EPQ

What are the technical details of Bitccoin and what are its uses?

Cryptography based EPQ

Jonathan Chiu
01/November/2019

Contents

1 Abstract

Bitcoin is a revolutionary decentralised cryptocurrency that seemed to be the trend in late 2017 where it was of interest to many investors; however, many do not know how the currency operates. This paper explores how the cryptocurrency operates through the use of mining that involves Merkle trees, the transactions that rely on cryptography and use of the currency. Bitcoin relies on mining to verify transactions instead of an intermediary bank, but the transactions could be a transfer of Bitcoin to fund illegal activity. Users trust the currency due to cryptography to use it as a medium of exchange due to the security it provides, and the value Bitcoin holds, however, the currency is unlikely to stay self-sufficient due to halving and its limited supply.

2 Introduction

Bitcoin is a revolutionary decentralised cryptocurrency that was created by Satoshi Nakamoto which removes the need for intermediary banks and puts the trust into cryptography. In this dissertation, I aim to outline how the Bitcoin operates, i.e. how mining works, how transactions take place involves Elliptic Curve Discrete Logarithm Problem (ECDLP) and its uses. There are two areas of mathematics that Bitcoin utilises, the first being how SHA-256 is part of mining (verification of transactions) and the second being how transactions are secure using digital signatures; Bitcoin makes use of Elliptic Curve Digital Signature Algorithm (ECDSA). I wish to discuss the uses of Bitcoin mainly how some users use the currency for illegal activity and how the currency maintains value.

"Is it a bubble waiting to burst" was one of the few articles published after the peak in Bitcoin's price. Bitcoin is a decentralised peer to peer cryptocurrency system that was created by Satoshi Nakamoto in 2009 that allows the virtual currency to be transferred. Bitcoin is used as a medium of exchange where users of the currency can purchase goods and services from merchants that accept the cryptocurrency.

Bitcoin has no intermediary banks involved in transactions and instead relies on miners on its network to verify transactions. Mining is the process of verifying transactions by using computational power to solve a mathematical calculation to verify the block. These verified blocks form a blockchain, and this is the public ledger which holds all the Bitcoin transactions to date.

Transactions make use of the private key and public key cryptography to ensure maximum security; as a result, the decentralised nature. Cryptography makes use of some mathematics that ensures that there are trust and security between two users in a transaction. Bitcoin makes use of the ECDSA, and this makes use of Elliptic Curves where it allows users to send Bitcoin without giving out their private address. The currency uses the ECDLP, which uses elliptic curves, which prevents users from finding out A's private address from A's public address.

Investors can purchase Bitcoin, but this would increase its price due to the value it has due to the fixed supply and the security the blockchain provides, which allow them to trust the cryptocurrency. Many users do not understand how the currency operates and merely use it as a way of trading. Therefore, I feel that this topic is worthy of exploration.

3 Literature Review

Before beginning my research, I expected to find that Bitcoin would appear as a gimmick than a currency. I was unsure of the concept of Bitcoin and the uses of Bitcoin but assumed I could find details on Bitcoin from secondary sources such as articles and books.

To gain a broader understanding of the concept of Bitcoin, I began reading sources that detailed the facts such as the "Bitcoin: A Peer-to-Peer Electronic Cash System". I am quite confident in this resource considering that the information about the notion of Bitcoin is indistinguishable, detailing the how Bitcoin works such as the use of the blockchain and proof of work which is when a miner produces a "valid hash" and would relay across the network, and other miners check the work. This source is credible as the report was written by Satoshi Nakamoto (the creator of bitcoin) himself and published in 2008. The paper was created by the creator of Bitcoin, indicating an impartial white paper, and gathered relevant information about the technical workings of the currency.

Within my range of literature, I have found evidence that supports both for and against the uses of Bitcoin. I have narrowed my extensive research by only including strong arguments in my study. It was a slight challenge to find evidence that did not show bias, reducing its quality as Bitcoin is still considered a gimmick, which often leads to biased opinions.

First, considering the broader effect of Bitcoin, The Rubin report featuring Ben Shapiro argues that Bitcoin is a "Marketing opportunity than anything else" and the same as "real estate". Shapiro is not an expert on Bitcoin, but a journalist and commentator and therefore his work cannot be considered entirely reliable. I should avoid using this source when concluding. However, it was an entertaining podcast to listen from a different perspective, which led me to question more detail on the uses of Bitcoin.

A common argument suggesting the disaster of Bitcoin mentions the weakness of Bitcoin, both as a medium of exchange and its perception. George Gilder's book "Life After Google" argues that Bitcoin is "incompatible with all modern money systems" as "Moneys are established and maintained to do what can't be done with bitcoins" and also goes further to suggest that "Gold is intrinsically scarce and valuable", but Bitcoin is backed by "computer cycles producing additional numbers of zeroes". However, he also mentions Bitcoin's" underlying technology will unbundle the roles of money" suggesting that the blockchain model is the future.

A different view is presented in Paul Vigna's book "The age of cryptocurrency" suggesting that Bitcoin allows the human populace to take charge of the means of their production and "rules of the game" and criticises the current global monetary system as having "serious problems". The source also highlights the blockchain as an honest architecture which allows everyone to keep honest and a "whole layer of banking bureaucracy is removed" suggest that there are flaws in the monetary monopoly control by countries. I was surprised by the information by Vigna and Gilder as I was unaware of the broad spectrum of contrasting perception about Bitcoin.

Similar accounts were highlighted in the work of Turpin, who claim that Bitcoin bypasses the traditional model of accepting payments. So the irreversible payments make it attractive to merchants which erases the problem of" chargebacks".

After evaluating the reliability of these sources, I found that George Gilder's book was one of the most credible considering that he is an investor and economist who has focused on Bitcoin's concept of involving the blockchain as well as being a Harvard graduate who has experience and knowledge of the subject which allow me to trust his work and use it further. The book by Vigna is reliable as he is an author and journalist who writes about Bitcoin and the article by Turpin was found in an academic journal rather than opinion pieces and so can be considered unbiased.

There has been some evidence against the use of Bitcoin, such as being used for illegal activity by criminals. An article from Eitan Azani and Nadine Liv suggest this point as their research report suggests that Bitcoin are transactions without systemic intercession such as PayPal but goes on to demonstrate that Islamic State had used Bitcoin to fund the struggle against the United States in 2012 in which four transactions took place. The criminal activity was a reoccurring theme in my research as displayed by Möser, Böhme and

Breuker who argued that Bitcoin had been associated with cases of investment fraud due to its design with "pseudonymous identities" (Public Keys). Foley, Karlsen and Putnin's paper considers the illegal activities that take place using Bitcoin. It has estimated that approximately one-quarter of all users, 25% and close to one-half of Bitcoin transactions (44%) are associated with illegal activity. The allied evidence found in these four sources does not surprise me given that the underlying architecture of Bitcoin of being decentralised has led to unintended uses of the currency for illegal transactions.

Foley, Karlsen and Putnins' findings seem reliable as Sean Foley is a lecturer of University of Sydney business school, Talis Putnins is a Professor in the Finance Discipline Group at UTS a member of the Quantitative Finance Research Centre, and Karlsen is a PhD student at UTS. Also, given that the Oxford university press published the article, this gives me the confidence to use and trust this work.

Azani and Eitan's work is relatively reliable given that some of their findings were from credible sources like the US Congress, a bicameral organisation of the Federal Government of the USA which allows me to trust and utilise their work.

Similarly, Möser, Böhme and Breuker's journal article seems a credible source considering that it is a study into money laundering tools with the use of Bitcoin which studies how Bitcoin transactions can be kept more anonymous through the use of "mixing services". This knowledge and expertise give me the confidence to base my conclusion on these sources.

It is the case that literature is arguing for encouraging the use of Bitcoin implying that Bitcoin's digital characteristics have been able to act as a solution to problems that arise from fiat currencies such as double-spending.

It is evident in Hurlburt, and Bojanova's article discusses the pros and negative aspects of Bitcoin and mentions how Bitcoins are transferred via a public key and private key cryptography. Hulburt and Bojanova seem to conclude that virtual currencies will "likely prevail on a global scale by engaging with the Bitcoin network. Furthermore, Hartwig Mayer's article considers the deeper mathematical aspect when transferring Bitcoin by relating to the underlying secp256k1 elliptic curves that correspond to cryptographic private and public keys. N. Mistry's work also coincides with this topic and explores the mathematical elements with Bitcoin such as how transactions make use of digital signatures.

Hulbert and Bojanova's work seems very reliable as Bojanova was a professor and program director of information and technology systems at the University of Maryland University College and Hulbert is the chief scientist at STEMCorp. Both authors seem to have expertise in the computing field and allow me to trust and utilise their work.

Mayer's article can be considered extremely reliable given that some of the findings were taken from some credible sources such as from the book "Elliptic Curve Cryptography" by the London Mathematical Society Lecture Note Series that was published by the University of Cambridge press. Mistry's work seems credible as some of his findings match that of the white paper by Sakamoto, which allows me to trust and use both authors' work and can be considered unbiased.

Dr Zeynep Gurguc and Prof William Knottenbelt's article seems to compare Bitcoin to the likes of gold stating that Bitcoin is similar to gold in the sense that it has a finite supply of 21m BTC and this would be mined and so has the features of gold. The article also provides a figure consisting of the similarities between government money, gold and Bitcoin and due to Bitcoin's finite supply, no central authority can "debase the value of Bitcoin", and this made the cryptocurrency more attractive to early adopters. Still, its exponential growth in popularity has caused unstable an unstable price.

The work of Dr Zeynep Gurguc and William Knottenbelt, Gurguc a research associate in the Innovation and Entrepreneurship Group and Knottenbelt is a Professor of Applied Quantitative Analysis in the Analysis, Engineering, Simulation and Optimisation of Performance group in the Department of Computing at Imperial College London. Their expertise in these areas makes me confident in basing my conclusion on this source as it seems highly reliable.

Olson and White's journal presents an alternative opinion as it discusses the lack of profitability of Bitcoin and Ethereum. The journal mentions the demand for cryptocurrency hardware has caused an increase in the price of GPUs (The RX570 specifically) and goes deeper into the increase of the network hash rate has made crypto mining less profitable for Ethereum. I wasn't surprised about the high use of energy due to mining due to the increase of "mining difficulty" and so more powerful hardware would be required that would still provide profitability by reducing electricity costs. Although it discusses the profitability of Ethereum, I can use their findings to base a conclusion for Bitcoin as the literature I have read suggest they both operate similarly.

4 Methodology

I read a large volume of secondary research as it was challenging to carry out active primary research for this topic, given that it centres around regulation and concept of Bitcoin. I have gathered a broad range of sources that provide credible and detailed arguments, allowing me to use them in my conclusion with confidence. Before choosing my sources, I read and scrutinised over fifty articles surrounding the topic and finally based my decision of which to take forward on those which could best hold their ground against counter-arguments. These tended to be, though were not exclusively, articles from academic journals. This initial work had allowed me to develop the final working title, and many articles suggested the broad details about how Bitcoin transactions worked although not at a profound level (Only going into essential public and private key cryptography)

When beginning to learn more about Bitcoin, I watched some educational documentaries like "Bitcoin: Beyond the bubble" which provided a basis of knowledge of the currency. My local library became a useful tool when sourcing articles as most of my research was found online through sources like JSTOR, available at the library. These enabled me to read a section of academic journals surrounding the topic. As I was gathering the most reliable sources, I came across one stepping stone which was to obtain a login to JSTOR, but this was not possible, so I had to download the articles from the library's computers. Obtaining articles this way was languid as I had to individually download each article and upload them on to the cloud to allow for annotating at home. While this was quite troublesome, to begin with, I was able to use Google Scholar, which provided some useful articles so that I could still gather and annotate resources while at home. I had used specific search terms such as "Bitcoin uses" but later added more advanced terminology like "proof of work", "SHA 256", "secp256k1" and "elliptic curves". By using these search terms, I was able to identify articles that directly relate to my working title.

I am taking this into account. I am confident in my sources as I have chosen the most reliable articles from my reading. However, I think it would have been useful to have more evidence of the profitability of Bitcoin pre-peak price, but it wasn't as popular at the time, so only a few journals were published before. Despite this, I can still expect to draw a detailed conclusion with the research that I have already acquired.

5 What is Bitcoin?

Bitcoin is a decentralised cryptocurrency that was created by Satoshi Nakamoto in 2009 after the financial crisis of 2008. The currency seemed to be used as an investment rather than a currency, so it seems many just chose to trade with it, but many do not know how the currency works. As a result of its decentralised nature, Bitcoin relies on miners on its network to verify transactions (mine) which involves doing mathematical calculations, the miner who first solves it using the power of their computers would receive Bitcoins as a reward. These verified transactions belong in the blockchain, which is a collection of all the transactions that have taken place. All nodes on the Bitcoin network would have an updated blockchain as miners are verifying transactions. Transactions are made by using the digital signature algorithm where a user's public address is generated from their private address, and the receiver would be able to verify that the sender's public address can only exist from that private address. Bitcoin has this seemingly cycle where it is self-sufficient as long as miners receive some payment to mine Bitcoin.

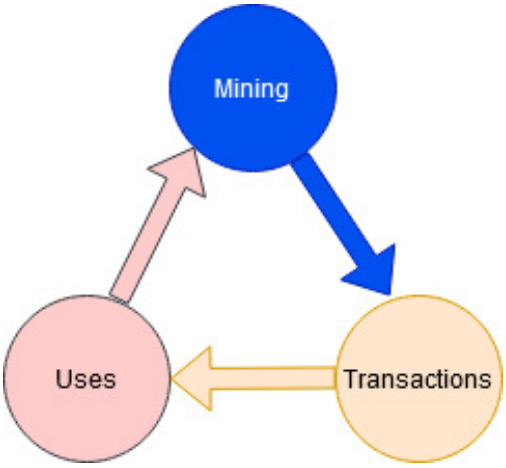

Figure 1: The Bitcoin Cycle

5.1 How Bitcoin is mined

The cryptocurrency can only exist due to mining which it is the process of verifying transactions and attempting to produce a valid hash. Satoshi Nakamoto had deduced a white paper that denoted a proposal of a new cryptocurrency that contained the concept and its workings. In his white paper, Nakamoto illustrates a proof of work chain and lists that the network "Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash[1]" In essence, this is an underlying concept of Bitcoin that prevents hackers from modifying the blockchain. I shall try and express a detailed abstraction of Nakamoto's proposed system which are the deeper workings of "mining". Mining makes use of a Merkle tree.

[1]Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. 2009. URL: `http://www.bitcoin.org/bitcoin.pdf`.

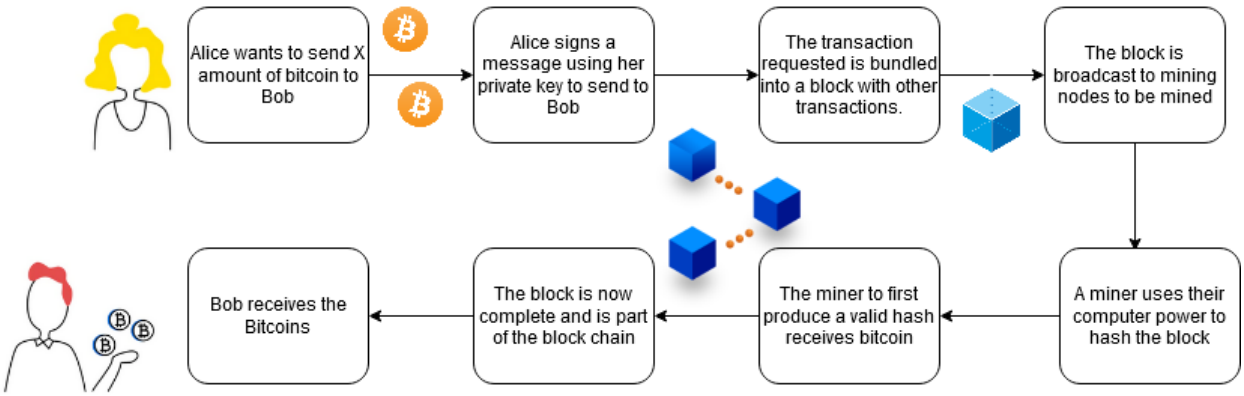

Figure 2: The process of Mining

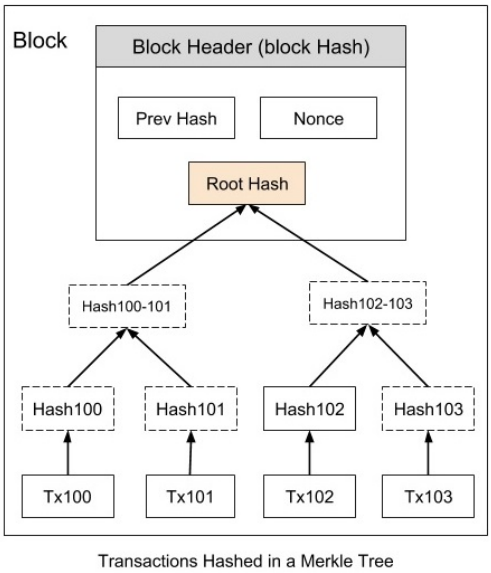

Figure 3: Merkle Tree

Let's consider figure 3, which illustrates an extremely simplified diagram of mining containing a Merkle tree in which the root is inside the block header. It is very similar to a typical champions league pyramid diagram. When a node on the Bitcoin network "mines" Bitcoin, in the simplest terms, we are verifying transactions that are saved in its memory pool[2] and attempting to produce a valid hash. At the bottom of our Merkle tree, the "children" of the tree consists of four transactions (in practice there would be hundreds) as denoted by "TxXXX". The transactions pair up and then hashed (to hash something is to take an argument, i.e. your input which would be placed in an algorithm and would give you a value which is the output and in the case of SHA-256, the value would always be 64 characters long) using SHA-256 repeatedly until we get to the root hash which is in the block header. The block header contains the root hash, the previous hash and the nonce. A nonce is a number that increments (1,2,3...) until the miner produces a valid hash. Now I shall consider the proof of work, i.e. mining is running "computer cycles producing additional

[2]Zeynep Gurguc and William Knottenbelt. "Cryptocurrencies: Overcoming barriers to trust and adoption". In: *Retrieved from Imperial College London website: https://www. imperial. ac. uk/media/imperial-college/research-centres-andgroups/ic3re/cryptocurrencies–overcoming-barriers-to-trust-and-adoption. pdf* (2018).

numbers of zeroes[3]". The reward for producing the correct hash (or in simpler terms, solving a "puzzle") is 12.5 BTC every ten minutes to ensure that the valid hash isn't found too quickly otherwise the difficulty (which is a target value generated in which the miner must find a hash value below this value) must be adjusted.[4] At the time of writing, the current reward is 12.5BTC. The previous hash is a hash value of the previous block which is in the block header; it is almost impossible for a hacker to modify the transactions on the Bitcoin network as this would completely change the hash value hence the inability to generate or copy more Bitcoins without mining directly. This technology is the underlying workings of Bitcoin as, without mining, there would be no one to process transactions; therefore there would be no Bitcoin, and the use of Merkle trees makes the system tamper-proof.

5.1.1 Why Mine?

Users of the currency cannot merely create 100 Bitcoins, and the currency retains its value as it relies on mining where specific nodes on the network use some of their processing power to verify transactions by solving a mathematical calculation. The node that successfully solves the mathematical calculation first would receive Bitcoins as a reward. Bitcoin has this seeming cycle which seems to be self-sufficient, but there is a Bitcoin cap of BTC 21m,[5] which would mean that there would be no monetary incentive for miners when this occurs, and this could ultimately end Bitcoin.

Bitcoin can only exist if miners continue to mine using their computational power in exchange for some Bitcoin. As we know, Bitcoin is a decentralised currency, as mentioned by Paul Vigna, who claims that Bitcoin has meant a "whole layer of banking bureaucracy is removed".[6] Instead of having a bank to get involved in monetary transactions, Bitcoin is dependent on miners to verify transactions, and in turn, this prevents "chargebacks[7]" and the ability to fraudulently "copy" more Bitcoin. Diving a little deeper, you may be questioning how we can "generate" more Bitcoin; when a miner produces a valid hash, they receive some Bitcoin as a reward and the transaction fees. Their hashed block would be relayed to other nodes on the Bitcoin network to verify this and add it to their copy of the blockchain. The miners are incentivised to mine Bitcoin due to the 12.5BTC reward as well as the block reward. They would also receive the fees attached to the transactions of that block. A miner produces the correct hash approximately every 10 minutes.[8] Aforementioned is the interval at which Bitcoins are created on average.

5.1.2 How much the miner would receive

To gain a greater understanding, I shall use an example as follows.

Suppose we had a block containing 1000 transactions and let's say that each of these transactions had a transaction fee of $60. The miner who can produce the valid hash would get:

$$\$60,000 + 12.5 \times \$16000 = \$260,000$$

(12.5 is derived from the current block reward, and $16000 is derived from the current price for one Bitcoin at the time of writing).

Of course, this does not take in to account the cost of mining due to the incredibly high computational

[3] G. Gilder. *Life After Google: The Fall of Big Data and the Rise of the Blockchain Economy*. Gateway Editions, 2018. ISBN: 9781621576136. URL: https://books.google.co.uk/books?id=4HwoDwAAQBAJ.

[4] Donald MacKenzie. "Pick a nonce and try a hash". In: *London Review of Books* 41.8 (2019), pp. 35–38.

[5] Rituparna Ghosh, Khondoker Haider, and Pedro Kim. "Bitcoin or Ethereum?" In: ().

[6] P. Vigna and M.J. Casey. *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. St. Martin's Publishing Group, 2015. ISBN: 9781466873063. URL: https://books.google.co.uk/books?id=Kv8CBAAAQBAJ.

[7] Jonathan B Turpin. "Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework". In: *Ind. J. Global Legal Stud.* 21 (2014), p. 335.

[8] Andreas M Antonopoulos. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

power required. Furthermore, the number of Bitcoins a miner would receive would fall as a result of "halving" (I wish to explain this later).

5.1.3 Longevity of Mining

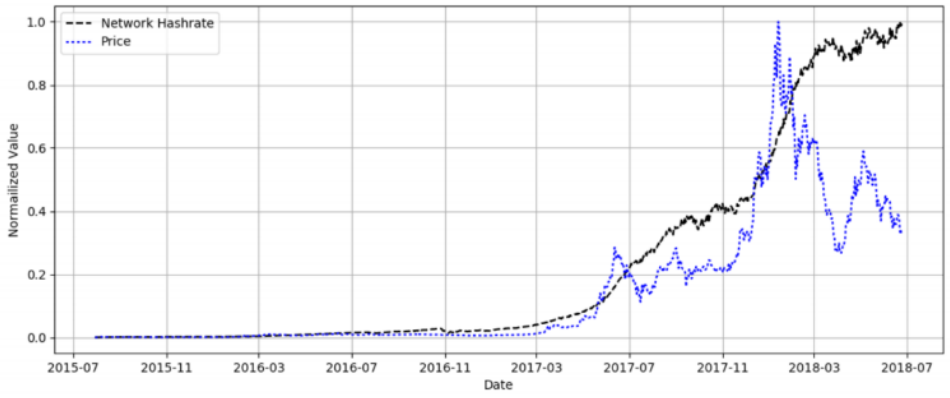

Figure 4: Alternative Cryptocurrency - Hash Rate vs Price

Mining is not sustainable due to halving and increasing hash rate. "Halving" occurs in Bitcoin every four years in which the block reward (as the word suggests) halves, and it is estimated that by 2048, the reward would only be 0.0125BTC for producing a valid hash. If we consider the profitability of a similar currency (As seen on Figure 4), Ethereum, there is evidence to suggest that mining strategies seemed to have worked for only five months after the currency was born before it became unprofitable due to the rapid growth of the network hash rate which has meant that difficulty has increased. It has caused an increase in costs[9] to be profitable. However, in the case of Bitcoin, there is a reduction in rewards as well due to halving.[10] Halving essentially means that Bitcoin would have little to no value, and due to the evidence by Olson, it seems that this would encourage Bitcoin owners to hoard as fewer Bitcoins generate which would mean that there would be little transactions. It seems that miners would be discouraged to process transactions due to the reduced reward for processing a block which means that Bitcoin would become worthless as there would be no way to verify transactions which would end Bitcoin due to its self sufficient and decentralised nature.

5.2 Transactions

5.2.1 Elliptic Curves

Before I discuss how transactions work in Bitcoin, I wish to introduce elliptic curves where someone can be able to create a public address from their private address. An Elliptic Curve over the $\mathbb{R}$ is a curve in a two dimensional plane whose points satisfy the *Weierstarss Equation*.[11] The *Weierstarss Equation* is an Elliptic Curve defined by $\mathbb{F}$ consisting of the set of points(x,y) that satisfy the general equation together with a single element O known as the infinite point.

[9]Sterling Olson and Reilly S White. "Mining Digital Gold: Boom or Bust for organic growth in Cryptocurrency mining operations". In: ().

[10]Miles Carlsten et al. "On the instability of bitcoin without the block reward". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 2016, pp. 154–167.

[11]Benjamin K Kikwai. "Elliptic curve digital signatures and their application in the bitcoin crypto-currency transactions". In: *International Journal of Scientific and Research Publications* 7.11 (2017), pp. 135–138.

Making use of elliptic curves relates to the Elliptic Curve Discrete Logarithm Problem (ECDLP). Bitcoin makes use of elliptic curves for creating digital signatures in transactions (which I shall discuss later). An elliptic curve has a general formula:[12]

$$y^2 = x^3 + ax + b$$

where a and b are curve parameters

This is where I shall now consider the ECDLP which relates to elliptic curves.[13] Bitcoin uses elliptic curves to derive a public key from a private address and is similar to that of the Diffie-Hellman encryption.

$$k = ga(Modn)$$

where a = the private address and g = generator point and n = a large prime integer

Where g is the generator point or some point on the elliptic curve, but it is different to Diffie-Hellman encryption in the sense that EDCLP adds g to itself a number of times and it is secure as we wouldn't know which two points were added to find the third point. To further my point, I wish to use a diagram below.

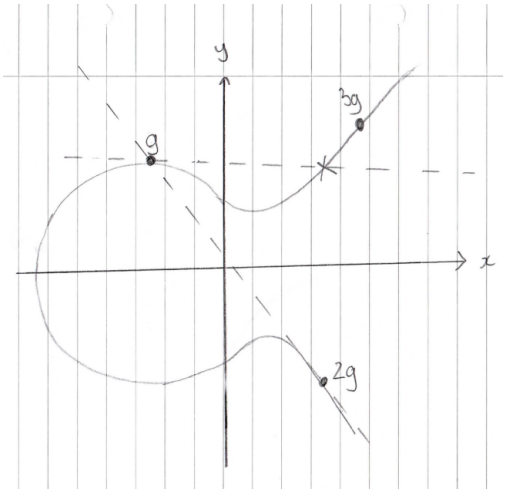

Figure 5: Elliptic Curve

$$g + g + g... = ag = aG$$

Figure 5 is my illustration of an elliptic curve. Point addition is the process in which we take tangents to the point of g and where the tangent intersects on our curve is reflected and denoted as 2g so we end up with some multiple or "addition" of g and eventually we would get back to where we started from but not after a long time as it cycles around the curve. To demonstrate this, I shall consider the point g, and I can add it a-times to itself to get the point on an elliptic curve.[14] Someone else won't be able to find out what our private address is from how many multiples of gs I have and the point on my curve. As Bitcoin makes use of elliptic curves, no one would be able to calculate what my private address (as denoted as a) was as we use point addition using our generator point and this would cycle around the curve. This process is seemingly random which makes it computationally impossible for some person to extract our private address as someone wouldn't be able to know which points I had used to get to a certain point as it is an incredibly

[12]Joseph H Silverman. "An introduction to the theory of elliptic curves". In: *Brown University. June* 19 (2006).
[13]Hartwig Mayer. "ECDSA security in bitcoin and ethereum: a research survey". In: *CoinFaabrik, June* 28 (2016), p. 126.
[14]Nitin N. "An Introduction to Bitcoin, Elliptic Curves and the Mathematics of ECDSA". in: ().

tricky process to reverse and this is known as the ECDLP.

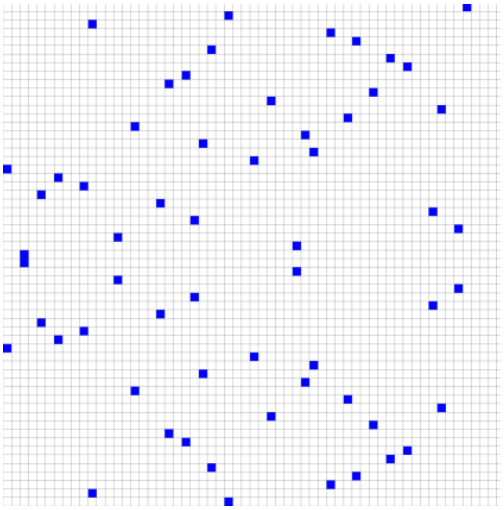

Figure 6: Elliptic Curve on an F59 Finite Field

Figure 6 is when point addition on an elliptic curve is done multiple times and makes it computationally tricky for someone to work out my private address. Performing elliptic point addition is easy, but reversing the process is computationally demanding since there is no point subtraction.[15] The fact that this discrete logarithm problem is very secure as someone won't be able to discover our private address from our public address so this means that no one else can access A's funds. As long as A doesn't lose their private key, they would always be able to find their public key as they are both mathematically linked, but this is not possible vice versa. The use of elliptic curves is one of the fantastic workings of Bitcoin cryptography. This irreversibility provides the basis of the Elliptic Curve Digital Signature Algorithm (ECDSA),[16] and I discuss how elliptic curves link with ECDSA in the next section.

5.2.2 How Bitcoin is transferred

I now wish to consider how Bitcoin is transferred. Bitcoins transactions use public key and private key cryptography.[17] Bitcoin makes use of Secp256k1 which refers to the parameters of the elliptic curve used to create a public address from a private address. Secp256k1's form is:

$$y^2 = x^3 + 7$$

In mathematical terms, we have a cubic equation.

$$y^2(MODn) = x^3 + 7(MODn)$$

The generator point in compressed form is = 0279BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798[18]

[15] N, "An Introduction to Bitcoin, Elliptic Curves and the Mathematics of ECDSA".
[16] Arnt Gunnar Malvik and Bendik Witzoee. "Elliptic curve digital signature algorithm and its applications in bitcoin". In: (2015).
[17] George F Hurlburt and Irena Bojanova. "Bitcoin: benefit or curse?" In: *It Professional* 16.3 (2014), pp. 10–15.
[18] N, "An Introduction to Bitcoin, Elliptic Curves and the Mathematics of ECDSA".

and the finite field is defined as:

$$n = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

A transaction would contain the number of Bitcoins to be transferred and a transaction unique digital signature. The receiver of the Bitcoins would give out their public key (also known as the Bitcoin address) so that we would know which address to send the Bitcoins. to[19].[20] However, a problem that arises is how do we know that we are spending our Bitcoins and not someone else's? I now wish to explain the digital signature algorithm:

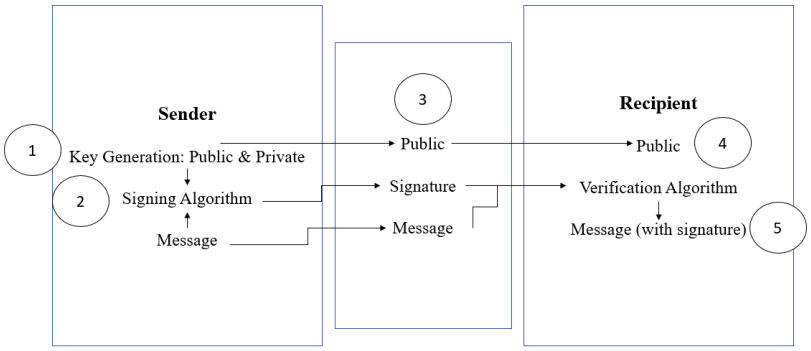

Figure 7: Bitcoin transaction

To create a digital signature, we make use of elliptic curves. Still, in this case, this ensures maximum security as it introduces randomness as each signature of a transaction is entirely different. First, we use key generation that would sign our message.

An Elliptic Curve Digital Signature Algorithm (ECDSA) key pairs are associated with a particular set of domain parameters on an Elliptic Curve. Let's assume that A's key pair has associated Elliptic Curve domain parameters:[21]

$$D = (q, FR, a, b, G, n, h)$$

To generate our private key and public for the transaction we do the following:[22]

1. Select some random integer d in the interval $[1, n-1]$
2. Compute $Q{=}dG$
3. A's public key is Q, and their private key is d

At the moment we have A's public address by multiplying some random number by the generator point to get a public key. We must now use these keys to create a digital signature.

Now D has the associated pair (d, Q). Let m be the message we wish to sign. Creation of the digital signature:

[19]Hurlburt and Bojanova, "Bitcoin: benefit or curse?"
[20]Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*.
[21]Kikwai, "Elliptic curve digital signatures and their application in the bitcoin crypto-currency transactions".
[22]Don Johnson, Alfred Menezes, and Scott Vanstone. "The elliptic curve digital signature algorithm (ECDSA)". in: *International journal of information security* 1.1 (2001), pp. 36–63.

1. Select a random integer k where $1 \leq k \leq n-1$
2. Compute kG = (x_1, y_1) and r=$x \ mod \ n$, if $r = 0$ go back to step 1
3. $k^{-1} \ mod \ n$
4. e = SHA-1(m)
5. $s = k^{-1}(e + dr) \ mod \ n$. If s=0, go back to step 1
6. A's signature for m is (r, s)

We have now generated a digital signature. Bitcoin transactions make use of outputs which refer to the transaction splitting into batches; an example was if A had 0.1 Bitcoins and A wanted to send 0.015 Bitcoins to B then the batch is split up, and two destinations addresses, 0.0845 Bitcoins would go back to $A's$ address and 0.015 Bitcoins to B (As displayed in figure 8). The inputs do not equal the outputs due to the $0.005 transaction fee taken by miners.[23] On the recipient end, they would use a verification algorithm which is all good if the transaction hasn't been tampered with as it proves that the signature can only exist from the correct private address.

Verification Algorithm:[24]

1. Verify that r and s are integers between $[1, n-1]$
2. Compute e =SHA-1(m)
3. $w = s^{-1} \ mod \ n$
4. Compute $u_1 = ew \ mod \ n$ and $u_2 = rw \ mod \ n$
5. Computer $X = u_1G + u_2Q$ If X=0 then reject the signature. Otherwise compute $v = x_1 \ mod \ n$
6. Accept signature if $v = r$

The general idea of the signature verification is to recover the point v using the public key and check whether it is the same point r that was generated randomly during the signing process. If it is the same, then the transaction is successfully authenticated; otherwise, the recipient would know if the transaction had tampered.

The reason why we use signature algorithms is that A can say they are spending their Bitcoins and not someone else's. ECDSA shows that we know the private address from a public address and this shows that we own some amount of Bitcoins based on if we know the private address in which the outputs are locked to.[25] It is also an extremely secure way of sending Bitcoin as each transaction has a unique signature, and only my public key in the transaction is made public.

[23] N, "An Introduction to Bitcoin, Elliptic Curves and the Mathematics of ECDSA".
[24] Johnson, Menezes, and Vanstone, "The elliptic curve digital signature algorithm (ECDSA)".
[25] Malte Möser, Rainer Böhme, and Dominic Breuker. "An inquiry into money laundering tools in the Bitcoin ecosystem". In: *2013 APWG eCrime Researchers Summit*. Ieee. 2013, pp. 1–14.

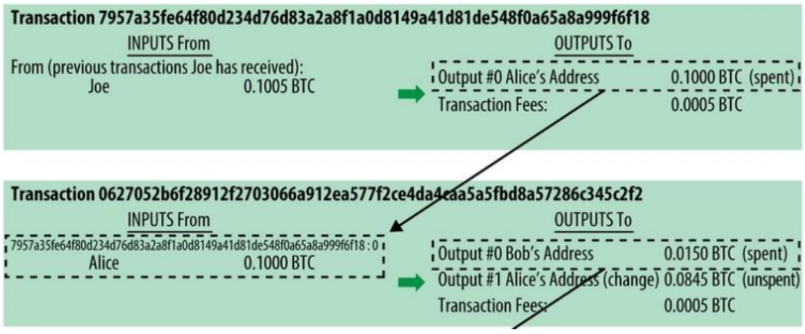

Figure 8: Bitcoin "Batches"

5.3 Uses of Bitcoin

5.3.1 Illegal Activity

We now have to consider the unintended uses of Bitcoin as a result of Bitcoin's decentralised nature. Bitcoin is used for online transactions as a medium of exchange and investment. The concept of Bitcoin, which makes use of the blockchain, has meant that criminals have access to fund illegal activity or allow the usual consumer to stay somewhat undetected on the government's radar. Bitcoin is transferred from one user to another without systemic intercessions, such as eBay or PayPal while relying on a decentralised system; and as we know, the network cannot be hacked. There have been some known cases in which Bitcoin had been used to fund ISIS in which a Bitcoin address was published on the dark web that followed the terrorist attack at the Bataclan theatre in Paris, France on November 13, 2015. A value of $3m was found on one wallet, and supposedly these helped fund their operations.[26] These statistics show that Bitcoin cannot be a reliable form of currency as it allows extremists to get funding by just merely publishing their Bitcoin address (public key) as the currency can not be monitored.

Furthermore, Bitcoin is heavily used on the dark web and cover a wide range of activities including sales of illegal goods, drugs, and weapons; assassinations; Ponzi schemes; money laundering; illegal mining; unlawful gambling and outright theft.[27] About 25% of Bitcoin users who use the currency and almost half of the Bitcoin transactions were for illegal activity. Around 36m transactions annually are illegal, with a value of $72b.[28] The evidence illustrates what type of people use Bitcoin and the scale of illegal activity that is associated with Bitcoin. Bitcoin or any cryptocurrency for that matter only seemed to have transformed the black market into a black market "E-commerce". In essence, cryptocurrencies seem only to facilitate the crime when either the buyer purchases a rifle or the seller receives the Bitcoin to increase their Marijuana farm supply. These are hazardous characteristics of a currency, and so Bitcoin should not be trusted. Indirectly, miners are profiting from potential illegal activity as they verify their transactions, and this is the seeming cycle of Bitcoin.

5.3.2 Blockchain

Bitcoin is a decentralised digital cryptocurrency that can maintain its value through its limited supply. The currency has a limited supply of 21 million Bitcoin,[29] and any government or organisation does not back

[26] Eitan Azani and Nadine Liv. *Jihadists' Use of Virtual Currency*. Tech. rep. International Institute for Counter-Terrorism (ICT), 2018. URL: http://www.jstor.org/stable/resrep17688.

[27] Hurlburt and Bojanova, "Bitcoin: benefit or curse?"

[28] Sean Foley, Jonathan R Karlsen, and Tālis J Putniņš. "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" In: *The Review of Financial Studies* 32.5 (2019), pp. 1798–1853.

[29] Michal Polasik et al. "Price fluctuations and the use of Bitcoin: An empirical inquiry". In: *International Journal of Electronic Commerce* 20.1 (2015), pp. 9–49.

it. Bitcoin seems to be used for trading and investors could buy more Bitcoin which would decrease the effective price for users and increases the market equilibrium price[30] thus making the value determined by supply and demand.

Bitcoin has a capped supply, and one cannot merely duplicate the currency due to the use of the blockchain. The blockchain is a public ledger which leaves a trail of all transactions, unlike cash, but this provides confidence within the cryptocurrency.[31] The blockchain relates to mining, as mentioned in 5.1, where the miner has unverified transactions in their memory pool, and transactions are in a block where the miner must try and produce a valid hash, this hashed block is then now part of the blockchain. The miner to produce a valid hash would receive Bitcoins as a reward, and this is the only way Bitcoin can be generated. The blockchain can maintain transactions, validate transactions and controls the generation of new Bitcoins. As a result of the blockchain, one cannot merely forge the currency, and so a user cannot duplicate Bitcoin. The confidence that Bitcoin provides as a result of the blockchain is one of the reasons why Bitcoin is used as a medium of exchange so can be used to buy goods and services due to the trust it provides as a result of mathematical hashing functions used in the mining process.

6 Conclusion

Security of Bitcoin is kept and built on trust as a result of Elliptic Curve Discrete Logarithm Problem makes it computationally impossible for someone to find a user's private key from their Bitcoin address. Users on the Bitcoin network have trust, and therefore Bitcoin wallets can be kept secure. Bitcoin does not forgive if A were to lose their private address as this is required to access funds, but this ensures that there are no backdoors to access A's funds.

The confidentiality kept between transactions is through using the Elliptic Curve Digital Signature Algorithm. Digital signatures are far more secure than in real life as everyone uses just one signature, but we know that in Bitcoin, the signature changes every time a user makes a new transaction and ensures authenticity on the Bitcoin network.

As criminals use Bitcoin, there would always be a dark impression when people use it as it can go under government radar so these activities are challenging to monitor so this could raise ethical concerns regarding its users. However, it is evident that there is trust with Bitcoin as a result of the blockchain which solves forgery, and it maintains its price through supply and demand.

Bitcoin makes use of mining, and this is the pinnacle of its existence. The use of Merkle trees which involve the previous hash, a nonce and the root header ensures that a hacker cannot modify the blockchain as it would require much effort to undo as the previous block would have its previous hash in its block. However, mining won't last forever due to it having a fixed supply and halving which dissuade miners so who would know what would happen when the currency system is Bitcoin capped. This could mean an end to the "Bitcoin Cycle".

[30] Susan Athey et al. "Bitcoin pricing, adoption, and usage: Theory and evidence". In: (2016).

[31] Huisu Jang and Jaewook Lee. "An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information". In: *Ieee Access* 6 (2017), pp. 5427–5437.

References

Antonopoulos, Andreas M. *Mastering Bitcoin: unlocking digital cryptocurrencies.* " O'Reilly Media, Inc.", 2014.

Athey, Susan et al. "Bitcoin pricing, adoption, and usage: Theory and evidence". In: (2016).

Azani, Eitan and Nadine Liv. *Jihadists' Use of Virtual Currency.* Tech. rep. International Institute for Counter-Terrorism (ICT), 2018. URL: http://www.jstor.org/stable/resrep17688.

Black, Carbon. *Cryptocurrency Gold Rush on the Dark Web.* 2018.

Carlsten, Miles et al. "On the instability of bitcoin without the block reward". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.* 2016, pp. 154–167.

Décourt, Roberto Frota, Usman W Chohan, and Maria Letizia Perugini. "BITCOIN RETURNS AND THE MONDAY EFFECT." In: *Horizontes Empresariales* 16.2 (2017).

Foley, Sean, Jonathan R Karlsen, and Tālis J Putniņš. "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" In: *The Review of Financial Studies* 32.5 (2019), pp. 1798–1853.

Ghosh, Rituparna, Khondoker Haider, and Pedro Kim. "Bitcoin or Ethereum?" In: ().

Gilder, G. *Life After Google: The Fall of Big Data and the Rise of the Blockchain Economy.* Gateway Editions, 2018. ISBN: 9781621576136. URL: https://books.google.co.uk/books?id=4HwoDwAAQBAJ.

Gurguc, Zeynep and William Knottenbelt. "Cryptocurrencies: Overcoming barriers to trust and adoption". In: *Retrieved from Imperial College London website: https://www. imperial. ac. uk/media/imperial-college/research-centres-andgroups/ic3re/cryptocurrencies–overcoming-barriers-to-trust-and-adoption. pdf* (2018).

Hileman, Garrick and Michel Rauchs. "Global cryptocurrency benchmarking study". In: *Cambridge Centre for Alternative Finance* 33 (2017).

Hurlburt, George F and Irena Bojanova. "Bitcoin: benefit or curse?" In: *It Professional* 16.3 (2014), pp. 10–15.

Jang, Huisu and Jaewook Lee. "An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information". In: *Ieee Access* 6 (2017), pp. 5427–5437.

Johnson, Don, Alfred Menezes, and Scott Vanstone. "The elliptic curve digital signature algorithm (ECDSA)". In: *International journal of information security* 1.1 (2001), pp. 36–63.

Kikwai, Benjamin K. "Elliptic curve digital signatures and their application in the bitcoin crypto-currency transactions". In: *International Journal of Scientific and Research Publications* 7.11 (2017), pp. 135–138.

MacKenzie, Donald. "Pick a nonce and try a hash". In: *London Review of Books* 41.8 (2019), pp. 35–38.

Malvik, Arnt Gunnar and Bendik Witzoee. "Elliptic curve digital signature algorithm and its applications in bitcoin". In: (2015).

Mayer, Hartwig. "ECDSA security in bitcoin and ethereum: a research survey". In: *CoinFaabrik, June* 28 (2016), p. 126.

Mora, Camilo et al. "Bitcoin emissions alone could push global warming above 2 C". In: *Nature Climate Change* 8.11 (2018), pp. 931–933.

Möser, Malte, Rainer Böhme, and Dominic Breuker. "An inquiry into money laundering tools in the Bitcoin ecosystem". In: *2013 APWG eCrime Researchers Summit.* Ieee. 2013, pp. 1–14.

N, Nitin. "An Introduction to Bitcoin, Elliptic Curves and the Mathematics of ECDSA". In: ().

Nakamoto, Satoshi. *Bitcoin: A peer-to-peer electronic cash system.* 2009. URL: http://www.bitcoin.org/bitcoin.pdf.

Olson, Sterling and Reilly S White. "Mining Digital Gold: Boom or Bust for organic growth in Cryptocurrency mining operations". In: ().

Polasik, Michal et al. "Price fluctuations and the use of Bitcoin: An empirical inquiry". In: *International Journal of Electronic Commerce* 20.1 (2015), pp. 9–49.

Silverman, Joseph H. "An introduction to the theory of elliptic curves". In: *Brown University. June* 19 (2006).

Turpin, Jonathan B. "Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework". In: *Ind. J. Global Legal Stud.* 21 (2014), p. 335.

Vigna, P. and M.J. Casey. *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. St. Martin's Publishing Group, 2015. ISBN: 9781466873063. URL: https://books.google.co.uk/books?id=Kv8CBAAAQBAJ.

Vranken, Harald. "Sustainability of bitcoin and blockchains". In: *Current opinion in environmental sustainability* 28 (2017), pp. 1–9.

Zimmer, Zac. "Bitcoin and potosí silver: historical perspectives on cryptocurrency". In: *Technology and culture* 58.2 (2017), pp. 307–334.