Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation, and International Development

Saifedean Ammous*
Lebanese American University

Abstract
Bitcoin is the first technology for the final transfer of digital goods online, facilitating instant global payments without intermediation. Bitcoin's operation is based on a distributed, decentralized, and transparent asset ledger that acts as an ongoing chain record of all transactions. The system issues coins to reward those who contribute processing power to the network's operation. The possibilities created by this innovation are significant for the world's poor, who could skip traditional political and financial institutions and move to digital currencies in the same way they have gone straight to using mobile phones and skipped landline telephones.

JEL Codes: F30, O31
Keywords: bitcoin, innovation, finance, development

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 with 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

* I thank Edmund Phelps, Ryan X. Charles, David Al-Achkar, Lynn Chouman, Amy Fontinelle, and an anonymous referee for helpful comments, as well as participants in the Center for Capitalism and Society at Columbia University's seminar series, and the New York University Colloquium on Market Institutions and Economic Processes. A Seed Fund grant from the Lebanese American University facilitated my research on this topic.

have benefited 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 exist, yet there remains one field where business continues as it has for decades: finance and banking.

As 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 twenty-five years is the automated teller machine (ATM),[1] adding: "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 much since the ATM allowed withdrawals outside of bank branch locations and bank operating hours. Transferring money continues to cost significant amounts of money and time for the majority of people. The most common method for nonpersonal payment today is still the credit card, which was invented in 1950, back when the vinyl record was the most prevalent method of listening to music recordings.[2] Since 1950, vinyl records have evolved to tape cartridges, four-tracks, compact cassettes, compact discs, and finally mass storage digital music players, while credit cards are still in use today, featuring glaring problems. Most notably, credit card 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.

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 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

[1] The ATM was actually invented in 1969.

[2] BBC, "Credit Card," *A History of the World*, n.d.

intermediation to prevent double spending—that is, to ensure that the payer has the funds and is 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.

But this changed in 2008, when a pseudonymously published nine-page paper laid out 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 economic development. Section 2 explains Bitcoin functionally, in terms of the technologies that constitute it, outlining four main functions: transfer of digital goods, the blockchain, the currency, and smart contracts. Section 3 outlines the main strengths and advantages of Bitcoin, while section 4 discusses other digital currencies and their importance and chances of success. This paper discusses bitcoin in particular, since bitcoin is by far the largest and most important digital currency, but the paper's main thrust concerns the actual technology of digital currencies. Section 5 provides a preliminary brainstorming of the impact that digital currencies can have on developing countries and on the world's poorest people, illustrating ways in which it can help the impoverished 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 extremely fast and cheap. Transactions appear for the recipient immediately and can be sent for free; the average transaction confirmation time for the period from January 2012 through June 2015 was 8.32 minutes, while the average transaction fee was 0.000412 bitcoin, or $0.0753.[3] This paper takes 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 limited-supply currency, and a technology for implementing "smart contracts." This section explains the basics of all four technologies.

A. Transfer of Digital "Goods"

The groundbreaking innovation of Bitcoin is that it is the first technology for transferring 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 is a method of copying, 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 nonrival 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 her PC, she 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 song's seller to ensure that it can be accessed by only one PC. Should the owner of that PC choose to transfer the song's key to someone else, she would immediately lose access to the song.

Through the use of cryptography, Bitcoin brings the scarcity, rivalry, 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 that 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, currency. Before Bitcoin, any form of direct payment between two parties was unworkable, because there was no way to guarantee that the payer

[3] Author's calculation based on data from blockchain.info. US dollar transaction fee calculated using closing price on day of transaction.

would reduce the currency balance in his account, or not use his balance for more than one payment. Any form of payment had to rely on a trusted third party that maintained a balance for the payer and payee and that checked the transaction against the payer's balance to ensure the balance was sufficient. The third party then debited the payer's account while crediting the payee's account. 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.[4] 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 space limitations; 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.

[4] 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).

B. 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. The essential function of the Bitcoin protocol can best be understood as the verification of the blockchain.

New transactions continue to be written into new blocks, which are added to the previous blocks, forming the blockchain: a common, transparent, global, and openly accessible asset ledger. The use of expended CPU power as verification protects the blockchain from manipulation by network members. The more members verify a transaction, the more CPU power has been expended on it. The definitive and accurate record of transactions is the one on which the most CPU power has been expended to verify transactions. Should a member of the network attempt to falsify the common record, she would need to marshal more than 50 percent of the network's total processing power to validate her forgery. Without the majority of processing power, the network would simply discard the transaction. This process ensures that 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 bitcoin mining, as it is the only way in which new bitcoins come into circulation.

The blockchain can be likened to a conspicuous board in the center of a town square that acts as the town's monetary medium, 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 buyer's account and crediting the seller's account, 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 it needs the CPU power of more than 50 percent of the total network to register a transaction. In July 2015, the size of the blockchain was more than 36 gigabytes.

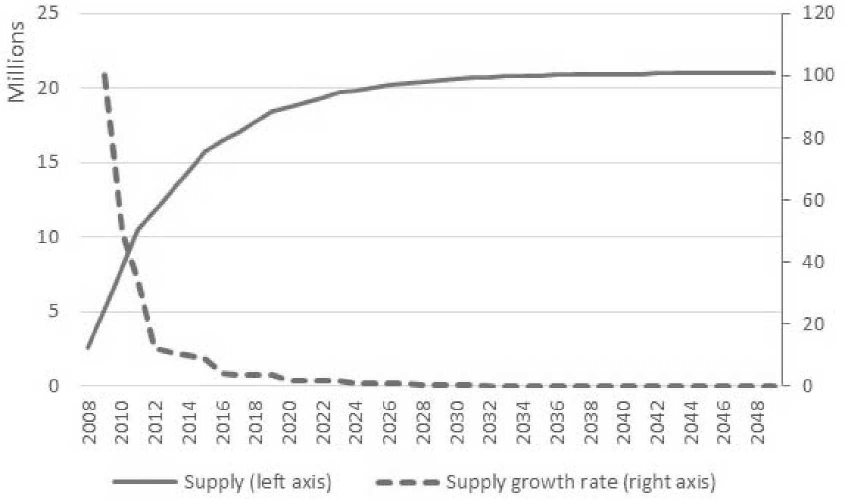
The blockchain obviates the need for a single third party to clear transactions, because honest transactions are inscribed on it and are globally viewed and accessible. There is no single individual or institution that is necessary for the transaction to take place. And this record of transactions itself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

C. 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 accounting 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 to 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 "seigniorage" 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 currency's inception, each new block contained fifty 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 twenty-five 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 the bitcoin supply will grow at a steadily decreasing rate, asymptotically approaching 21 million bitcoins. By July 2015, more than 14.3 million bitcoins (68 percent of the total supply) had already been mined into circulation, leaving fewer than 7 million to be mined over the coming decades. Figure 1 shows 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



Source: Author's calculations based on bitcoin algorithm generation frequency.

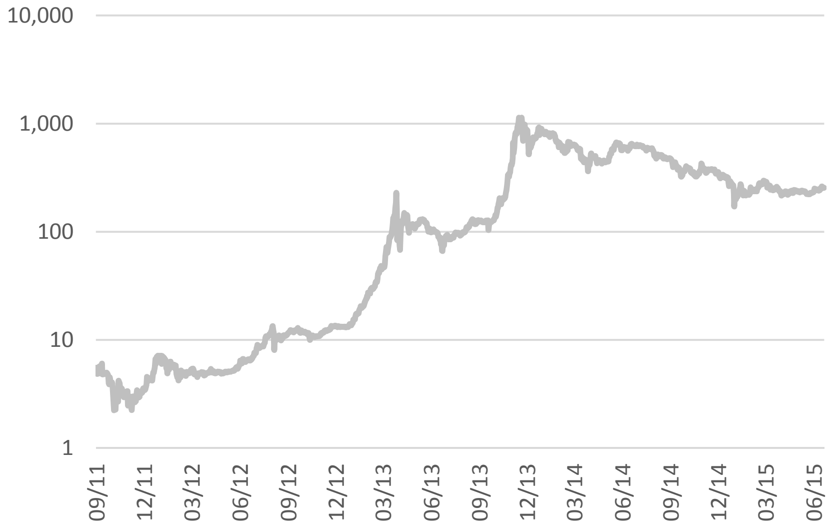
The bigger the network and the higher the number of transactions, the more mathematical work needs to be done to verify transactions, and the more CPU power users need to earn bitcoin rewards. As the network grows and currency adoption increases, bitcoin's real-world purchasing power also increases, thus ensuring that the block-mining reward, while 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 Bitcoin's design: if the network grows, the rise in the currency's purchasing power ensures that the reward to the computers that run the network increases, 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 bitcoin as a currency with no central bank, where a distributed mathematical set of rules controls the traditional tasks of the central bank.

With bitcoin, currency issuance is not handled by a central bank and human discretion, but according to the preprogrammed 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. The intermediation of payments is also not handled by a central bank, but by the collective effort of network members, who expend computer processing power on this task. The seigniorage from the currency's issuance 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 seigniorage from currency issuance to reward the expenditure of CPU power on validating transactions, or generating the blockchain. In other words, new coins are given 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 power on validating transactions, and the larger the incentive to expend CPU power on maintaining the network, ensuring it continues to run smoothly as transaction volume increases. There is also a minimal per-transaction reward for CPU expenditure transaction verification. For most of Bitcoin's existence, most transactions would be processed by miners, even with no transaction fees, as miners would be rewarded enough from mining fees. A minimal transaction fee is usually applied to transactions to get miners to process them quickly. If transaction volumes were to rise significantly, the transaction fee would increase. On the other hand, if the cost of computing power were to drop, making it cheaper for miners to process transactions, transaction costs would go down.

The Bitcoin network grows as fast as bitcoin adoption rises, or, in other words, as fast as the bitcoin economy grows. The money supply, however, only rises at a predetermined rate, which is roughly halving every four years, as the block reward declines. Though the supply of the currency is increasing, and will continue to do so indefinitely, the currency's real purchasing power has increased drastically in the six years it has been circulating. The increase in adoption explains the rise in bitcoin's purchasing power since circulation started in 2009. The first recorded exchange rate of bitcoins for fiat currency was 1,309.30 BTC for 1.00 USD, offered in October 2009 (Wallace 2011). By July 2015, the exchange rate had risen to fluctuate around 0.004 BTC for 1.00 USD, reflecting roughly a 330,000-fold (or 33 million percent) increase in the price of a bitcoin in US dollars in six years. The strictly limited amount of currency available means that the more Bitcoin technology catches on, the more bitcoin's purchasing power rises. It is this rise in bitcoin's value that provides a strong incentive to maintain 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)



Source: Data from bitstamp exchange, downloaded from bitcoincharts.com, July 4, 2015.

Bitcoin as a currency started off highly inflationary, but it is now moderately inflationary, with the supply growing at 209.13 percent in 2010, 59.41 percent in 2011, 32.67 percent in 2012, 14.94 percent in 2013, and 12.06 percent in 2014.[5] It is expected to grow at around 10 percent in 2015 and 9 percent in 2016. The growth rate will decline to around 4.5 percent in 2017, 1.7 percent in 2021, and 0.8 percent in 2025, then continue to drop further, becoming increasingly negligible.

[5] Author's calculation based on data from blockchain.info. Actual supply numbers differ slightly from theoretical numbers calculated in figure 1 as block issuance does not happen exactly every ten minutes.

It is instructive to compare the growth in the stock of bitcoins to the growth rate of the money supply of other major currencies. Table 1 shows the average, standard deviation, and the minimum and maximum annual growth rates of the broadest measures of the money supply for the major fiat currencies and for gold from 1984 through 2013. As it stands, these currencies' broadest available measures (the US dollar's M2, the Japanese yen's M3, the Swiss franc's M3, the 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 is so far. As bitcoin's supply is programmed to grow at a continuously decreasing rate, it should start growing at a slower rate than the historical average for all these currencies within the next decade or so.

Table 1. Average Growth Rate of Monetary Supply, 1984–2013

	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

Source: Author's calculations based on money supply data from the website of the St. Louis Federal Reserve bank. Gold data obtained from the World Gold Council website.

Gold has been the most marketable and liquid commodity on the market across time and space. This liquidity is due primarily to its 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 dwarfs the new annual production of gold every year, which is miniscule since gold is exceedingly rare and cannot be synthesized. These properties make gold the least inflatable commodity on the market, with an annual growth rate averaging 1.71 percent per year over the past 30 years and a standard deviation of only 0.15 percent. No other commodity comes close, since other commodities are perishable, consumable, and less rare. Hence, new annual production is always high compared to existing stockpiles. Should any other commodity or asset be used as a medium of exchange, its producers can easily and rapidly inflate its supply 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 gold has survived as a medium of exchange and store of value throughout time and across civilizations.

Gold will most likely continue to have a lower inflation rate than bitcoin for the next decade or so, 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. By 2025, bitcoin's growth rate will most likely be consistently and reliably the lowest among the world's major currencies and media of exchange.

The strictly limited supply of bitcoins 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 a 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 an economy of any size, since it is only the purchasing power of money in terms of real goods and services that matters, and not its numerical quantity. As Ludwig von Mises put it (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 (1976) emphasizes Mises's point: "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 economic growth 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 the Austrian theory of money, the limit on the supply of bitcoins is not an impediment to the currency's growth or adoption. If more individuals adopt the currency, 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 while ensuring that the rewards for miners increase in real value 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 gravitate toward 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 currency that appreciates in value incentivizes saving, as savings gain purchasing power over time. Hence, it encourages deferred consumption, resulting in lower time preferences. A currency that depreciates in value, on the other hand, leaves citizens constantly searching for returns to beat inflation, returns that must come with a risk, and so leads to an increase in investment in risky projects and an increased risk tolerance among investors, leading to increased losses.

Further, an economy with an appreciating currency would witness investment only in projects that 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 Mises (1949, p. 575) 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."

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 despite 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 is highly negative, as table 2 shows, averaging a negative 24.5 percent depreciation rate in the four years for which data are available.

Table 2. Bitcoin Depreciation Rate in USD

Date	BTC/USD	Depreciation rate
Dec. 31, 2010	3.3300	
Dec. 31, 2011	0.2118	–93.65
Dec. 31, 2012	0.0740	–65.05
Dec. 31, 2013	0.0012	–98.32
Dec. 31, 2014	0.0032	159.08

Source: Author's calculations using data from bitcoincharts.com.

If one were to perform the reverse experiment and analyze the performance of the US dollar from the perspective of the bitcoin economy, it would appear as a hyperdepreciating currency, depreciating at an average annual rate of 1,866 percent over the past four years, as table 3 shows.

Table 3. USD Depreciation Rate in Bitcoin

Date	USD/BTC	Depreciation rate
Dec. 31, 2010	0.30	—
Dec. 31, 2011	4.72	1,474.00
Dec. 31, 2012	13.51	186.11
Dec. 31, 2013	806.00	5,865.95
Dec. 31, 2014	311.10	–61.40

Source: Author's calculations on data from bitcoincharts.com.

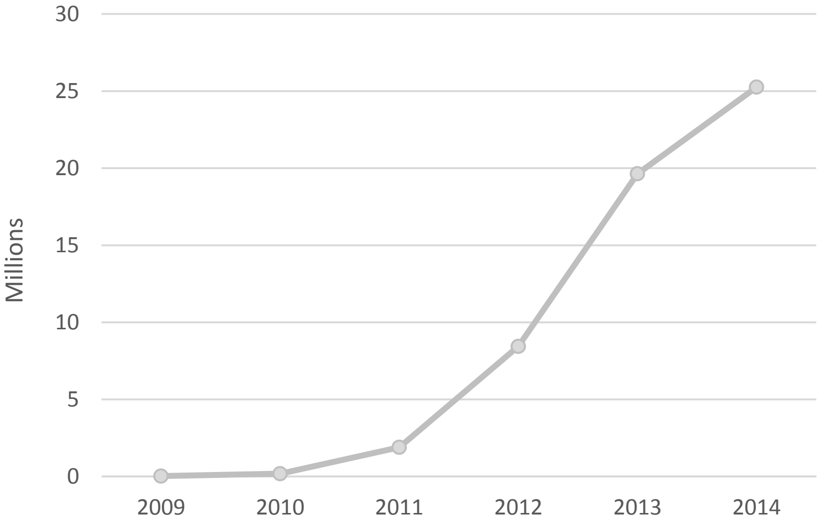
During this period, the number of transactions on the network has grown rapidly: whereas 32,687 transactions were carried out in 2009 (at a rate of 90 transactions per day), the number grew to 25,257,833 transaction in 2014 (at a rate of 69,199 transactions per day). The cumulative number of transactions reached 75 million transactions in July 2015. Table 4 and figure 3 show the annual growth.

Table 4. Total Annual Bitcoin Transactions

Year	Bitcoin transactions
2009	32,687
2010	185,212
2011	1,900,652
2012	8,447,785
2013	19,638,728
2014	25,257,833
1st half of 2015	18,491,721

Source: Author's calculations based on data from Blockchain.info.

Figure 3. Total Annual Bitcoin Transactions



Source: Author's calculations based on data from Blockchain.info.

The growth of the Bitcoin network so far, and the rapidly increasing number of transactions, in spite of the sharp rise in the purchasing power of bitcoins, lends credence to the Austrian view that a rise in the purchasing power of money is not harmful, and is, in fact, desirable. There seems to be no evidence so far to support the contention that a rise in the purchasing power of this currency would stall its growth, or the growth of the economy using it. As the value of bitcoins 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, 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 millibitcoins (1/1000 of a bitcoin). The bitcoin unit can be further divided into smaller units, all the way down to a satoshi, which is defined as 1/100,000,000th 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 that is becoming increasingly trivial in the age of computers, where prices can be quoted in any other currency or in gold, while transactions are settled in bitcoin at the spot rate.

D. 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 publicly accessible or encrypted, offering many potential applications that users have only just begun to explore. As a publicly accessible, transparent, and open ledger, the blockchain can be transcribed with what computer programmer and cryptographer Nick Szabo (1997) calls "smart contracts"—contracts transcribed in actionable computer code that makes them self-enforcing or self-executing, obviating the need for third-party enforcement. Such software can transparently and accurately assess compliance with contract terms, and based on it, carry out financial transactions in bitcoins, 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 in their real-world execution 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 nonexistent. Instead, all contracts currently must rely on a third party to oversee and enforce compliance with their terms. Such third parties include lawyers, police, judiciary, government agencies, and private corporations.

The blockchain introduces a new possibility for contracts: placing the contract transparently on the blockchain ensures 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 percent 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 and mutual consent, without the need for trust or enforcement. Strangers can enter binding agreements, trades, and employment contracts with one another knowing that the tamper-proof blockchain can reliably enforce the terms of the contract. The blockchain 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 six years, Bitcoin has gone from being a computer program installed on two computers sending digital coins with no real purchasing power to a global algorithm commanding the world's largest computer network, with the digital currency supply exceeding $3 billion in market value and being accepted by tens of thousands of merchants worldwide. All of this was achieved through the voluntary cooperation of networks the world over.

During this time, not a single attack or threat has succeeded in destroying the network. Five main aspects of Bitcoin's design make it appealing to users and resilient to attack: 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 voluntary participation.

A. Eliminating the Need for Trusted Third Parties

One of Bitcoin's most appealing features is that it 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 any one of the many computers in the network verifies the transaction. There is no need to trust any single individual or institution to carry out this transfer; miners compete among themselves to verify it, because verifying blocks of transactions means receiving 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 nothing from doing so. The network is designed to offer significant rewards to anyone who is willing to verify transactions honestly, eliminating 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; a credit card company; 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.

B. Payer-Initiated Payment

Bitcoin payments are initiated by the payer, and they 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 and require the recipient to be privy to important information that can be easily compromised.

A credit card transaction requires the payer to give the recipient their credit card information to enter it into a credit card processing terminal. This creates a major security problem. Many merchants maintain records of their customers' credit card information, which can be compromised later. By having the payment initiated by the recipient and dependent on the recipient obtaining sensitive information from the payer, credit card transactions are rife with fraud problems. In 2012, credit and debit card fraud accounted for approximately 0.522 percent of all credit card transactions worldwide, which cost payment card issuers, merchants, and banks $11.27 billion (Nilson Report 2013).

With bitcoin, the recipient only receives the payment itself and the payer's address, 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 merchants and third parties. For merchants, the finality of bitcoin transactions offers the advantage of not having to worry about potential chargebacks and payments that are canceled after the goods have been delivered.

C. Processing Power

As a result of the lucrative rewards for maintaining it, the bitcoin network has grown into the world's largest supercomputer by far. In July 2015, the processing power dedicated to bitcoin was estimated at around 4,533,399.51 petaflops, where a petaflop denotes a computer's ability to perform one quadrillion floating point operations per second.[6] 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. 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 more than 16,600 times larger than the processing power of the world's top 500 supercomputers combined. This system is perfectly incentive-compatible to ensure the network's continued

[6] Source: Bitcoincharts.com.

smooth operation: as more people demand bitcoins for financial transactions, the purchasing power of bitcoins increases, which increases the real value of the reward for expending processing power on validating transactions, ensuring that people dedicate more processing power to run the network.

D. No Single Point of Failure

The lack of a centralized authority to issue bitcoins and monitor transactions is another of Bitcoin's chief strengths. Not having a central server that processes all transactions means that the system has no single point of failure, making it extremely resilient, if not impervious, to attack or technical failure. A physical or digital attack that destroys any individual computer 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. An attack might hurt the individual owners of the targeted computers, but it 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 anywhere in the world can continue to communicate with one another, the blockchain can survive as a record of all transactions and coin ownership.

Bitcoin embodies Friedrich Hayek's (1945) concept of distributed knowledge and complex spontaneous order emerging from simple individual actions. Hayek's work was the inspiration behind Wikipedia (Mangu-Ward 2007), whose strength is that it does not rely on centralized authority, but on distributed knowledge. Distributed knowledge 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 network's distributed processing power ensures a far cheaper, faster, and more resilient method of payment than any technology reliant on a centralized intermediary. Further, the blockchain's simple algorithm, designed by an anonymous programmer, has evolved steadily over the past six years and been adapted to various other uses by individuals and groups. An entirely new ecosystem has emerged from it and will likely continue to evolve. No single mind could have overseen the complexity of this ecosystem, which is, as Adam Ferguson (1782) would put it, "the product of human action, not human design."

E. Voluntary Participation

The existence and operation of the Bitcoin network are entirely consensual: everyone who has traded bitcoins for goods, services, or other currencies, and everyone who has dedicated hardware processing power toward maintaining the network, has done so freely. Anyone who does not like the idea, for whatever reason, can completely isolate themselves from it and suffer no adverse consequences. Anyone who uses bitcoin accepts the associated risks. In contrast, the legacy fiat currencies and mainstream financial system expose users to risks they did not consent to. 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 with bitcoin. Good algorithm design combined with the transparency of open-source software and the 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 the Fed cannot regulate bitcoin: "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 any way" (Rushe 2014).

While several central banks have issued warnings to their citizens about the risks of Bitcoin, practically nothing can be done to stop or ban its use. Anyone with an Internet connection can access any of the many sites or services that utilize bitcoins. The only way governments can stop bitcoin adoption is by banning regulated financial institutions from using it, but whether financial institutions use bitcoin is largely immaterial to bitcoin, which essentially eliminates intermediation and replaces most functions 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 postal service's operation, but it is unlikely to cause any serious problems for the technology of email. In June 2015, New York state issued its BitLicense rules for digital currency companies, but these rules will not affect the Bitcoin network itself, only New York-based institutions dealing with bitcoins. Should the rules prove too onerous to businesses that use bitcoin, they will be unlikely to hurt bitcoin in the long run and will simply shift bitcoin activity outside of New York.

At its heart, Bitcoin is a program running and verifying mathematical operations perfectly transparently. The notion of governmental regulation of mathematical operations is meaningless; 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 political regulation dictates.

It thus seems that Bitcoin is extremely resilient to attack, whether by vandals, hackers, or government agencies. Bitcoin might even be termed antifragile 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. Countless hacking attempts have failed, but many of them have exposed weaknesses in the code and forced the network's operators 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 network's growth.

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 Bitcoin's inception. They copy Bitcoin's 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 early adopters. Peercoin is also programmed to continue to increase in supply at a rate of 1 percent 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 capitalization 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 are far greater than those of 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, bitcoin's market capitalization is 55.81 times that of the ten next-largest altcoins combined.[7] A large infrastructure of services, such as exchanges, online wallets, and merchant facilitators, has developed around bitcoin, and not around the other coins.

Second, 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 that 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 processing power behind Bitcoin, which is far larger than that of any other digital currency, making it far more resilient to attacks than altcoins.

These three reasons make it likely that bitcoin will remain the leading digital currency for the foreseeable future, though the opposite conclusion, that another currency will supplant bitcoin as the leading digital currency, cannot be discounted. Altcoins will continue to be the testing ground for innovations in digital currency technology, 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 innovation built on the bitcoin network itself, with various types of currencies and financial instruments layered on top of the bitcoin blockchain.

Whether the current bitcoin network is usurped by another digital currency with superior features, or it fails 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 that allow for financial transfers without

[7] Author's calculations based on data obtained July 4, 2015, from Cryptocoinrank.com.

trusted third-party intermediation. This technology cannot be uninvented, and it can find more and wider applications across various economic, legal, technical, and political avenues. It is this technology, more than bitcoin itself, that 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 went out of business in 2013.

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 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 have a qualitatively different, and potentially more transformative, effect on underdeveloped countries.

The world's poorest people live in countries with limited financial services, unaccountable governments, quickly 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 through 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 toward predation rather than production.

Bitcoin may provide populations living under predatory institutions with what Albert Hirschmann (1970) terms "exit": the ability 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 harms the elites. This can have a twofold impact: it can allow these populations to deal with productive private property institutions, and it can threaten the elites 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 payments are virtual.

Bitcoin offers the most promise to the billions of people who 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 related fees cannot cover the costs of intermediation. Further, in developing countries where political instability is higher, financial institutions face operating difficulties that reduce their services and reach. The developing world is well behind the developed world in terms of financial development, and it requires extensive investment in infrastructure, education, training, and capital accumulation to catch up. 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. Bitcoin's influence in developing countries could be similar to that of cell phones. Many developing countries also have underdeveloped telecommunication networks and minimal telephone penetration, but the invention of the mobile phone 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 could have.

A. Remittances

The market most ripe for disruption by digital currency is that of international remittances. The World Bank estimates global remittances in 2013 at $400 billion. At the end of 2013, the average cost of remittances was 8.58 percent of the amount of money transferred, with bank transfers costing an average of 12.33 percent, money-transfer operators charging 7.01 percent, and post office transfers costing 4.12 percent (World Bank 2013). By contrast, bitcoin transactions have cost $0.0753 on average from January 2012 through June 2015.

Sub-Saharan Africa has the highest average cost of remittances, at 12.55 percent of remittance value (World Bank 2013). 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 at low cost and very fast. The problem with this method is that bitcoin has not been 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 their actual 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,[8] which, as of mid-2015, charges only 3 percent and guarantees same-day delivery. BitPesa receives bitcoins from expats all over the world and pays out their equivalent in local currency to Kenyans, in cash and in person, via a domestic bank transfer or through the Kenyan mobile payment system M-Pesa.

If bitcoin adoption continues to grow, it will likely benefit services like BitPesa in the medium run, as more expats might be willing to buy bitcoin and send it to BitPesa. In the long run, however, bitcoin growth would likely undercut services like BitPesa

[8] See Bitpesa.co.

by making it easier for individuals to transfer bitcoin directly to each other at bitcoin's very low fees.

B. Microfinance

In the area of microfinance, transaction costs have the highest toll on the poor. Eliminating these costs would open 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. Such transfers are not possible today, since making the loan and each repayment would involve a transaction fee nearly as large 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 dozens of dollars, as they do today. But if the transaction cost is eliminated, or drastically reduced to the range for bitcoin transaction so far, 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 far lower than what borrowers in poor countries could get from local loan sharks or financial institutions. Given the prevalent and persistently low interest rates on deposits in developed economies, the opportunity cost of lending internationally is very low, and so 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 could receive their own payments in bitcoin, making accounting completely transparent and repayment automatic. This reduction in information asymmetry would reduce the risk associated with lending, as well as the transaction costs. At the margin, financing would likely shift from lending to direct equity investment that shares in profits and losses.

C. Development Aid

NYU economist William Easterly (2002) has written extensively about the incentive problems faced by the foreign and development aid industry. 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 noncompetitive 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 (2002, p. 53) proposes the idea of "aid markets," whereby donors can give recipients aid vouchers directly, and these recipients can then choose to spend their vouchers with the agencies that provide them with the services they want. While highly original and promising, Easterly's proposal has not been enacted, nor does it seem likely that it will be, due primarily to the large transaction costs and knowledge problems involved with distributing the vouchers and setting up voucher funds. As well, there is 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. Development agencies would then have to compete to get their funding from the recipients, and donors could track 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. The transaction costs in the current banking system make such transfers cost prohibitive. The reduction of transaction costs for international transfers could have an effect on development aid similar to that on microfinance. Peer-to-peer donations can reduce overhead and waste significantly.

One particularly promising application of peer-to-peer donations is in the case of natural disasters, which can severely damage an area's financial infrastructure, posing severe challenges to the mobilization of resources for relief efforts. Digital currencies can transform disaster relief by getting donations from around the globe to stricken areas immediately, when they are most needed. Resources and relief efforts can be mobilized far faster when those afflicted by a disaster have the 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.

D. 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 little cost. But payment remains complicated, especially in developing countries. Merchants in poor countries find it prohibitively difficult to access payment recipient solutions at financial institutions that 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 in a global marketplace and to compete purely on the quality of their goods, rather than their access to finance.

E. Capital Accumulation

The limited supply of bitcoin 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 and Rogoff 2009). The rapid rise in the value of bitcoins over the past six 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 for governments 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. This pressure could theoretically lead to a hyperinflationary collapse, or the threat of exit to bitcoin could force governments to act with more monetary responsibility in handling their currencies.

The world's poorest are usually citizens of countries that continuously experience currency devaluation. As discussed previously, the main advantage of a noninflationary currency is that it facilitates capital accumulation and leads to lower time preferences. 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, without having to wait for their central banks to achieve monetary competence. More capital accumulation leads to lower costs of production, lower prices, and increases in labor productivity. The use of sound money is indispensable for sustainable, long-term economic growth, and bitcoin could offer an internationally available online option for people to use money that cannot be easily inflated.

While bitcoin is still in its infancy, the currency's resilience suggests that its survival will challenge the very concept of government monopoly on money issuance. Bitcoin has so far survived for more than six years, during which it continued to perform flawlessly its core function of unintermediated payments while the supply increased largely according to its preset algorithm. Lindy's effect posits that the longer an idea has survived, the longer it is likely to survive into the future, and this effect suggests bitcoin's continued existence, reliably recording transactions while the currency supply increases predictably.

Meanwhile, government-issued currencies will likely face inflationary and deflationary shocks, bank runs, and panics, as they always have. The longer bitcoin survives, its iron-clad predictability is likely to make it more appealing an alternative to government-issued money. As awareness and knowledge of bitcoin spread, and as the technical knowledge needed to operate it becomes more rudimentary, it will become easier for people to switch from government currencies to bitcoin. From a game-theoretic perspective, the current coexistence of bitcoin and government currencies is an unstable equilibrium: the longer bitcoin exists, the more likely it is to continue, and the more attractive it becomes compared to traditional currencies. The two possible long-run stable equilibria for this game are (1) bitcoin no longer exists, or (2) bitcoin exists and other currencies are tied to bitcoin.

F. International Supralegal 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 agreements between strangers, offering citizens of developing countries a framework for transactions independent of the domestic judicial and executive branches. Further, the blockchain can act as a global reputation mechanism for its users, incentivizing them to abide by their contracts in order to gain a reputation of trustworthiness. Instead of relying on third parties to enforce contracts and to establish whether certain parties are worthy of contracts, blockchain technology can let every individual and organization develop its own reputation and brand online, with complete transparency.

VI. Conclusion

The institutional, governmental, and technological problems of developing countries create a formidable barrier for most of 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. Bitcoin could be life-changing to those individuals and could also offer credible competition to national monopolies in financial services, currency issuance, judicial systems, and credit provision.

Cryptographically secured, decentralized, distributed digital currency 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 explores role that these currencies can play in economic development and poverty alleviation. It is in developing countries that the costs of financial intermediation are highest and where the intermediation institutions are the most corrupt and least accountable. This paper attempts a preliminary brainstorming about the possibilities that digital currencies could open in the developing world.

Of the six possible applications for digital currencies in the context of development discussed here, the role of bitcoin as a limited-supply currency and store of value is perhaps the most significant. It might not be quick or easy for people in developing countries to develop the technical competence for wide and mass adoption of bitcoin for international trade, microfinance, remittances, and smart contracts, but even without mass adoption, the existence of a noninflationary alternative to modern fiat currencies and government-backed bank accounts presents a formidable challenge to government-issued money. In relatively small economies, even if a small number of currency holders were to switch some of their holdings to bitcoin, this switch could generate significant selling pressure on the currency.

References

Acemoglu, D., S. Johnson, and J. A. Robinson. 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): 207–32.

Bernanke, Ben S. 2002. "Deflation: Making Sure 'It' Doesn't Happen Here." Remarks before the National Economics Club, Washington, DC.

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.

Easterly, William. 2002. "The Cartel of Good Intentions: Bureaucracy versus Markets in Foreign Aid." Center for Global Development Working Paper 4, March.

Engerman, Stanley L., and Kenneth L. Sokoloff. 1997. "Factor Endowments, Institutions, and Differential Growth Paths among New World Economies." In *How Latin America Fell Behind*, ed. Stephen Haber, 260–304. Stanford, CA: Stanford University Press.

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

Hayek, F. A. 1945. "The Use of Knowledge in Society." *American Economic Review*, 35(4): 519–30.

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

Hosking, Patrick, and Suzy Jagger. 2009. "'Wake Up, Gentlemen,' World's Top Bankers Warned by Former Fed Chairman Volcker." *The Times*, December 9.

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

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

Mises, Ludwig von. 1949[1996]. *Human Action: A Treatise on Economics*. Irvington-on-Hudson, NY: Foundation for Economic Education.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System."

Nilson Report. 2013. Issue 1,023, August.

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

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

Rushe, Dominic. 2014. "Janet Yellen: Federal Reserve Has No Authority to Regulate Bitcoin." *The Guardian*, February 27.

Szabo, Nicholas. 1997. "Formalizing and Securing Relationships on Public Networks." *First Monday*, 2(9).

Wallace, Benjamin. 2011. "The Rise and Fall of Bitcoin." *Wired*, November 23.

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