Cryptosurvival: Survivability and Financial Analysis in a World of Volatility

EMSE 6099: Problems in Engineering Management

The George Washington University

Professor Jonathan Deason

Final Report

Date of Submission: April 22, 2021

Azamat Kulzhanov, *Department of Engineering Management & Systems Engineering*

Brandon McGee, *Department of Engineering Management & Systems Engineering*

Saurav Pantha, *Department of Engineering Management & Systems Engineering*

I. Introduction:

While only just entering its teenage years, cryptocurrencies have quickly gone from the dark corners of the internet to being traded on open markets by some of the financial market's largest players, the myriad number of cryptocurrencies seem here to stay. From the inception of the first Bitcoin in January of 2009 now over four thousand assets that are readily tradable globally, cryptocurrencies may have as of yet fallen short of their promise to create a decentralized global currency; but they have held their weight in importance[1]. As of April 2021, the total market capitalization of cryptocurrencies has surpassed $2 Trillion USD (Kharif 2021).

Such a sudden rise has not been without its consequences. Governments across the world are pondering regulations from treating them like traditional securities to an outright ban. The sheer energy consumption of cryptocurrency mining provides a theoretical ceiling to the amount the world's energy can handle. While the origins of this project was one in the search of profit, our team came to realize that the world of cryptocurrencies is still too nascent to be readily predictable (within reason) like traditional assets. Such a realization leads us down the path of investigating the potential future of cryptocurrencies; most importantly, will they even end up surviving to be more than a niche in the intersection of libertarianism and quantitative finance. Throughout this paper, we aim to understand the potential risks and benefits posed to cryptocurrencies from energy consumption to regulation, perform a basic survivability analysis and end up with our original financial analysis. Since starting, the market cap of cryptocurrencies has since doubled and major governments have proposed new regulations or even cryptocurrencies themselves. Seen below, is a quick glance at the ten largest cryptocurrencies by market capitalization and some key facts about them[2].

[1] In reference to data taken from Coinbase.com and CoinGecko.com on April 2, 2021 where Coinbase tracked and allowed trading in 4,598 assets and CoinGecko tracked trading in 6,638 assets.
[2] Sources can be found in the Appendix in Table A.1

Cryptocurrency (Abbrev.)	Creation Date	Category	Price per Unit (in USD)	Total Market Cap. (Apr 2021)	Verification/Consensus Method	Total Supply (fixed, not in current circulatio	Annual Energy Consumption	Sourc
Bitcoin (BTC)	Jan 2009	Currency	$63,427.00	$1.18 T	PoW (Proof of Work)	21,000,000	57.1 Billion kWh	1,2
Ethereum (ETH)	Sep 2014	Software platform	$2,363.00	$272.84 B	PoW [Announced switchover to PoS]	Unlimited	2.57 Billion kWh	1,3
XRP (XRP)	June 2012	Currency	$1.74	$173.71 B	Custom	100,000,000,000	474,000 kWh	1,4,5
Stellar (XLM)	Aug 2014	Currency	$0.62653	$66.06 B	Custom	Unlimited	n/a	1,2
Tether (USDT)	Feb 2015	Stablecoin	$1.00	$46.78 B	n/a, use of BTC blockchain	Pegged to USD, Unlimited	n/a	1,6
Cardano (ADA)	May 2017	Software platform	$1.44	$46.26 B	PoS (Proof of Stake)	45,000,000,000	~86,000 kWh	1,7
Chainlink (LINK)	Jun 2017	Application token	$38.04	$38.04 B	n/a	417,510,000	n/a	1,8
Litecoin (LTC)	Oct 2011	Currency	$269.96	$18.20 B	PoW	84,000,000	n/a	1,2
Bitcoin Cash (BCH)	Aug 2017	Currency	$825.62	$15.44 B	PoW	21,000,000	n/a	1,9
USD Coin (USDC)	Sep 2018	Stablecoin	$1.00	$11.16 B	n/a	Pegged to USD, Unlimited	n/a	1,10

Table 1.1: A quick summary of the ten largest cryptocurrencies

II. Literature Review & Major Considerations:

A. A Brief History

"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. . . . What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." - Satoshi Nakamoto, 2008[3] (Nakamoto 2008)

As noted in *The Explosion in Cryptocurrencies: A Black Hole Analogy,* the authors take note of the literal explosion in the amount of cryptocurrencies in a decade citing an increase in the number of available and tradable currencies has risen **266,900%** in a 126 month period (Ballis, Drakos 2021). This hints at our focus on trying to understand the survivability going into the future (see Figure A.1 in the Appendix for a graph of the market over time).

In the decade since its inception, Bitcoin remains the largest cryptocurrency by both market cap and public recognition. As will be discussed further below, one of the hindrances to any financial approach is the inherent correlation between Bitcoin and other cryptocurrencies. The market share of Bitcoin reached its lowest point in January of 2018 with one third of the market and with a current majority at 54%[4]. While their underlying technology may be different, it is hard to separate most individual cryptocurrencies from the Bitcoin market. While the market remains incredibly volatile, the biggest players can still be analyzed for any insights and risks.

B. Existing and Proposed Regulations

"The sovereign is a jealous god"[5] -Professor Steve Hanke (Patel 2021)

[3] From the origin document proposing the invention of Bitcoin; Satoshi Nakamoto is the pseudonym for the unknown Bitcoin founder.
[4] See Appendix Figure A.2 for market breakdown over time
[5] From The Decoder Interview Podcast from The Verge airing April 6, 2021

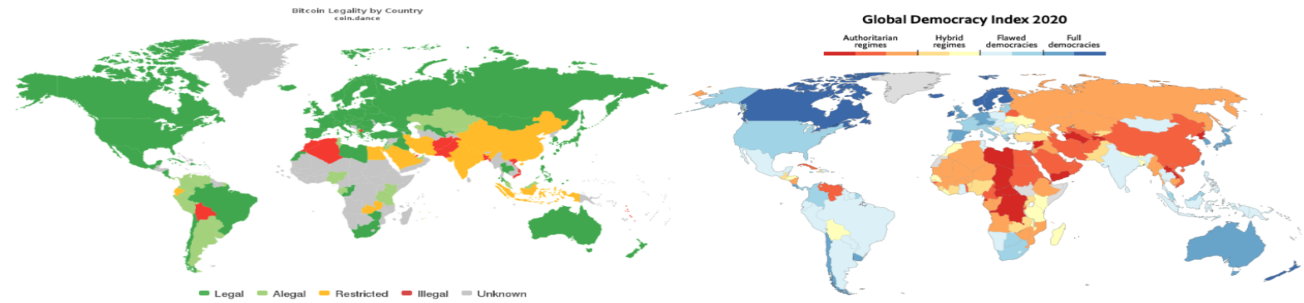


Figure 2.1. Existing legal status of cryptocurrencies in the world compared to a democracy index[6,7]

Shortly after entering the financial sphere, global governments began to understand the potential competition that cryptocurrencies could bring. As seen in *Figure 1* above, the world is relatively open to the concept of cohabitation in the competition for currency. However, this is primarily because cryptocurrencies are traditionally seen as financial assets and securities rather than as an actual currency competitor. In the online libertarian circles, this essentially means that Bitcoin and its successors are seen as failures having not meant their creative potential to compete with the US dollar. While some companies like PayPal and Square process cryptocurrency transactions (Molina, 2021), the real bulk of interest has come in the form of treating cryptocurrencies like traditional financial securities.

In the traditional OECD countries, cryptocurrencies are tolerated like other financial assets and taxed accordingly (Library of Congress, 2018). From this pool of countries, the main threat to cryptocurrencies come from the enforcement of anti-money laundering and anti-terrorism financing laws. During the latter days of the Trump administration (12/ 2020) in the US, the Department of Treasury's Financial Crimes Enforcement Network "FinCEN", filed a notice proposing new regulations that would require wallet platforms to maintain and disclose records of any transactions greater than a value of $10,000 within any 24 hour period (FinCEN, 2020). The proposed regulation would effectively tie the user to the wallet; with the wallet being the gateway to all previous transactions on that financial asset's blockchain history. Needless to say, such a regulation would render a decentralized network useless and remove its original attraction of anonymity. The criticism from FinCEN states that "cryptocurrency is

[6] Taken from coin.dance and verified with the 2018 *Library of Congress Report: Regulation of Cryptocurrency Around the World ((Global Legal Research Center at the Library of Congress 2018)*

[7] Referenced again below, Global Democracy Index from *The Economist*

used extensively in malicious ways, including to finance terrorism, launder money, and buy drugs and false documents. It has also become the financing of choice for ransomware attacks that have been "increasing in severity" and have targeted critical areas, like organizations conducting Covid-19 research" (Salzman, 2020). Since the change of the administration, however, there has been no further action[8].

The closest the United States has been to direct regulation came from the New York State Attorney General in February 2021. Targeting the *Tether* stablecoin[9], the state AG ended a virtual currency trading platform for engaging in misleading tactics. The main claim was that Bitfinex (the trading platform) made false statements about the actual backing of the stablecoin by shuffling around hundreds of millions of dollars between two firms to make it perceived that all issued Tether coins were backed by either USD or Euros arguing that the company promoted "a stablecoin without stability" (James, 2021). Resulting in penalties of $18.5 Million, this was the first, and only step, towards directly regulating cryptocurrencies as more than a financial asset in the USA. One of the key questions towards regulatory threats may become, how many people need to lose how much money for a democratic government to intervene? Below are examples of upcoming and existing regulations across the world.

In a 2020 economic uncertainty paper, the authors set out to analyze whether or not economic policy uncertainty index developed by Baker et al. can predict cryptocurrency returns (Cheng,Yen, 2020) (Baker et al, 2016). Comparing China, South Korea, Japan and the United States resulted in a statistically significant result only for Chinese economic policy uncertainty in 2017 around the time when the Chinese government banned trading in cryptocurrencies[10]. On the day that the People's Bank of China (PBOC) announced that it would close down initial coin offering and start to "crack down" on cryptocurrencies, the price of Bitcoin would fall by nearly 9% in a period of 12 hours (Imbert, 2017). Despite this threat

---

[8] The current Secretary Treasury Janet Yellen has also expressed doubt about cryptocurrencies, however, her main criticisms come from its inefficiencies as a currency (https://www.cnbc.com/2021/02/22/yellen-sounds-warning-about-extremely-inefficient-bitcoin.html)
[9] a stablecoin is a cryptocurrency pegged or backed by the value of an existing currency,
[10] China does not recognize cryptocurrencies as legal tender and the banking system is not accepting cryptocurrencies or providing relevant services. The government has taken a series of regulatory measures to crack down on activities related to cryptocurrencies for purposes of investor protection and financial risk prevention. Those measures include announcing that initial coin offerings are illegal, restricting the primary business of cryptocurrency trading platforms, and discouraging Bitcoin mining. (Library of Congress: https://www.loc.gov/law/help/cryptocurrency/china.php)

however, China still remains responsible for over 60% of the source for global cryptocurrency mining (Kharpal, 2021).

While China continues to harden (though slower and more lenient than predicted) its stance towards global cryptocurrencies, it has however taken a new aim into the same market it seeks to regulate.. To challenge the USD dominance in global trade, China has piloted its own cryptocurrency. The Digital Yuan is meant to have all of the proposed conveniences of existing cryptos, but with a key differentiator, it is controlled and monitored by the PBOC. The regional aspiration is to replace the 88% of foreign exchanges in the USD and grow the 4% of foreign exchange in Yuan (Areddy, 2021). The Wall Street Journal reports that the new system is designed to run parallel to 'hard' currencies with aspirations to replace it over time (Areddy, 2021). The biggest key to these developments however is that authoritarian leaning regimes can use the existence of digital currencies to increase their expression of power over their population by removing the decentralized nature of the platforms. Also noted in the Journal article is that the digital Yuan has already been used in state media campaigns that "shows a man in an American-flag shirt knocked out by a golden coin depicting digital yuan." The impact of all of this intimidation from the central government has resulted in a drop from 90% to under 1% of all Bitcoin being traded in the Chinese Yuan (Zhang, 2018).

In India, a similar approach is unfolding. In a January 2021 bill, the Indian parliament proposed a new regulation that would be among the strictest in the world. According to *Reuters*, the proposal would give cryptocurrency (all types) a six month period within enactment of the regulation to liquidate all assets before punishments are levied (Ahmed, Anand, 2021). While no official data is available, India is home to an estimated 8 million users holding over 100 billion rupees ($1.4 Billion). Despite threats however since the beginning of 2021, India's crypto exchanges have added over 20,000 users in the market heat up. The central bank has backed away from their 2019 proposal to have a ten-year jail sentence accompanying any guilty party that mines, generates or holds any type of cryptocurrencies. Notably, in a similar approach to the Chinese approach above, India has expressed interest in blockchain technology towards creating its own digital currency. Most notably in this development, is the harshness of the approach to decentralization, while remaining optimistic about use of blockchain for the government's own currency.

The two above trends show already powerful governments seeking to solidify their roles as the sole means of generation and moderation of currency. Just recently, a more troubling development has occurred in Turkey. For some background the Turkish Lira is expected to have inflated by 18% from April 2020 to April 2021[11] with a steady decrease in value since November of 2016 and a total 34% drop in value against the dollar since 2019 (Yackley, 2021). However, the leader of Turkey, Mr. Erdogan, seeks to stem the rise in popularity of cryptocurrencies, particularly Bitcoin, as the Turkish population seeks ways to hedge their wealth against the internal volatility. Turkey is currently the largest holder and trader in cryptos in the Middle East and ranks 29th globally in crypto transactions[12]. On March 22 of 2021, Erdogan sacked the country's central bank governor with little notice sending the currency plummeting. Such news only added to the Turkish population seeking to store value elsewhere. Within weeks, the administration announced new laws on cryptocurrencies that would ban private transactions between them in the country within a month (Malsin, Ostroff, 2021). While some financial monitoring can be valid, perhaps cryptocurrency crackdowns can be looked at as how free a country's people are. Country's higher on the *Global Democracy Index*[13] tend to regulate cryptocurrencies as financial assets, countries towards the bottom of the scale, or that are actively slipping, tend to see them as a threat to power.

C. Energy Consumption

On April 18, 2021, the price of Bitcoin dropped 14% in a single day in the largest drop in a two month span. However, unlike other 'corrections', this drop was not caused by direct threats in regulation or some greater macroeconomic trend, the key source of this drop originated in the Xinjiang Region of China. A power outage caused nearly half of the Bitcoin network to go offline for 48 hours. Within an

[11] Data obtained from: https://www.cnbc.com/2021/04/15/turkeys-central-bank-holds-interest-rates-sparking-investor-concern.html
[12] According to data from Chainalysis, a US-based blockchain analysis company.
[13] In reference to the Global Democracy Index from The Economist: https://www.economist.com/graphic-detail/2021/02/02/global-democracy-has-a-very-bad-year

hour, \$10 billion in Bitcoin had already been lost (Reuters, 2021). Luke Sully of Ledgermatic put it succinctly, “The power outage does expose a fundamental weakness; that although the Bitcoin network is decentralized the mining of it is not" (Reuters, 2021). China’s Inner Mongolia region alone accounts for 8% of all Bitcoin mining, with China in total responsible for ~65% of all global mining (for reference the US is ~7.2%)[14].

While the above outage was caused by flooding approaching key power plants, the headline causes a greater pause. How reliant is a decentralized network on random events? And furthermore, how much power will cryptos eat in the future? In *Cryptodamages* by Goodkind et al. estimate the monetary impact on health caused by the mining of Bitcoins in the US and China. Their results are staggering. The main finding is that for each \$1 in Bitcoin value created (mined) the value was responsible for \$0.49 and \$0.37 in health and climate damages in the US and China respectively through air pollution and other factors (see appendix for figure A.3, A.4) (Goodkind et al, 2020). The global consumption is truly staggering as seen in the chart below[15]:

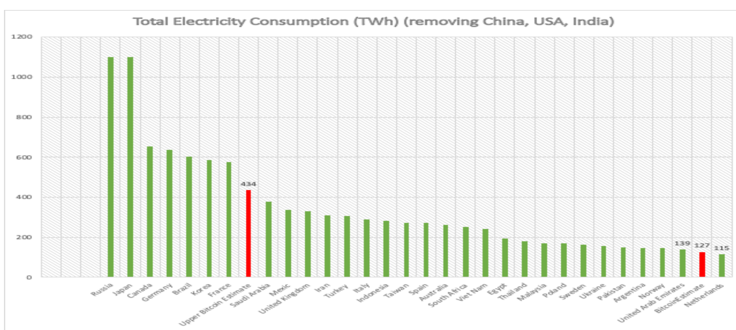


Figure 2.2 Energy consumption globally (data from US Energy Information Agency and Cambridge Centre for alternative Finance[16]

In approaching the survival analysis, it becomes apparent that if there should be an impending ceiling on the amount of cryptocurrencies in the world, it may very well be caused by energy consumption. In particular, the proof of work method of blockchain verification is extremely energy intensive. There have however, been demands to reduce energy consumption by implementing a Proof of

[14] Data from the Cambridge Bitcoin Electricity Consumption Index
[15] China, USA and India were removed to show a greater comparison, China has an annual consumption of 7100 TWh which distorted the graph
[16] A chart including China, USA and India has been included in the Appendix Figure A.5

Stake method described below. As a reference, the existing Ethereum blockchain uses the amount of two US households per transaction (Cuen, 2021).

III. Approach & Results:

A. Underlying Technology

The verification of cryptocurrency networks run off of blockchain technology as the backbone of both of the below mentioned methods of verification. A blockchain diagram has been included in Appendix Figure A.6. The most important component of any currency system is its method of exchange and validation. Since the purpose of holding a currency is to store value, it should be easily transferred between personnel to exchange goods and services. Additionally there should also be a mechanism to process those exchanges at scale and validate each one of them to ensure that there are no fraudulent cases. In the fiat currency world, 3rd party instruments like banks, digital wallets and card companies process these exchanges for a small fee. However, in the crypto space, this process is decentralized, and this is done by the members of the block chain network itself.

1. Proof of Work

Proof of Work was the original method devised by Satoshi Nakatomo when creating the first-ever cryptocurrency – Bitcoin. Proof of Work is more-or-less based on an advanced form of mathematics also often referred as "cryptography" in which certain nodes in the network (also called miners) solve complex equations to process a transaction and then consensus is formed among other miners in the network to validate it. Every equation is unique and requires a lot of computational power to solve it (as each miner is competing against another to solve it). In exchange for processing the transaction, the miner is rewarded a cryptocurrency as a payment.

Proof of Concept is quite common among Cryptocurrencies and Bitcoin, the most popular one uses it to process transactions. However, not only does it require a lot of computational power to process each transaction, since a consensus has to be developed among miners to add any transaction, it takes more time than in other mechanisms. Proof of Concept however the most secure among others and hence is popular among block-chain technologies.

2. *Proof of Stake*

Proof of Stake is a more recent development (2012) and is on its way to replace Proof of Work mechanism for processing block-chain transactions. In Proof of Stake, instead of developing a consensus among all the nodes to validate a transaction, there are certain validators who are randomly chosen based on their stake in the network to process those transactions. Unlike in Proof of Work, the validators do not need to solve complex equations or compete against each other through computational power. This ensures that a lot of energy isn't necessary to process transactions and more number of transactions can be processed in a shorter period of time. When a validator validates a transaction, a certain transaction fee is paid. However, if the validator validates a fraudulent transaction, a certain portion of the stake is lost.

The key drawback of the Proof of Stake system is that the chances of a node to be randomly chosen by the network to validate a transaction is directly proportional to its stake in the network. This means that smaller block-chain systems are vulnerable to manipulations by nodes that have higher stake in the network. If a particular node holds greater than 50% stake in the network, it is even possible for that to validate fraudulent transactions.

3. *Proof of Authority*

Proof of Authority is an even more recent development and is similar to Proof of Stake network. In this mechanism, a bunch of validators are chosen from the network based on their history of processing transactions. If a certain validator has a very high consensus rate (meaning less fraudulent transactions approved), there are more chances for the validator to be chosen to process transactions. Like Proof of Stake, since there is no requirement to solve complex equations or to compete with other miners for the reward, this mechanism is less energy-intensive and is more scalable.

Proof of Authority is also considered more secure as every validator's reputation is in line when validating a transaction. If validators approve fraudulent transactions, their reputations go down and they will be selected less frequently to process transactions (resulting in less rewards). Unlike Proof of Work mechanism which can be manipulated by nodes with higher computational power (large group of individuals who pool their computational power) or Proof of Stake mechanism by nodes with higher network stake (rich nodes essentially), Proof of Authority cannot be manipulated as its built on the reputation of honest validators.

4. Consensus Mechanism for Cryptocurrency Future

One of the reasons why Bitcoin might never replace the fiat currency is due to the limitations of the Proof of Work mechanism. Not only is the PoW system more energy intensive, it is also slow and is not scalable to be used for regular exchanges. Therefore even though the value of Bitcoin may be maintained as an asset due to its scarcity, it will not be able to replace fiat currency in the future.

One of the contenders to do so is Ethereum, which even though at the moment uses Proof of Work, it is currently on a verge of shifting towards the Proof of Stake mechanism. If this happens, Ethereum will be able to scale its existing infrastructure and nodes to approve more transactions while reducing the energy requirements. Even though Proof of Stake mechanism is vulnerable to richer stakeholders (stake higher than 50%), Ethereum is already too huge for that to be possible and hence should remain secure in the near future too. The only other prominent coin to already adopt Proof of Stake mechanism is Cardano but it has so far been unable to attract significant investors leading to higher volatility. Even though Proof of Authority seems to be the best consensus mechanism for the future, it is currently used by private financial institutions to run their internal block-chain technologies. We can expect any of those internal coins to develop prominence and hence emerge as a new cryptocurrency for the future.

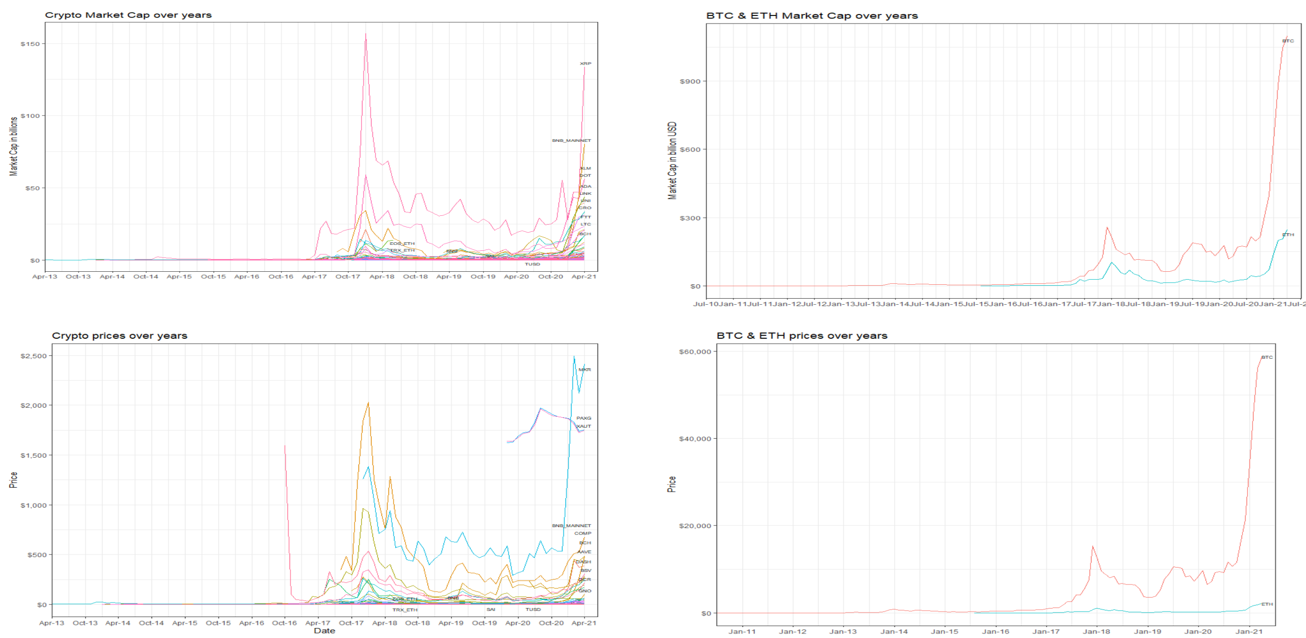
B. Exploratory Data Analysis

1. Time Plots

The first step to understand how the cryptocurrencies are performing is to check their general trend over time. Even though everyone is already aware of the exponential price increase of prominent coins like Bitcoin and Ethereum, it was important to see if the trend is similar for others too. Through basic time plots (below), we were able to identify certain patterns in crypto prices and market cap:

1. There has been an extraordinary increase in both market capitalization and prices for BTC; for ETH, prices have been relatively more stable but market capitalization has rapidly increased

2. A clear pattern can be observed for all cryptocurrencies where prices and market capitalization increase or decrease together (probably as they're all pegged to BTC)
3. Unlike BTC and ETH, most of the other cryptocurrencies haven't been able to reach the market cap/prices from January, 2018, which suggest that the latest crypto frenzy might not be as strong as it has been made of
4. Outside BTC and ETH, Ripple (XRP) and BNB Mainnet are emerging with large market cap while there are many high priced coins in the market without much of a market presence



(Above) Figure 3.1 - 3.4: Time plots of cryptocurrency prices and market capitalization (full size in AppendixA.7-A.10)

2. *Correlation Analysis*

Correlation analysis is a statistical method used to evaluate the strength of relationship between two quantitative variables. A high correlation means that two or more variables have a strong relationship with each other, while a weak correlation means that the variables are hardly related. In For cryptocurrency analysis, a correlation matrix using Spearman Correlation (uses ranks to remove effect of high volatility) was plotted for the Top 50 Cryptocurrencies (by market cap) to understand their price patterns in the market. Idea is to select cryptocurrencies with varying correlation so that any risk can be hedged.

In the correlation plot below, it can be observed that most of the cryptocurrencies have high correlation values (hence in red) while there are few exceptions - BTC (to some extent which is surprising), DGX, LINK, USDC, USDT and USDT ETHER. However, when dug deeper it can be noticed that these coins - DGX , LINK, USDT are peculiar cryptocurrencies. DGX is gold pegged, USDC is dollar pegged and USDT was marketed as dollar pegged (which isn't true).

$$\rho = 1 - \frac{6 * \sum d_i^2}{n\,(n^2 - 1)}$$

Where,
p = Spearman's rank correlation coefficient
d_i^2 = difference between the two ranks of each observation
n = number of observations

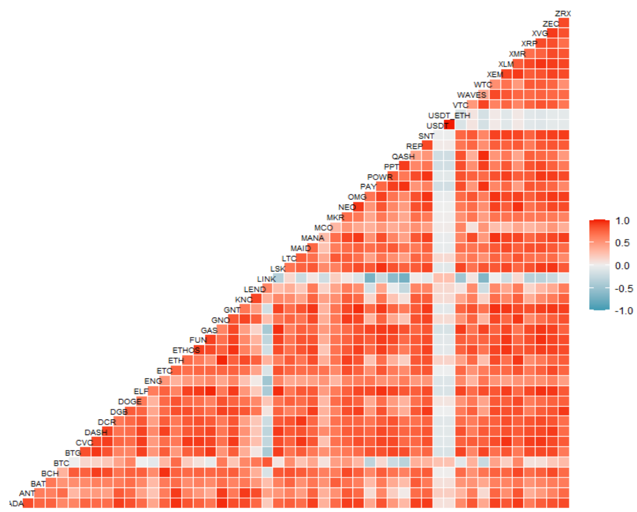


Figure3.5: Correlation matrix for cryptocurrency prices across time

C. Survivability

1. Bass Diffusion

The Bass diffusion model explains how emerging technology develops through time by assuming that "the probability of purchase at any time is related linearly to the number of previous buyers" (Bass, 1969). Bass defines two distinctive groups of a market – innovators and imitators. Innovators refer to a group of people who decide to use a new technology independently, whereas imitators usually arrive at this decision under social pressure. The influence of these groups on the popularity of new technologies is described by the following equation:

$$S(T) = pm + (q - p)Y(T) - q/m[Y(T)]^2$$

where,
S(T) = number of sales at time T
Y(T) = cumulative number of sales prior to time T
p = coefficient of innovators
q = coefficient of imitators
m = market size

S(T) and Y(T) were treated as a number of crypto-wallets created at time T and a cumulative number of crypto-wallets created prior to time T, respectively. The market size m will be switched to population size. For our model, we assume that one person can own only one crypto-wallet. The data for crypto wallet owners was derived from the blockchain.com website. The historical data covers years between 2011 and 2021. The population size data was collected from the UN website. The model refers to the population between the age ranges of 17 and 70 as potential owners of crypto-wallets. The average proportion of people falling into this range was 62%. The model is significantly dependent on the values of p and q. Despite suggestions of various researchers, it was decided to use historical data for a method proposed by Ganjeizadeh (2017). Specifically, the Bass's equation was reformulated into following quadratic equation:

$$n(t) = a + bN(t-1) - c(N(t-1))^2, \text{ where}$$
$$m = \frac{-b-\sqrt{b^2-4ac}}{2c}$$
$$p = \frac{a}{m}$$
$$q = p + b$$

Results of the regression of the historical data is presented by Figure 3.6.

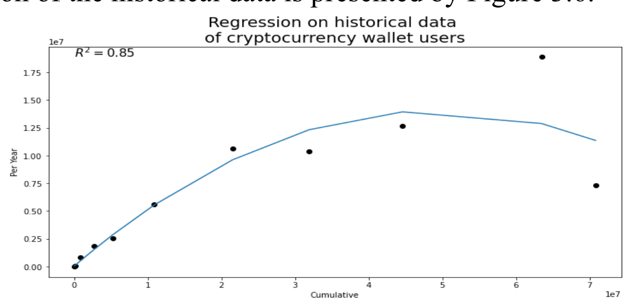
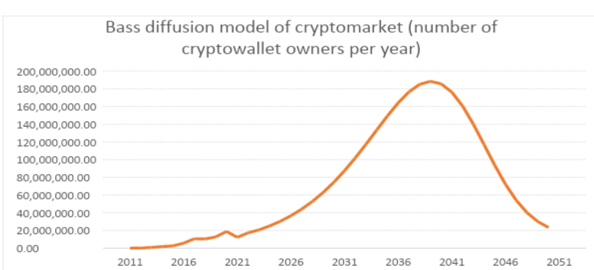


Figure 3.6:. A plot of regression analysis of historical data of cryptocurrency wallet users. Y axis represents the number of users added per year. X axis represents the cumulative number of users.

Regression provided with estimates of p and q values, which are 0 and 0.57, respectively. These values are significantly different from what other authors proposed. Nevertheless, inserting them into Bass's equation produced the model represented by Figure 3.7.



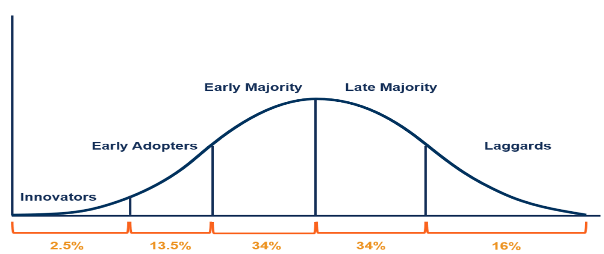


Figure 3.7: A diagram showing dynamics of crypto wallets owners Figure 3.8: Categorization of adopters of innovative technologies[17]

[17] *(Source: https://cdn.corporatefinanceinstitute.com/assets/diffusion-of-innovation1.png)*

through time. Number of users calculated on a per year basis.

The diagram suggests that cryptocurrencies will reach their peak popularity closer to the end of the 4th decade of the current century. *p* and *q* values suggested by Bass's research produced results differed only in 4-5 years. $p = 0$ can be explained by the significantly low amount of people in the innovator's group. Thus, the rise of popularity of cryptocurrency predominantly by imitators' groups may be described by the difficulty in understanding blockchain mechanisms due to its complexity.

Rogers (1995) augmented Bass's diagram by characterizing people by different groups (Figure 3.8). According to Rogers, the blockchain technology is at the beginning phase of early adopters and a critical mass of crypto-wallet owners is still not reached.

2. *SIR Epidemic Model*

Following the base population numbers used above, 62% of the 2020 global population resulted in nearly 4 billion potential users. All of these users can then be "infected" by the new craze of cryptocurrencies. In 1927, Kermack and McKendrick authored *A contribution to the mathematical theory of epidemics* in which the population was separated into three pools, the susceptible, the infected and the recovered (Kermack, McKendrick, 1927). This SIR framework has been used since to establish a set of differential equations used to model the spread of infectious diseases in epidemics. After the consultation of Prof.Chernicoff at GWU, we have decided to pursue this modelling further. The susceptible population was modelled as the potential crypto users, the infected as experimental users and the recovered are continuous crypto users. The analysis was simulated with different contagiousness and recovery times both simulated over the next two decades. The base population of existing users was taken to be 106 million based off of a 2021 *Business Insider* estimate. The implicit assumption in this model is that cryptocurrencies are contagious and would be used in a rapidly digitizing global economy as a widely accepted means of transaction. While this is a very bold assumption, the SIR epidemic model has the built in bias that contagions are blind and can thus take over a population relatively quickly. While the below trends most likely overestimate the penetration into the market, the two different trends should represent the potential paths forward.

On the left, we see a less contagious crypto market infecting .1% through its contact rate and with a slower mean recovery rate (in individuals per day). On the right, we have a twice as active “contagion” with a contact rate of .2% and a faster mean recovery rate.The latter results in a societal change towards the stance of cryptocurrencies as an excepted means of transaction while the former shows an experimental population that could be impacted by an unforeseen event such as stricter government regulations. These simulations also ignore any “forced contact” that could arise from an introduction of a national virtual currency. Full equations for these models can be found in A.11, A.12.

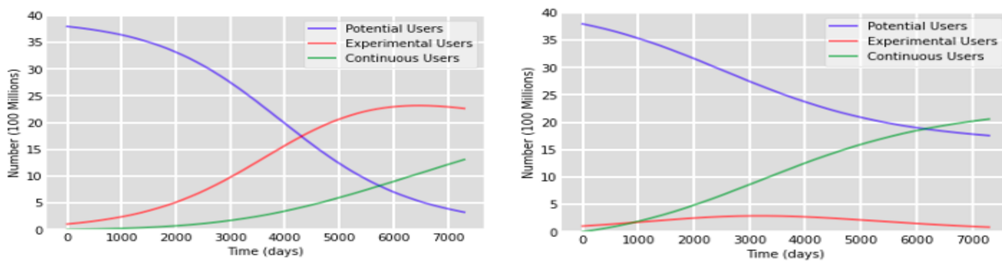
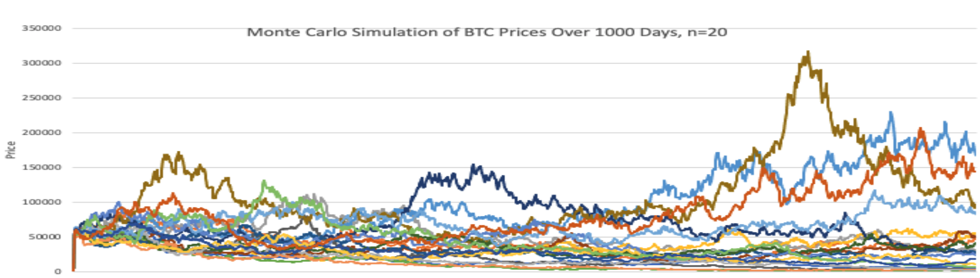


Figure 3.9, 3.10: SIR epidemic models over the next two decades (7300 Days), Left: Contact Rate = .1%, Mean Recovery Rate = 1/7300. Right:Contact Rate = .2%, Mean Recovery Rate = 10/7300

3. *Monte Carlo Simulation*

A simple Monte Carlo simulation was performed over a thousand day trading period using the current price of Bitcoin (~$56,000) and its abnormally high annualized volatility of nearly 75%. A simulation was also performed for Ethereum included in A.13 As will be pointed out in the financial analysis, it is very hard to confidently optimize an asset whose standard deviation is 64% of the base price.



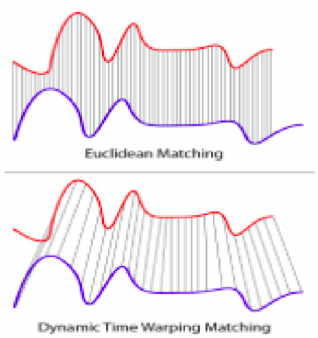
Starting Price	$ 56,600.00
Annual Volatility	74.48%
Daily Volatility	3.898%
Mean Price	$ 43,906.10
Median Price	$ 34,823.26
Std. Dev.	36063.88008
Percentiles	
5%	$ 3,793.60
95%	$ 112,908.96
25%	$ 19,987.63
75%	$ 57,747.48

Figure 3.11: Monte Carlo simulation of BTC (Left) and Statistical Highlights (Right)

D. Quantitative analysis of the Time Series Component

1. Dynamic Time Warping

Dynamic Time Warping (DTW) is a time series comparison algorithm which measures the similarity or dissimilarity between two-time series by calculating the Euclidean distance between them. Each time series data is first converted into a vector, aligned among themselves and after which the distance is measured. It has a wide range of applications which includes financial markets (to compare stock trade), speech recognition, route calculations, etc.



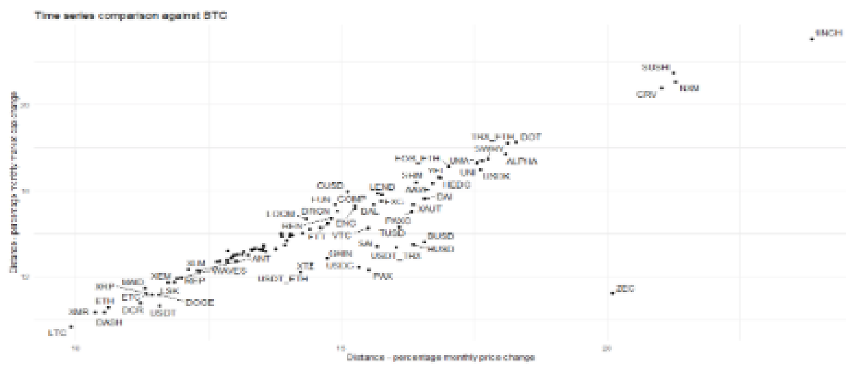


Figure 3.12, 3.13:.Wiki Commons: File:Euclidean_vs_DTW.jpg (Left), Comparison of cryptocurrencies vs BTC (Right)

Dynamic time warping allows the two curves to match up evenly even though the X-axes (i.e. time) are not necessarily in sync. Another way is to think of this is as a robust dissimilarity score where a lower number means the series is more similar.

For Cryptocurrency analysis, Dynamic Time Warping (DTW) was used to identify if there were certain cryptocurrencies which have had similar time series behavior in the past and therefore can be expected to perform well over time. To do that, monthly price changes and market capitalization changes were calculated across time for each cryptocurrency and then their Euclidean Distance was calculated against the BTC. All the cryptocurrencies, which have lower distance against that of BTC can be termed similar and can be expected to do well. In the chart above cryptocurrencies - LTC, XMR, DASH, ETH, DCR and USDT can be seen to have less distance to BTC and therefore could have similar market performance in the future.

2. *Time Series Forecasting using ARIMA/ARIMAX*

Any sequence of data that has been recorded over regular time intervals can be referred to as a time series. Any time series forecasting algorithm tries to understand the pattern behind these data points spread across that time interval and uses that pattern to predict what the new data points may look like. There are multiple time-series algorithms among which ARIMA – Auto Regressive Integrated Moving Average and ARIMAX - An Autoregressive Integrated Moving Average with Explanatory Variable are the two most widely used. An ARIMA model is characterized by 3 terms: p, d, q, where, a) p is the order of the AR term, b) q is the order of the MA term, and c) d is the number of differencing required to make the time series stationary. The general form for an ARIMA is below:

Predicted Yt = Constant + Linear combination Lags of Y (upto p lags) + Linear Combination of Lagged forecast errors (upto q lags)

Meanwhile, an Autoregressive Integrated Moving Average with Explanatory Variable (ARIMAX) model can be viewed as a multiple regression model with one or more autoregressive (AR) terms and/or one or more moving average (MA) terms (ElegantJ BI 2017).

ARIMA model that we built suggests that the prices of all the cryptocurrencies are expected to fall spectacularly anytime in the future. Since the prices of the cryptocurrencies especially BTC and ETH have reached unprecedented levels, it is not surprising for the model to predict a huge downfall. One of the general trends that is observed in the stock market is that any stock prices that go up will see a price correction at one point of time. However, in the case of cryptocurrencies, high volatility is observed and hence why prices are also expected to drop spectacularly.

When prices of BTC are included in the model (multiple scenarios - price increase, constant, price decline), the model expects the price of all cryptocurrencies to follow the suit. This is also a result that was already expected since the prices of cryptocurrencies are observed to be pegged to that of BTC.

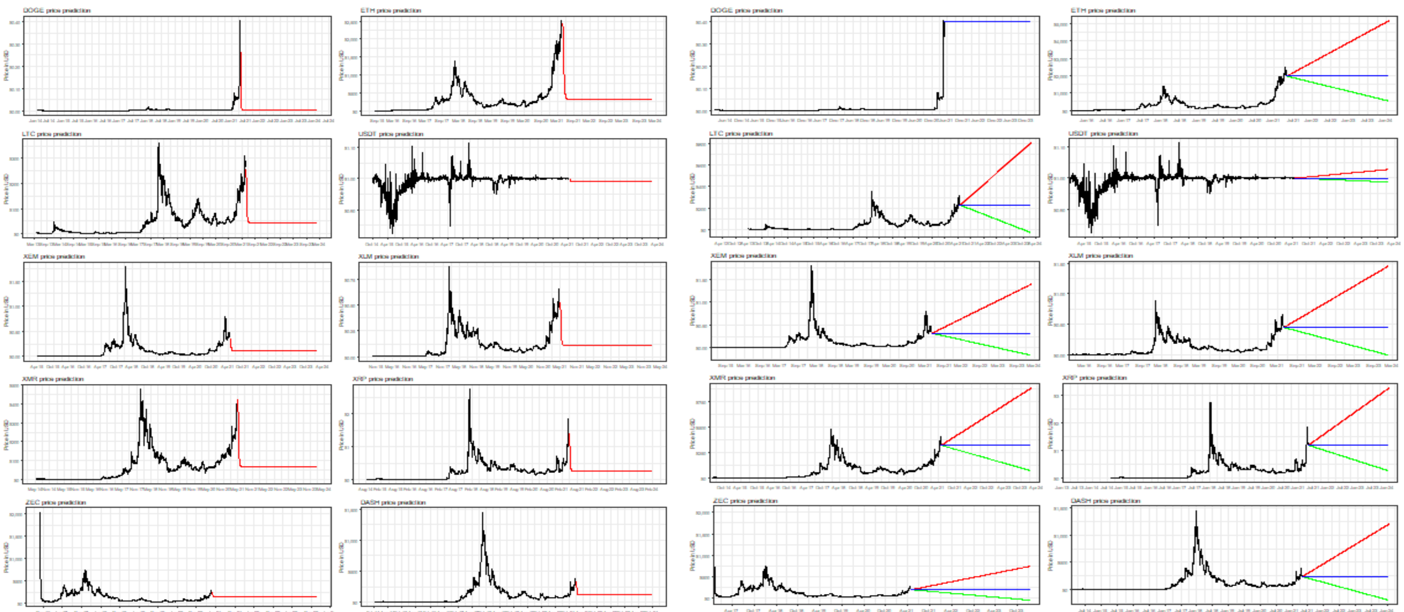


Figure 3.14 - 3.17: Cryptocurrency projections over next 5 years (left without BTC effect and right with it: increase-red, drop - green, blue - constant)

3. *Principal Component Analysis*

The Principal Component Analysis (PCA) refers to a method that reduces dimensionality of a data while keeping as much of its variability as possible. Specifically, it reduces noise present in the data and keeps only valuable information related to major patterns by usage of eigenvalues and eigenvectors.

Although there are more than 1000 cryptocurrency in the market, only 60-70 of them have enough historical data that can be used in PCA. As a result, 63 actively traded cryptocurrencies were chosen. The historical data was recalculated to represent weekly returns and further transformed into correlation matrix that was used to derive eigenvalues and eigenvectors via MINITAB software. In general, eigenvectors are coefficients that determine linear combinations of original data and generate principal component scores, whereas eigenvalues are variances of principal component scores. 63 cryptocurrencies generated 63 principal components but not all of them are useful.

	PC1	PC2	PC3	PC4	PC5	PC6
EIGENVALUES	23.8402	3.5943	2.166	1.7471	1.6752	1.5383
Percentage	37.8%	5.7%	3.4%	2.8%	2.7%	2.4%
Cumulative	37.8%	43.5%	47.0%	49.8%	52.4%	54.9%

Table 3.1: Showing eigenvalues of the first 6 principal components

Table 3.1 shows one part of results derived from PCA where the first 2 principal components captured cumulative 43.5% of variance of original data. There are two major rules that give a hint on how many principal components to retain and discard. The Kaiser's rule (Kaiser, 1960) suggests ignoring principal components that have eigenvalues less than 1. In our case, it corresponds to 14 principal components and 70% of captured variance. Whereas, "elbow rule" suggests to plot eigenvalues and discard those principal components that more-or-less follow a straight line.

According to Figure 3.18, all principal components, except the first 2, follow a straight red line suggesting that their contribution to overall analysis is minimal. Table 1 gives additional evidence by indicating that each principal component after the first 2 capture less than 5% variance of original data. Thus, it was decided to use only the first 2 components for further analysis and consider other PCs as a noise.

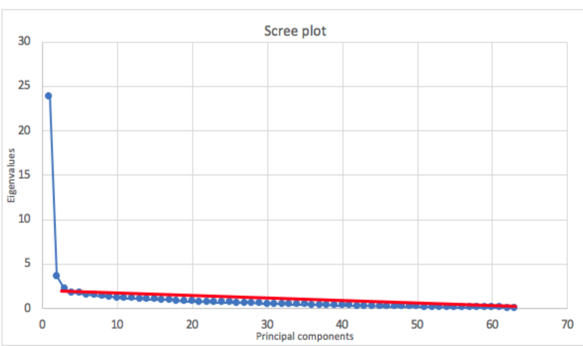


Figure 3.18: A scree plot showing eigenvalues of all principal components

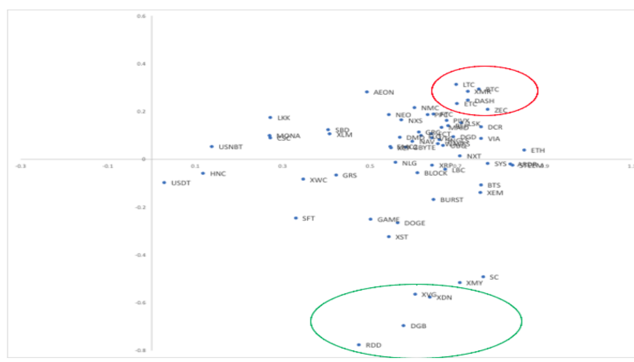


Figure 3.19: A loading plot of two principal components (PC1 – x axis, PC2 – y axis)

The next step in PCA analysis was to produce loadings of each crypto involved in the study. Loadings were created by multiplication of eigenvector values by root of corresponding eigenvalue. The result was plotted on Figure 3.19.

Figure 3.19 shows that all of cryptos are positively correlated with the PC1, represented by horizontal axis. Thus, PC1 can be referred to as a general state of the market where most cryptos have relatively positive returns. On the other hand, the second principal component (PC2), represented by vertical axis, implies that not all cryptos behave similarly in the market. For instance, Figure 3.19 showed that, in general, there are two groups that have negative correlation with each other – cryptos associated with BTC (red circle) and ones associated with RDD (green circle). The PCA suggests that when BTC group has positive returns, the RDD group has the opposite and vice versa. The cryptos that have PC2 loadings closer to zero can be considered as uncorrelated with these groups, hence can be ignored.

The results of PCA suggest that the crypto market is growing but there are groups that grow differently from each other. Nevertheless, if the investment decision was based only on PCA, it would advise to invest in those two groups to diversify the risk.

IV. Discussion & Conclusion:

Throughout the above analyses, we were limited in the scope of what we were asking our survival and financial models to perform. Part of this came from the recent history of cryptocurrencies resulting in a lack of data and solid foundation, while the other came from the "soft factors of uncertainty" such as government regulations and power consumption requirements. Knowing this, we performed a series of qualitative and quantitative analysis on cryptocurrencies to understand their behavior. The key insights from all of these analyses was that their behaviors over time have been highly errative, speculative and hugely dependent on their market perception at any given time.

Though the world remains an uncertain place with regards to major government crackdowns, it can be assumed that the major OECD countries will continue to allow the trading of cryptocurrencies like other traditional financial instruments even if they end up pursuing their own digital currency. This is because of the established foothold major financial players have created such as Goldman Sachs and PayPal investing in and allowing trades in major cryptos. As highlighted in the Tether anecdote above in New York, the main threat may arise from a government intervention when too many investors are misled and lose enough money to cause greater investigations.

As the market continues to mature, we predict that within the next two decades (see Bass and SIR models) the market will hit its peak, negating the effect of any national virtual currency. During this same time period however, newer innovations such as Proof of Stake and Proof of Authority will continue to grow in relevance for their increased speed and energy efficiency. At the current rate, with Proof of Work and Bitcoin domination, it could be expected that a form of “energy shaming” would gradually decrease its attractiveness. The original methods, while innovative, have simply not remained innovative enough in the rapidly developing market.

In our financial analysis, starting with the Monte Carlo simulation, we can see that the performance is wildly erratic. Again, this sums up our difficulty in predicting any future performance past basic survival. Any financial asset who’s standard deviation is more than half of the base value, is only realistically attractive to a risk-seeking investor. Having noted all of this, our financial analysis does show that with more history, and increasing market competition to weed out extremely uncompetitive cryptocurrencies overtime. While we expect Bitcoin to remain a dominant player in the industry, especially because of its built in inflation control through a supply limitation to be used as a store of value, we do not think it is the “future” for transactional cryptocurrencies due to its slow processing time as well as its energy demand. For this reason, we have taken into account a qualitative analysis of the energy and verification methods which will be more prevalent in the future such as Proof of Stake as well as Proof of Authority. In the near/medium term however, Bitcoin is still a market behemoth and is the single most important actor in predicting the price of other assets. Knowing this, and through our above financial analysis, we would expect an investor to seek assets that perform similarly to Bitcoin, but process some more efficient transactions and verification techniques.

Leading us to our end result where we have concluded that the use of cryptocurrencies has not yet peaked, and we expect that their use will continue to become more widespread, however there will be expected market consolidation. Our general recommendation would be to invest in Ethereum or XRP, which are performing well over time, have (or will have) updated consensus mechanisms and also show a similar performance pattern to that of Bitcoin. The use of cryptocurrencies will continue to require an investment in monitoring both aspects of a rapidly shifting qualitative and quantitative world.

Appendix:

Source #	Source Location
1	Coindesk.com
2	5/1/2015 An Analysis of the Cryptocurrency Industry , Farell
3	https://ethereum.org/en/history/
4	https://coinmarketcap.com/currencies/xrp/
5	https://xrpl.org/history.html
6	https://www.investopedia.com/terms/t/tether-usdt.asp
7	https://roadmap.cardano.org/en/byron/
8	https://cointhinktank.com/coin/chainlink
9	https://www.investopedia.com/terms/b/bitcoin-cash.asp
10	https://www.coindesk.com/price/usd-coin

Table A.1: Sources for Table 1

Figure A.1. Total market capitalization of the global cryptocurrency market over the past 8 years

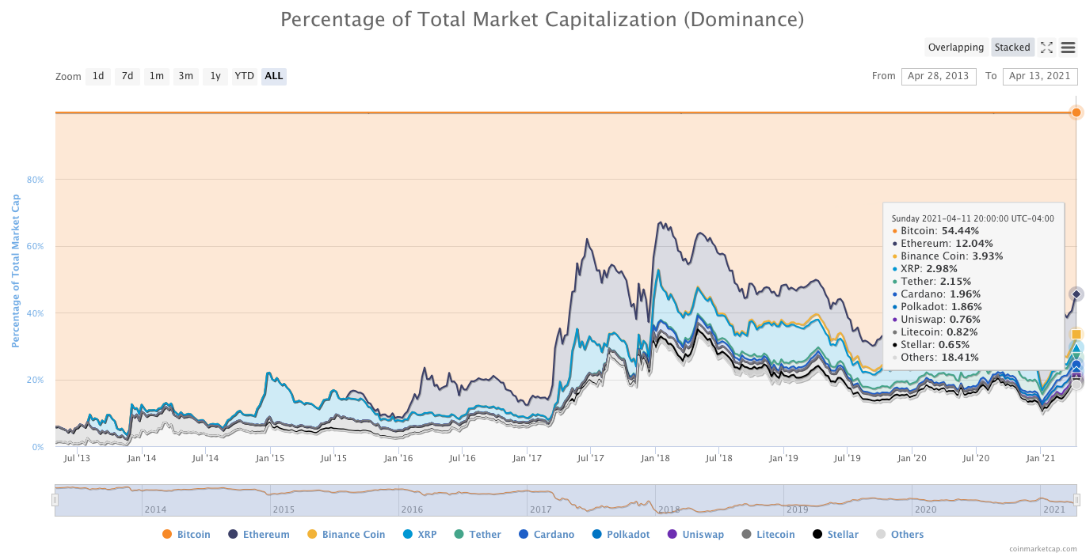
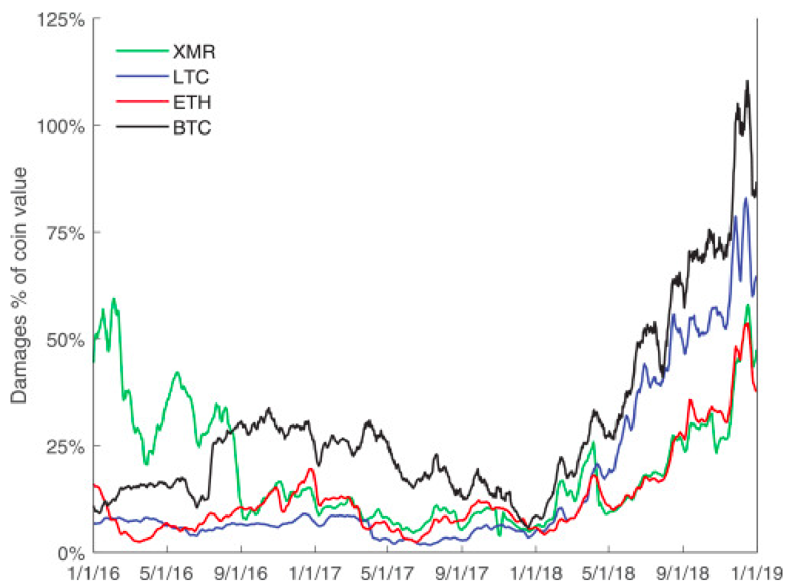
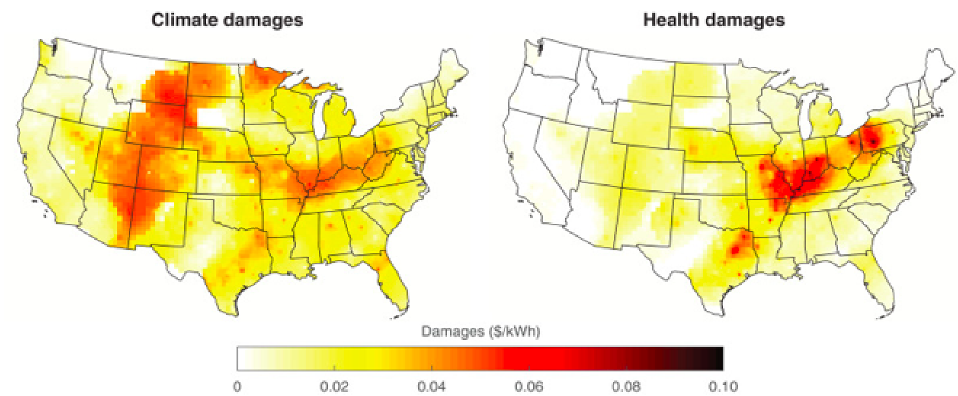


Figure A.2. Stacked cryptocurrency market capitalization, July 2013-April 2021[18]



[18] Taken from coinmarketcap.com/charts



Download : Download high-res image (988KB)   Download : Download full-size image

Fig. 1. Climate and health damages per kWh of electricity used in each location. The emission profile of electricity use in each location is a weighted average of the EGUs within 250 km, weighted by the inverse distance from the EGU and the quantity of electricity generated.

Figure A.3, A.4: Environmental Impact from Goodkind et al

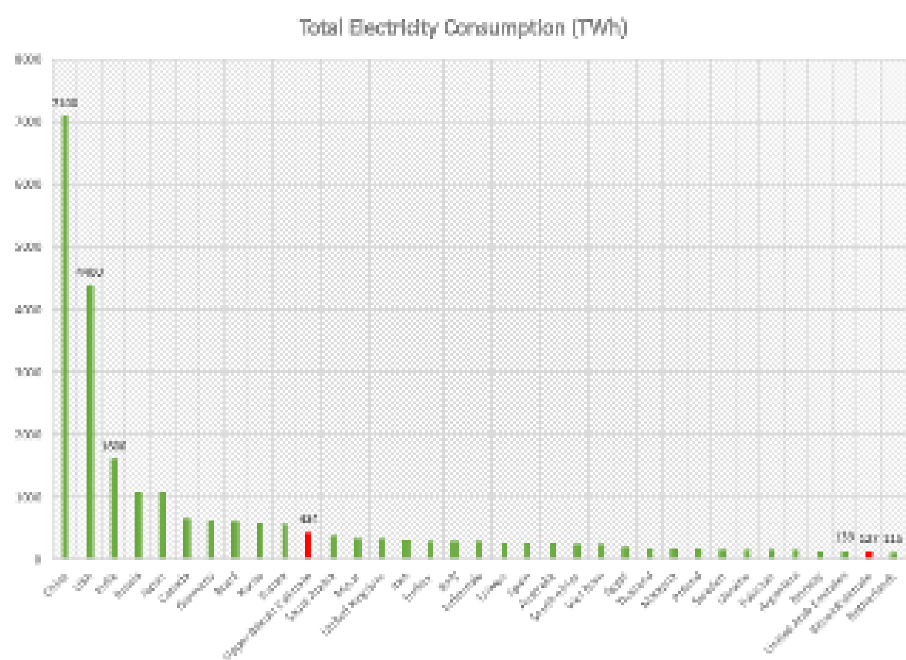


Figure A.5: Global Energy Consumption including China, USA and India

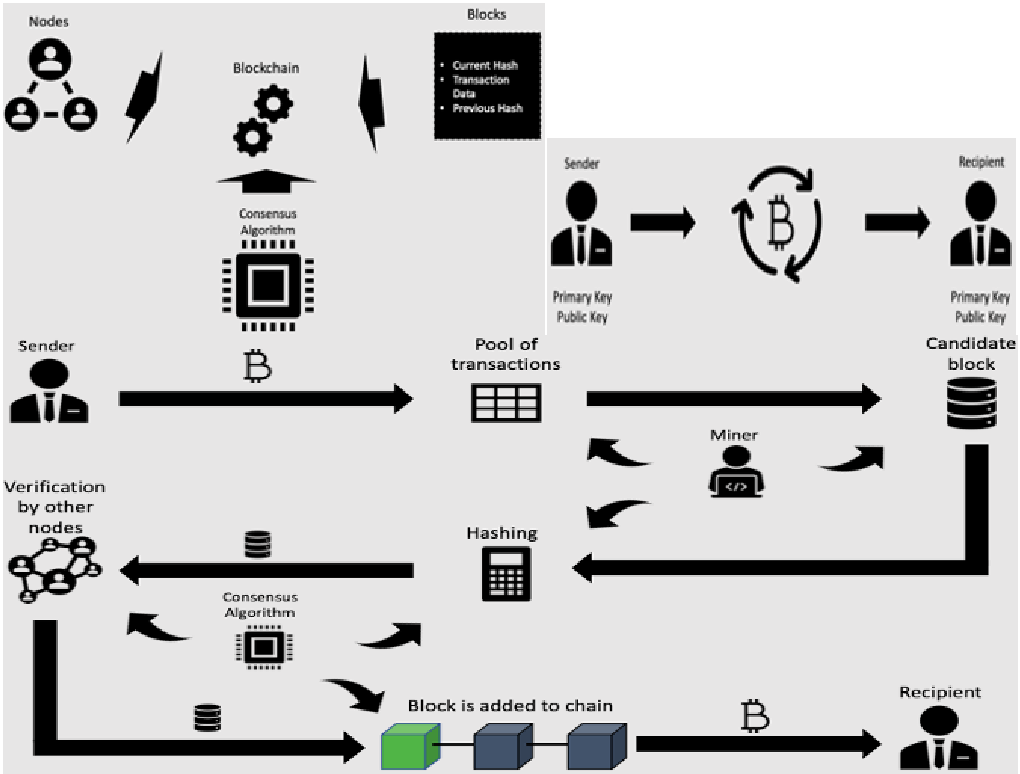


Figure A.6: A blockchain network

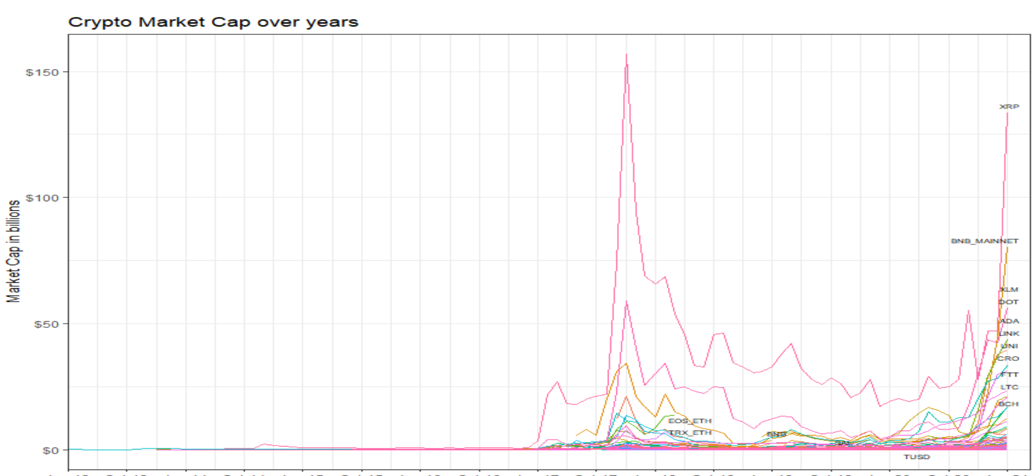


Figure A.7: Crypto market capitalization

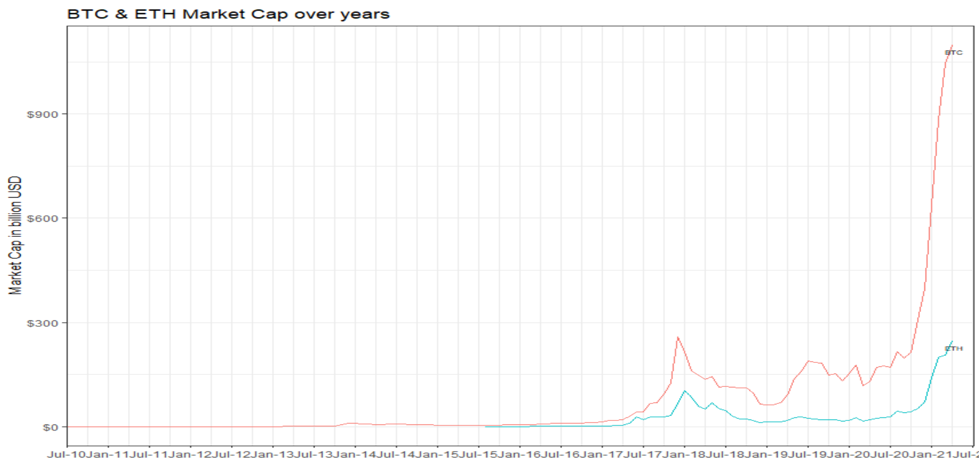


Figure A.8: BTC and ETH market capitalization

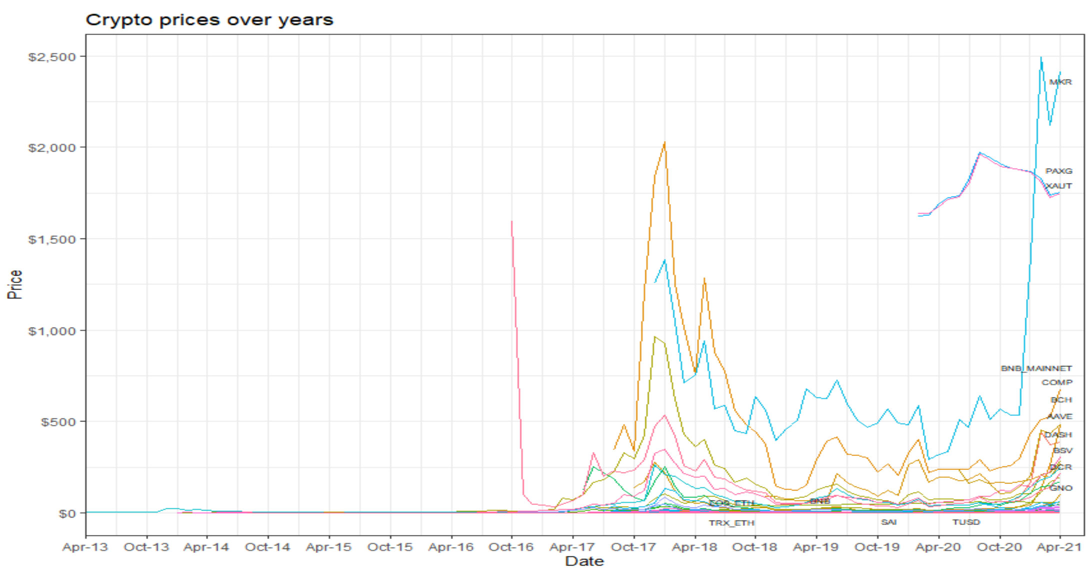


Figure A.9: Cryptocurrency historical prices

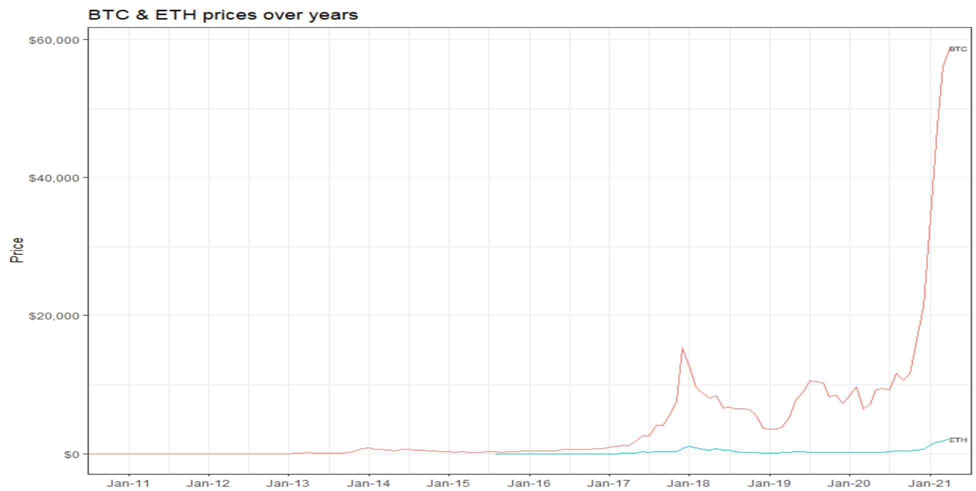


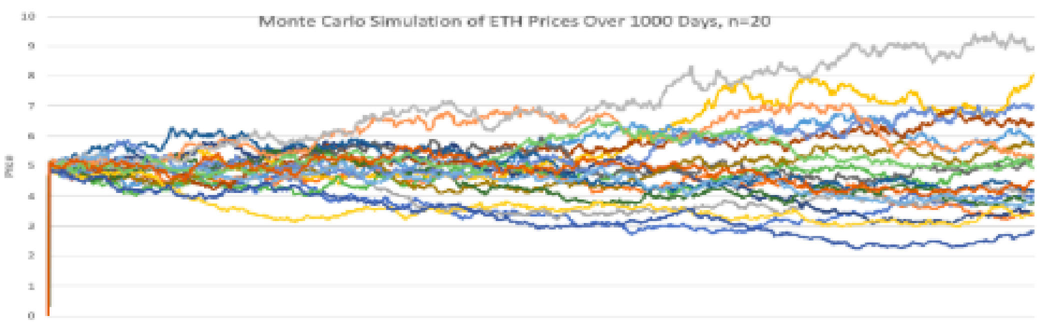
Figure A.10: BTC and ETH historical prices

```python
# Total population, N.
N = 3900000000 #62% of global 2020 population representing ages 17-70
# Initial number of infected and recovered individuals, I0 and R0.
I0, R0 = 106000000, 0 #data from business insider estimates 106 million active users in 2020
# Everyone else, S0, is susceptible to use initially.
S0 = N - I0 +R0
# Contact rate, beta, and mean recovery rate, gamma, (in 1/days).
beta, gamma = 0.0005, 1./7300 #7300 is 20 years

# A grid of time points (in days)
t = np.linspace(0, 7300, 7300)

# The SIR model differential equations.
def deriv(y, t, N, beta, gamma):
    S, I, R = y
    dSdt = -beta * S * I / N
    dIdt = beta * S * I / N - gamma * I
    dRdt = gamma * I
    return dSdt, dIdt, dRdt

# Initial conditions vector
y0 = S0, I0, R0
# Integrate the SIR equations over the time grid, t.
ret = odeint(deriv, y0, t, args=(N, beta, gamma))
S, I, R = ret.T
```

Figure A.11: Python implementation for a SIR model

$$
\begin{aligned}
\frac{dS}{dt} &= -\frac{\beta S I}{N}, \\
\frac{dI}{dt} &= \frac{\beta S I}{N} - \gamma I, \\
\frac{dR}{dt} &= \gamma I.
\end{aligned}
$$

Figure A.12: Kermack and McKendrick base equations



Starting Price	$	5.01
Annual Volatility		5.26%
Daily Volatility		0.960%
Mean Price	$	4.90
Median Price	$	4.85
Std. Dev.		1.089834927
Percentiles		
5%	$	3.21
95%	$	6.83
25%	$	4.27
75%	$	5.43

Figure A.13: Ethereum Monte Carlo Simulation

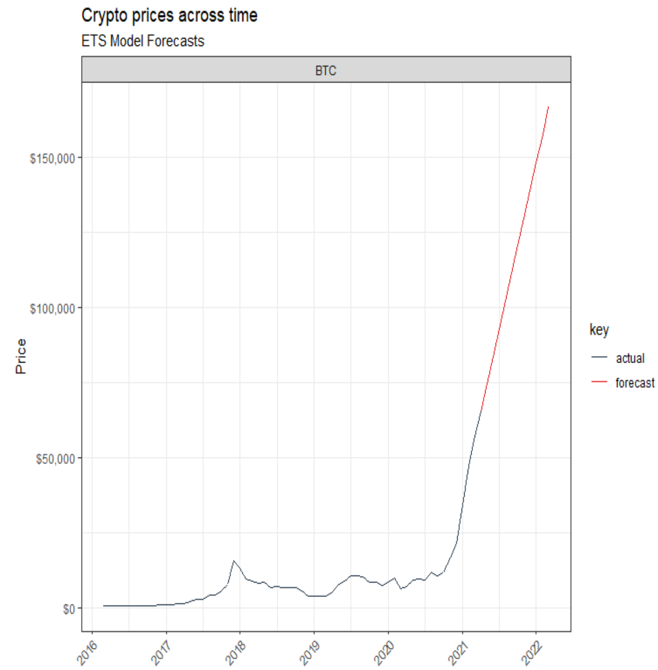


Figure A.14: BTC price prediction model

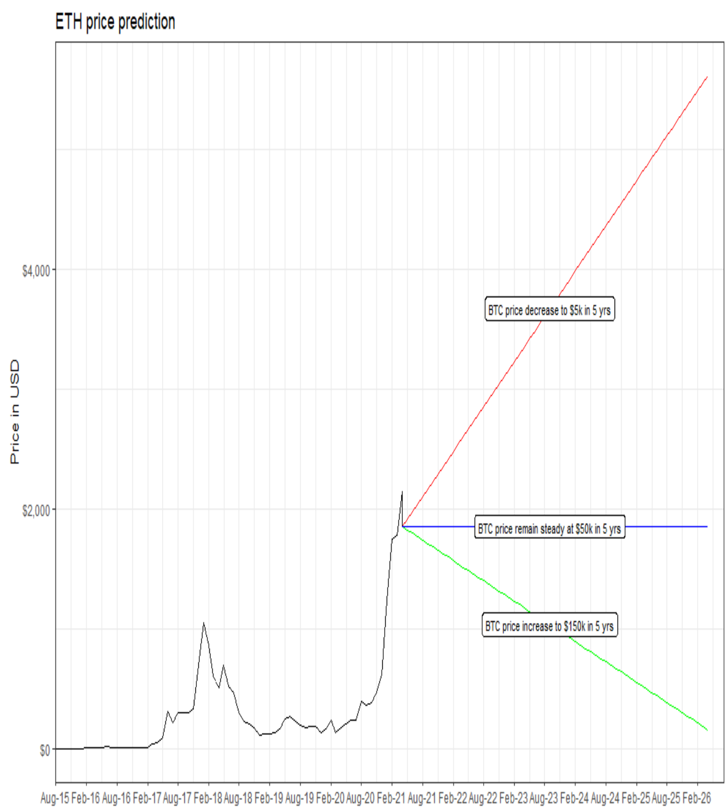


Figure A.15: ETH price prediction model

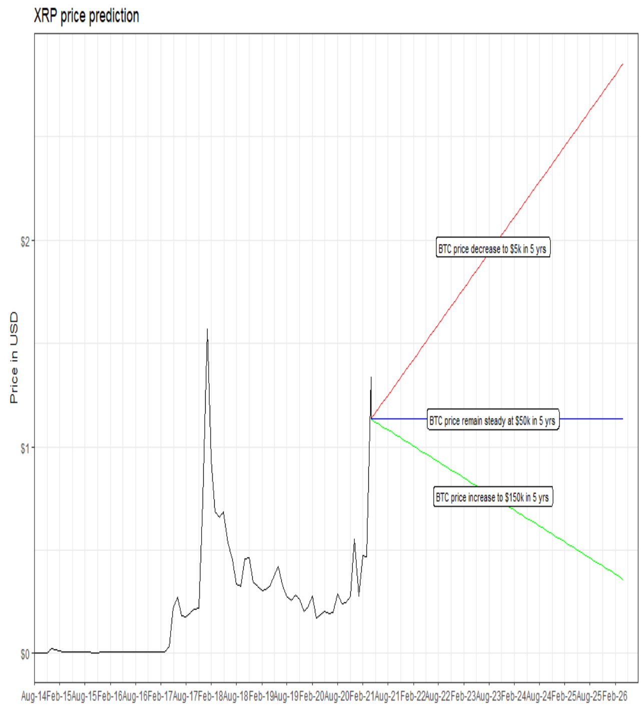


Figure A.16: XRP price prediction model

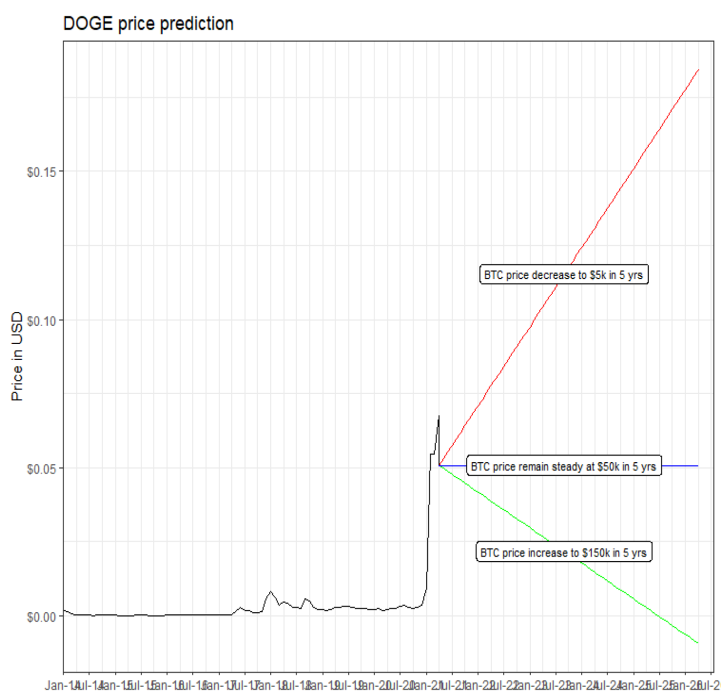


Figure A.17: DOGE price prediction model

Bibliography

Ahmed, Aftab, and Nupur Anand. 2021. "India to propose cryptocurrency ban, penalising miners, traders - source." Reuters. https://www.reuters.com/article/uk-india-cryptocurrency-ban/india-to-propose-cryptocurrency-ban-penalising-miners-traders-source-idUSKBN2B60QP.

Areddy, James. 2021. "China Creates Its Own Digital Currency, a First for Major Economy." *Wall Street Journal*, April 5, 2021. https://www.wsj.com/articles/china-creates-its-own-digital-currency-a-first-for-major-economy-11617634118.

Ballis, Antonis, and Konstantinos Drakos. "The explosion in cryptocurrencies: a black hole analogy." *Financial Innovation*7, no. 1 (2021): 1-8.

Bass, Frank M. "A new product growth for model consumer durables." *Management science* 15, no. 5 (1969): 215-227

Cuen, Leigh. 2021. "The debate about cryptocurrency and energy consumption." TechCrunch. https://techcrunch.com/2021/03/21/the-debate-about-cryptocurrency-and-energy-consumption/.

ElegantJ BI. 2017. "Leading India Stock Brokerage Firms Benefit From ElegantJ BI Solution." ElegantJ BI. https://www.elegantjbi.com/blog/leading-india-stock-brokerage-firms-benefit-from-elegantj-bi-solution.htm.

Financial Crimes Enforcement Network. 2020. "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets." Federal Register. https://public-inspection.federalregister.gov/2020-28437.pdf.

Ganjeizadeh, Farnaz, Howard Lei, Preetpal Goraya, and Erik Olivar. "Applying looks-like analysis and bass diffusion model techniques to forecast a neurostimulator device with no historical data." *Procedia Manufacturing* 11 (2017): 1916-1924

Global Legal Research Center at the Library of Congress. 2018. “Regulation of Cryptocurrency Around the World.” The Law Library of Congress. https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf.

Goodkind, Andrew L., Benjamin A. Jones, and Robert P. Berrens. "Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining." *Energy Research & Social Science* 59 (2020): 101281.

Imbert, Fred. 2017. “Bitcoin took a major dive after a big Chinese exchange said it is closing.” *CNBC*, September 14, 2017. https://www.cnbc.com/2017/09/14/bitcoin-is-dropping-right-now-after-a-big-chinese-exchange-said-it-is-closing.html.

James, Letitia. 2021. “Attorney General James Ends Virtual Currency Trading Platform Bitfinex’s Illegal Activities in New York.” New York State Office of the Attorney General. https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal.

Kaiser, H. F. (1960). The Application of Electronic Computers to Factor Analysis. Educational and Psychological Measurement 20, 141–151.

Kermack, W. and McKendrick, A., 1927. A contribution to the mathematical theory of epidemics. Proc. R. Soc. London A 115, 700-721. Proc. R. Soc. London A 115, 700-721.

Kharif, Olga. 2021. “Crypto Market Cap Surpasses $2 Trillion After Doubling This Year.” Bloomberg. https://www.bloomberg.com/news/articles/2021-04-05/crypto-market-cap-doubles-past-2-trillion-after-two-month-surge.

Kharpal, Arjun. 2021. “A major Chinese bitcoin mining hub is shutting down its cryptocurrency operations.” *CNBC*, March 2, 2021. https://www.cnbc.com/2021/03/02/china-bitcoin-mining-hub-to-shut-down-cryptocurrency-projects.html.

Malsin, Jared, and Caitlin Ostroff. 2021. “Bitcoin Payments to Be Banned in Turkey After Confidence Drops in Lira.” The Wall Street Journal, April 16, 2021. https://www.wsj.com/articles/bitcoin-payments-to-be-banned-in-turkey-after-confidence-drops-in-lira-11618570574.

Molina, Brett. 2021. “PayPal to let users pay for purchases at checkout using Bitcoin, other cryptocurrency.” *USA Today*, March 30, 2021. https://www.usatoday.com/story/tech/2021/03/30/paypal-let-you-pay-purchases-using-bitcoin-cryptocurrency/7058545002/.

Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-toPeer Electronic Cash System.” Bitcoin.org. https://bitcoin.org/bitcoin.pdf.

Patel, Nilay. 2021. “Is There A Future for Bitcoin? an Investor and A Skeptic Make Their Cases.” The Verge. https://www.theverge.com/22367951/bitcoin-future-nic-carter-steve-hanke-interview-decoder-podcast.

Portilla, Ricardo. 2019. “Understanding Dynamic Time Warping.” Databricks. https://databricks.com/blog/2019/04/30/understanding-dynamic-time-warping.html.

Reuters. 2021. “Bitcoin slumps 14% as pullback from record gathers pace.” *Reuters*, April 18, 2021. https://www.reuters.com/technology/bitcoin-falls-111-53356-2021-04-18/.

Rogers, Everett M. "Diffusion of Innovations: modifications of a model for telecommunications." In *Die diffusion von innovationen in der telekommunikation*, pp. 25-38. Springer, Berlin, Heidelberg, 1995.

Salzman, Avi. 2020. “Trump Administration’s Recent Cryptocurrency Crackdown Surprises Some.” *Barron's*, December 23, 2020. https://www.barrons.com/articles/trump-administrations-recent-cryptocurrency-crackdown-surprises-some-51608765714.

Yackley, Ayla J. 2021. “Turkey bans crypto payments for goods and services.” *The Financial Times*, April 16, 2021. https://www.ft.com/content/449f8ac5-be7b-4d50-b01d-fe5314109d6f.

Yen, Kuang-Chieh, and Hui-Pei Cheng. "Economic policy uncertainty and cryptocurrency volatility." *Finance Research Letters* 38 (2021): 101428.

Zhang, Laney. 2018. “Regulation of Cryptocurrency: China.” Lw Library of Congress. https://www.loc.gov/law/help/cryptocurrency/china.php.