International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Introduction to Cryptography

Bhavna Khosla

Grade XI

"Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value."

– **Eric Schmidt** (Google CEO)

The process of converting ordinary and plain text into unintelligible text and vice versa is known as cryptography. In this method, data is stored and transmitted in a specific form in order to make it available for only particular people to read and process. Its importance lies in the fact that it protects data from hacking and alteration, while making it useful for user authentication. Phil Zimmermann defines cryptography as "the science of using mathematics to encrypt and decrypt data". Bruce Schneier says, "Cryptography is the art and science of keeping messages secure."

Human beings organised themselves into tribes, kingdoms and groups as civilisations evolved over the years in history, which led to the emergence of thoughts pertaining politics and supremacy. This fueled the need to communicate secretly with one another, which in modern terms is known as cryptography. The usage of 'Hieroglyph' and 'Caeser Shift Cipher' have been excavated by historians. In the Second World War, most of the cryptography work was mainly for military purposes, in order to hide secret military information. The main purpose behind cryptography in the historical times was not to hide the message, but only to change its form in a way which would make it appear more dignified. Though the inscription was not a form of secret writing, it incorporated a transformation of the original text. Hence, it has been evidently seen that usage of cryptography was very popular in major early civilisations. Claude E Shannon known as the Father of Mathematical Cryptography, for he produced an article titled, "a mathematical theory of cryptography," which was released in 1949, four years later after it was written. His work inspired further cryptography research and his works have been cited as major influence by various cryptographers. Thus began modern cryptography, with the arrival of an encryption standard, development of a public key, hashing, cryptography politics and modern cryptanalysis.

The main difference between a traditional fiat currency and a cryptocurrency is that cryptocurrencies are decentralised in nature and are a global currency, not confined to a single country, and not backed by the central government. This is one of the advantages of using cryptocurrencies, as they are unaffected by the interfering governments. Otherwise, they are essentially the same- a medium of exchange used to store and trader value. There is a possibility of a merger between conservative banking and cryptocurrencies. Nonetheless, while cryptocurrencies will have to comply with the rules and regulations established, the banks will have to learn to play the new game strategically. A more liquid and fluid role has to be adopted by ditching the traditional operation methods.

There are four goals a modern cryptographic system needs to attain. These include CONFIDENTIALITY, which means that unauthorised persons cannot access information; IDENTIFICATION AND AUTHENTICATION: Information needs to be authenticated and identified before its exchange; INTEGRITY: No information can be altered for modification purposes and any alterations must be detectable; and NON-REPUDIATION: which is essential for the provision of legitimate and traceable digital transactions. These services offered by cryptography have enabled the conduction of business over computer networks in an efficient and effective manner.

However, there are other issues that affect the efficiency of the usages of information. This includes the difficulty to access a highly encrypted, authentic and digitally signed information for even a legitimate user at a crucial time, as the network can be hacked and rendered non-functional by an illicit user. One of the fundamental aspects of information security, higher availability, cannot be ensured through the use of cryptography. Another fundamental information security of selective access control cannot be realised. Cryptography does not guard against the vulnerabilities and threats that emerge from the poor design of systems, protocols, and procedures. Cryptography comes at a cost which is in terms of time and money. And finally, the security of cryptographic technique is based upon the computational difficulty of mathematical problems, which render the technique vulnerable. The biggest limitation is of course the fact that the internet is anonymous, so it is logical that crypto currencies are often used for illicit activities. Nevertheless, many cryptocurrencies use the Blockchain technology for identification which leaves a history of transactions - making it convenient for the police to track down illegal people. Just like any other currency, crypto currencies can be used for shady purposes. Statistics reveal that 0.5% of bitcoin transactions have taken place on the 'dark web' in 2019.

The most popular cryptocurrencies include Bitcoin (Market price: $ 39,896.90), Ethereum (Market price: $2,845.96) and Ripple XRP (Market price: $1.05).*

*The Market Prices outlined above are as of 26th May 2021.

History

"I think the fact that within the bitcoin universe an algorithm replaces the functions of [the government] ... is actually pretty cool. I am a big fan of Bitcoin."

– Al Gore (45th Vice President of the United States)

Pre-History

David Chaum and Dr. Stephen Brands were the pioneers of cryptography. Cynthia Dwork and Moni Naor‘s proposal in 1992 of adding value to the solutions of algorithmic problems was redeemed by Adam Back‘s hashcash developed in 1997 for spam control. Many cryptographers followed suit which paved the way for thousands of other cryptocurrencies like Bitcoin for financial activities.

Creation

Bitcoin was introduced to the world in the midst of a financial crisis by Satoshi Nakamoto who is assumed to be a pseudonymous person or persons who conceived the bitcoin idea in 2008 and subsequently set it up formally in 2009. The domain name ’bitcoin.org ‘was registered on August 18, 2008 with Nakamoto posting a paper with the words ’Bitcoin: A peer-to-peer Electronic Cash System ‘to a cryptography mailing list on 31st October of the same year. In the aforementioned paper, Nakamoto described Bitcoin as a decentralised digital currency. The word decentralised implied that there wasn‘t any single custodian of the currency instead it was a ledger of financial transactions which could be stored by anyone in the softwares. To summarise, it meant that coins could be sent on the peer-to-peer system with “NO INTERMEDIARIES LIKE BANKS INVOLVED”.

When it is said that ”NO INTERMEDIARIES LIKE BANKS ARE INVOLVED”, it does not imply that Bitcoin was designed in order to eradicate the need of banks or to undermine the government. It was simply to the replace the traditional payment systems to avoid the problems that these created. A number of schemes emerged in order to facilitate internet transactions of electronic money (digital cash), however the majority of transactions were made by the way of credit cards. A Peer-to-Peer (P2P) payment system, the most popular one being PayPal, was developed in order to allow individuals to transact directly and provided a mechanism to deal with banking institutions directly. These peer to peer processing networks have the capability to stop illegal transactions and therefore act as regulatory enforcement points. They, hence act as Financial gatekeepers-either through proactive actions or upon the receipt of court orders. And Internet payment intermediary could be used to eradicate undesirable activities occurring through the internet. In the case of bitcoin, the need of the intermediary was removed. This enabled its ability to have a true peer to peer electronic cash system. This can be effectively illustrated with the help of an example. Let's assume an entrepreneur decides to open an online business of handmade clothing from her native place. She wants people from all over the country to have access to the high-quality goods, so she seeks out and all country shipping company for delivery purposes. However if she used a block chain-based smart contract, she wouldn't need a middleman to set up the relation between her and the shipping vendor. Because the details of the agreement have already been recorded on the block chain, the encryption keys which both the parties have allowed them and their authorised users to view the contracts at any given time. Everyone involved has thus save their valuable time and money because of the eradication of the need to coordinate or pay the intermediary service. Middlemen do provide value, however it is not an unknown fact that the more people involved in the process, the longer it takes to complete and the more expensive it is. Any additional layer in a transaction is costly, unpredictable and variable. Thus, the elimination of the media release and the usage of Blockchain technology significantly reduces transaction costs and inefficiencies.

On 3rd January 2009, Bitcoin was launched with Nakamoto verifying the ’Genesis block of bitcoin ‘which successfully gave him 50 Bitcoins. At the outset, Nakamoto had mined approximately 1 million Bitcoins. Nakamoto ceased to participate in the network and passed the baton to Gavin Andersen, a developer who became the lead official at BitcoinFoundation, giving the bitcoin community its first official public face.

One year hence, the first Bitcoin transaction took place on 22 May 2010 when a Florida-based man ordered to Papa John‘s pizzas costing $25. He got them delivered to him for 10,000 bitcoins and essentially established the first real-world value of the Bitcoin which was 4 Bitcoins per penny. The vital moment has led cryptocurrency supporters to call May 22, the Pizza Day. Today that same transaction would value $114 million approximately.

A significant fragility in Bitcoin was seen on August 8, 2010 wherein the transactions weren‘t efficiently mined which let users create an unrestricted number of Bitcoins. This vulnerability was capitalised on 15 August of the same year. In a single transaction 184 billion Bitcoins or so were generated and sent to a pair of addresses. However, the transaction was configured in a short while and eradicated from the logarithm after the issue was resolved. Till date, this was the only considerable security inadequacy detected in the Bitcoin saga.

2011-2019

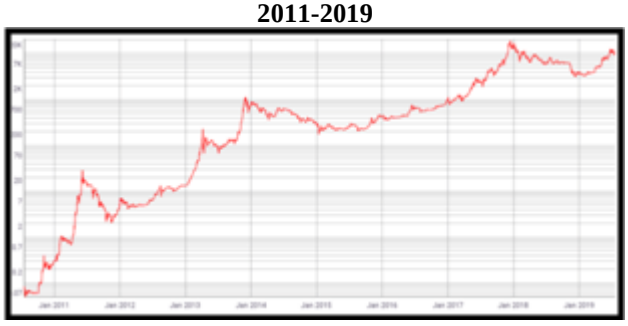


IMAGE CREDIT:
https://www.forbes.com/sites/ktorpey/2019/07/23/pantera-ceo-42000-bitcoin-price-by-the-end-of-2019-a-good-shot/?sh=113ecc445767

The first users of Bitcoin were black markets which included Silk Road, an online black market best known for sale of illegal drugs. Silk Road accepted Bitcoins as a mode of payment amounting to approximately $214 million. The values of Bitcoin started with $0.30 per bitcoin in 2011 and rose to $5.27 per Bitcoin in that year making a surge of almost 1655.90%. Bitcoin had rallied to a whooping $12.56 by the end of 2012 and during 2013 it now stood at $198.51 per Bitcoin. The significant spike made by Bitcoin ended in November 2013 at a price of $946.22 per Bitcoin.

In 2013, Bitcoin started with a mere $13.30 that rose to $770 per Bitcoin by 1st January, 2014. In March 2013, two independent chains were formed by the splitting of the block chain, which operated simultaneously. During this time Mt. Gox, a Bitcoin exchange based in Tokyo, Japan, temporary blocked Bitcoin deposits which led the prices to drop by 23%. In May 2013 accounts associated with the Mt. Gox were seized by United States authorities because Mt. Gox was not a registered money transmitter with FinCEN in the US. Later that year, US authorities seized ₿11.02 which marked the first time and agency of the government had taken into hold bitcoins. Chinese financial institutions were banned from using Bitcoins by the People's Bank of China on 5th December 2013 which caused the value of Bitcoins to be lowered significantly.

2014 saw the fall in prices of Bitcoins starting from $770 to $314. In 2015, the value started with $314 and ended at a steady $434. In 2016 prices soared and reached $998 by 1st January 2017.

Segregated Witness (SegWit), and implemented software change in the transaction of Bitcoin was approved on July 15, 2017 which rose the bitcoin price by almost 80% in that week. Starting with $998 in 2017, bitcoin prices rose to $13412.44 by January 2018. The former half of 2018 saw fluctuations in bitcoin prices ranging between $11480 and $5048. Bitcoin prices were severely affected by wrongdoings from other cryptocurrency exchanges. YouTube also deleted all the videos and content relating to Bitcoin in December 2019 but restored them later after concluding that they had "made the wrong call".

2020-Present

Image Credit: https://www.coindesk.com/bitcoin-prices-in-2020-heres-what-happened

2020 saw the biggest lowering of the economy since the Great Depression and witnessed bankers, money managers and companies adopting cryptocurrencies and digital assets. Bitcoin had a very humble beginning in the pandemic as it was considered to be an unconventional investment probably because the business tycoon Warren buffet had described it as having "no value". However Bitcoin's price at the end of the year soared at $28,000 and emerged as the topic of conversation among investors and firms.

Bitcoin did not take a lot of time to get its first major jolt in the year- jumping to $7300 as the United States geopolitical turmoil spurred its demand. February 2020 saw the surge in searches of the term 'bitcoin halving 'a once-every-four-years occurring phenomenon wherein price of Bitcoin would get cut by 50%.

March 2020, the devastating corona virus hit the economy and the Bitcoin prices declined from $10,500 to $8,000 but that was not a cause of worry because global market was getting equally hit as well. The swiftest and the deepest plunge of hitting $3850 occurred on March 12. Not, long enough later though, the crypto currency stood at $8600 in April.

Bitcoin's rise in 2020 despite the many things that make investors worry - Brexit, United States-China tension, a pandemic- is indeed remarkable. The Bitcoin started at a humble value of $4,748, but by the end of the year it rose to about $30,000.

This was different from the 2017 bubble, where in the bitcoin price rose about 20 times to almost $20,000 only to stoop down to $3,000 the next year. In 2020, the massive price rise was because of the huge influx of investors hailing from large scale institutions, which was different from 2017 where in the crypto currency market was dominated by individual small scale investors who invested in bitcoin purely because it stood outside the global financial system. The trust of billionaire investors like Paul Tudor, insurance giant MassMutual indicated that bitcoin has moved to the mainstream. JP Morgan, a former critic, now said that bitcoin could have a bright future which helped increase trust in the crypto currency. Consumer facing payment systems like PayPal allowed users to buy and sell bitcoins directly from their PayPal account, therefore the number of users excepting bitcoin as a payment method is growing manifold. Besides the enthusiasm related to its entry in mainstream, the COVID-19 pandemic led to central banks of various countries printing more money. This could possibly lead to inflation and thus reduce the masses purchasing power. In the face of this inflation threat, investing in bitcoin became to be considered a store of value. Central banks embracing crypto currencies is an indication that crypto currency is being viewed as the future.

The speculated halving arrived on May 11 which proved defective for the markets but emerged as an asset for markets psychology. This was because halving would occur every four years which would give Bitcoin analysts clarity about what the future would hold for Bitcoin, a decade or so from now.

Abruptly in June 2020, Bitcoin market went cold. The summer of DeFi, Decentralised Finance (the most common one: Ethereum) had arrived which deflated the Bitcoin prices but demonstrated the potential which digital assets possessed.

The winter of Bitcoin and the corresponding summer of the contemporary lasted till September.

October to December was the worst that the global economy had ever been in nearly a century which meant Bitcoin had an impressive gain as prices were a steady $10,800. December 16, prices stood past $20,000 setting a record and in a couple of days prices surpassed $23,000. Soon

exchanges of Bitcoin happened at an-all-time high $28,085. Thus the year of the pandemic proved to be an irresistible selling point as the Bitcoin had quadrupled its value.

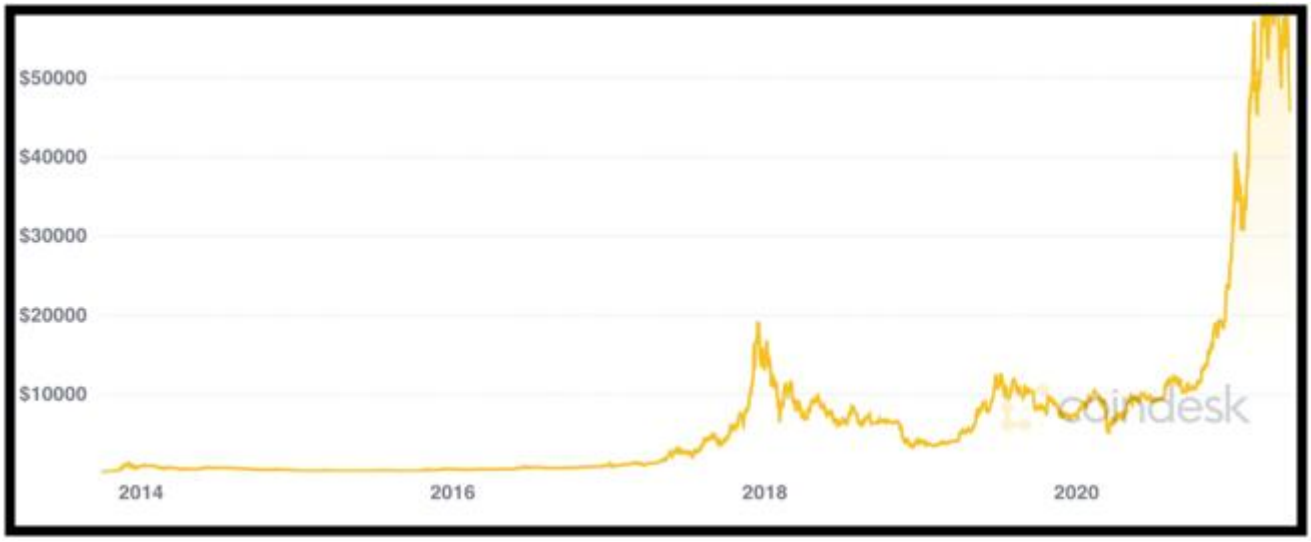


Image Credit: https://www.coindesk.com/price/bitcoin

Understanding Bitcoin

"I do think Bitcoin is the first [encrypted money] that has the potential to do something like change the world."
– Peter Thiel (Co-Founder of Paypal)

Bitcoin is the most widely known cryptocurrency which was developed in the year 2008 by a person or a group persons using the pseudonym Satoshi Nakamoto. Essentially a decentralised digital currency,Bitcoin has no central bank or a single administrator. Without the need of intermediaries, Bitcoin can be sent through the peer-to-peer network. The transactions are verified through Blockchain, a list of records which are linked via cryptography.

How do Bitcoins Work?

Bitcoin is a software, an entirely digital asset combining a set of protocols and processes. It runs on a protocol called the Blockchain. Blockchain comprises individual blocks of information which are arranged in a chronological manner. Any type of agreement made between the two parties can be put in a Blockchain which makes us understand that there is no need of a third party whatsoever. This has introduced us to a world of possible financial transactions in which banks or other such intermediaries are totally irrelevant. Block chain has also been referred to as "distributed ledger" emphasising that it is in public domain. Anyone can access a blockchain.

However not easy as it sounds, there are various complex steps to be followed in order to update a block chain. Since there is no centralisation, the users themselves verify the blocks of transactional data. The entire operation of maintaining a public ledger like the Blockchain is known as mining. Mining is a tedious and difficult course of work carried out by the network of Bitcoin users who trade among each other, called the network of miners. Bitcoin software adds to the difficulty of mining as it is an artificially time-consuming process. On the other hand Bitcoin's software limits the network to a single new 1-megabyte block of transactions for 10 minutes only, which makes the volume of transactions pretty lucid and understandable.

It's no surprise to know that Bitcoin miners are awarded for the work and do not verify transactions purely out of a desire to have the network work hinder less. The reward is in the form of halvings, occurring every four years. Herein every 210,000 blocks mined are cut in half. This system ensures that mining shall continue till the year 2140 when all Bitcoin gets mined and the miners remain incentivised by the fee they charge the network users. The aim is to ensure that healthy competition will keep the fee low. The most recent halving took place on May 11, 2020 wherein the reward for the miners was 6.25 bitcoins per blockchain mined.

Bitcoin investors usually buy their supplies from an exchange like the Coinbase, an online digital platform that enables transactions of cryptocurrencies, as most individuals are oblivious of the ups and downs of blockchain and mining. Though the exchanges are gaining popularity, they face the constant threat of legal, regulatory and security challenges because each country views digital currency with a different perception – an asset or a fraudulence platform. Thus, the regulations are constantly shifting. Bitcoin has by and large been secure through the years, but many thefts targeted at other crypto currencies led to the loss of millions of dollars worth token. The best example is that of Mt. Gox who announced the theft of 850,000 Bitcoins equalling almost $450 million. To this day neither has the money been recovered nor the bankruptcy which Mt. Gox Filed been overcome. It's therefore digestible to understand that investors and owners use keys and wallet is to safeguard their holdings which adds an extra layer of security to their transactions. A simple wallet has a number of private as well as public cryptocurrency keys which are used to track ownership and transact cryptocurrencies. The difference between public and private key is that the public key enables the user to make payments whilst the private key enables the user to spend cryptocurrencies from the address.

What determines the value of Bitcoin?

Currency is usable only if it is reliable, which implies that it can maintain its value without depreciating over a period of time. Since precious metals and commodities had a relatively stable value, they were a medium of exchange in historical times. Then, minted currencies took over in the form of paper money which did not have as much an intrinsic value as precious metals. A reliable currency must possess certain requirements which relate to scarcity, transportability, divisibility and counterfeiting among many others, apart from being a store of value. Bitcoin when subject to these qualifications fares pretty well. However the most difficult question that hovers about is exactly how much will the bitcoin be adopted? This offers another angle at evaluating the Bitcoin.

Inflation rates, monetary policies and other measures which usually affect the value of traditional currency do not affect Bitcoin as it is a decentralised currency not backed by any bank or a government. So, what are the factors which influence Bitcoin prices? The answer to this is cost of production through mining, supply of Bitcoin and the markets demand, rewards to miners for verifications, competing cryptocurrencies and regulations which govern its sales internally and various other elements.

Substantially therefore, the value of Bitcoin is influenced by supply and market‘s demand for it. For example the growth depreciated from 6.9% to 4.4% to 4% in 2016, 2017 and 2018 respectively. This led to the creation of a framework wherein the demand surpassed supply of bitcoin at a fast pace. Thus, the price of Bitcoin increased manifold.

When the maximum limit approaches, the demand of bitcoin increases which causes an upward vertical push in the price of bitcoin. Since more investors are accepting it as a medium of payment, its utility is increasing which makes it a suitable mood of exchange. The safety factor also has an advantage, as bitcoin security is governed by robust protocols and bitcoin is easily available through exchanges.

Unlike conventional stocks, owning bitcoin means owning a digital asset just like owning a dollar ($1) is owning a paper having value of $1. Bitcoin provides a win-win situation for both the miners and the owners. Miners earn by verifying transactions through rewards and the owners earn money as and when prices fluctuate.

The reason why Bitcoin is so expensive is because of the increase in demand and the simultaneous shrinkage in supply. Companies and users are favouring this crypto currency because of its potential at profitability and its ability to constrain inflation. Its resulting popularity has also caused increase in prices.

How to buy Bitcoin?

Investing in a digital asset is far more complicated than a traditional investment. However, the legitimacy of bitcoin exchanges improving day by day has made purchasing bitcoins seem simpler. A Bitcoin user needs several things including a cryptocurrency exchange account, a secured connection to the internet, a method of payment which may be credit card or a debit card or directly a bank account.

The first step is to choose a legitimate cryptocurrency exchange which can enable the user to trade the cryptocurrency. Since Bitcoin is an essentially decentralised currency having an individual sovereignty, some cryptocurrency exchanges allowed the clients to trade and invest anonymously and not enter personal information. Some of the most significant cryptocurrency exchanges in the United States include Coinbase, Kraken, Gemini and Bnance. The aforementioned exchanges (except Binance) offer bitcoin as well as numerous other altcoins. Using safe internet is an important thing while creating a cryptocurrency account. Using the two-factor authentication and unique passwords can do the trick!

The next step is to connect the exchange to a payment method which is quite similar to setting up a bank or a brokerage account. The user will need to gather all relevant personal information that the exchange may ask for. Once the identity is ensured, the user can connect the bank account directly or connect a credit or debit card. It is, however, advisable to avoid payment via credit or debit card because cryptocurrencies face a lot of price volatility. There may be variant fee for different banks. So it is imperative to have a thorough research to find out which option suits the user the best.

After the first steps are completed, the user can now purchase Bitcoin successfully. Bitcoin can be bought at any cryptocurrency exchange. Cryptocurrency exchanges have grown significantly which has led the once thought to be a scam to be considered trustworthy. Basically, creating an account with an exchanges all the user needs to do to enable himself to purchase bitcoin. However, some additional steps may be effected to ensure more safety and security.

A safe place to store your digital currency is a wallet-a bitcoin or cryptocurrency wallet. It avoids the risk of losing your investment or getting hacked. Having a currency in a personal wallet outside the exchange gives you the sole control over it. Bitcoin wallets can be classified as hot wallets (online wallets) and cold wallets (hardware wallets).

Alternatives to Bitcoin exchanges like Coinbase and Gemini are Bitcoin ATMs and P2P exchanges. Bitcoin ATMs are exchanges in which the individual can insert money in the machines which processes it to purchase the bitcoin. The P2P (peer-to-peer network) exchange adds in a personal touch and provides direct contact between the users.

Though choosing to buy bitcoin from exchanges is a simple and reliable way, if one has technical skills and the correct hardware, one can also mine bitcoins into their wallet. In the following paragraph I have illustrated a plethora of opportunities for bitcoin enthusiasts to mine the cryptocurrency into their wallets:

The first one is airdrops, which are basically free money that companies give away in order to attract people to the company and platform. Next is crypto freelance marketplaces which include Bitwage, earn.com, angel‘s list etc. The third one is to learn and earn crypto on coinbase earn, which is an online training program where you can learn about a specific crypto currency, then take a test at the

end of the training, and if you pass in that test, then pay in that coin. Micro-earnings, pay to clicks, and small service jobs are a low-risk way of making bitcoin online. Bitcoin faucets are another system of bitcoin distribution where bitcoin is given away for free to anyone who visits a particular website every half an hour. Signature campaigns and bounties are low income and low-risk way of earning bitcoin which are much less available today but you can still find them online. Trading in crypto currencies is by far the most obvious way to make bitcoin which means buying bitcoin with traditional currency and then selling it when it is more worth. Bitcoin affiliate programs is when you share a link with people and you invite them over to sign up the following link and the company that you do it for me what do you if any of the people sign up. Gambling is an effective way to earn fiat money, but many people do not know that crypto currencies can be gambled as well. There are hundreds of websites, blogs which focus on crypto currencies, which means that anyone who can decently write well about bitcoin or other major crypto currencies could end up making a lot of bitcoins. Earning crypto currencies by the provision of goods and services to people within the crypto currency community is also a good way to expect payment in crypto currency itself. For an investor, bitcoin futures trading is also a very good option. Undoubtedly, the most fun way to on bitcoin or any other crypto currency is by playing games. Huntercoin and Steem Monsters are the most popular bitcoin earning games. Show media influencers have a lot of potential to make money from the following, so if one is able to have people followed him based on the interest in cryptocurrencies, then one has the potential to leverage the people for his own financial gain.

Bitcoin Exchanges

An online or a digital marketplace where bitcoin can be bought or sold by using different currencies by traders is called a bitcoin exchange. The bitcoin exchange the third-party between the traders-the seller and the buyer, to be more specific between the ”maker” and the ”taker” respectively. It is therefore essentially a brokerage where money can be deposited through bank transfer or others of the like. It is a brokerage because of a price is paid for this service. This fee is the currency conversion fee, quite similar to a traditional bank when money is traded between two or more countries.

A decentralised exchange is operated without a central authority which offers trading bitcoins without the need of an exchange authority as an intermediary. Among the innumerable benefits of a decentralised cryptocurrency exchange, the first one is the decentralised nature of this particular exchange with gels with the decentralise nature of bitcoin itself. A decentralised exchange requires substantially less amount of personal information than a regular exchange for setting of cryptocurrency account. Next, the risk of theft or fraud is reduced as the user directly transfers assets to other users. Lastly, the centralised bank is not very susceptible to price volatility and criminal trading activity.

Coinbase is noted for being the best in the overall business in the United States. CoinBase has largely avoided cryptocurrency scams by offering custodial wallets for investors. It offers easy exchanges which has lowered the barrier of cryptographical investment by a great degree. Additionally, the solid variety of cryptocurrencies, extremely user-friendly interface and very high liquidity has led Coinbase to become a popular bitcoin exchange. However, just like the two sides of a coin, Coinbase has its own disadvantages which include high fees when the user has not updated the digital cryptocurrency exchange platform and is not using Coinbase Pro.

Next in the queue we have Binance, the world’s biggest bitcoin exchange by volume. Binance was founded by the developer Changpeng Zhau who previously created a high-frequency software. Initially based in China, Binance was removed from China due to its growing regulatory is regarding crypto currencies. Though Binance is considerably a safe Exchange medium, on May 7, 2019 it witnessed a major hacking resulting in 7000 bitcoins stolen from the exchange. However, when all the strings are pulled together and Binance is looked at, one can definitely say that the pros largely outweigh the cons.

The best decentralised exchange in the business is Bisq, wherein fees can be paid via BTC or BSQ (the companies on cryptocurrency). Bisq is a non-custodial exchange, so the user and he alone are entitled to control his funds. Bisq is easily accessible with no registration process. This is ideal for people wanting privacy or persons having no identification issued by the government, for example a driving license. Bisq offers many currency is ranging from the United States dollar to bitcoin. It‘s only disadvantage is that because it is decentralised and offers a peer-to-peer network it has low trading volumes. Nonetheless, it‘s still well worth it for some users.

Should You Invest for a Long Time or A Short While?

Financial situation and long-term goals should drive investments in crypto currencies. For people looking to grow their portfolio a long-term approach is warranted, while those looking for immediate goals a short-term approach should be adopted for quicKER potential returns.

Short-term investments are advisable for bitcoin and ethereum as they lead the market. However experiments shouldn't be done by investors in crypto currencies because in a short span of time the entire capital can get wiped out. The company needs to be understood and investors should have complete knowledge about the business model in case they invest in the long term. For the longer term, an investor can go for Nexo and Cardon. There are hundreds of crypto currencies in the market, wherein half don't have any intrinsic value or any business model. Therefore, investors should first verify if there is a business model associated with the currency they are planning to purchase.

It is essential to understand whether the transaction is actually happening and whether the traction is on the increasing side for an investor. More importantly, the investor should realise that investing in crypto currencies is very volatile and extremely risky.

Economics of Bitcoin

"Bitcoin is a techno tour de force."

– Bill Gates

There is no doubt that Bitcoin is a currency. 'The Economist 'in January 2015 and listed three useful qualities of bitcoin: "as hard to earn, limited in supply and easy to verify". Money has been said to be a store of value, a medium of exchange and a unit of account, which undoubtedly means that bitcoin has some way to go to meet the aforementioned qualifications. However, it is the best medium of exchange. The ability of Bitcoin to be a store of value has been limited because of the volatility it suffers. Retailers often except bitcoin but use other currencies as the mean unit of account.

While Bitcoin supply is almost transparent in nature available for everyone to see, the demand for Bitcoin is the opposite-it is opaque. This is because firstly, everyone has a clear image of the number of transactions done each day. Secondly, the price volatility and fluctuations cause price corrections and play a major role in determining the same. So, there is a very frail relationship between the increase in transactions and the simultaneous decline in the prices.

Financial Institutions

Opening a bank account for Bitcoin companies has been a difficult task because banks are scared to deal with cryptocurrencies, even if they truly want to. This can be clearly understood by looking at the closing of business bank accounts relating to Bitcoin by the National Australian Bank in 2014 and HSBC refusing to fund Bitcoin companies. Nevertheless, blockchain technology (the technology on which bitcoin is based) has been adopted by Australian Banks.

Bitcoin got the institutional trust in 2020. The UK-based asset manager Ruffer had stockpiled almost £550 million of Bitcoin since November of that year which summed up to 2.7% of the firm's AUM (asset under management). Thus, it made it evident that institutional money can no longer ignore a major portfolio diversification trend in bitcoin which understandably made the bitcoiners overjoyed. Whether financial institutions are making a terrible mistake or whether things are genuinely positively differently now can be briefly broken down into four key components for more effective understanding.

The first one is Bitcoin's asset class status which is quite hard to dispute. Bitcoins value has been associated with its incapacity of going to zero inspire of having central authority which is quite overpowering. Next up is bitcoin's volatility which is an important window into market forces that are being subdued. In 2020 too, this factor has in bitcoin's biggest adversary when it comes to the public's decisiveness about the wider adoption of this form of currency. Thirdly, bitcoin has fought the law and the law as anticipated has one. For quite some time now, bitcoin had to constantly face strict investment mandates and regulatory compliance. However, after formal regulation by several regulators and financial investors, this problem is now much more solved than the earlier obstacle it used to be.Lastly, bitcoin has defied scrutiny rather successfully. Define continuous critiques is not the best testament of success stand scrutiny is, which is why scientists have invited scrutiny in the past few years.

Bitcoin started far from the scientific method as a belief system but invited more scrutiny in the last 12 years, more than Donald Trump. However loathing and unpleasant, it may sound to the critics, Bitcoin has stood the test of time and despite the scrutiny it faced, it is still standing tall. This fact definitely constitutes something important. Of course, Bitcoin has yet to prove itself to be more efficient than traditional currency or traditional Fiat money. However, we can not deny its overall resilience and pliability. Here, we take a look at some of the big Bitcoin owners, as of June 2020.*

Institution	Assets Under Management (by firm)	Amount of Grayscale Bitcoin Trust, GBTC ($000)
ARK Investment Management LLC	$4,476,259,838	20,226
ARKW - ARK Next Generation Internet ETF	$4,476,259,838	17,136
KINETICS PORTFOLIOS TRUST - Kinetics Internet	$5,348,552,762	15,284
KINETICS PORTFOLIOS TRUST - Kinetics Paradigm	$5,348,552,762	13,995
Arkadios Wealth Advisors	$626,987,454	9,071
KINETICS PORTFOLIOS TRUST - Kinetics Market	$5,348,552,762	4,285
Corriente Advisors, Llc	$263,431,194	4,201
KINETICS PORTFOLIOS TRUST - Kinetics Small Cap	$5,348,552,762	2,187

As an Investment

Bitcoin is a risky and a dicey investment. You should weigh a number of considerations, especially your financial goals before deciding to invest in this cryptocurrency. Another important fact is the short history that bitcoin has had and the small-scale market it is traded within. Many Bitcoiners have referred to bitcoin as a new version of gold, however it is not verified whether it would work effectively as a large-scale asset, like gold.

Based on its history, it is surely know that bitcoin does have volatility in abundance, which for an investor is very convincing. Bitcoin is, in fact, an extremely winning investment. A humble beginning of no value in January 2009 so it's a pass $50,000 in February 2021, 12 years later. Since there are no closing bells to stop trading like a traditional market, bitcoin prices can move very violently. In 2020, it rose up by 350% but then was down by 64% in February and March. This was, of course, because of the global economic subsidence, due to the COVID-19 pandemic. It therefore cannot be argued that it has the ability to wildly oscillate within a day.

However, investing in bitcoin is not similar to investing in traditional currency. This is because the open market and the desires of the government that circulates these traditional currencies result in the price of the currency. Meanwhile, bitcoin‘s price depends entirely on what the investor desires to pay which makes it more of a sentiment-driven market. There is no limit on the maximum and minimum it can go. It‘s interesting to know that Satoshi Nakamoto had designed bitcoin to be a form of money. However, he retreated in 2010 and no news of them has been heard since.

There are many reasons to invest in bitcoin which include that the supply of bitcoin is stable, the trends in merchant and business adoption are increasing day-by-day, the price could further have an impetus if transaction volumes increase, despite the competition it faces from other cryptocurrencies it is highly improbable that it will get dethroned anytime sooner, the governments of many countries have a positive attitude Towards digital currencies especially bitcoin and more investors have started using it as a portfolio diversifying.

The question of whether to invest or not is solely dependent on your risk appetite. Barry Silbert, founder and CEO of Digital Currency Group has said, ”In 10 years, the price of bitcoin will be either zero or much higher than it is today and so, as such, anybody who puts money into bitcoin should only put money into bitcoin that they can afford to lose.*
individual consumers or consumer groups. As a matter of fact, bitcoin has started to appear to be more steady than gold. In 2017, for the very first time the price of bitcoin surpassed an equal ounce of gold with prices of bitcoin soaring. It has been observed that the bitcoin network‘s effect is proportional to the level of its adoption, in accordance with Metcalfe‘s Law.*

*https://www.forbes.com/sites/michaeldelcastillo/2020/08/06/valuable-sec-data-on-20-institutional-bitcoin-investors-could-soon-disappear/?sh=549d49661de2

*https://www.forbes.com/sites/laurashin/2015/12/11/should-you-invest-in-bitcoin-10-arguments-in-favor-as-of-december-2015/?sh=1096c0c42df

Price and Volatility

Bitcoin's price and value have been historically known to be quite volatile. It is no astonishment therefore that bitcoin price volatility is almost 7 times more than gold and approximately 18 times more than the US dollar. The bitcoin foundation claims that the volatility is caused because of inadequate fluidity. An eminent journalist of the Forbes magazine has contended that it is because of the surety of its long-term value. He further has justified the high volatility by saying, “ because people are still experimenting with the currency to figure out how useful it is.” Price volatility is not a matter of concern though,in online gambling and international remittances.

Bitcoin prices have ranged from appreciations to the depreciations known as ’bubbles ‘and ’busts‘. For instance, the value of bitcoin rose from $0.30 to $32 ultimately ending at $2 in 2011. During the 2012-13 Cypriot Financial Crisis (An economic crisis in the Republic of Cyprus in which the Cypriot banks were exposed to the insolvent or bankrupt local property companies), the prices of bitcoin increased to a high of $266 on 10 April 2013, before succumbing to $50 or so. Later that year on 29 November 2013, the price rose to $1242, the all-time high.

Economists have reasoned the peak to be because of a certain manipulation in prices. The following year, prices fell aggressively and in April the prices were a little more than the previous year’s 50% prices. Prices stood at $600 by August 2014. January 2015 witnessed the bitcoin prices being dropped to the lowest, around $224 since the 2013 spring. The industry was facing the effects of a prolonged decrease in prices. Bitcoin mining companies started flashing warning signs.

The next example is the 8% volatility in prices in a span of three months that is, October 2017 to January 2018. This volatility was almost twice the volatility bitcoin faced from December 2019 to January 2020.

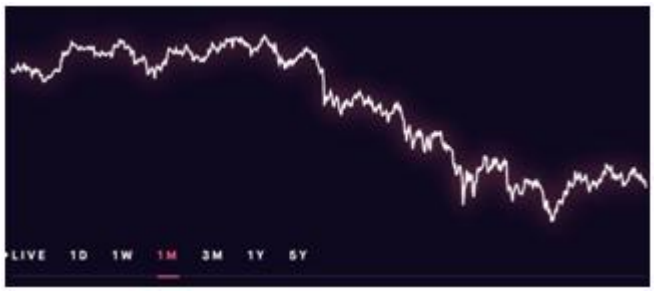
Economists are of the belief that the volatility will decline once the usage of bitcoin increases by businesses and

In this column, we take a look at the price of Bitcoin across six different spans of time: 1 day, 1 week, 1 month, 3 months, 1 year and 5 years.
Source: https://robinhood.com/crypto/btc

(As of May 28, 2021; 11:30 a.m.)

The price of Bitcoin went down by an estimated 4.48% on 28th May, 2021.

The price of Bitcoin went down by an estimated 7.25% from 22nd May to 28th May, 2021 (over a period of 7 days)



The price of Bitcoin went down by an estimated 32.34% from 28th April to 28th May, 2021 (over a period of 30 days).

The price of Bitcoin went down by an estimated 19.52% from 28th February to 28th May, 2021 (over a period of 3 months).

Volatility Index (VIX) of the Indian Stock Market v/s The Volatility of Bitcoin Market

India VIX indicates the volatility of Indian markets, perceived by an investor. India VIX and its volatility are somewhat parallel to each other. To say so, if India VIX has a higher value, the volatility will also rise, and vice versa. However, Nifty and India VIX show a huge inversely proportional relationship. When, India VIX rises, Nifty drops, and vice-versa.

Bitcoin's distinguishing volatility has been discussed above. Its volatility lies in its characteristic speculation. People, as observed, buy and sell Bitcoin like they would any other similar investment. This particular cycle of buying and selling has made Bitcoin so volatile. But then, how can Bitcoin be a currency if it is so volatile? When Bitcoin is used as a currency, faith is implied for quantifying it as a number. Any new invention is known to be volatile and so is bitcoin. It is quite normal for a potential global digital asset or any asset for the matter to be volatile which makes money to sound highly volatile.

Below, are two graphs which compare the volatility of India VIX and the Bitcoin Market from 2017-2021.

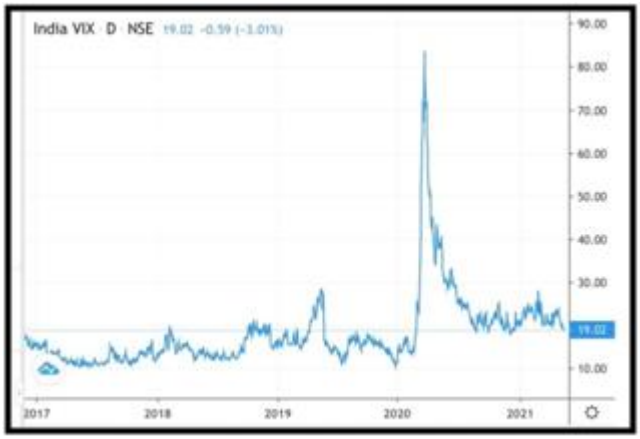


Image Credit: https://www.moneycontrol.com/indian-indices/india-vix-36.html

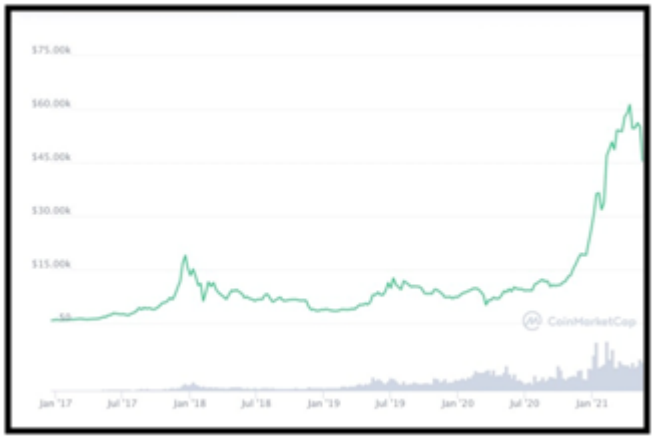
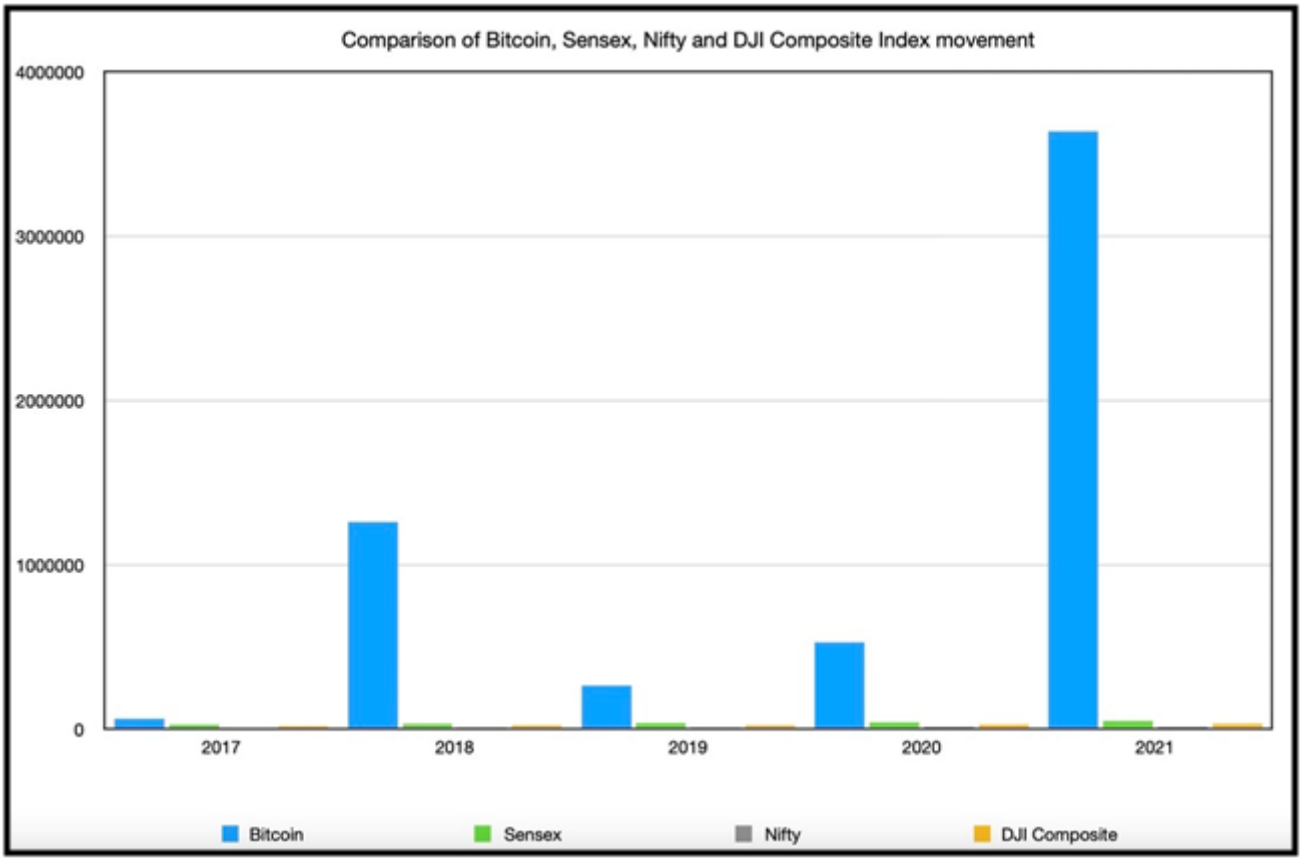


Image Credit: https://news.bitcoin.com/the-fear-factor-a-volatility-index-for-crypto-arrives/

Comparison of Bitcoin, Sensex, Nifty and DJI Composite Index Movement

The aforementioned column graph represents the value of Bitcoin, Sensex, Nifty and the DJI Composite Index over a period of 5 years, 2017-2021.



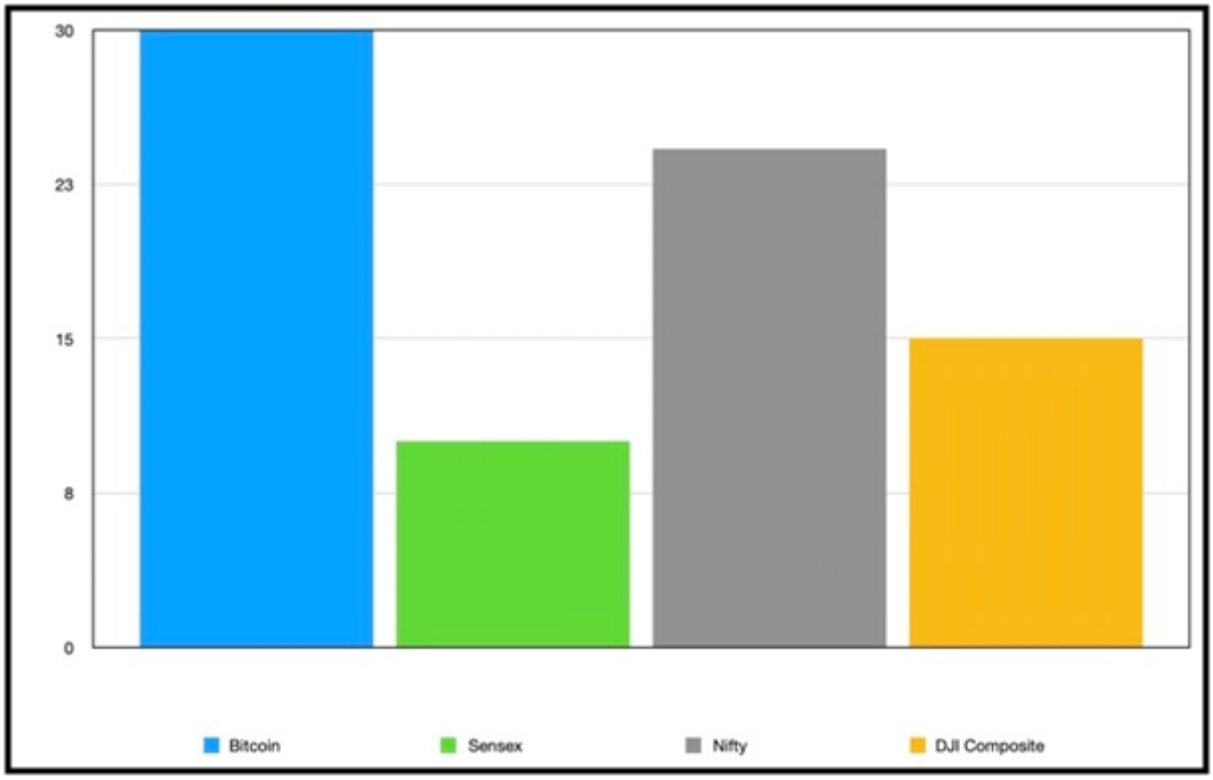
As is visible, the blue column (Bitcoin) has shown a sharp rise and fall and subsequent increase over the years. The green column (Sensex) has more or less remained stable and so has Nifty (Grey) and the Dow Jones Industrial Average Composite Index (DJI: Yellow).

The table outlines the value of Bitcoin, Sensex, Nifty and Dow Jones Industrial Average under the following year heads in Indian National Rupees (INR)

Description	2017	2018	2019	2020	2021
Bitcoin	60471	1259035	264137	527263	3635785
Sensex	26040	34056	36076	41575	49428
Nifty	7985	10558	10727	12226	13749
DJI Composite	19762	24719	23062	28645	30606

In this column, we compare the Compound Annual Growth (CAGR), which is the rate of return that is required for an investment to grow from its begging balance to the ending balance, assuming the profits were reinvested at the end of each year of the investment‘s lifespan. The CAGR is a representational figure and not a true return rate.

BITCOIN: According to a research report, the cryptocurrency market stood at $792.53 million and is estimated to reach $5190.62 million in 2026. The market is expected to grow at a compound annual growth rate CAGR of 30% in these seven years.



SENSEX: The CAGR of Sensex has been 10% over a span of 10 years. It has thus been observed that though the returns were muted, they surpassed other asset classes.

NIFTY: According a report published by ICICI Direct, ”Going forward, we expect Nifty earnings to grow at 24.2 % Compound Annual Growth Rate over FY21E-23E.”

DJI COMPOSITE INDEX: The Compound Annual Growth Rate (CAGR) of Dow Jones Industrial Average stands at 15.03%.

The CAGR in sales, of 5-12 % is considered to be good, while for small companies, 15-30% CAGR is expected for a period of five years. Start-ups are required to have a CAGR of 100-500% in order to be considered to be doing well in terms of rate of returns.

Bitcoin v/s Other Cryptocurrencies

”You can‘t stop things like Bitcoin. It will be everywhere and the world will have to readjust. World governments will have to readjust.”

– John McAfee

The differences between different cryptocurrencies are valuable for investors because they provide critical information on how cryptocurrencies are taxed and how the supply and demand relationship for each cryptocurrency will evolve in time, therefore influencing the marketers ‘ behavioural and buying habits. Bitcoin was the first decentralised cryptocurrency that was launched in 2009 and since then, many other cryptocurrencies have followed suit. While bitcoin is not a very easy currency to dethrone from the market, several other currencies like Bitcoin Cash, Ether, Ripple, and Stellar (XLM) pose a potential threat because of the rising demand for digital assets and technological progress and advancement.

Bitcoin, by far, is the biggest in the business when it comes to market capitalisation. It was created by Satoshi Nakamoto, a pseudonymous person, or persons, with the aim to safeguard financial transactions through a peer-to-peer network. It eliminates the need for a third party or an intermediary, ensures that transactions are incognito, and has drastically democratised money. Its biggest pro is it's brand name-the fact that is the best-known currency. However, its slow transactional speed and its special requisite of specialised mining technique are disadvantageous.

Bitcoin cash (BCH) is a digital currency that can be operated without any external operation or machinery. This digital currency was created in August 2017 as an offshoot to Bitcoin by a ’hard fork‘. A ’hard fork ‘is a terminology relating to blockchain technology, which is a significant change in a network‘s convention by making previously invalid blocks (transactions) valid, or converse. It was created in order to compensate for Bitcoin‘s slowdown in the speed of transactions. Bitcoin Cash can process more transactions per second than Bitcoin because of the larger block size which is 8-megabytes as opposed to Bitcoin‘s 1-megabyte. Its advantage lies in the purpose of its creation, faster transactions than Bitcoin. Nonetheless, it requires specialised mining equipment just like Bitcoin.

Ripple is another popular cryptocurrency that supports RippleNet, a payment network used by eminent banks and financial institutions like American Express and Santander. Many economists question the credentials of Ripple as truly being a decentralised cryptocurrency because it operates in a very different way than other digital currencies. the fact that it has a terminal velocity in transactions is a major

supremacy. Its major con is that RippleNet can be used without its supportive cryptocurrency, Ripple.

Stellar (XLM) is pretty much the twin of RippleNet as it operates in a similar way. Stellar, however, can process transactions in innumerable currencies. A cryptocurrency called lumens (XLM) sustains Stellar. Lumens play an important anti-spam role besides being used for financial transactions on the network. The anti-spam role is performed because of the underlying fact that a minimum fee is required to be paid for each transaction. It has an edge over the others because it amalgamates with banks, and as mentioned above, it can be used to process transactions in various currencies. The only drawback is that it not widely acknowledged as other cryptocurrencies.

Ether, a cryptocurrency developed by the Ethereum network, allows the users to themselves code and release decentralised applications (frequently known as 'dapps'). It also enables them to generate smart contracts that automatically imposes their stipulations. Hackers are prevented from spamming the ether network by destroying small amounts of ether for each transaction processed. The merit is that it can be used beyond the cryptocurrency on the Ethereum network and not to mention, the brisk transaction speeds. Its only deficit is the uncapped supply which could possibly lead to inflation in prices.

Despite being older than most of its contemporaries and having fewer applications than them, Bitcoin's value never ceased to soar in the recent times. It still remains the biggest cryptocurrency in terms of market capitalisation. This means that reputation is an essential component for the success of any cryptocurrency and subsequently, its value.

Image Credit:
https://www.reddit.com/r/CryptoCurrency/comments/7tkpvn/btc_vs_eth_gain_comparison_from_november_2017/

The Red line indicates Bitcoin whilst the candles are representatives of Ethereum developed, Ether.

Bitcoin in India

'Bitcoin is a very exciting development, it might lead to a world currency. I think over the next decade it will grow to become one of the most important ways to pay for things and transfer assets."

– Kim Dotcom (CEO of MegaUpload)

The cryptocurrency market in India has been thriving and booming by the day due to the enthusiasm added by retail investors and their faith in the business. Over 10 million cryptocurrency investors have contributed to the market and the number is in reality, snowballing. However, there is a factor which is holding millions of Indians back and that is the aspect of it being considered illegal. And, that is not true. Cryptocurrencies are a hundred percent legal in India. This does not mean that it is regulated. It is unregulated, there is no regulatory framework to govern its volume output or tradings. Nonetheless, the Indian government is looking into providing a cryptocurrency regulation soon.

In 2018, the Finance Minister released a statement with was followed by a circular issued by the Reserve Bank of India. The statement said: "The Government does not consider Cryptocurrencies as Legal Tender or Coin and will take all measures to eliminate the use of these Crypto Assets in Financing Illegitimate Activities or a Part of the Payment System The Government will explore the use of Blockchain technology proactively for assuring in Digital Economy."* This stamen reveals that the government was never against cryptocurrencies, however it only condemned and intended to limit its usage in illicit activities by means of blockchain technology. This was a great step towards the building of a healthy cryptocurrency environment. It also said that the government will not consider it as a mode of payment or financial transactions. Nothing was said about not holding it as a digital asset.

In 2020, the fast progress made by The United States, Singapore and other developed nations inspired the Indian Finance Ministry to reconsider its decision. The supreme court of India retracted the RBI circular of 2018 which led banks to resume their transactions in cryptocurrencies. On one hand, Indian equity markets were touching the lowest rates every day, while on the other hand cryptocurrencies were rallying one after the other. Finance Minister, Nirmala Sitharaman ji said: "From our side, we are very clear that we are not shutting all options. We will allow certain windows for people to do experiments on the blockchain, bitcoins or cryptocurrency. A lot of fintech companies have made a lot of progress on it."*

Popular Indian cryptocurrency exchanges include; WazirX, BuyUCoin, CoinDCX, Bitbns, Zebpay, CoinSwitch and Goittus.

Amit Bhardwaj, an Indian fraudster is known to have a net worth of 1.86 billion dollars. He is the founder of GB Miners, who apparently has hoaxed many Indians by inventing Bitcoin-based Ponzi schemes. He is allegedly known to own the maximum number of Bitcoins in India.

Currently, there are more than a thousand cryptocurrencies, which put the investor in a fix as to which cryptocurrency to invest in. Bitcoin, Litecoin, Ethereum, Cardano and Dogecoin are by far the most popular and reliable cryptocurrencies for an Indian investor to invest in, according to newsroompost.com.

The three steps an Indian investor needs to follow in order to invest rightly in the cryptocurrency market are outlined

below. First, the investor needs a source to buy the cryptocurrency through an exchange like WazirX or an online platform like PayPal. Secondly, a

cryptocurrency wallet is required to store the blockchain link and in order to have access to cryptocurrency coins. And last but not the least, the investor needs to have a list of cryptocurrencies which he thinks are safe to invest in than the others, because of the relative stability in prices.

Cryptocurrency owners are hedging risk by these three cryptocurrency hedging strategies. Hedging is a risk management strategy which eliminates losses in investments which results in the reductio of potential profits to be deemed upon the firm. The various reasons to hedge the risk of cryptocurrencies includes, lack of regulation, susceptibility to hacking, and the market volatility. The first hedging practice we put in action is Short Selling of Bitcoin. The technique involves selling an asset, and making others believe that its value will fall and eventually you can buy it back later for a lower price, thus making a profit. This can be understood by the graph depicted below:

The next way is hedging bitcoin with CFDs. CFD stands for Contract for Difference which is a financial contract that pays the difference in the settlement price and allows investors to profit from the price movement without owning the asset. Thus, you can essentially decide the price of bitcoin without even having to open an account with an exchange, free from the hassle of a digital wallet. In short, SHORT CFD TRADE..PRICE DECLINE..PROFIT TO CFD. Lastly, hedging of bitcoin with future, which was introduced by the CBOE. Future is a financial contract in which trading an asset is agreed upon by two parties on a particulate date in the near future. Hedging of bitcoin with future is seen as providing a legal way for participants in the market to lock in a market price.

Unlike traditional stocks and shares in the market, bitcoin and other crypto currencies do not have a demat account. A demat account is used to hold shares in an electronic format. The purpose of having such an account is to hold shares that have been bought by the investor or has been dematerialised, that is converted from the physical form to an electronic form, thus making trading convenient for investors in the online way.

The future of Bitcoin in uncertain, as was its past and as is its present. A total ban on trading in cryptocurrencies is apprehensive. Investors fear the exudate of cryptocurrency business and talent from India, something which had occurred right after the RBI‘s existential threat in 2018. Then, Indian experts in the blockchain software technology moved to Switzerland, the US and Singapore, were the Cryptocurrencies were being regulated, unlike India where they are legal but unregulated. A blanket ban on its usage, will have a similar effect. India shall see a halt in blockchain innovation, which in turn will have a domino effect on governance, economy and the nation‘s energy.

*https://economictimes.indiatimes.com/markets/forex/forex-news/are-your-crypto-investments-legal-heres-everything-you-need-to-know/articleshow/82259869.cms

Advantages of Bitcoin

”Bitcoin is here to stay. There would be a hacker uproar to anyone who attempted to take credit for the patent of cryptocurrency. And I wouldn‘t want to be on the receiving end of hacker fury.”

– **Adam Draper**

As bitcoin is steadily gaining fame and popularity, all the more people are entering into the cryptocurrency trading environment. It‘s extremely imperative to understand the pros and the cons of investing into bitcoin, if you are planning to do so. Bitcoin has stood out from the uncountable cryptocurrencies available because of its wild price volatility. Hence, after understanding the importance and advantages, users can start trading in cryptocurrencies to

achieve better results. Here are few advantages traders can easily get when they totally engage in trading Bitcoin.

Bitcoin has far more liquidity than its peers by a significant margin. Thus, users can retain most of its intrinsic value while converting to traditional currencies like the US dollar or the Pound Sterling. Thus, Bitcoin is more or less very similar to a fiat currency, although it is not possible yet to trade Bitcoin in reality in any desirable quantity which can be done with the US dollar or other major currencies of the world.

Bitcoin is increasingly being accepted as a mode of payment by many merchants. It‘s practically possible to virtually buy any item using bitcoin now, by using popular online platforms. If reducing your usage of fiat currencies if, on your agenda, Bitcoin is surely going to be a great alternative.

International financial transactions are as easy as domestic transactions when using Bitcoin. There is no hassle involved as in the case of a conventional currency. Unlike fiat currencies, international transaction fees are not associated. Further, the international transaction fee is relatively less as opposed to international credit card and ATM fees ranging from 3% to even 15% in the case of traditional currencies. The reason why cross-border financial transactions using Bitcoin are way easier is that Bitcoin is sought-after almost in every corner of the world.

While operating a traditional bank account, say for US dollars or any other fiat currency, or an online bank account, or making payments via an online credit card, your privacy isn‘t protected. It is only safeguarded from handing over cash or a credit card across the counter physically. Online accounts are of course well protected but not from hackers. Hack attacks are clearly linked to the user because their expenditure and reception of electronic funds can be tracked by public authorities. Comparatively, Bitcoin‘s but in privacy protection software has enabled users to keep their bitcoin accounts separate from their public accounts. It's definitely possible to track down Bitcoin flows in the peer-to-peer network, however, it is not possible to configure as to whom are these flows directed towards.

Bitcoin is a decentralised currency, so it is not issued or its distribution is not controlled and managed by a state entity, like a central bank. Therefore, it is not subject to political influence. It is very difficult for any government to seize bitcoin or temporarily freeze it with regards to any legitimate criminal activity or as a redistribution of political acts because it exists outside a political system. This is often the case in suppressive countries like Russia and China. This fact along with its popularity and liquidity is free of any obligation for its creator. The less popular cryptocurrencies are identified by their concentrated holdings. This enables the creator to delude the supply and value of the currency relative to the competition. This, undoubtedly, negatively influences other cryptocurrencies ‘holders.

Only 21 million Bitcoins to ever exist, Bitcoin‘s inbuilt scarcity feature will very likely underpin its long-term value as opposed to fiat currencies. In case anyone wants to produce more bitcoins, then they have to change the source code. Due to the fixed supply, the principle of economics is applied wherein there is a shortage of supply and huge demand. Hence the prices keep on increasing day by day. As on 8th June, 2021, 18.7 million bitcoins are already mined leaving 2.3 million bitcoins yet to be mined. Once these are unlocked, then the rules may need to be changed to facilitate additional bitcoins. It took 10 years to mine 18.7 million bitcoins. Now only 2.3 million bitcoins are left to be mined which should not take more time.

Bitcoin also has a very strong chance of standing higher against its non-scarce cryptocurrency counterparts, like Dogecoin (a Bitcoin alternative). Thus, its scarcity has in a way infused it with inherent value, the likes of gold and other precious elements.

Traditional currencies, controlled by their respective government entities are known to be non-scarce. New units of currency are created by central banks at their own will. For instance, the global financial crisis of the late 2000s resulted in the US Federal Bank creating trillions of dollars as part of a quantitative easing program. These policies make economists restless and insecure, though their long-term effects are still unclear.

Legal Status and Regulatory

Warning

’’Bitcoin was created to serve a highly political intent, a free and uncensored network where all can participate with equal access.”

– **Amir Taaki**

The regulation of bitcoin is difficult because of its decentralised nature and its online trading exchanges located in many nations. Nonetheless, the usage of bitcoin can be banned and probably be criminalised. The consequent closure of exchange and the termination of the peer-to-peer network constitutes a temporary or de facto ban. The legal status, too, is undefined and varies considerably in different countries. A ban on bitcoin often results in the termination of other cryptocurrencies as well.

To date, nine countries have imposed an absolute ban on cryptocurrencies, including bitcoin, which are Algeria, Bolivia, Egypt, Morocco, Iraq, Nepal, Vietnam, the United Arab Emirates, and Pakistan. Bahrain, Bangladesh, China, Colombia, the Dominican Republic, Indonesia, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia, and Taiwan are the fifteen countries in which an ’implicit ban ‘ has been applied (source: Library of Congress).

Bitcoin miners in Iran were required to sell bitcoin to the Central bank of Iran which would use it for imports, as per the announcement made by the Islamic Republic News Agency in October 2020.

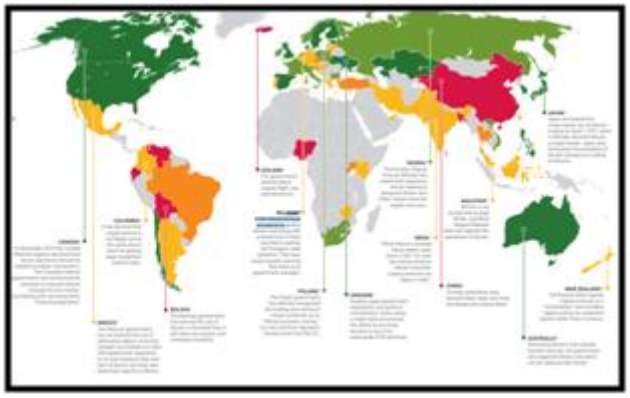


IMAGE CREDIT:
https://blogs.thomsonreuters.com/answerson/wp-content/uploads/sites/3/2017/10/World-of-Cryptocurrencies-graphic.pdf

While Bitcoin is legal in the United Kingdom, the government has stated that bitcoin is unregulated and is treated as a foreign currency, and is regarded as 'private money'. No VAT (Value-added tax) is due on the value of bitcoin, thought is exchanged for the pound sterling or for other currencies, the euro or dollar. In the case of a flow of supply of any goods or services which are sold in exchange for bitcoin (or any other cryptocurrency) VAT will be levied. The profits earned or the losses faced shall be subject to the capital gains tax, in relation to cryptocurrencies. The CryptoUK, an industry body, aiming to improve the standards of bitcoin in the industry, has put across a proposal that shall ensure extra security measures by the proviso of Anti-Money Laundering.

Bitcoin is legal in the United States. It has been classified as a convertible decentralised virtual currency by the Department Of The Treasury, and as a commodity by the Commodity Futures Trading Commission, CFTC. Cryptocurrency exchanges operating in the United States are required to register with the Financial Crimes Enforcement Network, FinCEN, as a money services business, enforce an anti-money laundering program, and lastly, maintain records to be reported to the FinCEN which include Suspicious Activity Reports and Currency Transaction Reports.

Here we take a look at the volume of Bitcoin trading in various countries in the year 2020. Statistics reveal the interest in Bitcoin trading has been significantly observed in Africa and Latin America in comparison to the world's most developed economies. For instance, the Bitcoin trading volume in Nigeria was twice that of the European Union while, Columbia's was twice Canada's trading volume in the year 2020.

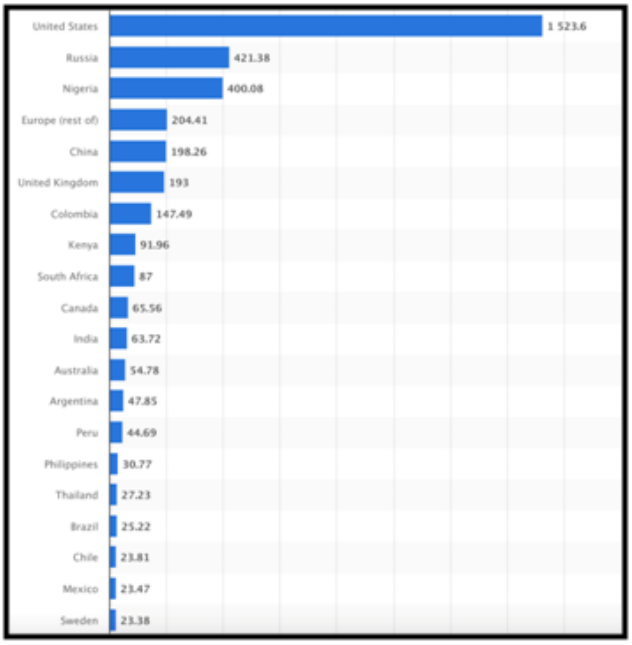


IMAGE CREDIT:
https://www.statista.com/statistics/1195753/bitcoin-trading-selected-countries/

Views by supporters and critics*

"Bitcoin, it just seems like a scam,I don't like it because it's another currency competing against the dollar."

— **Donald Trump**

It has become very onerous for the distinguished personalities in finance, technology and governance to ignore the meteoric rise in the popularity and adoption of bitcoin. Many people have an opinion and perceive its almost 565% gain in the past one year in different ways. The potential of digital currencies has much been debated about since the pseudonymous Satoshi Nakamoto described the cryptocurrency technology in a nine-page thesis in the year 2009. Here's what influencers and the most illustrious in the field have to say.

Elon Musk, the co-founder of Tesla.Inc, founder and chief designer of SpaceX, and a centibillionaire has voiced his support for Bitcoin saying that, "money is just data that allows us to avoid the inconvenience of barter. That data, like all data, is subject to latency and error. The system will evolve to that which minimises both" (February 20, 2021). In fact, Elon Musk, one of the richest man in the world, announced in March 2021 that Tesla.Inc had bought $1.5 billion worth of bitcoin and subsequently would start accepting Bitcoin as a mode of payment.

Adam Back, a British cryptographer and the CEO of Blockstream has bitcoin, as is clearly evident from what he said on June 2, 2020, "The current environment is causing more individuals to think about hedging. It is causing people to think about the value of money and looking for ways to preserve money. It's a difficult environment to get any yield." Adam Back has been cited as a probable Nakamoto candidate alongside Hal Finney and Nick Szabo. He also invented Hashcash which is used in the Bitcoin mining process.

Zhao Chengpeng, a Chinese-Canadian business executive and the founder and CEO of Binance, the world‘s largest cryptocurrency exchange by volume has chronicled the 2020 halving by saying these words, ”The halving should be very positive for the crypto industry. As long as there is a currency that offers a very high degree of freedom, that allows people to transact globally, that‘s really cheap to use and very safe, we care about those fundamental things. If another coin does that, I think it benefits all of our societies and that‘s a very positive thing for the industry” (May 11, 2020).

Warren Buffet, the well-known American investor and business tycoon has combatted bitcoin several times. The CEO of Berkshire Hathaway Inc. said on February 24, 2020 that, ”Cryptocurrencies basically have no value and they don‘t produce anything...It doesn‘t deliver, it can‘t mail you a check, it can‘t do anything, and what you hope is that somebody else comes along and pays you more money for it later on. But then that person‘s got the problem. But in terms of value: zero.”

Nouriel Roubini, chairman at the Roubini Global Economics one of Bitcoin‘s fiercest critics has said, ”[Bitcoin is] maybe a partial store of value, because, unlike thousands of others, it cannot be so easily debased because there is at least an algorithm that decides how much the supply of bitcoin raises over time, because for most of those other ones, literally, is done ad hoc, and they're being debased faster than what the [U.S. Federal Reserve] is doing," in an interview with Yahoo Finance. He also had claimed on February 2, 2018 that Bitcoin ”is the mother of all bubbles and is also the biggest bubble in human history if you compare it to, say, the Mississippi bubble or the tech bubble or tulip mania or South Sea Bubble...Now it has crashed by about 60% compared to the peak of mid-December. It has crashed 30% in the last week and 10% today...the fundamental value of Bitcoin is zero.”

Jeremy Grantham, a British investor and co-founder of Grantham, Mayo, & van Otterloo (a Boston-based asset management firm) said on January 3, 2018, ”Having no clear fundamental value and largely unregulated markets, coupled with a storyline conducive to delusions of grandeur, makes this more than anything we can find in the history books the very essence of a bubble.”

Bill Gates, the American business magnate, software developer and the second-richest man in the world was a proponent of Bitcoin and had described Bitcoin as being ”exciting because it shows how cheap it can be. Bitcoin is better than currency in that you don‘t have to be physically in the same place and, of course, for large transactions, currency can get pretty inconvenient.” On October 2, 2014. However, on February 27, 2018 he described it in a contradictory manner. He said, ”The main feature of crypto currencies is their anonymity. I don't think this is a good thing. The government‘s ability to find money laundering and tax evasion and terrorist funding is a good thing. Right now crypto currencies are used for buying fentanyl and other drugs so it is a rare technology that has caused deaths in a fairly direct way.” Two years hence he said, ”I do think people get bought into these manias who may not have as much money to spare. So I‘m not bullish on Bitcoin. My general thought would be that if you have less money than Elon [Musk], you should probably watch out” (February 25, 2021).

Joseph Bernhard Mark Mobius is an American-born German fund manager and investor who is also the founder of Mobius Capital partners LLP. Extract from ’https://www.moneycontrol.com/news/business/markets/mark-mobius-good-opportunity-to-buy-indian-stocks-despite-covid-crisis-cryptocurrency-a-very-risky-area-6910361.html' Mark Mobius called cryptocurrency a "very risky area". He said that it is difficult to predict the direction of cryptocurrency prices and questioned how easy it is to convert them into "real money”. He also disagreed with the idea that bitcoin, the world's largest cryptocurrency, could replace gold as a hedge against inflation. "I can't have a crypto ring whereas I can have a gold ring —that‘s the real difference," he said.

It’s interesting to learn about the verbal spat between legendary investor Warren Buffet and the stock trading app Robinhood. Warren Buffet called Robinhood a speculative and casino-like trading app in the stock market from which it benefits. At Berkshire Hathaway’s annual meet on May 1, 2021, Buffet said that Robinhood has, “become a very significant part of the casino aspect, the casino group, that has joined into the stock market in the last year or year and a half.” Robinhood, who aims at democratising investing, defended itself soon after. A Robinhood spokesperson told CNBC, ”There is an old guard that doesn‘t want average Americans to have a seat at the Wall Street table so they will resort to insults. The future is diverse, more educated and propelled by engaging technologies that have the power to equalise. Adversaries of this future and of change are usually those who‘ve enjoyed plentiful privileges in the past and who don‘t want these privileges disrupted. Their criticisms are unfortunate but they prove why Robinhood‘s mission is in fact critical.The new generation of investors aren‘t a ’casino group. ‘They are tearing down old barriers to investing and taking control of their financial futures. Robinhood is on the right side of history,”

Source:*https://www.cnbc.com/2021/05/01/warren-buffett-says-robinhood-is-catering-to-the-gambling-instincts-of-investors.html*

*https://www.forbes.com/sites/billybambrough/2020/11/13/nouriel-roubini-cryptos-fiercest-critic-admits-bitcoin-could-be-a-partial-store-of-value/?sh=3d27e6721615

Criticism of Bitcoin

“Right now Bitcoin feels like the Internet before the browser.”

– Wences Casares (Founder of Banco Lemon)

Bitcoin may be the future version of our traditional fiat currencies. But that makes it all the more imperative to know the serious risks associated with investing in bitcoin. Bitcoin has been severely criticised for its use in illegal and criminal activities, its price volatility and thefts and hackings from cryptocurrency exchanges. It has been characterised as a

speculative bubble by various economists at various times. Here, criticisms that have been addressed many times have been outlined.

The first criticism, which has been mentioned several times is that bitcoin is so volatile that it is quite doubtful whether it can successfully be a store of value. Bitcoin is volatile because of a perfect supply inelasticity and a decentralised market. Bitcoin owners and investors have given credence to the fact that volatility is the price they pay in order to access this digital asset which, they believe will have significant untapped potential. The volatility can also be justified because of the absence of any central power or authority, like a central bank, which could intervene to virtually subdue the volatility. It has, however, been observed that with more adoption, bitcoin‘s volatility can substantially decline over time.

The second criticism we have is that Bitcoin has failed to be a mode of payment. It is believed by economists and investors that Bitcoin, as a matter of fact, deliberately has an expensive and aa limited capacity, so that it can offer decentralisation and invariability. This has led many to have the opinion that bitcoin can only be used as a mode of payment in the case of small and low-value transactions. John Pfeffer, co-founder of Pfeffer Capital says, ”As a means of payment, it can perform better than incumbent technologies in specific instances (think international payments), but Visa, Apple Pay, Google Pay, PayPal and fiat currency work well and better than cryptocurrency for most day-to-day payments.” *

The third criticism in the queue is that Bitcoin is wasteful. It has been severely criticised for the amount of non-renewable energy and electricity it consumes while mining. at the end of 2017, an estimated one to four gigawatts of electricity was consumed due to mining alone. In 2018 alone, it was reported that minima activities utilised about 2.55 gigawatt of energy. Bitcoin was ranked among the ’TOP 30 ENERGY CONSUMING COUNTRIES OF THE WORLD ‘by the University of Cambridge in 2021 as it reportedly consumed more than 178 (TWh) annually. To combat the situation, miners have started mining in regions like Iceland, where plentiful geothermal energy and cool air (from the Arctic) is free, Tibet where hydroelectric power is available and is other places like The State of Washington, Austria, and Quebec to reduce costs incurred by electricity consumption.

The fourth one, and by far the most addressed, is that bitcoin is used for illegal and illicit activities. This criticism is similar to critiquing the internet for hosting fraudulent websites (dark web) or censuring cash for its usage in criminal activities. Bitcoin is really neutral which offers core properties that have an overall positive impact on society. Nevertheless, it may, of course, be used in illicit practices by miscreants who deliberately take advantage of the decentralised and censorship-resistant characteristics of bitcoin. It is important to note that though bitcoin is pseudonymous, it is not anonymous. Sophisticated technology has been improved and developed by blockchain analytical firms to trace criminal activities. Data shows that comprehensively, the number of bitcoin transactions relating to illegal activities is, in fact, very low.

The fifth in the row is that Bitcoin is not backed by anything. It is not backed by any decree, industrial utility, or cash flow. The only elements it is backed by a code and the consensus that exists among the primary stakeholders.

Last but not the least, there is a possibility that it can be replaced by a competitor. Many unsuccessful attempts have been made by digital assets to curb bitcoin‘s growing popularity and its adoption. However, to date, none of the competitors have been able to achieve the efficiency bitcoin has. Even though bitcoin‘s software is open-source and can be developed and improved, its inherent network effects and the acceptance of its key stakeholders cannot be replicated so easily.

*https://medium.com/john-pfeffer/an-institutional-investors-take-on-cryptoassets-690421158904

What does the future hold for bitcoin?

”Bitcoin may be the TCP/IP of money.”
– **Paul Buchheit** (Creator of Gmail)

Bitcoin, introduced almost a decade ago, aimed at revolutionising the financial sector in the industry. The first decade of this cryptocurrency was marked by a number of scandals and misconceptions. The surge in prices was not alone, but alongside came a whole lot of criticism. However, the optimistic enthusiasm of investors has been doubled regarding its future. Therefore, it can be rightly said that this decade will prove to be very critical in determining its future, and existence. Certain areas in the bitcoin ecosystem if paid attention to buy investors can surely restructure the financial network. Currently, it is viewed as a means of payment and a store of value. Investors are especially eager to gain profits from its price volatility. However, the obstacle of security and scaling have prevented both from really happening.

Economists, like Brad Garlinghouse are of the opinion that cross-border transactions and global partnerships will be crucial for the future of Bitcoin, or any other cryptocurrency for the matter. For years, crypto has been the most economical way of sending payments and financial transactions by migrant workers to their families, as the preposterous transaction fee is not applicable. International financial transactions account for billions of dollars on a daily basis. Remittances, too, are payment methods which are very expensive.

NFTs, non-fungible tokens, have much more power than then some perceive it to have. They're many uses include those associated with digital collectibles. Garlinghouse said, "Growing up, I had a baseball card collection, and the ability to trade baseball cards is very high friction. If you're able to issue an NFT associated with every individual baseball card, the traceability of that goes way up. When you talk about art, collectibles, music, there's a lot of use cases here that are very compelling.”*

Predictions regarding bitcoin are very clear, whether bitcoin had a wider adoption, more usage as a medium of exchange in the past decade. Cryptocurrencies and the blockchain technology have moved far from the earlier perception of

merely understanding the fundamentals or comprehending it for the purpose of technological curiosity. It has now entered the mainstream business and has formed the core of business conversations.

*https://www.inc.com/amrita-khalid/ripple-brad-garlinghouse-crypto-currency.html

Conclusion

'I am very intrigued by Bitcoin. It has all the signs. Paradigm shift, hackers love it, yet it's derided as a toy. Just like microcomputers."

– Paul Graham (Yahoo Store)

Bitcoin is an exhilarating revolution that can greatly develop human welfare and initiate innovational developments in communications, financial transactions, and business in a highly beneficial way. A decentraliSed currency was once nearly impossible, however, bitcoin's intrinsic use of clever encryption via the public key and an efficient peer-to-peer network has solved the impending aforementioned issue. All the core properties have enabled the creation of a payment system that has reduced transaction costs and international remittances while significantly assuaging poverty.

It has allowed privacy in terms of legitimate financial transactions made in online mode and has enabled a surge in new financial developments. An escape from monetary mismanagement and capital controls have been provided. However, just like the two sides of a coin, Bitcoin as a 'digital cash 'can be used in illicit activities, especially money laundering and illegal trade. Though it may sound tempting to critics, banning bitcoin is not the solution to the problem of money laundering and illegal monetary trade, because banning bitcoin is more or less the same as banning fiat currencies I.e. cash, which is not a solution to these social ills.

Albeit Bitcoin could possibly fail to perform its function as a payment system and ultimately as a digital currency. The bitcoin economy might get sabotaged by an unanticipated problem. In the future, there might be a superior cryptocurrency that could outweigh bitcoin and completely replace it. The possibilities for failure cannot be counted on our fingers, but bitcoin can never fail because of its complexity in workings and its far-flung potential which the policymakers might claim they did not comprehend. It is imperative to allow experimentation to continue in this field, not for the sake of Bitcoin alone, but for the sake of innovation.

Institutionalisation is important for the cryptocurrency business to alleviate the scale, drive growth and build trust. Organisations undauntedly face a lot of obstacles when dealing with cryptocurrencies which they need to channel through a cryptocurrency lens. There is an acute need of a framework which is comprehensive to prepare themselves for a revolutionised future.

We are heading towards a future where financial transactions through cryptocurrencies may become the standardised process. Keeping the new forms of assets and tokens are one side of the horizon, but a completely redefined marketing conditions and new network of investors will significantly have an impact over the next couple of years.

Glossary*

'Bitcoin actually has the balance and incentives right, and that is why it is starting to take off."

– Julian Assange (Founder of Wikileaks)

1) **Cryptography**- The study of mathematical methods for all the types of information security is known as cryptography.
2) **Cryptanalysis-** The science associated with the techniques of deciphering these mathematical methods is known as cryptanalysis.
3) **Cryptology-** The collective term used for the study of cryptography and cryptanalysis is coined Cryptology.
4) **Encryption-** In order to prevent unauthorised access, information or data is converted into a code using mathematical techniques, which is known as encryption.
5) **Protocol-** This term refers to the primary set of rules which allow data to be shared between operating computers.
6) **Plaintext-** Plaintext refers to the unencrypted information in a form that can be deciphered without the need of a specific key or a decryption device. It is the input in a crypto system.
7) **Ciphertext-** The algorithm which is applied to the plaintext to produce Ciphertext is known as cipher. The unreadable output of a crypto system, which is unreadable till it has been converted to plaintext is known as Ciphertext.
8) **Decipher-** The process of converting text written in a code or mathematical methods into normal comprehensive language is known as deciphering.
9) **Encipher-** The process of converting text normal comprehensive language into a code or mathematical methods is known as enciphering.
10) **Cryptocurrency-** A cryptocurrency is a digitalised currency which is maintained and tun by a decentralised system instead of a conventional central authority, in which transactions are verified using technologies, like the Blockchain.
11) **Bitcoin-** A type of digital currency in which a record of transactions is maintained and new units of currency are generated by the computational solution of mathematical problems, and which operates independently of a central bank.
12) **Blockchain-** All the transactions made using bitcoins are registered in a public ledger, which can be viewed by anyone in this world. This public record is called a blockchain.
13) **Block-** A block is a part of the blockchain which records the most recent transactions, which are verified through the process of mining.
14) **Decentralisation-** Decentralisation means that there is no country or organisation who owns the Bitcoin network. All work is partitioned between the people who own bitcoin. The users need to communicate with each other and send information to each other, instead of approaching an organisation such as a bank.

15) **Satoshi Nakamoto-** Satoshi Nakamoto, the brain behind Bitcoin, is the name of the person or persons who posted the cryptography mailing list in 2008, which was indeed a turning point in the history of cryptocurrencies.
16) **Mining-** The blockchain is checked every ten minutes to confirm transactions. This process is carried out with the help of bitcoin mining. Bitcoin mining involves using a computer to perform mathematical calculations, to check the authenticity of every transaction and to confirm them.
17) **Hashing-** Hashing, in simple language, means taking an input string of any length and giving out an output of a fixed length. the transactions are taken as input and run through a hashing algorithm which gives an output of a fixed length, in the context pf Bitcoin.
18) **Halving-** Bitcoin halving refers to the process of halving the bitcoin mining rewards after a set of 210,000 blocks have been mined. As of 2021, there have been three halving. The first one in 2012, the second one in 2016 and the latest one in 2020.
19) **Change-** When the unspent output of a transaction is used as the input in a new transaction, 'change 'is returned if the amount is higher than required. This is fairly like simple mathematics.
20) **Private key-**In bitcoin transactions, you have a password, using which you can spend the bitcoins from your bitcoin wallet through a cryptographic signature. This password should never be revealed to anyone.
21) **Double storage-** Double spending conventionally means spending the same money twice. However, in case of digital currency, our money is in the form of bits, which are much easier to copy and hence double spending is theoretically possible. Bitcoin prevents double spending, because of all the transactions being stored in the blockchain and getting verified by the miners.

*https://blog.unocoin.com/10-commonly-used-bitcoin-terms-explained-b50e8c484a44