Bitcoin and Cryptocurrency: Myths and realities
Part 2: The Journey

This is a story of secret beginnings. A story of a brilliant idea, born of trying times. A tale of ups and downs, theft and despair, and triumphant comebacks. The story of an underdog, attempting to overcome the odds. No, this is not a fairy tale, but a real-live story of a…… currency. Yes, you read right – currency. This is the story of the beginning of Bitcoin and its journey through the years. And the best part? The story isn't quite finished... yet.

Now I'm sure many of you will know bits and pieces of this story that I'm about to begin: who is the founder of Bitcoin – Satoshi Nakamoto; why did he start this new currency – because of the 2008 financial crisis; how did he manage to fix the problem of double-spending that had been plaguing the digital currencies of the time – by using blockchain. But this is a mere summary of what is, quite truthfully, a saga. And as the saying goes, the devil is in the details… So, let's dive in!

Legend has it, that Satoshi Nakamoto first began working on the concept of Bitcoin in 2007, but the concept was only documented and presented to the public through his Bitcoin whitepaper in October of 2008. What was so special about this little old paper? Well, for one, it described the Bitcoin currency, but far more importantly it detailed the use of a new technology called blockchain so that the Bitcoin currency could never be copied, thus solving the problem of double-spending. About a week after the white paper was published the Bitcoin Project was registered on SourceForge.net – a website that was focused on the development and distribution of open-source software. A couple of months later, on January 3 of 2009, the Genesis Block was mined.

Got a few questions after reading that last sentence? I'm sure you do. So, let's get some answers. First off, what is mining? Well, if you read on, there's a whole section dedicated to mining, so we'll get to that in a while. For now, simply think of mining as a highly competitive, magical process that results in a miner (a user on the Internet) finding a Bitcoin – much like miners in the old ages finding gold nuggets! Secondly, what is a Genesis Block? That, I believe we should find out right now. The Genesis Block or Block 0 of the Bitcoin blockchain is the granddaddy of **every** other bitcoin block out there. How is this possible? Well, each new block that is created in the blockchain is connected to the one that came before it hence they all trace back to Block 0. Generally, the difficulty of mining blocks is so great that it requires a specialized graphics card but Satoshi Nakamoto was able to mine Block 0 by simply using a CPU since, at the time, the difficulty was set to 1 – much like the first levels of a computer game would start at a difficulty level of 'Easy'. Compare that with a difficulty level of

10,183,488,432,889 - which is the difficulty level of mining a block on the Bitcoin blockchain as at the time of writing this article – and you will perhaps begin to get an inkling of how the Bitcoin blockchain has expanded in the past decade or so.

Unlike in any of the blocks that came after, Satoshi Nakamoto decided to leave a little message in the code of Block 0. It read "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". This was a reference to an article that appeared in the London Times on the day that the Genesis Block was created, and it provided details on yet another bailout of banks by the British government. Although the message was brief and didn't give any more details as to why this article was important, many have interpreted this as a message from Satoshi, expressing his distaste for the banks and the middlemen and pointing to yet another reason why he created a more people-driven currency.

A lesser-known, yet interesting fact about the Genesis Block is that throughout the years, people have been treating it as a sort of wishing well. How so? Well, the original Genesis Block contained 50 Bitcoins in total and these have never been spendable – they have always stayed put. But since the beginning of the system people have been sending bitcoins to this address (yes this 'address' business **will** be explained later!) as a sort of tribute to the creator, in the process quite possibly making all of those coins un-spendable! The Genesis Block is, for many Bitcoin aficionados, synonymous with Satoshi Nakamoto, so in a way, sending Bitcoins to this address is a way for them to be closer to their Crypto God, the Creator of the Bitcoin Universe.

After establishing the Genesis Block, Version 0.1 of Bitcoin was released on January 9, 2009, and interestingly enough, in the release note of the software, Satoshi talked about the fact that the total circulation of Bitcoins would be 21 Million, meaning that there would only ever be 21 million coins in the Bitcoin ecosystem. Now, no one really knows why Satoshi decided on this exact figure, although as is common with everything related to Bitcoin, there are many theories floating around, and in this case, many of those theories tend to be highly technical.

To put things into perspective, let us say that the overall supply of Bitcoin can be divided into **three parts**. One is **circulating supply**, meaning the number of coins that are out in circulation, either being traded or held by users on the network. Certain cryptocurrencies have all their coins pre-mined, or release all the coins from the beginning of the project, or even mine the coins over time. Irrespective of which method is used, the circulating supply means whatever is available and circulating at present. Second is the **total supply** – referring to the number of coins in existence at the moment. This would include all created coins, whether in circulation or not. And thirdly, there is the **maximum supply** for a coin – meaning that if a number exists for maximum supply, then that particular coin will not be created again once it

reaches this number. According to CoinMarketCap, an aggregator website on cryptocurrency information, at the time of writing this article, the total circulating supply of Bitcoin stood at 17,907,850 – roughly 18 million coins. With a maximum supply of 21,000,000 coins, this means that we have a further 3 million coins to mine.

And this perhaps is the best place to delve into the question of mining. Now I do plan to get a little technical here, so those of you who don't want to clutter your brain with the details should skip right on ahead. For the rest of you brave souls, let us start with the basics. Simply put, mining is a way for you to earn cryptocurrency without having to buy it using money. Interestingly, when Bitcoin first started, mining one block would earn a miner 50 BTC (Bitcoin). In 2012, it was halved to 25 BTC, in 2016 again halved to 12.5 BTC and is expected to go down to 6.25 BTC in 2020. This halving process occurs once in every 210,000 blocks or roughly every 4 years. Right, back to the topic at hand - what do miners actually DO, when they mine? They are in essence being paid to work as auditors of the system. They are verifying past Bitcoin transactions to ensure that double spending has not occurred.

Imagine that you had a Rs.100/- note and a copy of that same note. If you were to go out and spend both those bills, someone taking the trouble to look at both bills carefully would know that the serial numbers on the notes are the same and hence would know that one of them is a fake. What miners do is somewhat similar to this. Currently, when a miner has verified 1MB (megabyte) worth of transactions to ensure there is no double-spending, then they are eligible for the reward of 12.5 BTC. Eligible – yes but not certain to receive it. Why? Well, in order to receive the reward, the miner has to meet two conditions. One is that he has to verify 1MB worth of transactions. But secondly, he has to be the *first* miner to get the right answer to a numeric problem. For those of you interested in the Bitcoin jargon, this process is known as '*proof of work*'. The good news here is that there is really no advanced mathematics involved in this process – it's just a lot of guesswork. What the miner is actually trying to do is come up with a 64-digit hexadecimal number called a 'hash', that is **less than or equal to a given target hash**.

Think of it this way. I have 4 friends to whom I say that I'm thinking of a number between 1 and 100 and they're required to guess what it is. My number is 25. A and B guess numbers above 25 and therefore are immediately out of the running. C guesses 24 and D guesses 20. They'd both be right because 24<25 and 20<25. No extra points for C just because he guessed closer! C and D are **both** eligible for the reward. This happens quite often in the Bitcoin network where multiple miners guess right and the decision for the reward is then based on which miner has verified the most transactions. So, transpose this problem of guessing the number to the Bitcoin network – now the number that the miners are guessing is not between 1 and 100 but a

64-digit number and instead of just 4 people guessing, there are now millions. There are pages and pages of more details for anyone interested in the subject of mining but since too much of a good thing is never advisable, I believe it is in our best interests to gently leave this topic here.

Now, considering the trying circumstances under which Bitcoin was created and the substantial amount of thought and effort put in to launching this currency, you would think that the first transaction of Bitcoin - when the currency was actually used to buy something in the real world - would be a momentous occasion, and the product being bought would be of considerable importance. You would be wrong! The first real-world transaction of Bitcoin was for 10,000 BTC in 2010 and it took place in Jacksonville, Florida when a programmer by the name of Laszlo Hanyecz used it to buy…… pizza. At the time, the exchange rate for BTC to USD put the pizza around $25, but at the height of its price of $19,783.06 per 1 BTC in 2017, this particular pizza was worth $197,830,600. Imagine that!

Bitcoin was not, however, always used to buy such innocuous things as fast food. As the value of Bitcoin increased over the next few years and more people started to join the network, the people who conducted dubious business on the fringes of society also began to take notice of this currency. One of the first of these was Ross Ulbricht, otherwise known as Dread Pirate Roberts, a drug trafficker - among other things – who founded Silk Road in 2011, a marketplace on the dark web. He worked on the simple ethos that people should be free to buy and sell whatever they want – regardless of minor complications such as legality. It is said that an estimated $1 billion worth of Bitcoin transactions took place on Silk Road before the FBI seized all the owner's assets and shut down the website in 2013. And in doing so, the FBI allegedly became one of the wealthiest Bitcoin owners in the world! And this is simply one example of how Bitcoins are being used for criminal transactions.

Features of Bitcoin

Much like any new invention on the planet, there are both good and bad uses of Bitcoin. But what allows this currency to be so versatile, so fluid? More to the point, how is it possible for criminals to use this currency for their transactions so easily, rather than, say, using dollars or euros. The answer may lie in the inherent features of Bitcoin.

There are a few major characteristics of Bitcoin that make people sit up and take notice. The first is that, as per its design, Bitcoin is **decentralized**. Satoshi Nakamoto built the Bitcoin network to be independent of any governing authorities, and it does exactly that by maintaining all of its transactions on a distributed ledger network - the Bitcoin blockchain - all over the world. There is no Central Bank to control the system, and no government to shut it

down. If all the nodes of the blockchain in a certain country *were* to be shut down, the rest of the nodes around the world would continue to keep the network running, thus making sure that the system doesn't operate on the whims of the all-powerful.

Because of its decentralized nature, and the encryption methods used for recording transactions, Bitcoins are said to be more **secure** than fiat currency kept in a bank account. How so, you ask? Well, money in a bank account is on potentially precarious ground – theoretically, banks can be susceptible to theft, hacks, financial crisis or asset seizures by the government. Comparatively, Bitcoin is less susceptible to all of these dangers.

In today's business landscape, banks and financial institutions would take pride in knowing all there is to know about their clients – their names, addresses, phone numbers, credit history, spending habits and more. But as privacy becomes a rare commodity in the present day and age, there emerges ever more frequently, the customers who are unhappy with this state of affairs. Bitcoin was tailor-made for these people. The Bitcoin wallet - the address at which a person's Bitcoins are kept - does not need to be linked to any sort of personal information, allowing the users to remain **anonymous**. The addresses are simply a bunch of complicated strings made out of numbers that are accessed using the owner's private encryption key. And so, you can simply send or receive Bitcoins without revealing your identity. While this is useful for people who simply don't want their finances to be tracked by banks, it has also become god's gift to criminals, allowing them to engage in criminal activities without anyone being the wiser.

However, this anonymity only extends up to a certain level. Every single transaction ever performed on the Bitcoin network is recorded on the blockchain. Although it may not show personal information, it is theoretically possible to see every transaction that has occurred using a single Bitcoin address and to also see how much money is in a particular wallet at a given time. But, as intended, it is almost impossible to tell who a Bitcoin wallet belongs to. So, although anonymity has been achieved, **transparency** has also been built-in.

As we can see, Bitcoin is a bit of a contradiction: it appears to be anonymous, yet its transactions are transparent for the world to see; the network's transactions are decentralized and stored in multiple locations around the world yet all of those transactions remain completely secure. Now at this point, if you were to be asked whether Bitcoin was a bad bet or the next best thing since sliced bread, I imagine it would be a little difficult to answer. We simply don't know enough - yet. But perhaps it would be helpful to list down some of the pros and cons of this cryptocurrency…. Let's begin:

Pro: Satoshi Nakamoto built Bitcoin with *freedom* in mind. Freedom from governing authorities, imposed fees and forced methods of transaction. I believe it is safe to say that Bitcoin has achieved this objective of freeing the people. Perhaps it has been a little *too* successful in this attempt since some dark web marketplaces will only accept Bitcoins as payment in order to keep the authorities unaware as to the questionable nature of their business transactions. Is this the kind of freedom that Satoshi had in mind when creating Bitcoin? Perhaps not.

Con: *Legality* has often been an issue that has plagued Bitcoin since its inception. The precise lack of a central authority which gives Bitcoin its freedom, also creates this issue of legality, since there really is no authority in the world to claim it as its own thereby legitimizing its existence and its rights as a currency. So, because of this fact, different countries around the world have been taking wildly differing stances on Bitcoin throughout the years. Some countries allow and encourage the use of Bitcoin while some have banned it and its entire community. The fact that Bitcoin appears to have a special appeal to the criminal classes is also a point that favors the factions who believe Bitcoin should be disallowed and outlawed.

Pro: Owning a Bitcoin wallet means absolutely no one can steal your money from your wallet without you knowing it, which promises *safety* for your funds. As a user, you can also take steps to protect your money with backup copies and encryption algorithms. This means that you, the user, is in *control*.

Con: However, being secure in the knowledge that the 1,000 BTC in your wallet today will also be there tomorrow, will mean nothing if you can't ensure the value of those 1,000 coins. And this decision is not up to the user - it depends on so many minute variables. Now, this may be true of other currencies as well – most currencies do display some form of ups and downs, but the sheer breadth of *volatility* displayed by Bitcoin during the past few years has made even the most risk-taking investors take a step back and think twice about their decisions. The price of Bitcoin has had a rollercoaster ride, going to all new heights simply to plummet almost to the ground straight afterward and such volatility is simply not a desirable trait in a currency looking to make its mark on the global economy.

Pro: Fiat currencies have always enjoyed portability but Bitcoin has taken it to a new level entirely. Since it is a digital format of money, users can place as many Bitcoins as they would like on a flash drive and simply carry it around wherever they go or even store it online.

Con: No matter how portable your money is, it's rarely useful if the money is not recognized wherever you're going. And this is Bitcoin's next biggest problem. A huge majority of the

businesses in the world are still completely ignorant of the existence of Bitcoin and hence has no concept of exchanging their goods or services for a cryptocurrency.

Pro: As we've seen earlier, double spending is not an issue for Bitcoin, so counterfeiting the currency is a non-issue. Therefore, users can rest assured that they are not being fooled into accepting money that has already been spent elsewhere.

Con: Although your money is secure, it is only spendable so long as you have the key to your wallet. The keys, which are basically unique alphanumeric passwords to the Bitcoin wallets are essential for the smooth operations of the wallet. Lose that and you've basically lost your wallet.

So, here we are, complete with a history lesson of how Bitcoin came to be and how it's been doing so far. We've talked about the good, the bad, and the ugly. So then, back to my question: is Bitcoin a bad bet or the next best thing since sliced bread? If you still don't know the answer to that question, well, you're not alone. It's been more than a decade since Bitcoin was introduced to the world and we still can't seem to agree – is it good or is it bad; is it black or is it white. But, like most things in life, Bitcoin falls somewhere in the grey. It *is* what you make of it. What we can be sure of is that Bitcoin is a currency of the people, *by* the people, and *for* the people. We must simply understand how to use it, wisely.

Author – Piyumi Dias

The views expressed in this article are those of the author's and do not necessarily reflect those of the Central Bank of Sri Lanka.