Bitcoin and Cryptocurrency: Myths and realities

The Beginning

Bitcoin, Blockchain, and Cryptocurrencies are the new phenomena of the 21st century. There is so much hype surrounding these subjects that it is almost impossible to ignore them and how they may affect our day to day lives. However, not all of us may be in the know when it comes to the maze of jargon surrounding Bitcoin. Blockchain, Distributed Ledger Technology, cryptocurrencies, Initial Coin Offerings; what does any of it mean? Are you feeling left behind when the 'techies' speak of block transactions, peer-to-peer networks, and crypto-assets? Were you one of those people who thought 'mining' simply meant digging the earth for minerals??

Well fear not, for many of us are in the same boat! Most of us are unsure of how to get ourselves some Bitcoins, or even if we really should! Some of us wonder how distributed ledgers even work and how blockchain could possibly be termed the technology of the future.

But this state of affairs is to be expected. With any new technology, there comes a learning curve, a passage of time where people make an effort to understand the new technology, how it works, its applications and most importantly, how it can be used to benefit themselves. However, it is imperative that we do not take too long to catch up with these new developments, lest the rest of the world leaves us behind.

So then, where to begin unraveling the mysteries of Bitcoin, Blockchain, and Cryptocurrencies….? Well, the simple explanation would be, that cryptocurrencies are a type of digital money that uses encryption for security purposes and that Bitcoins are a type of cryptocurrency which runs on a technology called blockchain…….. Seems a tad complex? I would agree. So, let's start with the basics first – cryptocurrencies. Or more appropriately, let's go back a little further to digital currencies, and its forefather - currency.

Simply put, currency is the system of money in general use in a particular country – I don't believe we can get any simpler than that. Digital currency, then, is a **type** of currency that is available in digital format, as opposed to the physical banknotes and coins that you and I are familiar with. This digital currency is also known as digital money, electronic money or electronic currency. But for our purposes, digital currency would suffice. Now, digital currency is a blanket term, used to cover all sorts of electronic money, including, cryptocurrencies. Therefore, cryptocurrencies are simply a variety of digital currencies but are considered special, since they utilize encryption techniques to ensure the safety of the currency, thus making them difficult to counterfeit. Sidebar: What is encryption? It is the process of converting information into a code, to prevent unauthorized access. However, not only are cryptocurrencies secure, but most of them are also decentralized, meaning they have no central authority – such as a

Central Bank – to control them. The pros and cons of this feature are endlessly debatable. But that is a different discussion for a different day.

Another feature of cryptocurrencies is that they do not require an intermediary to validate transactions. What kind of intermediaries validate transactions you ask? Why, banks of course. Each time you make a transfer of money to another person using your bank account, the bank is in fact, vouching for you and the availability of funds in your account. But cryptocurrencies require no such mechanism, hence is an alternative form of payment, allowing you to make payments directly to other people, without the presence of an intermediary. Theoretically, this opens up a whole new payment avenue for the average person: a much faster avenue than what is currently available. For example, sending money back to your family, instantly, without incurring heavy commissions would be a possibility.

So, here's what we have so far: Cryptocurrencies are a type of digital currency that acts as a medium of exchange between people, enabling direct payments between individuals. So far, so good. Now, to move on to the main event – Bitcoins. How do Bitcoins relate to the cryptocurrencies we've been talking about so far? Simple – Bitcoins **are** a type of cryptocurrency, in fact, most would agree that Bitcoins were the first cryptocurrency in the world.

Bitcoin was first introduced to the world in the year 2009 as a brainchild of Satoshi Nakamoto, who to this day remains anonymous. But, if he has a name, then he can't be anonymous, right? Wrong. Satoshi Nakamoto is a pseudonym – we don't know if he is in fact, a he, a she, or a they. In reality, it has been theorized quite widely, that Satoshi is a collection of like-minded people who decided that the answer to the 2008 global meltdown was a decentralized digital currency capable of making instantaneous payments. More on this later, but for now, let's return to the identity of Satoshi. While some deem him to be a group of people, others are convinced that Satoshi Nakamoto is a group of 4 companies: **Sa**msung, **Toshi**ba, **Naka**michi, and **Moto**rola. A rather farfetched theory suggests that Nakamoto is an anagram of "NATO amok", suggesting that the North Atlantic Treaty Organization had something to do with the creation of Bitcoin. Theories abound on the true identity of the creator of Bitcoin, some far less believable than others, however, the truth is, we don't really know who it is, for sure.

As to the reason why Satoshi decided to introduce Bitcoins to the world – many believe that a major contributing factor was the financial crisis of 2008. But what do Bitcoins and a financial crisis have to do with each other? The answer is liable to be a bit long-winded but bear with me as I attempt to explain.

During the olden days, when people didn't earn so much, their money was kept on their person or in their houses. But with more earnings came more risk. Thus, people wanted assurance for the safety of their money and decided to turn to banks to keep their earnings safe. Banks also

started attracting more customers by offering customers various options on their deposits. But, interestingly enough, when you deposit Rs.1000 with a bank, the bank is in fact, not required to keep the entirety of that Rs. 1000 with them. They are legally allowed to spend a certain percentage of that money, say 90%, and keep just the remaining Rs.100, just in case the customer requires some of their deposit back. Simplistically, if a bank has only this one customer, and he asked to withdraw more than Rs.100 at one time, the bank would not be able to comply. However, banks have thousands of customers, and they rely on the fact that realistically, not all of their customers will want all their deposits at any given time. So, for example, out of total deposits of a Rs.100 million, the bank will only keep Rs.10 million on hand, to settle its liabilities to depositors.

What do they do with the rest of the money? They invest and loan it out to their customers. And this is where our story ties into the financial crisis. Banks in the USA started giving out risky loans to their customers who had poor credit scores. And as one would expect, customers started defaulting on these loans. Having loaned out their deposits to customers who were no longer able to pay back the money, the banks found themselves unable to pay back their depositors and consequently collapsed and filed for bankruptcy. In addition to the risky loans, banks had also made some questionable investments that did not yield the expected payoffs, thus compounding the problem. Attempting to stop the landslide effect of the bankruptcies, the American government tried to bail out some of the sinking financial institutions. Now, here's the kicker – the banks lost the money that customers had entrusted them with, meaning that the customers would never get their money back. So, the government offering bailout money should be a welcome reprieve. But the money the government was offering was in fact, also the people's money, collected by way of taxes! A little like rubbing salt into a wound…

The government's actions, although a boon to failing financial institutions, were not well received by the general public. And because of the interconnectedness of the modern world, the events taking place in the USA were transmitted to the economies of other countries thus bringing the world economy to a standstill. Following the events of the crisis, people started demanding a currency that was not controlled by a central government or a central authority. The reason being that when people entrusted their money to banks, banks lost customer money and the government, as a stopgap, not only offered government money as bailouts but started printing more money, so that there would be more money available to the public, which had the adverse effect of reducing the value of money in circulation. Since the government had no upper limit on the amount of money they could print, there would always be a certain amount of uncertainty as to the value of people's money.

And here ends our long-winded story of how the financial crisis led to the birth of Bitcoin. People simply wanted a currency that was not controlled by the government and thus subject to its whims: Bitcoin had no central authority to control it. People wanted a non-inflationary

currency: Bitcoin had a limit on the number of coins that could be in circulation and a fixed rate at which new Bitcoins could be produced. People also wanted a system in which their money and trust did not need to be placed in an intermediary, such as a bank, where there was no guarantee that the bank wouldn't make bad investments and lose all their money: Bitcoin solved this problem by allowing users to directly transact with each other, in a peer-to-peer network.

So, it appeared that Bitcoin was the answer to many prayers at the time. But these problems had more or less been in existence before the financial crisis of 2008. There were also digital currencies in existence prior to the invention of Bitcoin. What then, made Bitcoin special? What made it unique and able to provide a solution to the many problems that were brought to the forefront because of the crisis of 2008? The magic of Bitcoin, was in fact, its solution to the double-spending problem. And now at this point, I believe it would be prudent to make yet another detour, to understand the concept of double-spending.

Precious metals and paper-based currencies have been used throughout history, for the purpose of conducting transactions. When these transactions are conducted, the person in possession of the currency must typically relinquish it in order to receive the goods or services being sold. Because the exchange of money is physical, there is no danger of the same currency being spent twice by the same party, for the simple reason that they no longer have possession of it. Conversely, with digital currencies, there is no actual physical money to relinquish when making a payment, thus giving rise to the problem of double-spending, which is when a person spends the same currency for two or more transactions. Before the advent of Bitcoin, this posed a major dilemma for digital currencies because each unit could be spent an infinite amount of times, thus giving each unit no real value.

In 2008, with the white paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto provided a unique solution to this problem – blockchain technology. In this paper, Satoshi went on to explain how financial transactions still depended on a trusted third party for validation in order to prevent double-spending and how that was no longer necessary with blockchain technology. The detailed workings of blockchain technology is a different article altogether, but suffice it to say that blockchain technology is basically a universal public ledger that records every single transaction to ever take place in the Bitcoin network. Each transaction is validated by 'miners' on the network before they are added to the blockchain, ensuring, among other things, that the currency has not been spent already. Miners on the network are rewarded for validations by awarding them with a small amount of Bitcoin. Thus, banks are not required and every transaction is verified to ensure that double spending does not take place.

So, here's what we know so far: the creator of Bitcoin was Satoshi Nakamoto who created the cryptocurrency as an alternative payment method, after the financial crisis of 2008. It was

created using blockchain technology and solves the problem of double-spending. Now, it appears we have a basis on which to understand the workings of Bitcoin.

Where do you keep your cash? In your wallet, I'd wager. Likewise, Bitcoins, the digital currency, is also kept in wallets. These are digital wallets that can be installed either on computers or mobile phones. Installing such a wallet will automatically create a Bitcoin address. This address can be given to people, much like a bank account number, so that they may make payments to you. These payments, or indeed any transactions utilizing Bitcoin are recorded in blocks in the blockchain, the shared public ledger, on which the Bitcoin network runs. The integrity and the order of the blocks within the blockchain are enforced using cryptography.

When a transaction occurs using Bitcoin, values are transferred between the Bitcoin wallets of the sender and receiver. Each time a transaction goes out of a wallet, the wallet uses an undisclosed piece of data called a private key to sign the outgoing transaction. This provides incontrovertible proof that the transaction originated from that particular wallet. This signature also prevents alterations of the transaction once it has gone out, thereby upholding the integrity of the transaction. All Bitcoin transactions are transmitted to the entire network and in a best-case scenario, can be confirmed within 10-20 minutes by the network's miners. Mining is a process through which pending transactions in the network are confirmed using a distributed consensus system and then incorporated into the blockchain. This is just a complicated way of saying that a certain majority of miners on the network must agree that this transaction is genuine in order for it to be confirmed.

Transactions awaiting confirmation are placed in what is termed a 'block'. These blocks are created according to very strict cryptographic rules that are verified by the network and help prevent previous blocks from being modified. Due to these rules, modification of a single block on the blockchain would lead to subsequent blocks on the chain being invalidated, making it simple to pinpoint unauthorized manipulations of the blockchain. Additionally, since a majority consensus is needed to validate a block, this prevents rogue individuals from simply inserting any kind of transaction into the blockchain.

So, as we can see, the mechanism through which the Bitcoin network conducts its business appears to be well thought out and secure. In fact, many people around the world thought so too, and as a result, the Bitcoin phenomenon has taken the world by storm. It was so successful, that an entire ecosystem has sprung up around it, from other cryptocurrencies following in Bitcoin's footsteps to currency exchanges especially set up to trade in cryptocurrencies. Newer cryptos such as Ethereum and Ripple have become so popular that they have begun to chip away at the huge market share that Bitcoin enjoyed in the earlier days. A major reason for this market erosion is that Bitcoin simply had not anticipated this massive adoption of the currency and therefore did not plan for transactions on such a mass scale.

Today, the Bitcoin network has become a sluggish behemoth that consumes more electricity in a year than the entire country of Switzerland and takes hours upon hours to verify a simple transaction. This could hardly be called a conducive environment for instantaneous peer-to-peer transactions. Therefore, when Bitcoin began to fall behind on its primary objective of rapid peer-to-peer payments, cryptos such as Ethereum and Ripple began to raise their heads. According to the CoinMarketCap website, a prominent cryptocurrency statistics aggregator, as of July 2019, the number of cryptocurrencies in the world amount to more than 2300 and their total market cap stands in excess of $266 Bn. Not too shabby for a concept launched just over a decade ago.

As a concept, Bitcoins are a wonderful idea, introduced to the world by an inspired inventor and adopted by the disillusioned masses. However, practically speaking, the Bitcoin boat, has a few gaping holes. This is not to say that the world has not benefitted from this endeavor – the ecosystem surrounding Bitcoin has proved itself beyond measure – especially with regards to blockchain technology. It is simply that even with the best of ideas, there is always room for some improvement!

Author – Piyumi Dias