B.Sc. Essay in Business

Cryptocurrency and Bitcoin:
A possible foundation of future currency
why it has value, what is its history and its future outlook.

Sindri Leó Árnason

Leiðbeinandi: Guðrún Johnsen
Faculty of Business Administration
June 2015
Cryptocurrency and Bitcoin: A possible foundation of future currency

Why it has value, what is its history and its future outlook.

This is a bachelor’s of science essay that counts for 6 ECT credits in the School of Social Sciences, Faculty of Business Administration, at the University of Iceland

© 2015 Sindri Leó Árnason

Printing: Verslunarfélag Reykjavíkur

Reykjavík, 2015
Preface

This is a bachelor’s of science essay that counts for 6 ECT credits in the School of Social Sciences, Faculty of Business Administration, at the University of Iceland. I chose this topic because I had become interested in Bitcoin and cryptocurrencies in 2013-2014 when their media coverage boomed. I had already done some research on this topic beforehand and as I am studying finance at the University of Iceland I wanted to research what Bitcoin’s future impact on the business world could possibly be. I would like to thank Guðrún Johnsen who is a lecturer at the School of Social Sciences, who helped guide me through writing this essay and my father, Árni Leósson, who helped read over my essay, fixing spelling and grammar mistakes as well as helping me develop essential arguments.
Summary

The goal of this project was to find out what exactly cryptocurrency, such as Bitcoin, is and why it has value, what its future outlook is and if it could become the mainstream currency of the future. Bitcoin is a fully decentralized currency. It has value because its supply is limited and there is demand for its low transaction costs, anonymity, investment possibilities and possibilities for use in illegal activities. Its future outlook is questionable as Bitcoin has a few severe disadvantages such as high price volatility, susceptibility to hacking, no protection from a central bank and no consumer protection. It is therefore unlikely that it will catch on as an established currency to the general public, as its two main strengths, anonymity and low transaction costs are not necessarily what the average consumer demands. However the technology behind cryptocurrency and Bitcoin can be applied to other currency or payment systems which could have a lasting impact on how people spend money in the future.
Table of Contents

1. Introduction ........................................................................................................................................ 7
2. An introduction to cryptocurrency and Bitcoin .................................................................................. 8
3. Why do cryptocurrencies such as Bitcoin have value? .................................................................. 11
4. The vulnerabilities of Bitcoin ............................................................................................................. 15
5. Using Bitcoins in the corporate world .............................................................................................. 17
6. Regulating Bitcoin ............................................................................................................................. 19
7. Using Bitcoins as an investment ........................................................................................................ 20
8. The future of cryptocurrency ................................................................................................................ 22
9. Future innovations in currency payment systems .............................................................................. 23
10. Conclusion ......................................................................................................................................... 24

Sources .................................................................................................................................................. 26
Table of figures

Picture 1: Ancient Roman Coin, minted by Pinarius Natta (149 B.C.) (Colla, P. 2015)......... 7
Picture 2: Official Bitcoin logo (Bitcoin, 2015)........................................................................ 8
Picture 3: Bitcoin Price vs. USD from March 19th 2014 to March 19th 201............... 13
Picture 4: Bitcoin Price vs. USD from January 1st 2015 to 19th March 2015.................... 13
Picture 5: Shows the regulations on Bitcoin from a few different countries....................... 20
1. Introduction

Money is one of the most valuable and sought after commodities in the world. Most people interact with money in nearly every facet of their life, whether a person intends to go to the hairdresser, buy groceries or invest in a home, money is necessary in the modern economy for transactions for goods and services. Money has had many forms in human history with the oldest form of money being bartering. Without any official currency people would directly trade one good for another, such as trading a horse for a cow. This form of money however is very inefficient as the odds of finding someone that required a horse for the exact same good that the other person required are quite low. Clearly a medium of exchange needed to be developed. A medium of exchange acts as an intermediary instrument in order to make trading more efficient. During the time of bartering this would include some easily traded goods like weapons or animal skins. It was sometime around 600 B.C. that the first official currency was minted. (Beattie, A. 2015.)

Minted currency used to be made from a mixture of silver and gold which were stamped with a picture to denote the face value of the coin. These coins were minted by Lydia’s (in today’s Turkey) King Alyattes and it increased the countries trade significantly resulting in the empire becoming one of the richest in Asia Minor. Around 600 B.C. the Chinese started developing paper money and moving away from coins, however it took Europeans a much longer time to start using paper money. Eventually banks would make bank notes for people to carry around instead of coins which had their value backed up in silver or gold coins. (Beattie, A. 2015.) Little by little printed paper money, as we know it today, became the norm.

This way money eliminates the problems with bartering and acts as a stable medium of exchange. Pricing goods and services, and trading, becomes much easier and more convenient when everyone accepts the same money as currency. In today’s economy the main source of money is fiat money, a legal tender protected by a government using regulations and laws that create the much needed trust in money and thus creates its value. Fiat money is supplied by a countries central bank which maintains the stability and supply of currency through its monetary policy. With increasing technology and innovation new types of money have been invented. (Simpson, S. 2015)
One of the most controversial new innovations of money are Cryptocurrencies, a form of internet currency often called digital money or cyber currency. The most important feature of cryptocurrency is that it is not issued by a central bank, nor is it protected by regulations or law, making it impervious to government interference. The most widely known and controversial cryptocurrency is Bitcoin, which was launched in 2009. As Bitcoin is the most widely known and used cryptocurrency in the world, the subject matter of this paper will largely focus on Bitcoin. (Cryptocurrency, 2015) What is cryptocurrency and Bitcoin, why does it have value, what is its future outlook and could it become an established mainstream currency?

2. An introduction to cryptocurrency and Bitcoin

Innovations in money have made it possible to make transactions using private digital currency without any interference from any organizations such as a bank. These digital currencies use peer-to-peer networks and software with freely available source code to redistribute and modify the currency as users see fit.

“Bitcoin and similar digital currencies are called crypto-currencies by some because the underlying algorithms and security are intimately related to digital cryptographic algorithms.” (Dwyer, 2014)

Digital money is similar to the electronic storage of our regular debit card accounts however the real difference lies in how the currency can be transferred without any possibility of interference by banks or other intermediaries. The currency is thus fully decentralized, and unlike fiat money the government cannot affect the value of the currency. (Dwyer, 2014)

The first cryptocurrency created is Bitcoin. Bitcoin was created by a developer, or a team of developers, under the name of “Satoshi Nakamoto”. The currency uses SHA-256, a cryptographic system designed by the U.S. National Security Agency. (Graydon, C.) Bitcoin is currently the most widely used and known type of digital currency with a total value of $3.069 billion and over 13 million total Bitcoins in circulation. Every Bitcoin created has an association to a specific key or address which makes each Bitcoin unique. A Bitcoin transaction is when one Bitcoin moves from one address to another. A public database records every transaction.
or trade of Bitcoin. The database is called the “block chain”\(^1\). Each Bitcoin exists inside the database and thus no coins are held outside of it. The supply of cryptocurrency depends on “mining”. Each individual Bitcoin is added onto the database through this mining process. (Dwyer, 2014)

Mining cryptocurrency is done using a computer and it is scaled on hashes per second. Every time someone successfully solves a block and mines a coin, a new hash\(^2\) is created. Bitcoin exclusively relies on hash functions. Powerful mining computers are required to mine cryptocurrency effectively but the complexity of the algorithm means that the CPU will consume a lot of resources. (Dwyer, 2014) Over time, less and less Bitcoin will be supplied from mining, while the algorithm becomes more complex. The mining process will keep increasing in difficulty and as the data chunks become larger and processing it becomes more difficult, the resources used and cost will increase while the rewards diminish. The reward for mining used to be 50 Bitcoins per block while today it has been reduced to 25 per block. The supply of Bitcoins is fixed and the rewards have been programmed to halve every four years. Thus the mining process becomes less profitable as time goes on and the supply of Bitcoin slows down. (European Parliamentary Research Service, 2014) Unless an individual has a specifically designed mining computer, the cost of mining a hash is more than the price of the Bitcoin. Essentially, mining is a contest. Multiple miners are all working at the same time to find a hash. Computational problems that have been solved by miners are a certain “proof” that verifies that a certain miner has successfully mined a block. An eventual limit has been put on the total supply of Bitcoins. The announced limit is 21 million Bitcoins. During the process of mining the Bitcoin is added to the block chain. As such, any evidence of a person’s ownership of Bitcoins is stored entirely in the block chain, a database of Bitcoins in circulation. Owners of Bitcoins use digital “wallets” to keep track of their own balance and for transaction purposes. (Dwyer, 2014)

\(^1\) A public ledger „which acts as a digital financial record book with a record of all Bitcoin transactions in chronological order“. (European Parliamentary Research Service, 2014) The blockchain can be viewed by all computers in the network, but it does not contain any personal information about the people who conducted the transactions. Making the blockchain a public domain has the purpose of verifying transactions, eliminating the need for a third party. (European Parliamentary Research Service, 2014)

\(^2\) A hash function is simply computer data. They are large numbers and are used for Bitcoin generation. It is a mathematical equation and the hash rate means how many blocks (equations) are being solved per second. The difficulty of solving a hash comes from the fact that the number is restricted to be less than or equal to some value. (Dwyer, 2014)
The wallet can be likened to an excel spreadsheet which records and tracks a person’s balance. It does not contain the Bitcoins themselves. Bitcoins, as mentioned before, have an association to a certain “address”, a public key in Bitcoin transactions. This public key cryptography method encrypts and decrypts messages for verifying each transaction. Bitcoins are sent to each person’s public key and they are stored in the owner’s private key. Should an intruder, e.g. a computer hacker, gain access to someone’s private key, he can then send Bitcoins to his own public address using the private key, stealing the Bitcoins. The person will only know the public key and not the private key and will not be able to recover his Bitcoins. It is therefore essential to keep the private key encrypted and safe from intruders.
3. Why do cryptocurrencies such as Bitcoin have value?

One of the biggest problems with digital currency is that bits are very easy to create and reproduce on computers. For a currency to work in an economy it must be extremely hard to reproduce. Also, to have value a currency has to have some protection against multiple spending of the same coin – it has to move between owners when spent. Reproducing digital currency is much easier than with physical ones. A solution to this problem is having a trusted central authority that keeps records of transactions with the currency and also certifies each transaction. The largest cryptocurrency, Bitcoin, took another route to stopping this problem. (Dwyer, 2014)

Transaction with Bitcoin occurs strictly in peer-to-peer networks of people where no institution or central authority is certifying exchanges. A peer-to-peer network is a connection between two personal computers that can interact or transact with each other without connecting to a separate server computer. (Cope, J. 2002) As said before, Bitcoin also relies on open source software. Open source means that the programming code has little or no copyright restrictions, has been distributed digitally to anyone in the world and any person who so desires has the ability to edit the code. Open source is therefore similar to peer-to-peer networks as the development is done by the participants, such as programmers, and not a central figure. (Dwyer, 2014) Using this open-source method and peer-to-peer networks, Bitcoin has been able to use authentication measures to solve the reproduction problem. As mentioned before, all transactions with Bitcoin are recorded in a database called the block chain. Many websites keep copies of the block chain which they keep updated. Since Bitcoin has successfully countered the reproduction problem it is able to create value. However, a currency must also have a certain amount of demand to have value. (Dwyer, 2014)

One reason for using digital currency is how low the cost of money transfer is. Transferring money digitally requires no physical money to be transferred and is also instantaneous. It is also hard to prevent people from bringing their Bitcoin wallets into another country and trading cryptocurrency for local currency. Certain demand thus comes from the possibility of avoiding currency controls or government interference. The marginal benefit of such a transaction can be much higher than the marginal cost. Another reason for the demand of digital currency is anonymity. (Dwyer, 2014) Another possible source of demand for cryptocurrency is thus people who wish to participate in online black markets, using the anonymity of Bitcoin.
The Silk Road, an online anonymous marketplace, was one example of such black markets. The Silk Road used Bitcoin as its main exchange currency. The marketplace was used to sell governmentally controlled substances and illegal narcotics where transactions were hidden behind the anonymity of Bitcoin and shipped anywhere in the world. In a paper by Nicolas Christin the revenue made by all the sellers was estimated to be about $1.2 million a month. In the same paper, Christin, using a 29-day moving average to compute the statistic, found out that Silk Road transactions corresponded to about 4.5% to 9% of all Bitcoin exchanges. When this marketplace was taken down by the FBI, the price of Bitcoin immediately dropped. (Christin, 2015) This suggests that the appeal and demand for cryptocurrency comes from its anonymity and use in illegal transactions. Although Bitcoins are not inherently anonymous, owners can take steps to hide their transactions, especially through international Bitcoin exchanges such as Mt. Gox.

The Mt. Gox. Exchange, which was located in Tokyo, was the biggest international Bitcoin exchange. People all over the world traded Bitcoins on the exchange through computers. The exchange was order-driven which means that certain people would offer Bitcoins up for bid and the coins were traded through such market orders. With data collected by Mt. Gox and other exchanges, it is possible to look at the price history of Bitcoin on exchanges. (Dwyer, 2014)

The price of Bitcoin on exchanges has had a major increase. The first transaction on the Mt. Gox exchange was a transaction of 20 Bitcoins for the sum of $0,04951 and according to Bitcoincharts.com the price of a single Bitcoin as of today (19th February 2015) is $240,820. There has however been much controversy surrounding the price of Bitcoin. Historically the price has been very volatile and it tends to increase and decrease by a lot. On the 30th of November, 2013, the price high of Bitcoin was $1163 and on March 3rd, 2014, about 3 months later, the price had fallen to $586. (Dwyer, 2014)
Picture 3 – Bitcoin Price vs. USD from March 19th 2014 to March 19th 2015. Shows the extreme volatility in the price of Bitcoin as the price per Bitcoin falls from $511.50 on April 16th, 2014, to $479.98 on April 18th, only two days later. The price has continued this fluctuation throughout the year but is on a downward spiral. On March 19th 2015 the price of a single Bitcoin is $256.78 and at the same time last year, March 19th 2014, the price of a single Bitcoin was $609.00. (Quandl, 2015)

Picture 4 – Bitcoin Price vs. USD from January 1st 2015 to 19th March 2015. Bitcoin is still showing signs of volatility to start the year of 2015. The price increases and decreases regularly throughout these 2 and a half months. The price falls from $278 on January 10th, 2015 down to $176.50 on January 14th, 2015. (Quandl, 2015)

With this price volatility, as shown in pictures 3 and 4, it can be argued that the demand for Bitcoin comes from being a high risk investment rather than for use as a currency. Also, less than 1000 people own almost 50% of total Bitcoins in circulation. This could have a cartel

---

3 If few entities control the majority of the supply they can create an agreement between each other to regulate the supply and manipulate prices for bigger profits. This is especially dangerous with Bitcoins as it has no consumer protection making it very easy to manipulate the supply. The few people who own almost half the Bitcoins can act as a single producer, manipulating the price on the market. (Cartel, 2015)
effect on the pricing of Bitcoin, especially if the market experiences a shortage of Bitcoins. (European Parliamentary Research Service, 2014)

Cryptocurrencies such as Bitcoin thus have value in peer-to-peer networks to authenticate transactions and solve the problem of easy reproduction. Transferring money digitally is very cheap and instantaneous, it can be used to bypass government interference, and its price is very volatile which has captured the interest of some investors. Demand for the currency also comes from people wishing to spend money on black markets, utilizing the anonymity of Bitcoins.
4. The vulnerabilities of Bitcoin

The decentralized property of the Bitcoin network protects it from attacks. A decentralized system can protect itself better from an attack but it is not completely invulnerable. Some attacks on Bitcoin are still theoretically possible. (Massive Bitcoin thefts, 2013) Research has shown that Bitcoin miners have spent much more on electricity costs and specialized equipment than the overall worth of the Bitcoins they mined. This research showed that people had spent $17 million on mining while the rewards amounted up to $4.4 million. As mentioned before it becomes progressively harder to mine Bitcoins over time and it slowly becomes less profitable. Miners have tried to combat this by pooling their resource together, producing a synergy to increase computational power and share the bigger rewards. (European Parliamentary Research Service, 2014) In theory, by pooling together resources like this an entity with enough computing power could control the majority of the mining (over 50% of hash rate mining by one entity) and in doing so take control of the network and then have the ability to manipulate the block chain, this is called a 51% attack. This would make it possible to reverse transactions and spend the same Bitcoins multiple times (otherwise known as the double-spending problem). This problem however has been mitigated by the developers of the Bitcoin protocol. Mining is already designed to constantly switch pools, which keeps any one individual from graining 51% power. The network also requires six confirmations of each transaction in a separate block, which makes reverting transactions and getting them confirmed more difficult. This is however still a legitimate concern for Bitcoin. Computer technology is continually improving and problems such as this serve to increase motivation for Bitcoin miners to figure out ways to attack the system and profit from it. Another problem with Bitcoins are dust transactions. (Massive Bitcoin thefts, 2013)

Dust transactions, otherwise known as denial of service attacks (DOS), are attacks which interrupt a service. In the past, it was possible to send multiple transactions of a minimum of $0,00000112 to one user, which would fill up and bloat the block chain, making it too large and crashing the network. This problem has been patched by the developers by putting a fixed limit on the amount of transactions allowed to be sent to one client but there is still the risk of talented code hackers to bring down the network. Since Bitcoins and cryptocurrencies are a code-based currency, there is always the present danger of code-based attacks. (Bradbury, D, 2013) Bitcoin has been in the center of controversy for many massive digitally related thefts. An example of this is the Sheep Marketplace – a marketplace that opened following the shutdown of the Silk Road black market. The website announced a security breach and
eventually went offline with over $40m worth of Bitcoins lost. People have speculated that the website was set up with fraudulent intentions from the start to rob users of their Bitcoins. Given the anonymous nature of the cryptocurrency system, it may be impossible to track down these thieves. In Denmark, a Bitcoin payment processor, had security faults which had the company lose, at the time, 1$m worth of Bitcoins. (Massive Bitcoin thefts, 2013) The biggest international Bitcoin exchange in the world, Mt. Gox, also crashed down by the hands of thieves. As Bitcoin is open source developers are continually adding new features. During this process new bugs may come to the surface which hackers can take advantage of to attack the network. Although many people carefully examine the source code before a release, there is still a possibility that major security vulnerabilities get through, as they can be difficult to spot. (Bradbury, D, 2013)

The fall of Mt. Gox, which at one point was regarded as the pinnacle of Bitcoin trading and estimated to count for 70% of global cryptocurrency transactions is an example of the dangers of code-based attacks on Bitcoin and cryptocurrency. The fall of Mt. Gox which accompanied a loss of over 700,000 Bitcoins, was attributed to a code-based theft attack. This attack is the biggest digital currency theft in history. With the bankruptcy of the largest international exchange, hundreds of millions dollars’ worth of Bitcoins disappeared. The effect of this brings up the problem that comes with decentralization. (Schumpeter, 2013)

As the currency is designed to be decentralized to prevent any kind of interference it also does not have the safety guarantee that fiat currency has. When Mt. Gox fell, there was no entity or financial regulator that would come to the rescue. The money was all gone with no way of getting it back or to get any kind of support. This shows a glaring problem with Bitcoin and cryptocurrency – there is no insurance or guarantee after a loss and there is a big danger of code-based attacks or other kind of attacks as people get increased knowledge of coding and computer technology.
5. Using Bitcoins in the corporate world

People use virtual currencies everyday so the concept is not a brand new phenomenon. Examples range from credit card reward points and airline miles to online video game currencies. It is the decentralized peer-to-peer function of Bitcoin that gives it unique properties. Businesses and corporations are continuously looking for new ways and innovations to increase sales. Bitcoins have some advantages and disadvantages in the corporate world. Bitcoin does, in a way, protect itself from a country’s economic instability.

Bitcoins are digital and float against other currencies and as such are protected against economic instability or issues such as political unrest. Despite this, as discussed before, the price of Bitcoins is very volatile which comes from speculations, media coverage and uncertainties as the currency is still in its infancy. For corporations, this amount of volatility is unacceptable. Virtual currencies also lack liquidity to the point that it would be very hard to use it as an alternative to fiat currencies. If most corporations decided to actively use Bitcoins in their daily business, the demand for virtual currency would create an imbalance in supply and demand, further increasing price volatility. (Bob, S, 2013) However this is quite appealing to those who are wary of high inflation from badly run monetary policies of central banks. (Wu, C, Vivek, K, 2013) The supply that miners can add into the circulation is too limited for widespread use. The currency also lacks a formalized market. (Bob, S, 2013)

The decentralization, one of the core designs of the currency, also limits options for corporations when looking to transact. This will increase the cost of transaction as more time and resources will be required by corporations for each transaction. The lack of security that comes with decentralization is also a huge risk for corporations. If something goes wrong, corporations will have no source of help. This will increase the risk of theft as it will have a much bigger impact and bigger risk of bankruptcy than with fiat money. An example of this kind of bankruptcy is the fall of Mt. Gox. (Bob, S, 2013)

Virtual currency such as Bitcoins, although decentralized, are not exempt from taxation. “According to the IRS, virtual currencies are treated as property for taxation purposes. As such, wages and payments to independent contractors paid in the form of Bitcoins are taxable using applicable income tax rates” (Wu, C, Vivek, K, 2013) Thus the currency cannot be used by corporations to avoid taxes. Bitcoins could however be used by corporations to bypass capital control.

In Iceland, capital controls were implemented in the wake of the 2008 crisis. The purpose was to prevent further depreciation of the Icelandic Krona. Capital controls give homes
and corporations limited investment opportunities internationally. Buying large amounts of foreign currency with Icelandic króna was made impossible with these controls which were originally supposed to be short term but have now lasted over six years. Since then companies and investors have attempted to bypass these controls as investing internationally can be very lucrative. (Björn Ingi Björnsson, 2014)

Bitcoin has currently not been accepted as an official currency by the government in neither Iceland nor any other country. Investors are free to buy Bitcoins with their domestic currency. The Bitcoins can then be moved out of the country and sold for a foreign currency. This method however does not apply for Icelandic investors as foreign exchange activities using Bitcoin has been prohibited in Iceland. Bitcoins cannot be used as a way to bypass capital controls for Icelandic investors. (European Parliamentary Research Service, 2014)

This method was popular in China where similarly strict rules govern the supply of foreign currency. The Chinese government subsequently responded with laws that make Bitcoin transactions considerably harder and banned financial corporations from accepting the currency. It is thus difficult to determine how effectively Bitcoin can bypass capital control but in theory it is possible. (Björn Ingi Björnsson, 2014)
6. Regulating Bitcoin

Due to the anonymous nature of the currency, Bitcoin has the foundations to be used for illegal activities such as theft, money laundering and tax evasion. Few governments have set strict capital controls on the currency and many have covered it in tax laws. Central banks around the world have warned consumers on the risks that come with the currency such as lack of consumer protection and high price fluctuations. Research on fraudulent activities with the currency is limited due to the anonymity of the currency making it difficult to obtain data. (European Parliamentary Research Service, 2014)

Identifying traders is difficult as transactions do not require a bank account and no third party organizations are involved in trading. Bitcoin has possibilities for tax evasion but most likely not at a large scale as the number of Bitcoins in circulation is limited and the volatility in its price is high. Security experts worry that drug cartels have used this digital environment to launder their profits and technically proficient criminals may have thought of additional ways to bypass the system. The first arrest of Bitcoin money laundering was made in the US in January 2014, following the introduction of anti-money laundering guidelines that apply to the use of Bitcoin. The EU has not created any specific regulatory laws on Bitcoin. The biggest issue with regulating Bitcoin stems from the fact that it cannot be classified as a legal tender or a financial derivative/commodity. Japan has announced it as a commodity, the US treats it as property while Germany classifies it as private money. The biggest restrictions on Bitcoin is in countries with strict capital controls such as China or Iceland. (European Parliamentary Research Service, 2014)

In China, people are free to trade Bitcoins while banks are not allowed to transact with them. Bitcoin use is prohibited by legal entities as well as citizens in Russia and any foreign exchange activities with Bitcoins are banned in Iceland. In Germany, Finland, Japan and the USA, profits from mining, profits from increase in value or profits from currency exchange are all subject to taxation. In Japan banks are prohibited from exchanging Bitcoins. (European Parliamentary Research Service, 2014)
Picture 5: This table shows the regulations on Bitcoin from a few different countries.
Source: (European Parliamentary Research Service, 2014)

7. Using Bitcoins as an investment

In 2013 the price of Bitcoin grew exponentially and the media reported many stories of people getting very wealthy due to Bitcoin investments. A research paper conducted by Chen Y. Wu and Vivek K. Pandey, researched Bitcoins ability to act as an investment in a portfolio. They attempted to examine if Bitcoin could act as a normal currency and did this by examining its correlation of daily returns compared to other major currencies, stocks, real estate, multiple indexes and gold. The research concluded that due to the limited daily transactions of Bitcoins they failed to serve as a general medium of exchange. Stores that have accepted Bitcoin still tend to price their goods with fiat currencies and the volatility of the price of Bitcoin suggests the currency is very risky. The paper considers Bitcoin to be more of an illiquid financial asset, rather than an efficient medium of exchange. Although the media has reported stories of people getting very wealthy, the daily returns were accompanied by the largest risk of any of the currencies examined in the paper and Bitcoin had the largest standard deviation. However
Bitcoin does seem to serve for diversification in an investment portfolio. (Wu, C, Vivek, K, 2013)

The paper concluded that daily returns of all of the major currencies and major asset classes had little to no impact on the returns of Bitcoins. Chen and Vivek found that Bitcoins added to an investment portfolio increased returns and lowered risk of loss. Thus it can be concluded that Bitcoins act as a financial asset that enhances a portfolios efficiency with diversification due in big part to its unique properties of floating above the market. (Wu, C, Vivek, K, 2013)

As a financial tool Bitcoin is thus too risky and volatile to act as the core asset. However its unique design means that it is hardly affected by economic unrest and other assets or currencies making it very useful for diversifying a portfolio.
8. The future of cryptocurrency

The future of cryptocurrency is open for interpretation. In an age of credit cards, debit cards and online bank accounts the prospect of digital currency is not as jarring as it might sound. Transferring money digitally is very convenient, instantaneous and cheap. However, Bitcoin seems to be too complicated and unsafe for mainstream use. There is not much demand for a decentralized currency from the average consumer. For it to work as an established currency, there would inevitably need to be an increase in regulation and consumer protection which in turn will increase Bitcoins transaction costs and reduce the anonymity, its two biggest appealing factors. (European Parliamentary Research Service, 2014) There are also not many applications for the use of Bitcoins in the corporate world. Decentralization increases the risk of bankruptcy and so does the volatility in its price. Bitcoin can be used to bypass capital controls but only to a limited extent. Bitcoins in an investment portfolio increase returns and lower risk but are too risky to act as a core asset – they are useful for diversifying a portfolio. Bitcoin also lacks the liquidity that other fiat currencies have, it is vulnerable to code-based attacks and untraceable theft.

It is thus unlikely that much demand for Bitcoin will come from anyone apart from investors looking to diversify their portfolio, customers with an interest in cryptocurrencies and customers looking to transact anonymously on the black market. The lack of demand is evident in the rapid fall of Bitcoin’s price. It is unlikely that many stores will accept Bitcoin and that it will garner any widespread application. There is however plenty of room to expand within the field of cryptocurrency as its technology is very promising.

Some want ownership of an asset such as a car, for instance, to be represented by a Bitcoin, utilizing its cryptographic technology. This technology would make it easier for people to manage ownership of physical assets as it would all be digital. Bitcoin tokens of ownership could be sold or rented out. This kind of „smart property” would turn the blockchain into a sort of registry of ownership of any physical asset. The innovation of cryptocurrency and its cryptography are an invention that could have many other applications. Another example would be that international banks could use this Bitcoin-like cryptography system to move money or create their own crypto-currencies. (Swanson, 2015)
9. Future innovations in currency payment systems

One of the biggest and most widely used innovations in handling currency are debit and credit cards. The reason why these are so popular in the mainstream is due in part because of their ease of use. This innovation eliminated the need to count physical money when shopping, it reduces the weight of your wallet by removing the need for banknotes and coins, it increased safety as digital payments are much easier to track and banknotes are practically untraceable. For an innovation in currency to be successful and replace fiat money and the debit card, it needs to improve on those properties. So far Bitcoin has been unsuccessful with that as it is neither safer nor more convenient, however it is more anonymous and has low transaction fees, which is not necessarily something that the general public desires. It is however very possible that the cryptocurrency technology gets used in future innovations regarding currency and it is very likely that the future of currency will keep heading into the digital world such as using mobile phones for payment transactions.

Using mobile phones exclusively for payments could possibly improve on the convenience factor of debit cards as it would eliminate the need for a wallet during transactions. It would be just as safe in use as cards and possibly even safer, using cryptocurrency’s technology. Apple has recently tried to enter this market. “Apple pay” is a mobile-based payment system created by Apple. It launched with support and acceptance from 220,000 business outlets in America, including big franchises such as McDonald’s restaurants. Apple has made mobile payments very convenient with payments being almost instantaneous using a fingerprint reader on the phone and possible network deals with banks to lower transaction fees. (Emptying Pockets, 2014) In my opinion it is far more likely that an innovation like Apple pay, rather than Bitcoin, will catch on with the mainstream consumer as it is consumer protected, increases convenience and possibly lowers costs.
10. Conclusion

Money is one of the most valuable and sought after commodities in the world, affecting people in almost every facet of their life. One of the most controversial new innovations in this field are cryptocurrencies. It is a currency that is not protected by governmental regulations or law, making it impervious to government interference. The currency is fully decentralized, and unlike fiat money the government cannot affect its value. The first cryptocurrency created, and the most widely used, is Bitcoin.

A ledger called the block chain, publicly records all transactions with Bitcoin keeping the users completely anonymous. The supply of Bitcoins comes from „mining“, a process which involves computing complex algorithm with increased difficulty over time, making it more expensive and resource intensive and thus less profitable as time go by.

The demand for Bitcoin comes mainly from its decentralized and anonymity, low transaction costs, use for illegal transactions and as a financial instrument to profit from its price volatility or to diversify a portfolio. Other possible uses for Bitcoin include measures to avoid currency controls or other sources of governmental interference and for tax evasion. There are however many disadvantages associated with the currency.

As the currency is decentralized there is very little consumer protection, stolen Bitcoins are lost forever and Bitcoins are highly susceptible to code-based attacks. The price is very volatile and thus it is highly risky to hold on to many Bitcoins as well as lacking the liquidity that official currency has.

The currency is also subject to taxation in many countries such as the US, Japan, Finland and Germany. Countries with strict capital control such as China and Iceland have also recognized the currency and prohibited transactions, eliminating possibilities of bypassing capital control restrictions.

As it stands, Bitcoin is unlikely to catch on as an official currency for the general public as it has too many faults and has too many risks whereas its strengths are necessarily not something that the general public desires in an established currency. For an innovation in currency to be successful it needs to improve on what the debit card and credit card has to offer. It has to be more convenient, safer and accepted by merchants worldwide. An example of a possibly more successful payment method is Apple pay. However the technologies and innovation found within Bitcoin and the cryptocurrency can still be applied to other technology and innovations, such as the mobile-based payment market that Apple has entered.
The technologies that come with Bitcoin have many mainstream applications and it is very possible that some kind of implementation of cryptocurrency's technology and mobile-based payment system with cryptocurrency integration could be the future of mainstream payment systems. It will be very exciting to see the future technological innovations in currency and payment systems and although Bitcoin will most likely not be a largely popular established currency in the future, its technology will surely have widespread future implications.
Sources


