Bitcoin-ing the Future: A Force to be Reckoned With

The digital revolution has brought forward many radical changes in our society. From the way we communicate, to the way we process and store information, to the way we conduct our business. But even after the advent of the Internet and the Digital Age, the way we exchange money stays the same. Behind the modern banking system is still the same archaic methodologies that existed a century ago. There have been initiatives to change this through the introduction of 'virtual currency'. Bitcoin, which is the first decentralized virtual currency to be capitalized in the market, was created by a group of programmers who based it on mathematical proof of ownership and transfer (Castillo). It is a cryptocurrency that is entirely digital and has a defined value for exchange similar to customary currency but without relying on arbitrators like banks or a centralized governing structure. In a bid to re-invent the monetary system, the concept of digital money was introduced as an alternative when people were the most accepting of trying a radical way of finance and money. Proposed during the Financial Crisis of 2007-2009, when the international banking system was collapsing due to the downfall of Lehman Brothers and the general trust on banks was faltering, it quickly gained momentum. Initially in its adolescence, Bitcoin attracted a lot of controversy and angst from the financial world. But eventually it started to shape out to be a valuable asset that could potentially grow into being an appreciated addition to the economy. The promise it showed attracted people's attention, but still left them anxious to actually invest in it. Although the idea's sources are not directly identified, the name "Satoshi Nakamoto" is always associated with the concept and was the name under which the first reference implementation was created. It is still unsure whether Satoshi is an individual or a group that created Bitcoin and the mystery behind the name continues. In spite of its elusive origins, Bitcoin has had the involvement of academics and enthusiasts who have helped the ecosystem mature. Although the use and popularity of Bitcoin keeps increasing, as a new currency it is very volatile and unstable. This paper aims to touch upon how it works, its creation or "minting" through mining, analyze it using standard definitions of money, and the hurdles the system needs to cross before it can be completely adopted as a part of our economy. In totality, the paper will aim to answer the question why Bitcoin should be taken seriously and how Bitcoin could become a deep seated part of our current monetary system, if not a replacement.

What is Bitcoin?

Bitcoin is a cryptocurrency, similar to any other currency in its nature. Understanding bitcoin will be easier if we understand three aspects of the BTC (Bitcoin Currency): *buying*, *selling* and *mining*. Since the money is not printed or manufactured, the only way to bring new money into the system is through *mining*. The process of mining is defined as "the process of adding new money creation / transaction data to the Bitcoin's public ledger of past transactions", on the Bitcoin website (Bitcoin.com). Simply put, mining is when miners solve math problems and gain a certain number of coins in exchange. Only 21 million in Bitcoin currency can exist in total by 2140 and as of this time, 11 million are already in circulation. In a bid to accumulate the limited, a frenzy of miners are competing with colossal rigs of supercomputers to mine the coins. Business aficionados who see value in this rising and stabilizing mode of currency are pouring billions of dollars to hoard as much of it as possible, as fast as possible.

Creating Bitcoins for circulation - Minting through mining

Much like gold, Bitcoin has become a limited and hard to acquire commodity that can be mined. For transactions to take place, there needs to be enough currency in circulation so that it can be used by users. While the conventional currencies have a central authority who 'mints' more currency and releases for circulation, the only way to introduce new bitcoins in the system is through mining. Since Bitcoin is a decentralized and independent platform, there is no governing body that is regulating the flow of money. It is open to the public and anyone with the hardware, internet and some knowledge can access the transparent system. Mining a block quiet literally means solving a puzzle made of compiled blocks and earning rewards for the same. This 'puzzle' is the aforementioned proof-of-work that needs to be cracked using a high computational device. The first 'miner' to solve the puzzle earns the 'block reward' which doubles as the new currency that is introduced in the system and a transaction fee as a personal reward for the miner's efforts. Each mined block gets added as a transaction on the public ledger that Bitcoin maintains on its distributed network. There is a cap to the amount of Bitcoins that can be given out in a day, which is no more than 1800 BTC. This makes the competition all the more aggressive, with miners using huge computational power in order to mine more. But the

problem here is that with more computational power, the difficulty level of the puzzles keeps increasing. With more miners on the network, each person gets only a fraction of the reward. More than the difficulty of solving the puzzle, finding a block to solve is tough. With the increase in popularity over the last few years, mining blocks has become more difficult than ever, in 2017.

The competition soars further with increased use of special hardware that can take the intensity of the challenges of mining. Huge mining centers are built around the world that are put to work to find and solve blocks. Although there were several giants who scrambled at the beginning of the rise in Bitcoin's value to completely milk the mounting prospect, mining companies in China currently hold the cream of the cake. Around "60% of the Bitcoins hash power" is held by companies like F2Pool, AntPool and BW that are based in China (Tuwiner). This amount of hash power indicates that they mine 60% of all new bitcoins. A side effect of this large scale phenomenon is a shortage in the availability of GPUs. Colossal mine farms like these use GPUs in a staggering amount for their repeated hashing computations and the shortage has inflated the prices of parts like the Radeon RX graphics card, which has also become harder to find. Another difficult and negative side effect of mining is the increased use of electricity to power the rigs that are constantly solving complex computer algorithms. According to the Global Cryptocurrency Benchmarking Study report released by the University of Cambridge, "mining facilities consume a total of 288 megawatts (MW) to power cryptocurrency - mainly bitcoin - mining" (Rauchs). Because of this need of immense electricity, mining farms are mostly based in arctic regions that can reduce the power spent on cooling. The biggest mining is found in the Northern hemisphere. China is one of the leading miners because of the availability of cheap electricity and land. But the large energy footprint because of this high computation need is causing environmental enthusiasts to lash out at the industry of mining. In light of this, many large miners are switching to renewable resources like hydroelectric dams to generate their power (Boden).

But if mining farms are doing all the mining and getting all the bitcoins, what do individuals who want to utilize this opportunity do to compete? For individuals without the resources of big mining farms, there are mining conglomerates that bring such independent miners together. To give everyone a chance and even out the mining reward, 'pool mining' was introduced. "Pooled mining is a mining approach where groups of individual miners contribute

to the generation of a block, and then split the block reward according the contributed processing power" (Bitcoin.com). So instead of feeling thwarted by the business giants who own rows and rows of mining rigs, pooled mining brings together individuals and gives them a chance to compete and mine bitcoin. Another similar service provided by the Bitcoin community is 'cloud mining' for those who do not have the knowledge or hardcore hardware required for the business of mining. Mining pool operators hold a lot of power in their hands since they can decide to run their preferred client implementations but the interdependent ecosystem provides a way in which more people can be involved in the adoption of Bitcoin.

Bitcoin - Real Money or Wannabe?

The Oxford dictionary defines money as "a store of value over time and across people, firms, and countries". It needs to have a value compared to products or services, act as an exchange for such commodities and possess a relatively stable price of its value so that it can be bought and sold for a similar or higher amount. It needs to be universally accepted and readily passed around by the members of the community. But in more technical terms money needs to have three main functions: "a medium of exchange, a unit of account, and a store of value" (Mankiw). In accordance to this definition, how does Bitcoin bring value so that it can be used as currency? Bitcoin is a radical change from the generally accepted state currency in the way that it does not depend on intermediaries and is decentralized. There is no central body to regulate or influence the price or even monitor the amount of it that is in circulation. It all depends on a computer algorithm, its users and their consensual agreement to keep it in circulation so as to uphold its value. Does this lack of a central body deter Bitcoin from being considered a monetary medium or is it independently valuable? Let's look at each of the three functions that determines if Bitcoin can be used as a monetary medium.

First, let's look at Bitcoin's ability as a store of value. Value is created when a particular commodity is considered as valuable by a majority of the community. For example, in the case of gold, it took people time to realize and understand the metal and its properties. The more people that started accepting the metal, the more it was in demand. The increase in demand created 'value' for gold. People were willing to pay increasing amounts of money in exchange for it, just to procure it before others. Its limited availability increased its value all the more. The

same can be said about Bitcoin. It creates value because of the high demand in which people regard it. The increasing difficulty in mining is directly reducing the availability and easy access of bitcoins. The reduced obtainability increases its value. Like Information Economist Alstyne says, “Bitcoin has value because people accept it—the same reason any form of money has value” (Alstyne). Its limited production of only 11 million for another 100+ years is another factor that increases its demand. Although economists might argue that the value of Bitcoin could go below the base value to a negative price, and that people seek stability so that they can use the hoarded money for later use, Bitcoin has a steady future based on its current rate of growth. Over time, because of its popularity, investors and adaptation, Bitcoin will have a store of value that results in profit for the people who own it.

The other question to ask about Bitcoin’s use as a monetary medium is how it can be considered as a ‘unit of account’ (Krawisz). Unit of account is something that can be used to value goods and services, and settle debts. To understand more about this, let’s look at the various ways in which Bitcoin can be considered a unit of account. For a currency to be considered as a unit of account it needs to possess divisibility and low price volatility. For divisibility, Bitcoin is optimal because of the way in which it can be divisible up to a certain number of decimal points and still be considered a valuable amount. But a resulting problem arises due to its extreme divisibility which causes the value of a product to extend up to 4 to 5 decimal places that confuses the average consumer who is used to simpler currency number systems generally with 2 decimal points. The second is the unusual volatility of Bitcoin. In the financial world, volatility is defined as “the degree of variation of a trading price series over time”. Increased volatility indicates a higher risk of holding that asset because of its possible price degradation. Bitcoin’s biggest problem in being considered as a good unit of account is its high volatility index which in July 2017 was recorded as roughly around a high 6%, compared to the low 1.2% volatility of gold (BuyBitcoinWorldwide). Experts say, “Because the value of a bitcoin compared to other currencies changes greatly on a day-to-day basis, retailers that accept the currency have to recalculate prices very frequently, a practice that would be costly to the merchant and confusing to the consumer” (Chuen). But as a concept of currency that was released less than a decade ago, the instability in the price of Bitcoin is only to be expected. The volatility rate has been quite stable for the last 2-3 years compared to 2013- 2014 (BuyBitcoinWorldwide). Since being released in 2009, many possible solutions like creation of

bitcoin capital markets and an increased adoption rate have been discussed in the community that could potentially make bitcoin less volatile.

As a convertible virtual currency, i.e. a digital asset that can be converted into a physical currency, Bitcoin naturally fits the definition of being a medium of exchange. It is also accepted in exchange for goods and services by a large number of providers and merchants across the world, including popular companies like Overstock and Zynga. However, the IRS clearly states in its 2014 tax guidance report that virtual currency like Bitcoin "operates like "real" currency—i.e., the coin and paper money of the United States or of any other country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance—but it does not have legal tender status in any jurisdiction" (Internal Revenue Service). This means that although the form of payment is recognized in the country but cannot be used directly equivalent to the fiat currency of the jurisdiction, and make payment to extinguish a public or private debt, or meet a financial obligation. Bitcoin in reality is a way better medium of exchange than regular currency because of its versatile ability to be able to be transferred anywhere from anywhere. With no transaction fees or dependency on a third party or difficulty in changing it to and from a country's currency, it is currently the fastest way to transact and send funds. According to an empirical research done by the Federal Reserve Bank of Boston, where they compared transactions that used fiat money and virtual currency, it was found that it is a huge advantage for online retailers because of how "accepting bitcoin lowers merchants' costs by reducing payment processing costs, chief among which are the credit card interchange fees, typically on the order of 2 to 4 percent" (Wang). Bitcoin's ability to make e-commerce effective will not only result in more people using it for its convenience but also create a boom in the online business world since it is mainly optimized for online transactions.

Applications, Acceptance and Economic Impact

Bitcoin's use in its initial stages was limited to the Silk Road and pornographic websites where a hidden identity was most useful. Like Popper wrote in his book, "Within the Bitcoin world, there had been a common assumption that people looking to buy illegal or unsavory goods were likely to be among the first to have an incentive to use Bitcoin" (Popper). Since Bitcoin cannot be traced back to a user, the use of it on Silk Road, the black-market of the dark

web for drugs, was immediate. The Silk Road website although was shut down in the October of 2013 and the FBI seized up to 173,991 Bitcoins which is worth over $44 Million USD according to the current exchange rate (FBI). Next up was the adult industry and the one to introduce Bitcoin as a form of payment was Mind Geek. “The IT conglomerate is the leading service provider for the porn industry, and the company was one of the first to offer the customers bitcoin as a form of payment”, according to Forklog (Forklog). But growing beyond the stages when it was only used for illegal and questionable things on the dark web, Bitcoin has gained maturity in the open market amongst leading global companies. The list includes Overstock, Expedia, Shopify, Foodler etc. who were among the first Fortune 500 companies to adopt Bitcoin as a form of payment (Moreau). Many of the brick and mortar companies have also started accepting Bitcoin in a bid to appeal to more customers. Payment processors like Coinbase and Coinkite enable the businesses to accept Bitcoin as payment and charge around 1%, which is better than the average 2.5% charged by credit card companies (Franco). While the suspension of the intermediary between the merchant and customer is a huge selling point for a business with the option of virtual money, it is more useful to employ a professional processor to deal with the exchange between BTC and fiat currency. With the reduced transaction fees for the customer and the low credit recall expense for the seller and its seamless transacting with overseas counterparts, using Bitcoin is a win-win situation for both the parties.

Another important field where Bitcoin is making a big impact on the economy is the mining business. “At the current rate of 25 bitcoins per block, the total mining revenue for a year is around 1.3 million bitcoins”, says Franco in his book about Bitcoin (Franco). Besides the actual mining of bitcoins itself, the small industries of computer parts and data centers also have a huge upside. The equipment manufacturers benefit from the huge orders of CPUs and GPUs that go into the mining and because of the complexity of the computation, they require frequent upgrades. Beyond GPUs came the age of ASIC (application-specific integrated circuit) which “is an integrated circuit (IC) customized for a particular use [bitcoin mining], rather than intended for general-purpose use” (Wiki). Because of their increased computational power, data centers are needed to host these equipment in a high density power and cooling environment. “The total hashing power of the Bitcoin network is currently 79 PH/s, which is 564 times higher than the 140 TH/s it handled just a year ago” (Bhaskar). This is more than the combined computing power of all the supercomputers in the world right now. As the economics of mining gets

progressively profitable, the investments in the arena can be found to be growing as well. In the Wedbush report by Luria and Turner, over 200 million USD was invested in Bitcoin mining equipment during 2013 and assuming the same progression would increase by another 200 million in the next few years (Luria). This can already be seen in the way AMD ran out of stock for its popular graphic cards that are used in mining. According to CNBC, "AMD is one of the market's best performing stocks in the past year with its shares up nearly 170 percent in the past 12 months", due to its increased demand among miners.

More than being its own independent transaction medium, Bitcoin also enables the free flow of cash that can be exchanged for federal currencies. This is enabled by ATMs and exchange agents who trade Bitcoins and provide actual value in physical cash. In countries like Argentina and China where money cannot be taken outside the country, a system like Bitcoin's becomes essential. According to Franco in his analysis of Bitcoin applications in business, on exchanges he states that "Some advocates argue that there might be demand for derivatives based on this exchange rate: miners might want to sell bitcoins forward, while payment processors might want to buy call options or sell put options" (Franco). This increases the dynamics and flow of currency in the Bitcoin market including forward trading, where customers can buy and sell Bitcoins more freely where the exchange is directly denominated with its equivalent in fiat currency. The exchange market will open up a whole new business based off of managing Bitcoins and the interchanging of it into other currencies. Enabling this would be third party software or agents who provide the wallet services to take care of the exchange. A problem that is recognized by the cryptocurrency community is the involvement of third parties in the process which is in contradiction to the ideals of Bitcoin in upholding its purity and independence from intermediaries. But thanks to a constant innovation model in the unrestricted development arena of Bitcoin, innovative ideas to solve the risk factor associated with the involvement of third parties are underway.

Technical and non-technical problems

Besides solving the problems of exchange and creating a ripple in the financial world, Bitcoin has some cons that bother the community of customers. On one side there are technical issues and then there are economic and legal issues. On the technical side, a lot of talk has been

going on about the double-spending problem which is when a user is able to spend the same number of coins twice on the network (G. O. Karame). Despite the strict algorithms of blockchain, timestamping and proof of work, it has been made possible to hoodwink the system in several cases (Buntinx). The limited number of transactions per second that can be handled by the networking power of Bitcoin has been another matter of concern amongst users. The throughput is seriously limited compared to its plastic currency competitors. “Visa’s network is said to handle about 2,000 transactions per second around the world on average, and capable of handling 10,000 transactions per second during busy periods”, compared to the transaction power of Bitcoin which only does seven transactions per second (Narayanan) . Another technical problem is with the weakening of the hash algorithms on which the entire security of the system is dependent on. There has been a recent project called “The large bitcoin collider” that aims to break into bitcoin wallets by using brute force to generate all possible keys (Pearson). Network issues and disturbances are to be expected on a peer-to-peer system that is entirely dependent on the consensus between nodes. Due to failed internet or intentional subversion of nodes, the updates might not be all in sync amongst all the peer nodes. Malicious attacks like the DDoS (Distributed Denial of Service) attack could also affect the Bitcoin network bringing down the exchange providers by flooding the servers and creating traffic (Das).

On the other side of technical issues in the Bitcoin network is the socioeconomic factors that is most relevant in the economic and legal world. The value fluctuation that Bitcoin goes through on a regular basis is a matter of concern for investors. The volatility is mostly caused by the lack of widespread adoption and no regulatory body to oversee the stabilization. The confidence of consumers on the profitability of Bitcoin needs to grow worldwide for the price of Bitcoin to stabilize. But since its introduction in 2009, the value has definitely stabilized according to its reduced volatility index of 6% from a high of 12% between 2013- 2014. Another issue that still has legal experts scratching their heads is the taxation policy on Bitcoin. Due to its anonymous system, it is impossible to track a person’s transactions and tax them using any simple method. It is essential for Bitcoin to be interwoven in the international business exchange web if it can ever be adopted as a medium of payment. Due to this disconnection from the banking system and the lack of access to the infrastructure of the currently built economy that the majority of the population still trusts, “bitcoin has proven vulnerable to fraud, theft, and subversion by skilled computer hackers” (Yermack). Instead of being considered as an

alternative to the fiat system of money, it needs to coexist with the current monetary system that we have in place and just be considered an upgrade in the way in which we transact.

In Conclusion

The transaction between buyers and sellers has taken different forms over the years from barter to gold to paper. But once we reached banking, we've stayed on the same system for centuries. The way we transact might have seen changes through online banking and paying with our smartphones, but behind that is the archaic system which wastes resources. According to the Federal Reserve System of United States, "The 2017 currency budget is $726.6 million" for printing on average 6.9 billion paper notes (FRS). The fiat system of finance operations is obsolete with less granular transactions that are not up to speed with the nimbleness that is required in the fast paced digital world. There is a need to update the way we transact in this age of voice controlled purchases and automatically scheduled future transactions. Although the use of Bitcoin in the dark web or gambling websites raised questions about its ethics, its popularity was only because of its anonymity. Besides its flaws, Bitcoin has proven to be a valuable asset and a profitable investment option given its steady rise in market value and adoption rate while being an excellent medium of exchange. The value of it increases as the trust in its profitability increases amongst users. It is being taken seriously by economists, legal experts, technologists and governments alike; persistently increasing in popularity.

Bitcoin has overcome the weaknesses of both fiat and gold-based money, by being mathematically deterministic about the growth of rate and increase in value (Yermack). By being used along with the current economic model and a little regulation, Bitcoin can prove to be a valuable upgrade. In such a structure, Bitcoin would get closer in acceptance and use to touch the fiat currency model and "If Bitcoin is big enough to matter, then it is big enough to get regulated" (Narayanan). Although the inclusion of Bitcoin as an upgrade to the fiat system or adding regulations to it would mean deviation from the original aim of Bitcoin, it would also represent the dynamic way in which the environment is growing in accordance to the regular economy. It significantly reduces transaction fees, increases the velocity of money that can be moved, makes micropayments possible, and enables developing nations to gain access to banking services they would not otherwise have access to (Turpin). Further, the conception of a

truly global, digital currency opens the door to an expansive amount of future innovations on a global scale. Businesses and technologists are envisioning new ways of investing, banking, and doing business while expanding the ways in which everyone else can be a part of this. With the velocity of business constantly growing and at a time where instant gratification is most valued, Bitcoin has the potential to be an instrument to reduce the lag that our current monetary system possesses.