menger, Carl. 1892 [2009] *On The Origins of Money*. Auburn, AL: Ludwig von Mises Institute, 2009.

McConnel, Campbell, Stanley Brue, and Sean Flynn. 2009. *Economics*. New York, NY: McGraw-Hill.

Mises, Ludwig von. 1949 [1996]. *Human Action: A Treatise on Economics.* 4th Edition. California: Foundation for Economic Education.

Nakamoto, Satoshi. 2008. *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin.org/Bitcoin.pdf

The Nilson Report. Issue 1,023. August 2013. Available from: NilsonReport.com.

Reinhart, Carmen and Kenneth Rogoff. 2009. *This Time Is Different*. New Jersey: Princeton University Press.

Rothbard, Murray. 1976 [1997] “The Austrian Theory of Money” In *The Logic of Action One: Method, Money, and the Austrian School*. Pp.297-320. Cheltenham, UK: Edward Elgar

Rushe, Dominic. 2014. “Janet Yellen: Federal Reserve has no authority to regulate Bitcoin” theguardian.co.uk. 27 February.

Szabo, Nicholas. ‘Formalizing and Securing Relationships on Public Networks’. *First Monday*. Volume 2, Number 9 - 1 September 1997.

Wallace, Benjamin, 2011, “The Rise and Fall of Bitcoin,” Wired, November 23, 2011.

The World Bank Payments System Development Group. 2013. *Remittance Prices Worldwide.* Issue 8, December.