

ANALYSIS OF CRYPTOCURRENCIES: WHY BITCOIN IS LEADER?

Anu Priya¹, Dr. Shruti Garg²

¹BIT, Mesra, Ranchi

² Assistant Professor, BIT, Mesra, Ranchi

Abstract. Analysis of any currency is done to identifying and quantifying uncertainties, estimating their impact on results. Cryptocurrency, as an encrypted peer-to-peer organize for encouraging digital bargain is created in 2008. i.e., Bitcoin is the most prominent example. It characterizes their exchange rates versus U.S Dollar by fitting parametric dispersions to them. Then analyze the Blockchain (BC), the introduced technology behind the Bitcoin cryptocurrency system, considered both alluring and critical for ensuring enhanced security and privacy for diverse applications in many domains. Another new investment opportunity, new cryptocurrencies known as altcoins. This altcoinuses similar cryptography technology but employs different algorithmic design. Cryptocurrencies may revolutionize digital trade markets by making a free streaming exchange framework without fees. Bitcoin has presented a SWOT (Strength, Weakness, Opportunity, and Threat) analysis, which lights up a few of the later occasions and developments, that may influence whether Bitcoin contributes to a move in the financial ideal model.

Keywords: Cryptocurrency, Bitcoin, Blockchain, Altcoin, Encrypted, Exchange Rates

1 Introduction

The first world's most familiar and common cryptocurrency is Bitcoin. It can be sent or received from a channel of transfer protocol i.e., client to client as well as peer-to-peer. This can be organized without the involvement of additional participant in very straight and extent manner. Exchange of digital currency is confirmed by the network hubs, by proper utilization and implementation of cryptography and is recorded in an open widely spread records, well known as the blockchain (Relatively a new technology).

Blockchain (BC), the innovation behind Bitcoin cryptographic money framework, is fundamental for shaping the spine for guaranteeing improved security and protection for different applications in numerous different spaces including the Internet of Things (IoT) biological system. Universal research is at present being led in both scholarly community and industry applying Blockchain in differed spaces. The Proof-of-Work (PoW) numerical test guarantees BC security by keeping up an advanced record of exchanges that are thought to be unalterable.

Furthermore, BC utilizes an alterable Public Key (PK) to record the clients' character that gives an additional layer of protection. The effective appropriation of BC has been actualized in assorted non-money related frameworks, for example, in internet voting, decentralized informing, conveyed distributed storage frameworks, confirmation of-area, social insurance et cetera. Decentralization allows the blockchain technology to have increased capacity, better security, and faster settlement. (Kuo, Lee, & Wang, 2018)

Cryptocurrency is a way to exchange money digitally. They are implemented by the theory of solving encryption algorithms to create unique hashes that are finite in number. The opening of unbelievable exploratory cryptographic forms of money known as altcoins. The altcoins utilize comparable cryptography innovation however utilize diverse algorithmic plans.

cryptocurrencies and the latent blockchain technology have advantages that have spurred their growth, Currencies have two basic roles, the essential and most basic part of a money is to go about as a comprehensively acknowledged medium of business. In the above setting, Governments set incomes, and incomes are the greatest single installment in any economy. For example, people in general will dependably request the legislature sponsored monetary standards since they are utilized for paying incomes. As per the writing, an association could get a digital money against offers of merchandise, yet it would then need to pay company incomes, finance incomes and deals incomes in government-sponsored cash. What's more, the organization would go out on a limb as a swapping scale chance. In the event that the legislature upheld money ascends in an incentive against the cryptographic money the association would be in danger of noteworthy misfortune. The auxiliary part of a cash is to go about as a store of significant worth. Individuals need to trust that what their money can purchase today and tomorrow. So as to direct the estimation of the money, the national bank faces a considerable measure of bothers to keep up the estimation of cash balanced out. (Investment & Americas, 2017)

There are many ways of earning money through cryptocurrency, one of the safe way to earn money in cryptoland is "Buying and Holding". Where buying a good cryptocurrency that includes a crucial utilize case and holds them until they get a reasonable marketshare. For example, cryptocurrencies like Bitcoin, Ethereum, Litecoin, Monero etc. So, in this paper, we are performing the analysis of Bitcoin because at present a lot of media attention is there, and its total market value has reached 20 billion USD in March 2017. More importantly, several central banks begun as of late to investigate the appropriation of cryptocurrency and blockchain innovations for retail and large-value installments. For example, the People's Bank of China aims to develop a worldwide digital currency based on blockchain technology. (Chiu & Koeppl, 2017) Bitcoin is one of the most popular cryptocurrency since 2009, the market price of Bitcoin increases from an essential value of \$0 to a value \$6,386.07 at the time of this composing. Too as compared with the other celebrated cryptocurrency, the esteem of Bitcoin is more shown in figure 1.

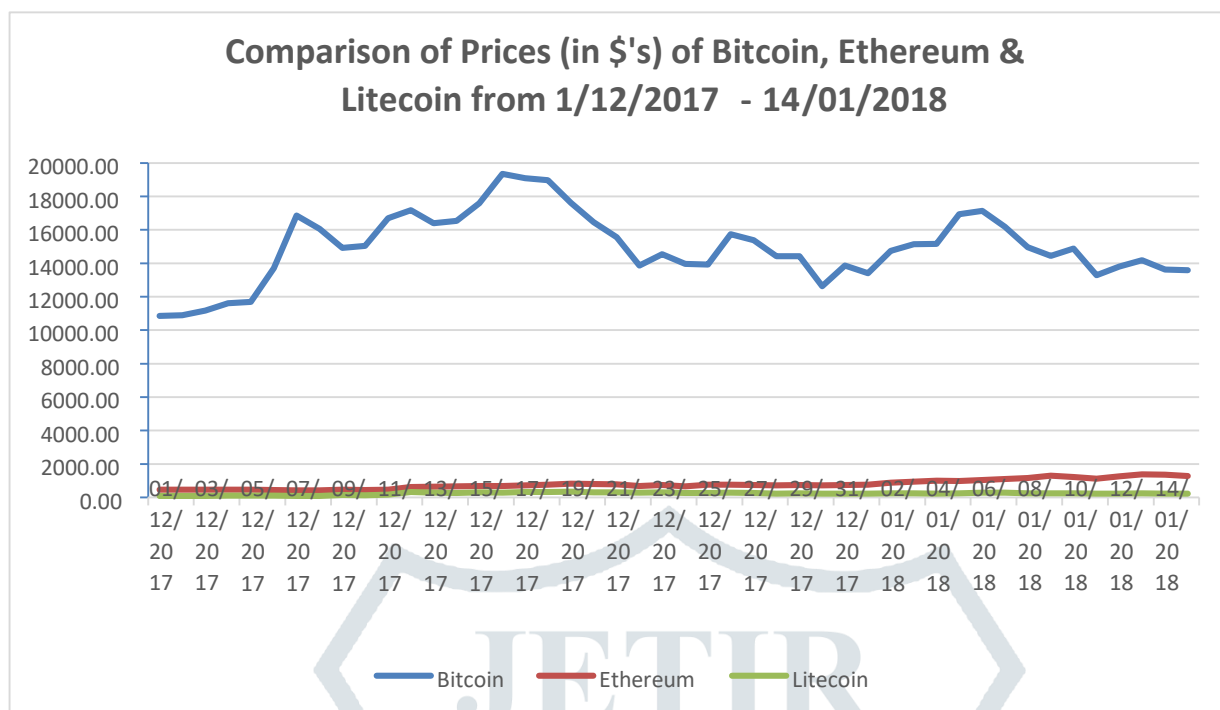


Figure 1. Comparison of cost prices of Bitcoin, Ethereum & Litecoin.

The closing prices of the major cryptocurrencies like Bitcoin, Ethereum and Litecoin were comparing from December 2017 to January 2018 as this was the time when the instability of crypto-currencies was very high. It was seen from the chart that there's the most noteworthy instability of Bitcoin and the costs for the Bitcoins appear a declining slant but at the same time, Ethereum and Litecoin comparatively appearing expanding slant as they are recently presented coins into the advertise. (Bhosale, 2018)

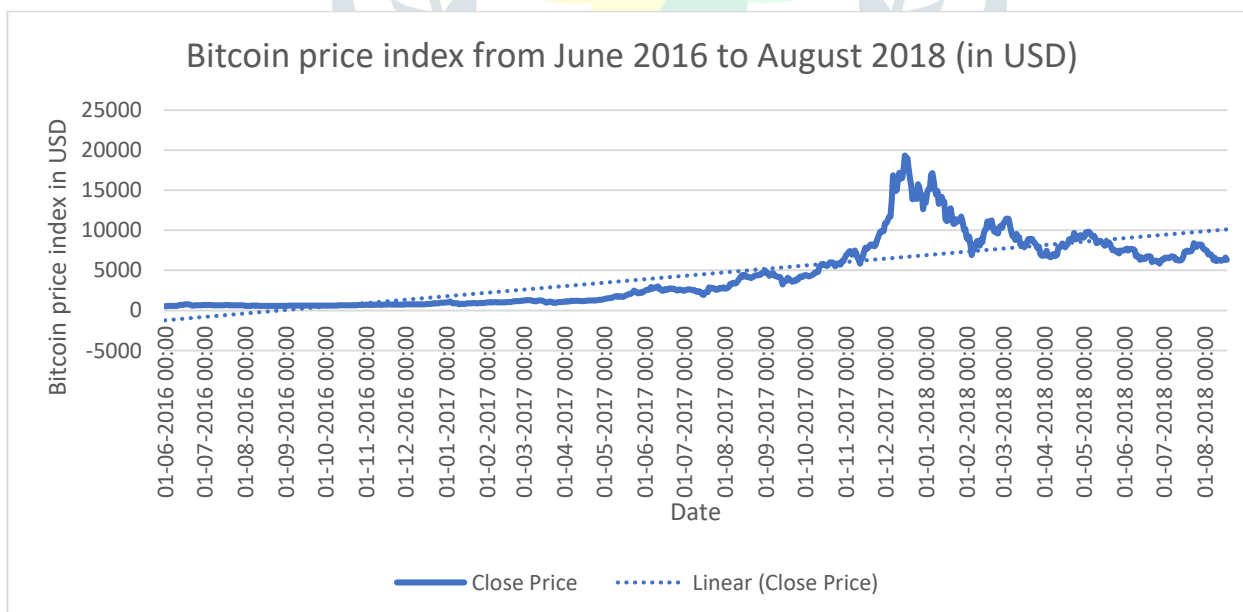


Figure 2. Market price value of Bitcoin from June 2016 to August 2018

Source: coindesk.com

In figure2. shows the cryptocurrency of Bitcoin value from June 2016 to August 2018, where the close price value is 577.86 and 6312.83 respectively. In which dark blue line shows the variation of closing price of Bitcoin and the dotted line shows the average closing price of Bitcoin where closing value increases exponentially. The average close price value is increased upto 10000 in the year 2018 from the year 2016.

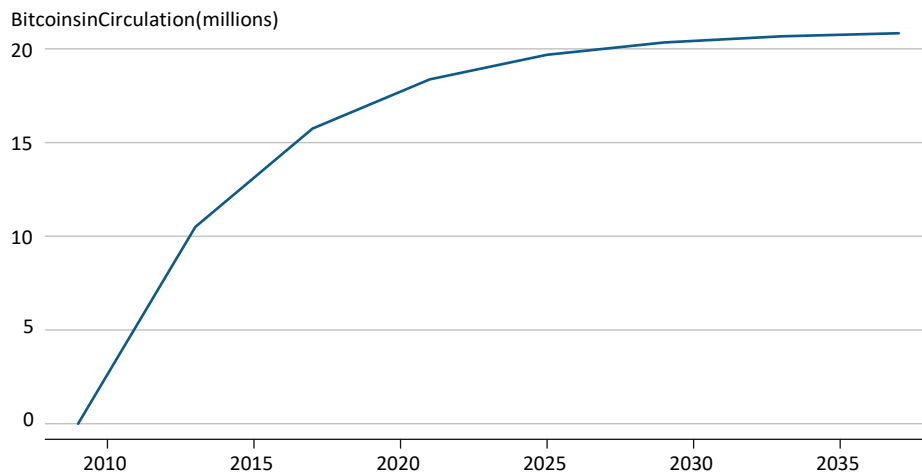


Figure 3. Bitcoin in circulation: Schedule to converge to 21 Million Units.

(Berentsen & Schar, 2018) In this paper they have given an analytical data in figure 3. the Bitcoin in circulation approx 21 million USD up to the year 2035.

In this section, we described the most popular cryptocurrency Bitcoin and also about Blockchain technology used for Bitcoin. It has been shown that how cryptocurrency earns money by using “buying and holding” property and why Bitcoin is more popular than other cryptocurrencies using graph data by comparing the three most popular cryptocurrencies.

2 Literature Review

The certain goal of this paper is to focus on the study of Statistical Analysis of cryptocurrencies. Devries, 2016, focuses statistical analysis of the top seven type of cryptocurrencies i.e., Bitcoin, Ripple, Litecoin, Monero, Dash, MaidSafeCoin, and Dogecoin. The investigation and results for the exchange rate of Bitcoin when contrasted with the U.S. Dollar by utilizing a noncausal autoregressive process with Cauchy mistakes. The results demonstrate that the delivered Bitcoin/USD conversion scale indicates nearby patterns which shows a time of theoretical conduct from web based exchanging. By teaching, this is certain that the greater part of the digital currencies display considerable trails. By utilizing one of the segregation criteria of the log likelihood, AIC, AICc, BIC, HQC and CAIC for the fitted distribution, the got results demonstrate that none of the distributions used to give the best fit commonly over the information for all the cryptographic forms of money. In any case, locate the exact and summed up strategy for hyperbolic conveyance which gives the best fit for the Bitcoin and LiteCoin; the normal inverse Gaussian distribution gives the best fit for Dash, Monero, and Ripple; the generalized distribution allows the best fit to Dogecoin; the Laplace distribution gives the best fit to MaidSafeCoin. Ramifications of these outcomes are in the case of risk management, where one may need to find out the VaR and ES for risk, yet in addition for investment purposes. (Osterrieder, Chan, Chu, & Nadarajah, 2017)

Kuo et. al., 2018, focused on the broadening part of digital currencies and investigate the likely plausibility that may produce chronicled information when contrasted with the attributes of cryptographic forms of money and the conventional resource classes and analyzed the static relationships between them, and additionally the dynamic conditional correlations. The outcome which appears, the CRIX (CRptIndex) and cryptocurrencies can be a decent alternative to help the enhance portfolio dangers in view of the relationships existed between the cryptocurrencies and traditional assets are consistently low as a comparison to the average daily return of most cryptocurrencies is higher than that of the traditional investments. (Kuo et al., 2018)

Portfolio examination investigates the execution subsequent to processing CRIX to a specific portfolio that especially comprises of the traditional assets, (for example, S&P 500, PE, REITs, and gold). The return and standard deviation of CRIX and six regular investments. CRIX has maximum return value, and it is the special case that lies on the gainful limits, while the return from oil is the minimum with relatively high level of risk. As per the transition map of portfolio performance, S&P 500 and CRIX overwhelms the portfolio, though alternate ventures just offer to the portfolio when the portfolio risk is most minimal. Amidst every one of the seven alternatives, oil appears to have the least profitable investment. The mean variance spinning tests, the amplifying impact of CRIX and cryptocurrency stands just for the worldwide least difference portfolio, not to the tangency portfolio. Also, sentiment analysis suggests a good investment opportunity to make available for investors with an annualized return.

Phillip, Chan, & Peiris, 2018, did the empirical data analysis shows Cryptocurrencies exhibit long memory, leverage, stochastic volatility, and heavy-tailedness. Ripples are not dependent on any third party for redemption, such as it is the only currency with no counterparty credit risk. Due to this safety feature, Ripples has been progressively used by banks and large corporations as their preferred settlement infrastructure technology due to minimized future exchange rate volatility risk. As compared to all other cryptocurrencies Ethereum (ETH) and Dash are more user-friendly. There is a larger community-based approach with computer programmers actively making both Cryptocurrencies easier, safer and quicker to use. Sometimes Bitcoin takes up to 48 h to send money from one user to another, this is the biggest criticism of Bitcoin. ETH uses smart contracts to use blockchains as compared to Bitcoin and Dash is the only currency that uses rapid transactions, which solves the longer

confirmation timeproblem of Bitcoin. This can be perceived that ETH and Dash have lower liquidity risk than Bitcoin.(Phillip, Chan, & Peiris, 2018) The price of the Ethereum currency grew over 13,000% from 2014 to 2017.(Bhosale, 2018)

As per the originator of Litecoin, Charles Lee, Litecoin was considered as a silver against bitcoin which was dealt with as a gold. The distinction amongst Bitcoin and Litecoin is that for mining Bitcoin overwhelming preparing and quick registering is required dissimilar to, Litecoin which can be mined by a typical personal computer with lesser processing power. The fundamental motivation behind Litecoin was to process smaller value transactions quick. Mintchip is likewise a cryptographic money which is made by the administration organization like Royal Canadian Mint. MintChip is a smart card that holds electronic value and can exchange safely from one chip to the next. Like Bitcoin, MintChip does not require individual recognizable proof but rather dissimilar to Bitcoin, it is supported by a physical money, the Canadian dollar.(Bhosale, 2018)

The request of the Blockchain idea and innovation has developed past its utilization for Bitcoin age and exchanges. It can either be public or private, contingent on the extent of its utilization. Public Blockchains that limit the access to only either read or write. In actuality, a private Blockchain limits to itsdesignated trusted participants only. The significant favorable circumstances of the Blockchain are execution innovation which is public and decentralization. The properties of its security, privacy, traceability,inherent data provenance and time-stamping has seen its own reception past its particular application areas. The Blockchain itself and its variations are currently used to secure any sort of transactions, regardless of whether it would be human-to-human interchanges or machine-to-machine. Its appropriation imagines to be most secure particularly inside the worldwide development of the Internet-of-Things (IoT). Its decentralized application built up worldwide Internet which is exceptionally charming as far as guaranteeing information excess and thus survivability. The Blockchain has been chiefly perceived to be reasonable in creating countries where guaranteeing trust is a noteworthy concern. Consequently the creation of the Blockchain can be viewed as essential and much required additional part of the web that was absent in security and trust some time as of late. Blockchain innovation still has not achieved its development with a desire for a long time as novel applications continue to be realized all inclusive.

Poon & Dryja, 2016 made the Bitcoin Blockchain scalable by a network of Micropayment channel. If all business is utilizing the Bitcoin as micropayment channel which was conducted inside a network, to perform 7 billion people to make two channels per year with limitless business inside the channel, it would require 133 MB blocks (pre-assumed 500 bytes per business and 52560 blocks per year). The current generation of computers will be able to perform a full node with old blocks pruned out on 2TB of storage, with a network of instantly confirmed micropayment channels whose payments are encumbered by time locks and hash lock outputs, Bitcoin can scale to billions of users without custodial risk or blockchain centralization when transactions are conducted securely off-chain using bitcoin scripting, with prosecution of non-cooperation by dispersing signed multisignature transactions on the blockchain.

Heilman, Kendler, Zohar, andGoldberg displayed an obscure attack on bitcoin's peer-to-peer network that undermines bitcoin's center security ensures, permitting attacks on the mining and agreement framework, counting N-confirmation double investing and antagonistic forks within the blockchain.The attack is for nodes with public IPs. They invent mathematical models for the attack and prove them with Monte Carlo simulations, measurements, and experiments. At that point,they illustrate the experiment of the attack by performing its own live bitcoin nodes and finding that an attacker with 32 distinct /24 IP address blocks, or a 4600-node botnet, can overshadow a casualty with over 85% likelihood within the attacker's most exceedingly worst case. Furthermore, even a 400-node botnet sufficed to attack own live bitcoin nodes. At long last, they proposed countermeasures that make eclipse attack more troublesome whereas still protecting bitcoin's openness and decentralization; a few of these were consolidated in a later bitcoin software upgrade.(Heilman, Kendler, Zohar, & Goldberg, 2015)

Peter D.DeVries, 2016 didSWOT analysis of Bitcoins in which displayed the later occasions and developments that seem impact whether Bitcoin Contributes to shift in economic standards.At the beginning of the strategic planning process or during a blueprint refresh. The whole authority group should be intensely included since they should have the capacity to see over the organization and offer knowledge into the competitive environment and/or trade scene. When the authority group offers appropriate recommendations regarding strengths, weaknesses, opportunities, and threats, then it will end up with a SWOT analysis that has the validity to be utilizedpractically in the strategic planning process.(Jackson, 2018)The strength of the Bitcoin has quality by the plan to create it a viable currency that has lifted it in status over the years, more strikingly the fixed limit of bitcoin that will exist. The US Dollar Index (Desjardins 2016) stated Bitcoins as the best performing currency of 2015. An exponential growth in Bitcoin flow will motivate vendor acceptance to accommodate customer needs. Theoretically, this would be a cyclical process effect. As vendors are adopting the cryptocurrency technology more efficiently which will result in capitalize the benefits of users. (Devries, 2016)Bitcoin has few internal weaknesses that cannot be modified easily because weaknesses are the parts of its design.Bitcoin's has the highest capacity among all cryptocurrencies even though the price of Bitcoins is at risk in a shallow market. According to the status of the currency in its current market and states, Cryptocurrencies are seemed to be a mature form of currency. This problem can be rectified by analyzing the further growth and adoption theoretically. (Devries, 2016)

Cryptocurrency is in a novel position as a precursor in a conceivably transformative innovation for the long-standing money related frameworks. Bitcoin's innovation enables the people to trade money without the cooperation of another confided in party, similar to a bank, to overview the transactions. The transactions can hit with any number of unexplained expenses as it crosses borders, making it hard to send the right add up to another business. A decent case of this sort of crisis require is an online company who is suffering from a denial-of -service(DoS) attack and is looking forward to getting immediate protection from a network security providing company. Bitcoin's (one of the biggest openings) go about as a kind of ware, like gold. (Devries, 2016)

Bitcoin has a couple of obstacles to clear for client acknowledgment to become widespread. In a review performed by PwC, absence of central ownership of cryptocurrencies means that any endeavor to remediate this promoting issue utilizing ads could hypothetically enable the contributing to organization's opposition. This isn't perfect for an advertising design. Cryptographic forms of money have likewise observed extortion and robbery, by and large because of broken framework setups by trade organizations. These hacks by and large make the news, and can without much of a stretch persuade the layman that they are perilous areas to put their cash. (Devries, 2016)

3 The Future

Defenders of cryptocurrency contend it being secure from financial changes or worldwide vulnerabilities. Cryptocurrency cash is additionally being vouched as a "safer" option. However, significant capriciousness within the esteem of cryptocurrencies is a set up the truth and one which cannot be undermined. Questions moreover proceed to be raised around the supply and request flow and whether virtual cash can genuinely be considered a "currency".

Cryptocurrency and underlying Blockchain industries are still working, in the coming future, we are able to see lots of progress in it. There are also difficulties in design although not impossible. In reality, digital cryptocurrency generally has a fair share of disappointments. But in spite of them, numerous people still accept cryptocurrency has a bright future.

4 Conclusion

Although different researchers performed various kind of analysis of various cryptocurrencies like Bitcoins, altcoins, ripples etc. All different type of analysis found that Bitcoins are leading cryptocurrency as its performance is stably higher since 2015. Bitcoins are also found reliable for banking and other secure transactions because it develops a worldwide digital currency based on blockchain technology. Cryptography is used to produce a mathematical function to be solved by the blockchain ensures in which always observed highest security credentials. It has caught the eye of the investors and this is often because of the security it offers together with its trust and robustness as a system. The figure 4 is showing growth of Bitcoins from 2016-2018. In figure 2, shows the cryptocurrency of Bitcoin value from June 2016 to August 2018, where the close price value is 577.86 and 6312.83 respectively. Thus one can suggest bitcoins as best cryptocurrency for investors. Bitcoin has also introduced a SWOT (Strength, Weakness, Opportunity, and Threat) analysis, which focuses up a some of the subsequent instances and processes, that might have an impact on Bitcoin which either participates for the advancement in the field of the financial ideal model.

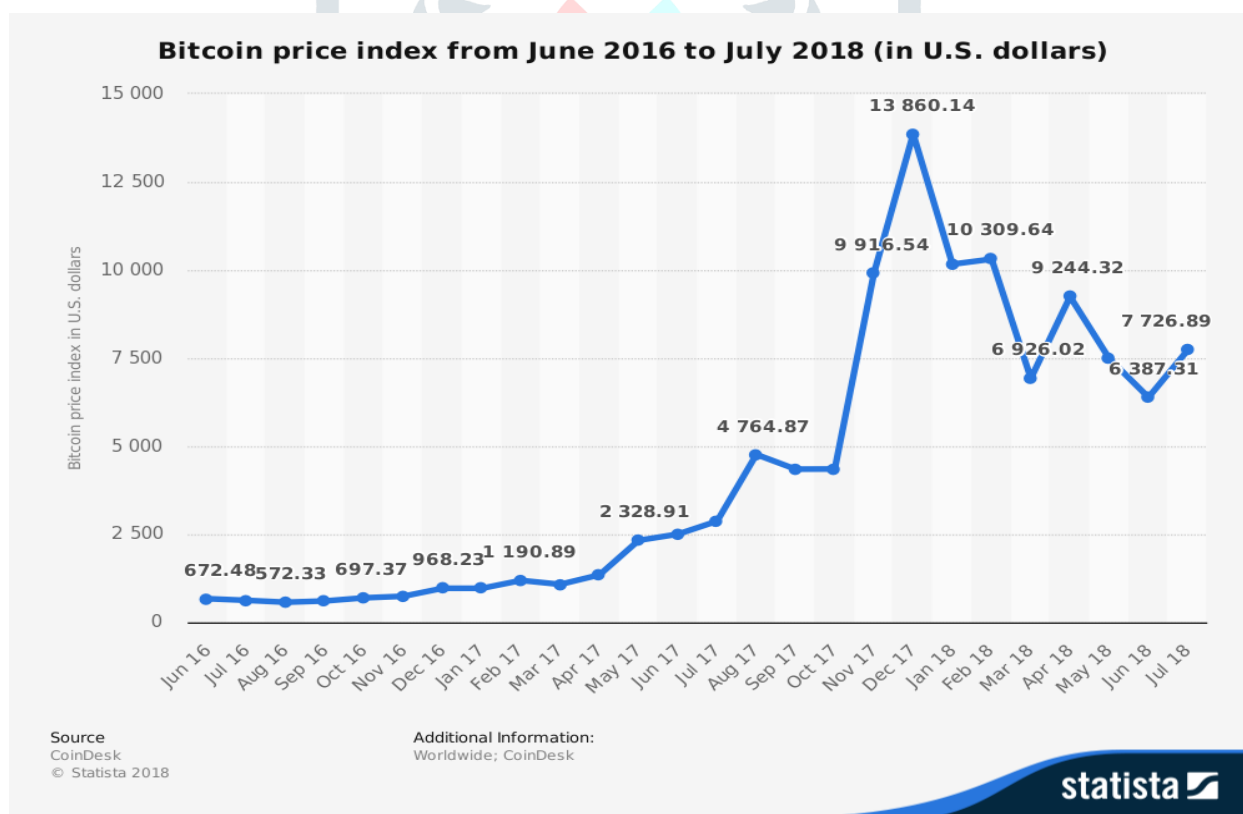


Figure 4 is showing growth of Bitcoins from 2016-2018

References

1. Berentsen, A., & Schar, F. (2018). A Short Introduction to the World of Cryptocurrencies. *Ssrn*, 1–16. <https://doi.org/10.20955/r.2018.1-16>
2. Bhosale, J. (2018). Volatility of select Crypto-currencies : A comparison of Bitcoin , Ethereum and Litecoin, *6*(March), 132–141.
3. Chiu, J., & Koepl, T. V. (2017). The Economics of Cryptocurrencies – Bitcoin and Beyond. *Ssrn*, 1–40. <https://doi.org/10.2139/ssrn.3048124>
4. Devries, P. D. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future. *International Journal of Business Management and Commerce*, *1*(2), 1–9.
5. Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse Attacks on Bitcoin’s Peer-to-Peer Network. *USENIX Security Symposium*, (August), 129–144.
6. Investment, C., & Americas, O. (2017). Cryptocurrencies, <https://www.ubs.com/content/dam/WealthManagementAmericas/cio-impact/cryptocurrencies.pdf>.
7. Jackson, T. (2018). *A Detailed SWOT Analysis Example* <https://www.clearpointstrategy.com/swot-analysis-examples/>
8. Kuo, D., Lee, C., & Wang, Y. (2018). Cryptocurrency: A new investment opportunity?, *20*(3), 16–40. <https://doi.org/10.3905/jai.2018.20.3.016>
9. Miraz, M. H., & Ali, M. (2018). *Article. Annals of Emerging Technologies in Computing (AETiC)* (Vol. 2). Retrieved from www.aetic.theiaer.org
10. Osterrieder, J., Chan, S., Chu, J., & Nadarajah, S. (2017). A Statistical Analysis of Cryptocurrencies. *Ssrn*, (February), 1–23. <https://doi.org/10.2139/ssrn.2948315>
11. Phillip, A., Chan, J., & Peiris, S. (2018). A new look at Cryptocurrencies. *Economics Letters*, *163*(November), 6–9. <https://doi.org/10.1016/j.econlet.2017.11.020>
12. <https://www.statista.com/>

