Does Bitcoin have a future as a recognized tender worldwide?

Conor Tighe, *Student, GMIT.*

***Abstract*—**

This paper offers an in-depth analysis of bitcoins architecture and the blockchain technology which it uses to execute decentralized operations. After examining the technology, we look back on the major events which influence the development of bitcoin, its community and its price along with economic studies that give us an insight into the value of the coin. Considering the volatility and scale-ability issues reviewed in the research provided we could say it is too early into bitcoins life cycle to say for certain if bitcoin will ever become a globally accepted tender. What we can draw from the research provided is the large amount of major companies currently accepting the tender, the growing bitcoin community that continue to put faith in the coin and the huge underworld economy operating on the dark web which uses bitcoin as its main vessel for doing business means bitcoin is strong enough to potentially develop into a worldwide tender in the future.

Keywords*—*Bitcoin, Cryptocurrency, Blockchain.

I. Introduction

Bitcoin is a cryptocurrency published on the October 31, 2008 by an unknown programmer or group of programmers under the name of Satoshi Nakamoto. It was the first decentralized digital currency that did not require overhead administration by an organization or individual, making it one of the staple technologies of the information age. Along with the publication of the currency came a research paper titled [1]Bitcoin: A Peer-to-Peer Electronic Cash System explained how the system operates and protects the coins and users. The paper went on to describe a peer-to-peer system and its decentralized operations, [1]"network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed". This system would become known as the block-chain or honest-chain, the block-chain is the underlying technology behind bitcoins independence from governments and banks. Users of the cryptocurrency did not have to rely on outside intervention from a 3rd party for their online transactions as this mathematical proof-of-work approach eliminated the need for each person involved to give their identities to the 3rd party. The block-chain has proven itself to be an efficient and fast approach to handling online transactions by the sheer popularity of bitcoin and its daily use across the world. [2] A 2016 survey from the tech giant IBM reported that 65% of major banks plan on implementing the blockchain by 2019. The invention of the block-chain itself could be considered just as innovative as bitcoins with many other cryptocurrencies like Ethereum using the design pattern for coin circulation. By examining bitcoins infrastructure, economics and history I will attempt to discover reasons to consider bitcoin a legitimate currency beyond digital gold and answers to how reliable is this proof of work system and how can we tell if the bitcoins that utilize it have a practical future?

II. Bitcoins infrastructure

A. The Block-Chain

The block-chain that is referred to when talking about bitcoin is known as the honest chain, which is powered by the collective CPU processing power of hardware around the world known as miners. These machines vary from high performance computers to pools of less efficient computers working together but all the systems contributing share the same goal. Roughly every 10 minutes mining computers will collect a group of pending transactions know in the block-chain as a block and use it to create a mathematical puzzle. As Satoshi explains in his paper [1] the first miner to solve the puzzle will announce it to the rest of the network, then other miners will validate the solution while checking if the person sending has enough in their bitcoin wallet balance to complete the transaction. Once enough miners approve the block it is added to the ledger which is updated across the network. [3] The incentive for these miners to contribute to the block chain is for every solution to a block found bitcoins are given as a reward as of now. This reward was 50 bitcoins before it was halved on the 28th of November 2012, it halved again on 7th of October 2016 to become the current reward of 12.5 and will eventually drop to 6.25. This is because the reward schedule set by Satoshi Nakamoto is the only way to create new bitcoin and with a cap of 21 million bitcoins to be allowed to exist the reward for mining bitcoins is set to half ever 4 years. [4] 16,579,938 bitcoins have been mined as of me writing this paper with an average of 1800 being mined each day. The next halve will take place on the 15 Jun 2020 with the rate bitcoin is being mined at, this process will continue until the reward payout has halved a total of 32 times and the final bitcoins are released to the world at 0.00000042 bitcoins per block.

B. Blocks and transactions

The website blockchain.info displays data related to individual blocks along with and transactions within the block. We can examine the data within the [5]block 487093 as an example to see the bitcoin transactions stored within. This block was mined by a Chinese mining pool known as

AntPool which is the largest pool in the world, as of now mining 25% of blocks. [5]This block contains 1636 transactions while taking up 1020.542 Kb and although we can view the addresses that sent and received these bitcoins we cannot trace see the identitys behind them. If we look at the transactions the final exchange at the top of the list is AntPool being rewarded 12.5 generated bitcoins plus the transactions fees. The design of a bitcoin is similar to a digital receipt or a linked list data structure. Transactions are done by signing the hash of the last transaction and the public key of the new owner of the coin. Then these are added to the end of the coin. The way bitcoin preserves its integrity is though the miners. While double spending is normally prevented by having an overseeing authority track the balance of each user, [1]Satoshi designed a system where every miner knows about every transaction in the entire block-chain ledger. This way everyone knows what has already been spent and where it was sent to and as the number of confirmed transactions arise the higher the demand for the required computing power to reverse what has already been done, meaning no one can change any previous transaction without it being obvious to all other miners contributing to the growth of the public ledger. When a miner confirms that there was no double spending of the coins by checking the ledger back to when the coins where generated he then adds it to a block and shares it with the network by broadcasting its hash with the added previous hash. This whole process is how the block-chain operates coin circulation.

C. Proof of work

Since there are no organization overseeing bitcoin once a password to a wallet is forgotten the bitcoins are lost forever, its hard to distinguish between how many have been lost for good and how many are being held onto to be sold. Lost bitcoins are not destroyed just made inactive, Lost coins only make everyone else's coins worth slightly more. Think of it as a donation to everyone. - Satoshi Nakamoto[1]. One of the first things mentioned in the [1]paper when discussing the proof-of-work is [6]Adam Back's Hashcash. What Satoshi is referencing here is a proof-of-work algorithm which was invented in 1997. This was usually used to protect against denial-of-service attacks using cryptographic hashes such as SHA1, SHA256 or SHA3. This method is what blocks within the block-chain use so the miners can validate what block will come next in the chain. Each block uses the hash of the previous block as what is referred to as the block identity or id, you can think of this as a lock string. To generate the hash of the block being validated, we take this block id and combine it with a nonce which is provided by the miners CPU power, this 2nd string can be thought off as a key. The hash that is taken as the solution is the first miner to produce a SHA256 hash that has a header starting with a specified number of 0s set by the block-chains difficulty. The block-chain difficulty fluctuates depending on the rate of blocks being produced. The target for the block-chain solution rate is 2016 blocks being validated every 2 weeks. Which means if it took the miners 12 days to solve 2016 blocks then the difficulty will be increased by 20% so the next 2016 blocks will take longer to mine.

III. Economic landscape

As of date of publishing(11/2017) bitcoins value reached an all-time high of [23]8,226.0 euro and validating its credibility to many who doubted it would last as far as 2017, this is an amazing milestone considering it was once only worth a couple of cents. Many in the technology and economics industries doubt its stability and usability, labelling the currency as a bubble with no real-world use. This could be a result of bitcoins volatility through-out the years. An excellent thesis by [7]Benjamin M.Blau on bitcoins Price dynamics and speculative trading in bitcoin found that during 2013, speculative trading contributed to the unprecedented rise and subsequent crash in Bitcoins value nor do we find that speculative trading is directly associated with Bitcoins unusual level of volatility", referencing the 5000% increase in value bitcoin experienced in 2013. There has been a recent divide in the Bitcoin community, one of the many arguments towards using bitcoin is the way the system prevents a monopoly by treating every miner equally as anyone could solve a blocks puzzle. A recent [10]article from Jeff John Roberts does a great job in explaining how a monopoly has risen from bitcoin but not in the traditional capitalist fashion, company's like Bitmain have started to become dominate forces in the bitcoin community making up for 28.9% of all the processing power for the blockchain. Mining has become a business in itself, this is the cause of the split in the chain branches on August 1st, 2017 resulting in the creation of Bitcoin Cash(BCC) which favours miners as it increases the block size to 8MB allowing them to process more transactions. Individuals that have stockpiled large amounts of bitcoin can have major influence on the value, for example it is [8]estimated that Satoshi Nakamoto owns one million bitcoins or roughly 4.75% of the 21 million that can exist. If he was to dump these coins onto the market the value would crash. Both Japan and Germany have recognized bitcoin as tender allowing vendors to accept it as payment. Other countries havent been as enthusiastic though, Ecuador banned bitcoin in 2014 as they introduced their own digital currency for its citizens. Despite this its [9]reported that the use of bitcoin among the people of Ecuador continues to grow, and although illegal the authorities have done little to enforce the ban.

IV. Historic events in bitcoins history

By observing the effects of major events through-out bitcoins history we can see can get a better insight into bitcoins reliability in the future. On the January 3, 2009 the first block for storing transactions was created which would be known as the [12]genesis block. Then on October 5, 2009 the [13]New Liberty Standard posts the first bitcoin exchange rate, allowing bitcoin users to trade what they have mined. The value given was 1,309.03 BTC to 1.00 dollar, the reasoning behind this price was that was typically the cost of

electricity when mining bitcoin at the time. [14]On the May 22, 2010 the first known real-world use of bitcoin took place when Laszlo Hanyecz used 10,000 BTC to purchase two pizzas and have them delivered to a house. On February 9, 2011 bitcoin hit its first major milestone reaching a value of 1.00 dollar per coin, causing news outlets to cover the currency. Come 2012 we start to see major companies on the internet take bitcoin much more seriously, by November 15, 2012 [15]WordPress had announced they will start accepting bitcoin as payment. In a blog they explained the reasoning for this was the limits of using payment services, they stated that PayPal alone blocks 60 countries. The decision to include bitcoin was to broaden their horizons allowing people from Haiti, Ethiopia, or Kenya to make payments on their site. [16]Dell would adopt the currency on July 18, 2014, later that year Microsoft would declare that they would now accept bitcoin on December 11. On 26 February 2014 the first counter exchange opened in Hong Kong, allowing individuals to aquire coins in person for the first time. [17]On the October 22, 2015 the EU would declare that no value added tax would be applied to Bitcoin.

V. Bitcoins association with illegal activity

Then on June 1, 2011 we seen a spike in value when the media website [18]Gawker covered the illegal market The Silk Road which was using bitcoin for trading illegal goods online, accessed through [11]TOR a anonymous routing software developed in 2002 by US Navy seals and now available to the public. This attention raised the value from 7.79 Euro to 14.90 Euro in 10 days. On February 11, 2012 both Paxum and Tradehill parted ways with bitcoin as result with its growing association with illegal activity. On October 1, 2013 the arrest of Ross Ulbricht, owner of The Silk Road took place. This resulted in a seizure of [21]30,000 BTC by the FBI from the illegal market places holdings, 3 weeks later 144,000 BTC are found in Ross Ulbricht personal holdings, he would later receive life imprisonment[20]. The hearing on bitcoin held by the [19]US senate on November 18, 2013 following the demise on the silk road would lead to a price jump from 685.75 to 1072.83 dollars as the senate came to the conclusion that bitcoin was a promising technology, Jennifer Shasky Calvery, Director of the U.S. Government's Financial Crimes Enforcement Network said, We want to operate in a way that does not hinder innovation. On June 27, [22]2014 the same 30,000 seized bitcoins where auctioned back onto the marketplace by the US Marshals in batches of 3000. Although the Silk Road has fallen many illegal market continue to operate on the dark web.

VI. Bitcoin integration into applications

For our Final Year Project[24], we are in the process of designing and creating a bitcoin wallet built on a MEAN stack. We are considering using bitcoinJs[25] as the library for receiving and sending bitcoins. This is a JavaScript library used for interacting with the bitcoin blockchain. The library is installed through NodeJS using the command npm install bitcoinjs-lib. We also have been investigating the blockchain.info API[26] for bitcoin integration along with displaying block data. As bitcoin addresses are simply generated strings we will represent the addresses with a QR code to allow users of the application to easily send and receive money. We also plan on using Google maps to display bitcoin related locations to users and a bitcoin information section to show the most recent price and how it compares to other currency's. All though we are still designing the system architecture, so these technologies are subject to change but so far bitcoin integration seems to be very developer friendly.

VII. Conclusion

Considering this was the first live blockchain cryptocurrency and yet the most successful use of a blockchain to date is an achievement. When answering the question Does Bitcoin have a future as a recognized tender worldwide? we can now say it is a possibility with the information reviewed in this paper but its unrealistic to answer with any certainty with so many unknowns at this stage of the currencys lifespan. There has been great progress in 2017 for bitcoin with an all-time high price reached. There have also been some difficulties within the communities with some users breaking away to form their own coin, [27]Bitcoin Cash. This divide was a result of a disagreement among the community on how to handle the blockchains scale-ability issues that where starting to take effect with transactions taking days to complete and the size of the blockchain growing rapidly which is required to be downloaded and stored on all local machines using a hardware wallet. There where still disagreements among the users of bitcoin even after many leaving to create Bitcoin Cash, the rejection of applying SegWit which was the concept of taking the script which contained the signature and public key and moving it to an external block allowing us to fit more transactions into a block and speeding up the transaction process time for each exchange. Taking these recent events in the cryptocurrency community into account, at this time we cannot say if bitcoin will be a currency that unifies individuals and merchants worldwide or even still be the dominate cryptocurrency in the future. With the large amount of major companies currently accepting the tender, the growing bitcoin community that continue to put faith in the coin and the huge underworld economy operating on the dark web which uses bitcoin as its main vessel for doing business, it looks like bitcoin will be relevant for years to come.

References

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* , Official paper published 9th January2009

[2] William Suberg, *IBM: 65% of Worlds Major Banks to Use Blockchain By 2019* , Article from news.bitcoin.com published on September 30, 2016

[3] Coindesk, *How bitcoin mining works* , Article https://www.coindesk.com/information/how-bitcoin-mining-works/ September 30, 2016

[4] Luxembourg S.A.R.L, *Live chart showing how many bitcoins currently exist* , Chart: https://blockchain.info/charts/total-bitcoins

[5] Luxembourg S.A.R.L, *A recording of the block 487093, its transactions and how it relates to other blocks in the blockchain* , Block: https://blockchain.info/block/00000000000000000003bb7154d70526f28b40dea24d0ad929eaabd6bd6ebd544

[6] Adam Back, *Hashcash - A Denial of Service Counter-Measure* , http://www.hashcash.org/papers/hashcash.pdf, 1st August 2002

[7] Benjamin M.Blau, *Price dynamics and speculative trading in bitcoin Volume 41* , http://www.sciencedirect.com/science/article/pii/S0275531917303057, October 2017

[8] Rob Price, *The mysterious creator of bitcoin is sitting on a $700 million fortune* , http://uk.businessinsider.com/satoshi-nakamoto-owns-one-million-bitcoin-700-price-2016-6, 14 June 2016

[9] Kevin Helms, *Use of Bitcoin in Ecuador Continues to Grow Despite Government Ban* , https://news.bitcoin.com/use-bitcoin-ecuador-grow-government-ban/, May 28, 2017

[10] Jeff John Roberts, *Does Bitcoin Have a Mining Monopoly Problem?* , http://fortune.com/2017/08/25/bitcoin-mining/, 25th Aug, 2017 https://blockchain.info/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

[11] TOR FAQ, *Tor is a software generally used to browse the internet annoymously and access .onion websites.* , https://www.torproject.org/docs/faqWhyCalledTor

[12] Genesis Block, *This is a view of Block 0 on Blockchain.info which is reffered to as the Genesis block* , https://blockchain.info/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

[13] New Liberty Standard, *A link to the New Liberty Standard webpage showing the first value of Bitcoin* , https://web.archive.org/web/20091229132610/http://newlibertystandard.wetpaint.com/page/Exchange+Rate

[14] Coindesk, *Article by coindesk explaining the first real world bitcoin transaction and how its celebrated among the bitcoin community* , https://www.coindesk.com/bitcoin-pizza-day-celebrating-pizza-bought-10000-btc/

[15] Wordpress, *The official post from wordpress explaining their choice to accept bitcoin* , https://en.blog.wordpress.com/2012/11/15/pay-another-way-bitcoin/

[16] Dell, *Dells official explanation on why they decided to accept bitcoin* , https://blog.dell.com/en-us/we-re-now-accepting-bitcoin-on-dell-com/

[17] CNBC webstite, *CNBC report that the EU will treat Bitcoin like regular money* , https://www.cnbc.com/2015/10/22/bitcoin-now-tax-free-in-europe-after-court-ruling.html

[18] Gawker blog, *First major media coverage of the silk road* , http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

[19] Homeland security hsgac.senate, *US Senates websites statement on bitcoin and silk road* , https://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies

[20] NY Times website, *NY Time reporting on the results of Ross Ulbricht trial relating to the silk road* , https://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html

[21] CNN Money, *money.cnn provided the statistics and details of the silk road seizure and the bitcoin obtained* , http://money.cnn.com/2013/10/02/technology/silk-road-shut-down/

[22] ABC News, *ABC News report the auctioning of the bitcoins from the silk road* , http://abcnews.go.com/US/tim-draper-bought-auctioned-bitcoins-seized-silk-road/story?id=24399619

[23] Investing.com, *A Graph showing the most up to date values assigned to Bitcoin from the exchnge Bitfinex* , https://www.investing.com/currencies/btc-usd-historical-data

[24] Our Group Github, *The repo we will be using to manage our project* , https://github.com/Smurfgalway/Final-Year-Project-Applied-Diss

[25] BitcoinJs Github, *The offical repo for the bitcoinjs library* , https://github.com/bitcoinjs/bitcoinjs-lib https://github.com/Bitcoin-ABC/bitcoin-abc

[26] Blockchain API, *The official page for using blochain.infos API* , https://blockchain.info/api

[27] Bitcoin Cash, *Adjustable Blocksize Cap for Bitcoin* , https://github.com/Bitcoin-ABC/bitcoin-abc