Chapter 16
Risk Analysis of Cryptocurrency as an Alternative Asset Class

L. Guo and X.J. Li

Abstract The purpose of this study is to analyze the risk of cryptocurrencies, as an alternative investment. In particular, we find the wealth distribution of the cryptocurrency, evaluate its corresponding effects on the market and analyze other risk factors resulting in the death of altcoins. The paper concludes that the closer the right tail of wealth distribution approaching the Power-Law model, the more stable the market will be. This result is quite useful for investors to make decisions when investing in cryptocurrencies.

16.1 Introduction

As a representative of cryptocurrency, Bitcoin was developed by an anonymous hacker in 2009. Within 4 years' development, the price of Bitcoin had reached higher than $1,000 by the end of 2013. What's more, the total number of Bitcoins that can be mined has been limited within 21 million while it appears to be a more complicated question to calculate the amount of gold that can be mined. As a result, during the period when the gold price has collapsed, Bitcoin appears to be a better store of value than gold for investors.

Besides, Bitcoin can be used to make online purchases via mobile phones or other devices. Popular with the techno tribe, the currency is regarded as being beyond the reach of government regulation – the anonymous founder of Bitcoin introduced the idea of a distributed block chain to prevent the counterfeiting of Bitcoin (Lee et al. 2014). The block chain, also known as the public ledger, is a technical innovation that solves a 20-year-old problem called the General Byzantine problem (Lam et al. 2014), which is a problem all distributed systems face. For instance, how to reach

L. Guo (✉)
Lee Kong Chian School of Business, Singapore Management University,
50 Stamford Road, Singapore 178899, Singapore
e-mail: liguo.2014@pbs.smu.edu.sg

X.J. Li
College of Letters and Science, University of California, Berkeley, CA, USA
e-mail: lxjpub@gmail.com

W.K. Härdle et al. (eds.), *Applied Quantitative Finance*, Statistics and Computing,
DOI 10.1007/978-3-662-54486-0_16

consensus in a system without any central authorities instructions or how to prevent the double spending of digital currency.

In 2014, the Bitcoin Central partnered with a French bank becoming a registered Payment Services Provider (PSP) under the European Union Law. It means that Bitcoins now can offer debit cards, account insurance and other banking facilities to the Bitcoin owners. This phenomenon became a breaking news because the amount of Bitcoin value is becoming infinite due to the excess demand of market which changed drastically from its original value. Nowadays Bitcoin has already gained worldwide attention, as people can sell products or services overseas by using Bitcoins and make profits immediately. There are more than twelve million Bitcoin users including digital miners, traders and small business owners.

Meanwhile, similar cryptocurrencies or alternative cryptocurrencies (aka. altcoins) are proliferating, and there are now over 400 active altcoins in the market (Lee et al. 2014). Examples of popular cryptocurrencies include Bitcoin, Ripple, Litecoin and Dogecoin (Coinmarketcap.com, 2014). However, many of the coins are ephemeral and become inactive shortly after they are launched. Such coins are known as dead coins e.g. Auroracoin (AUR), Alcohoin (ALC), 2chcoin (2ch), 66coin (66). Digital currencies can potentially play a major role in lowering the cost of financial services and enable financial institutions to reach out to the unbanked banking and the under-banked (Ignacio et al. 2014). As a payment system, digital currency can contribute to the banking and achieve the goal of financial inclusion for being advocated by 90 countries in the Maya Declaration as well as the Bill and Melinda Gates Foundation (gatesfoundation.org, 2014). Therefore, it is important to investigate the factors that determine the success of a coin as we can then avoid similar pitfalls in the future when constructing a new coin, which can benefit the less privileged and those at the bottom of the wealth pyramid (XiangJun et al. 2014). To this end, we have decided to compare the different characteristics of Auroracoin and Bitcoin to figure out those risk factors leading to the death of Auroracoin but the success of Bitcoin. The present paper adopts a complete empirical methodology for detecting Power-Laws introduced by (Clauset et al. 2009). To verify whether the whole range of the upper tails of wealth distributions obeys the Power-Law model. We estimate both the Power-Law exponent and the lower bound on the Power-Law behavior.

The paper is organized as follows: Sect. 16.2 shortly describes our data sets drawn from the original blockchain and other sources. Section 16.3 presents the statistical framework introduced by Clauset et al. which is used for measuring and analyzing Power-Law behavior in empirical data. Section 16.4 is the empirical analysis while Sect. 16.5 serves as the conclusion.

16.2 Data Collection

Data are collected mainly through the following four methods:

16.2.1 Parse the Balance Information of Each Address from the Downloaded Block Chain Using C++

A source code written in C++ by John W. Ratcliff was used and modified. Basically, this program provides us the balance information of each address which can be used to find the wealth distribution of both Bitcoin and Auroracoin.

16.2.2 Parse Other Fundamental Variables of Bitcoin

Blockchain.info contains all the fundamental variables of Bitcoin market except for the balance information. The data include market price, transaction volume, developer's revenue, etc. All the data were downloaded in CSV format and R 3.1.2 was used to group the data together and calculate the aggregate where appropriate.

16.2.3 Historical Price Data for Auroracoin Are from a Data Provider Named Myip

Myip is a data provider that stores the historical price and transaction volumes of Auroracoin. Additionally, different from Bitcoin, the block chain explorer of Auroracoin doesn't have the historical price, so we have to use this data provider to collect the historical price of Auroracoin.

16.2.4 Parse Other Fundamental Variables of Auroracoin from Online Block Chain Explorer Using Python

We obtained the data of other fundamental variables of Auroracoin from the Block Chain Explorer. Figure 16.1 shows how the webpage looks like.

16.3 Methodology

In the beginning, we believe it is necessary for a coin's wealth distribution to follow a pareto optimal distribution. The reason is that, in the initial stage, we expect to see "Top few" users to develop the market and their wealth of the coin takes large position of the overall market. Indeed, the existence of "Top few" users are necessary for a coin to survive and gain popularity, hence shaping the overall wealth distribution to follow a power law. So in the paper, the first hypothesis we want to test is that

AuroraCoin 123101

Short Link: http://explorer.auroracoin.eu/b/12dF1oi8os

Hash: bd4055064262d2f7742a42472e5c350aa0064416935d5aa57ad857fc0b1c6165
Previous Block: 83f8a8b3dff6dee0642aebcc47858d40f6167d95ea9b48c46c808594ad77f548
Next Block: d093fff0f67f0366a8a84031ccf903a3e265604cade9cdaf47a693fdcb96b002
Height: 123101
Version: 1
Transaction Merkle Root: 612e55180bc4507e087252045411c751be13a78d2d89de379e6c1fc5cce9e7ba
Time: 1431477552 (2015-05-13 00:39:12)
Difficulty: 440.196 (Bits: 1c0094e1)
Cumulative Difficulty: 19 550 578.013
Nonce: 23539883
Transactions: 2
Value out: 50
Transaction Fees: 0
Average Coin Age: 128.82 days
Coin-days Destroyed: 12.58998842
Cumulative Coin-days Destroyed: 70.7386%

Fig. 16.1 Original Data from Blockchain

whether the wealth distribution is one of the key factors that determine the success of a crypto currency. In fact, by plotting the wealth distribution of both Bitcoin and Auroracoin, we find the right tail of both wealth distribution seem to follow the Power-Law model. Hence, in the paper, we fit the wealth distribution using the Power-Law model. There's no denying that there are some other candidates to fit the wealth distribution, such as Log-normal distribution, which has a similar pattern as Power-Law. However, as a preliminary study, we do not focus on the comparison of density functions.

In order to find the Power-Law behavior in wealth distributions we use a toolbox proposed by Clauset et al. (2009). A density of continuous Power-Law model is given by

$$p(x) = \frac{\alpha - 1}{x_{min}} \left(\frac{x}{x_{min}}\right)^{-\alpha} \tag{16.1}$$

The maximum likelihood estimator (MLE) of the Power-Law exponent, $\hat{\alpha}$, is

$$\hat{\alpha} = 1 + n\Big\{\sum_{i=1}^{\infty} \log \frac{x_i}{x_{min}}\Big\} \tag{16.2}$$

where $x_i; i = 1, 2 \ldots n$ are independent observations such that $x_i > x_{min}$. In the meantime, x_{min} can be found by minimizing the well-known Kolmogorov–Smirnov (KS) statistic, which can be defined as follow:

$$KS = \max_{x \geq x_{min}} |S(x) - P(x)| \tag{16.3}$$

In the equation above, $S(x)$ stands for the CDF of the data for the observations with value at least x_{min} while $P(x)$ represents the CDF for the Power-Law model that best fits the data in the region $x \geq x_{min}$. Hence, the lower bound on the Power-Law, x_{min}:

$$x_{min} = \underset{x_{min}}{\operatorname{argmin}}\, KS \tag{16.4}$$

The next step in measuring Power-Law involves testing goodness of fit. A positive result of such a test allows us to conclude that a Power-Law model is consistent with a given data set. Following Clauset et al. again, we start with fitting a Power-Law model to data using the MLE for α and the KS-based estimator for x_{min}. Meanwhile, we have the KS statistic for this MLE fitting. Next, we generate the synthetic data sets with scaling parameter $\hat{\alpha}$ and lower bound x_{min} from previous step. To be more specific, the synthetic data sets have the Power-Law model above the estimated x_{min} and have the same non-Power-Law distribution as the original data set below $\hat{x}_{min}$. Then, Power-Law models are fitted to each of the generated data sets with the KS statistics calculated. Finally, we define the p-value of the test as the fraction of data sets for which their own KS statistics are larger than the KS found in the empirical data set. Hence, the Power-Law hypothesis is rejected if this p-value is smaller than the chosen threshold. In the reference (Clauset et al. 2009), Clauset et al. rules out the Power-Law model if the estimated p-value for the test is smaller than 0.1.

16.4 Empirical Results

In this section, we compared the wealth distribution of two different altcoins, Bitcoin and Auroracoin to illustrate the importance of achieving a Pareto optimal distribution. After that, we further test the predicting power of wealth distribution, defined as the frequency distribution of public addresses of the digital currency under study. In particular, we examine the following hypothesis that the wealth distribution within the system has predictive power over its lifespan and price. On top of that, we also study the different characteristics of both coins and document the important features that lead to the survivorship of the cryptocurrency.

16.4.1 Data Visualization

We first plot a histogram of frequency of public addresses of Bitcoin and Auroracoin, as we have shown in Figs. 16.2 and 16.3.

It seems that Auroracoin does not appear to follow a distinct Power-Law distribution while the distribution of Bitcoin does. In the meantime, although the wealth

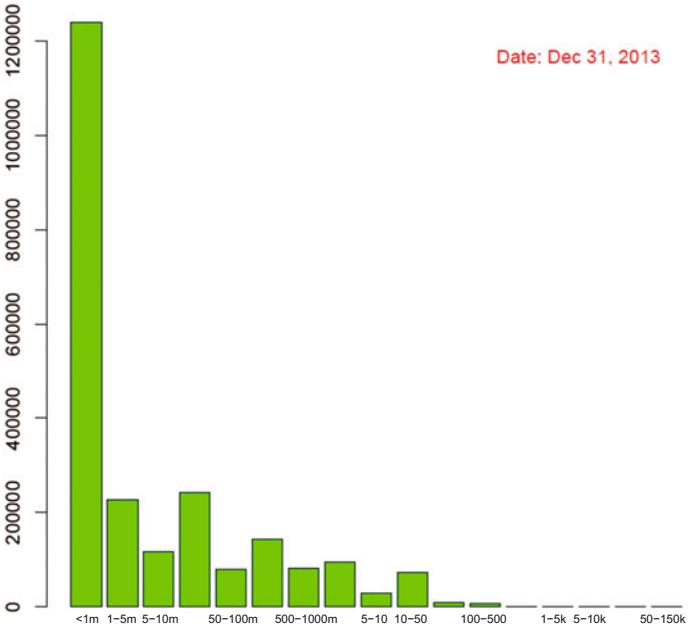

Fig. 16.2 Bitcoin Histogram. XFGHistWealthD

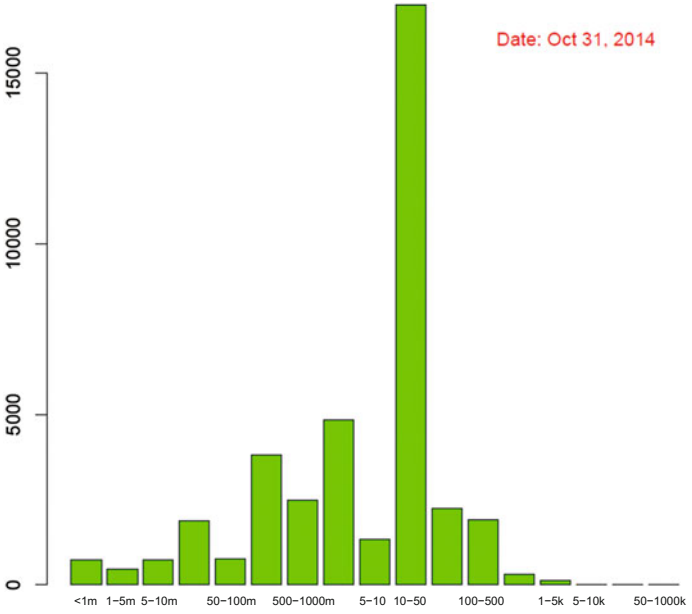

Fig. 16.3 Auroracoin Histogram. XFGHistWealthD

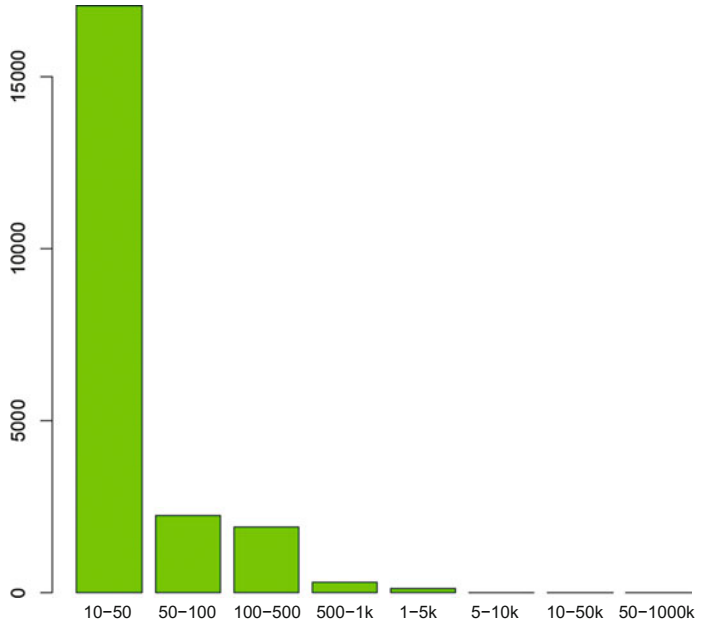

Fig. 16.4 Right Tail Auroracoin Histogram. XFGHistWealthD

distribution in Auroracoin does not exhibit Power-Law distribution on the whole, the tail part of the distribution does seem to follow a Power-Law distribution (shown in Fig. 16.4). Therefore, when calculating the α, x_{min} is set free and is automatically determined by the programme to minimize the Kolmogorov–Smirnov statistics. The motivation is to investigate if the Power-Law parameters for the right side of the distribution have any explanatory power for those fundamental variables of cryptocurrencies. Table 16.1 lists the fundamental variables treated as dependent variables in the following regression.

16.4.2 Power-Law Estimation and Empirical Analysis

In this section, we fit the wealth distribution of Bitcoin and Auroracoin using the Power-Law model. For the Auroracoin, only the right tail seems to follow the Power-Law pattern so the x_{min} is optimally selected by minimizing the KS statistic in the Auroracoin case.

Shown in Figs. 16.5 and 16.6, α of Bitcoin increases smoothly while α of Auroracoin goes up and down. What's more, the α shows no significant predicting power on those fundamental variables in terms of Bitcoin while for the Auroracoin, its significant predicting power is not only limited to the price movements but also applicable to other fundamental variables with average R-square $= 0.65$, much larger than that

Table 16.1 Variable list

Variable list	Definition
Days destroyed	A measure of the transaction volume of Cryptocurrency. If someone has 100 BTC that they received a week ago and they spend it then 700 bitcoin days have been destroyed
MB.1	The total size of all block headers and transactions
Difficulty	A measure of how difficult it is to find a new block compared to the easiest it can ever be
Hashrate	The estimated number of billions of hashes per second the bitcoin network is performing
Market cap	Total number of bitcoins in circulation * the market price in USD
Market price	Price of Cryptocurrency
Miners revenue	(Number of bitcoins mined per day + transaction fees) * market price
Network deficit	Difference between transaction fees and cost of bitcoin mining
No. of deals	Total number of unique bitcoin transactions per day
Ratio	Transaction volume/USD exchange volume

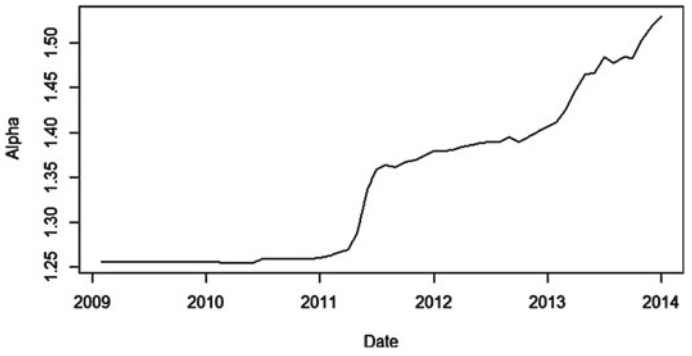

Fig. 16.5 Bitcoin Power-Law Estimation using whole sample. XFGPowerLawAlpha

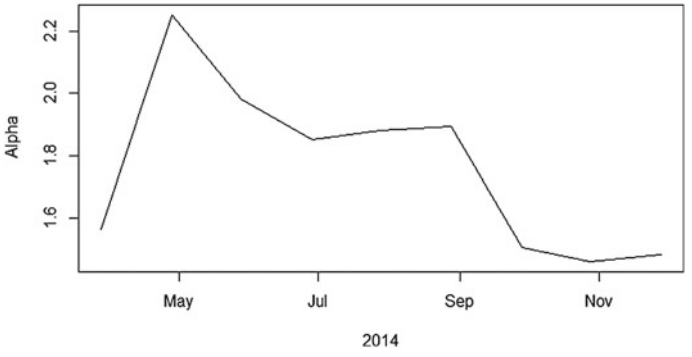

Fig. 16.6 Auroracoin Power-Law Estimation (Right Tail). XFGPowerLawAlpha

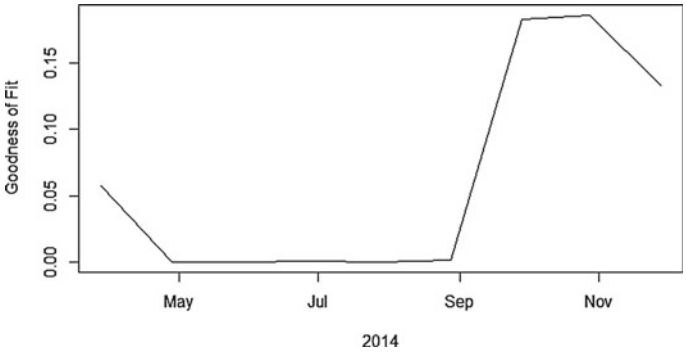

Fig. 16.7 Goodness of Fit of Auroracoin (Right Tail). XFGPowerLawP

of Bitcoin. In addition, all the fundamental variables have been taken first-order difference so that the variables put into regressions are stationary. We are surprised about these findings as it contradicts to our expectations. Auroracoin is short lived after it is launched while Bitcoin is one of successful crytos in the market. Why the distribution of a dead coin play an important role in determining the market of a deadcoin but has no effects on Bitcoin? To answer this question, we further test the goodness of fit on wealth distributions of Bitcoin and Auroracoin respectively. Results suggest that none of the models survives – for Bitcoin, all p-values across the whole sample period are 0, indicating the whole sample doesn't follow Power-Law. Similarly, with respect to the Auroracoin, p-values above 10% level only occur in 3 months, suggesting that only 3 of them can be fitted using the Power-Law distribution (see Fig. 16.7).

Given the goodness of fit, we know that the $\hat{\alpha}$ in both cases cannot reflect the wealth distribution very well. In Bitcoin case, $\hat{\alpha}$ has no prediction power over the market which is not due to the wealth distributions lacking impact on the market but because the $\hat{\alpha}$ cannot stand for the wealth distribution of Bitcoin market. As for the Auroracoin case, it becomes an another story – although the fitted α cannot reflect the wealth distribution of Auroracoin, it shows significant prediction power on those fundamental variables. Looking into the regression, we note that only 8 observations are included in the regression, so the estimation results may not be so convincing. Later, daily data instead of monthly data should be tested in order to expand the samples. Running the Power-Law model for a long time made us neglect the checking of regression results using daily data.

Keeping in mind that we have already selected the optimal x_{min} for Auroracoin to fit the Power-Law distribution but not for Bitcoin, it is safe to conclude that wealth distribution of Auroracoin market doesn't follow the Power-Law distribution and for the Bitcoin market, using the whole sample to fit the wealth distribution is inappropriate. Therefore, we try to improve the model by analyzing the right tail wealth distribution of Bitcoin with x_{min} optimally selected in order to improve the goodness of fit of the Power-Law model.

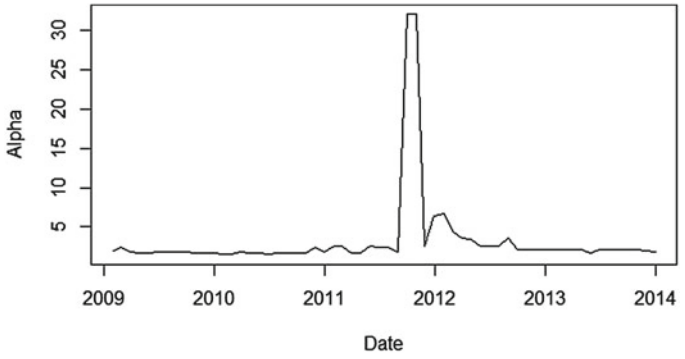

Fig. 16.8 Bitcoin Power-Law Estimation (Right Tail). XFGPowerLawAlpha

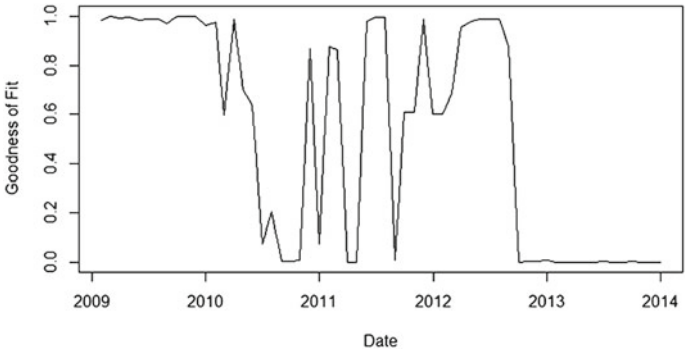

Fig. 16.9 Goodness of Fit of Bitcoin (Right Tail). XFGPowerLawP

Figures 16.8 and 16.9 suggest that although the overall wealth distribution of Bitcoin doesn't follow Power-Law, its right tail perfectly fits the Power-Law distribution. Besides, the p-value varies dramatically before the end of 2012, while the majority of p-values are above 10% level, indicating that the right tail wealth distribution of Bitcoin market follows the Power-Law distribution well. However, the p-value drops below 5% level after September 2012, implying that the wealth distribution deviates a lot from the Power-Law distribution. This is quite consistent with the sharp increase of price from the end of 2012. It is believed that when the price explodes, the Bitcoin market will begin to deviate from its previous state due to the extraordinary amount of investors in the market. As we know, there are multiple big events happening during that time. On 15th Nov, 2012, Wordpress as one of the 25 most popular domains on the web, its move paved the way for later retail ventures of Bitcoin. On 25th March, 2013, the Eurogroup, the European Commission, the European Central Bank and the International Monetary Fund orchestrated the 10 billion bailout to fortify the flagging Cypriot economy. As a result, the increasing trading volume broke Mt. Gox in April. Then on 18 Nov, 2013, US Senate held a hearing of Bitcoin. Afterwards and most importantly, Bitcoin was accepted in China. Chinese people were free to

participate in the Bitcoin market finally. BTC China achieved a trading volume more than twice of the second place in Mt. Gox. Within one year, the Bitcoin price jumped from $11.04 to $1075.16. Of course, all these events exerted profound effects on the Bitcoin market and thus causing the wealth distribution deviating from its previous status.

In terms of α value, we note that it jumps to 32.06 in Sep 2011. That is because earlier that month, Mt. Gox was hacked. A copy of the users' database was leaked and was used to launch attacks against accounts held by users of the MyBitcoin online wallet service, because they shared the same password on both sites. The attack resulted in thefts of over 4,019 BTC from about 600 wallets. Consequently, the Bitcoin market experienced a downward trend in the following months. Even large Bitcoin holders began to sell the coins, increasing the diversification of the Bitcoins. As the α parameter stands for the diversification of the wealth distribution – a higher α means that wealth is more diversified. As a matter of fact, Alpha increases a lot in the following months. However, the wealth distribution of that time still follows the Power-Law. We believe that this event exerted a great influence on the market, but it is not strong enough to disrupt the whole market, which is different from the case when the market price exploded to $1000 with big events (Tables 16.2 and 16.3).

However, the Auroracoin doesn't follow the Power-Law distribution even considering the right tail of wealth distribution. In the wealth distribution plots in Fig. 16.3, the air-dropped amount is seldom spent by the recipients for Auroracoin. The value of Auroracoin is thus severely undermined. What's worse, since the coins are acquired for free as opposed to arduous processes such as mining or trading, people do not show appreciation for the coin, which leads to its death. Nonetheless, for Bitcoin, as mining is required, people do think the coin worth a certain amount of value. Over time, the wealth distribution of Bitcoin edges towards Pareto distribution (in previous analysis, we have already concluded that wealth distribution of Bitcoin followed Power-Law and so in this part we mainly refer to the optimal Power-Law distribution indicated by the α). Pareto is a mathematical model that the wealth distribution in the real world follows, and more and more people start to use it for various reasons, such as analyzing international fund transfer. It can be easily verified – excluding in high volatile periods when big events happen and the price explodes. The Power-Law parameter, α, has been increasing evidenced by Fig. 16.8. On the contrary, the wealth distribution of Auroracoin has not shown many changes during 2014 and certainly does not follow the Power-Law distribution (Fig. 16.7). Therefore for a coin to survive and gain popularity, attaining Pareto distribution is absolutely helpful.

However, using the truncated sample, the $\hat{\alpha}$ still does not show any significant predicting power over those fundamental variables (Table 16.4). The reason is that, for most months, the x_{min} is too large to be considered in the majority of observations. For example, in some months, less than 100 observations are counted when fitting the Power-Law distribution while the whole sample size for that month amounts to 20 million. In other words, α has lost some generality if the truncated sample size is used. That is why the diversification of wealth, treating α as a proxy, has no predicting power over fundamental variables, while the right tail of wealth distribution follows the Power-Law model.

Table 16.2 Predicting power of Bitcoin wealth distribution

	Days destroyed ($*10^6$)	MB.1	Difficulty ($*10^6$)	Hashrate ($*10^6$)	Market cap ($*10^6$)	Market price	Miners revenue ($*10^6$)	Network deficit ($*10^6$)	No. of transactions ($*10^6$)	Ratio
(Intercept)	2, 934.07***	6, 594.04***	506.68*	4.52*	5, 146.12*	424.53*	1.93*	−1.92*	15, 63***	152.65***
	(534.17)	(1, 333.22)	(275.29)	(2.47)	(2, 946.43)	(242.76)	(1.07)	(1.06)	(3.04)	(19.95)
D_Alpha	5, 786.83	11, 592.00	1, 134.81	9.79	13, 487.32	1, 129.65	5.08	−5.04	26.88	246.75
	(5, 483.28)	(13, 685.48)	(2, 825.86)	(25.33)	(30, 245.12)	(2, 491.93)	(10.95)	(10.88)	(31.23)	(204.80)
R^2	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.02
Adj. R^2	0.00	−0.00	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.00	0.01
Num. obs.	59	59	59	59	59	59	59	59	59	59
RMSE	4,088.67	10,204.73	2,107.13	18.89	22,552.61	1858.13	8.16	8.11	23.29	152.71

$^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$

XFGPowerLawEst1

Table 16.3 Predicting power of Auroracoin wealth distribution

	Days destroyed ($*10^6$)	Cost. transaction	Difficulty	Transaction volume ($*10^6$)	Market price	No. of transactions	Transaction.fees
(Intercept)	0.01	1.26	28.01	50.17	−2.37*	1, 376.34	0.00
	(0.06)	(5.89)	(194.34)	(292.66)	(1.12)	(5, 544.57)	(0.00)
D_Alpha	0.06**	67.63**	2, 083.06**	3, 198.36**	−13.83***	61, 054.08**	0.03**
	(0.02)	(19.53)	(644.66)	(970.80)	(3.70)	(18, 392.50)	(0.01)
R^2	0.60	0.67	0.64	0.64	0.70	0.65	0.62
Adj. R^2	0.53	0.61	0.57	0.58	0.65	0.59	0.56
Num. obs.	8	8	8	8	8	8	8
RMSE	17104.18	16.63	548.99	826727991.81	3.15	15662.94	0.01

***$p < 0.01$, **$p < 0.05$, *$p < 0.1$

XFGPowerLawP

Table 16.4 Predicting power of Bitcoin right tail wealth distribution

	Days destroyed ($*10^6$)	MB.1	Difficulty ($*10^6$)	Hashrate	Market cap ($*10^6$)	Market price	Miners revenue ($*10^6$)	Network deficit ($*10^6$)	No. of transactions	Ratio
(Intercept)	1, 915.90***	1, 896.68***	1.93*	15, 159.10*	99.66	10.32	0.08	−81, 039.97	5.35***	92.70***
	(410.62)	(576.45)	(0.99)	(7, 985.15)	(105.59)	(15.36)	(0.16)	(0.16)	(1.45)	(23.54)
D_Alpha	35.60	66.73	0.28*	477.30	−23.21	−3.67*	−34, 639.12	3, 4505.21	0.18	−5.14
	(57.63)	(80.90)	(0.14)	(1, 120.63)	(14.82)	(2.16)	(23, 107.99)	(22, 949.44)	(0.20)	(3.30)
R^2	0.01	0.02	0.11	0.01	0.07	0.08	0.06	0.06	0.02	0.07
Adj. R^2	−0.02	−0.01	0.08	−0.02	0.04	0.05	0.04	0.04	−0.01	0.04
Num. obs.	35	35	35	35	35	35	35	35	35	35
RMSE	2,429.22	3,410.29	5.88	47,239.87	624.65	90.89	0.97	967430.57	8.57	139.28

$^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$

XFGPowerLawP

Table 16.5 Predicting power of goodness of fit (Power-Law periods)

	Days destroyed ($*10^6$)	MB.1	Difficulty ($*10^6$)	Hashrate	Market cap ($*10^6$)	Market price	Miners revenue ($*10^6$)	Network deficit	No. of transactions ($*10^6$)	Ratio
(Intercept)	1, 567.09	731.37	−1.93	−32, 421.78	−505.22	−79.12	−0.67	0.66	2.54	75.43
	(1, 966.83)	(2, 767.07)	(4.96)	(37, 198.99)	(510.27)	(74.67)	(0.80)	(0.79)	(6.97)	(116.19)
P_value	402.97	1, 343.61	4.45	54, 748.14	694.53	102.68	0.86	−0.85	3.25	19.61
	(2, 211.73)	(3, 111.61)	(5.58)	(41, 830.81)	(573.81)	(83.97)	(0.90)	(0.89)	(7.83)	(130.65)
R^2	0.00	0.01	0.02	0.05	0.04	0.04	0.03	0.03	0.01	0.00
Adj. R^2	−0.03	−0.02	−0.01	0.02	0.01	0.01	−0.00	−0.00	−0.02	−0.03
Num. obs.	35	35	35	35	35	35	35	35	35	35
RMSE	2442004307.47	3435.57	6158266.21	46185.99	633553438.34	92.71	993133.43	986436.90	8649344.11	144.26

$^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$

XFGPowerLawP

So now we relax our hypothesis by considering another indicators, the goodness of fit and p-value. The smaller the p-value is, the more the true wealth distribution deviates from the Power-Law distribution. Then the new hypothesis becomes that whether the extent of wealth distribution approaching the optimal Power-Law distribution has its significant predicting power on the Bitcoin market.

Similar to α, we test the predicting power using sample where the goodness of fit is above 10% and the results suggest that increase in the goodness of fit has no significant impacts on the fundamental variables, evidenced by Table 16.5. Namely, whether the right tail of wealth distribution approaches the Power-Law rarely affects the Bitcoin market. The result may not be reliable since the sample we used in the regression only covers the periods that appear to follow the Power-Law. The p-values are relative stable across the time and the overall market environment. Hence, the effect of approaching Pareto optimal distribution cannot be fully reflected by the market during those periods. After that, we reestimate the predicting power of Clauset's goodness of fit by including in the non-Power-Law periods. This is another great advantage of using p-value to measure the whole market. In the case of α, we are restricted to do so since when P drops below 0.1, the wealth distribution doesn't follow Power-Law and hence α loses its ability to explain the market. Generally speaking, the goodness of fit has more general effects on the cryptocurrency market. We mainly test the following most related two hypothesis:

1. Whether a wealth distribution that follows Power-Law does improve the stability of the market.
2. Whether approaching the Power-Law distribution can significantly reduce the fluctuations of the market.

Table 16.6 shows the estimation results of the state variable (according to Clauset's criterion, we regard the periods whose goodness of fit below the 10% as non-Power-Law periods). Especially, this dummy variable exhibits significant predicting power on those fundamental variables. What's more, we note that the sign of the coefficient of this dummy variable is always opposite to the sign of the constant. Namely, when the right tail wealth distribution follows the Power-Law model, the changes of market cap, market price, transaction fees and other fundamental variables become much smaller compared to the changes during the non-Power-Law periods. This indicates that when the wealth distribution follows Power-Law, the Bitcoin market would become more stable than otherwise.

Above result is consistent with what we observed in Fig. 16.9 — evidenced by the strong price explosion starting from the 3rd quarter of 2013. We suspect that the wealth distribution doesn't follow Power-Law distribution during that period. In fact, it can be easily verified by analyzing the goodness of fit –. After the middle of 2013, p-value drops to almost 0, indicating that the previous stability has been disrupted. We may also note that the p-value drops below 10% level during the 4th quarter of 2011, which is also consistent with the Mt. Gox hacker event (Table 16.7).

From the above analysis, again, we claim that during the non-Power-Law period, the price movements or other fundamental variables can hardly be explained by the wealth distribution parameter, α, since the stability has been disrupted. However, this

Table 16.6 Predicting power of goodness of fit (Dummy)

	Days destroyed ($*10^6$)	MB.1	Difficulty ($*10^6$)	Hashrate ($*10^6$)	Market cap ($*10^6$)	Market price	Miners revenue ($*10^6$)	Network deficit ($*10^6$)	No. of transactions ($*10^6$)	Ratio
(Intercept)	4, 729.47***	13, 341.79***	1, 220.46***	10.90***	12, 211.28***	1, 001.94***	4.48***	−4.45***	30.72***	235.46***
	(780.87)	(1, 734.68)	(412.39)	(3.70)	(4, 443.42)	(366.34)	(1.61)	(1.60)	(3.99)	(27.99)
Ps	−3, 106.03***	−11, 534.05***	−1, 218.81**	−10.89**	−12, 094.98**	−988.87**	−4.37**	4.34**	−25.81***	−142.98***
	(1, 013.84)	(2, 252.22)	(535.42)	(4.80)	(5, 769.12)	(475.63)	(2.09)	(2.08)	(5.19)	(36.35)
R^2	0.14	0.32	0.08	0.08	0.07	0.07	0.07	0.07	0.30	0.21
Adj. R^2	0.13	0.30	0.07	0.07	0.06	0.05	0.05	0.05	0.29	0.20
Num. obs.	59	59	59	59	59	59	59	59	59	59
RMSE	3,825.46	8,498.14	2,020.28	18.12	21,768.22	1,794.68	7.88	7.84	19.57	137.15

$^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$

XFGPowerLawP

Table 16.7 Predicting power of goodness of fit

	Days destroyed ($*10^6$)	MB.1	Difficulty ($*10^6$)	Hashrate ($*10^6$)	Market cap ($*10^6$)	Market price	Miners revenue ($*10^6$)	Network deficit ($*10^6$)	No. of transactions ($*10^6$)	Ratio
(Intercept)	4, 561.26***	12, 718.87***	1, 164.89***	10.40***	11, 637.72***	953.34**	4.25***	−4.22***	29.31***	227.43***
	(769.83)	(1, 736.26)	(404.46)	(3.63)	(4, 356.72)	(359.25)	(1.58)	(1.57)	(3.99)	(27.78)
P_value	−3, 225.63***	−11, 981.52***	−1, 285.86**	−11.48**	−12, 717.66*	−1, 036.50*	−4.55*	4.52*	−26.79***	−147.93***
	(1, 123.74)	(2, 534.47)	(590.40)	(5.29)	(6, 359.60)	(524.40)	(2.30)	(2.29)	(5.83)	(40.55)
R^2	0.13	0.28	0.08	0.08	0.07	0.06	0.06	0.06	0.27	0.19
Adj. R^2	0.11	0.27	0.06	0.06	0.05	0.05	0.05	0.05	0.26	0.18
Num. obs.	59	59	59	59	59	59	59	59	59	59
RMSE	3,858.93	8,703.33	2,027.44	18.18	21,838.82	1,800.79	7.91	7,86	20,02	139.24

$^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$

XFGPowerLawP

fluctuations have been well captured by the Clauset's goodness of fit. Afterwards, we continue to test the second hypothesis that during the whole sample period, whether approaching the Power-Law distribution which is indicated by the p-value, has any predicting power over those fundamental variables. The estimation results have been shown as below:

As expected, all the fundamental variables listed above are significantly affected by the p-value and the change of directions also meet our expectation – when p-value increases or the wealth distribution approaches the Power-Law distribution, the changes of transaction fees, the price movements, market cap and other fundamental variables become much smaller than otherwise, suggesting that the Bitcoin market becomes more and more stable when the wealth distribution approaches the Power-Law distribution.

16.5 Other Risk Analysis

Apart from those shortages reflected by the Auroracoin, more reasons are required to be considered as dangers for a coin to survive. The current section provides more aspects to investigate these reasons.

To begin with, many coins died because of badly designed mechanism, especially the block reward scheme. It could be a too complicated scheme, for example, Aircoin (AIR) adjusts the block rewards in response to the exchange rate in order to target a gradually rising exchange rate. The reward halving time was supposed to be about once per five years, therefore it is hard to comprehend given the mining reward adjustments to target an exchange rate. Or like the case of EToken (ETOK) where the block reward for the latter block such as the ten thousandth block. People tended to abandon the block once it was mined, eventually leading to the death of the project.

Secondly, the developer issues. Some coins like BellaCoin (BELA) died since its developer is completely unknown. Some coins faded simply because the developer disappeared after launching the coin, for example, the Melange (SPICE). Besides, the anonymous developer of the BatCoin claimed to be attacked during the night of 3rd–4th, April in his home and hospitalized by an assailant intent on stealing the premined coins. If that's true, then clearly he was not anonymous to the assailant. If that's false, then he made a small but respectable profit on the premine. Either way, he hindered the development and support of Batcoin like a hot rock.

Thirdly, there are moral issues causing the death of coins. On one hand, pure IPO scams occurred (NeonCoin, VisaCoin, etc.) where developer just disappear with the money. On the other hand, plenty of coins are malware. For instance, Nerdcoin contained a key logger and a wallet stealer and Oreocoin contained a remote desktop exploit. Moreover, there is a keyboard recorder in the Thecoin and the developer apparently hoped to get the passwords people were using for their wallets.

To add up, the uniqueness of a coin also affects its survival. Some coins died because they are clones or forks of other coins. To name a few, FairBrix is clone of Tenebrix and FairQuark is clone of Quark. Nucoin, Nutcoin and Stop are all forks

of NXT. Moreover, duplicate names can jeopardize a coins prosperity, too. Taking Aircoin (AIR) as an example, apparently there are at least two different coins both named Aircoin and both trading with the symbol AIR. One is effectively dead and the other apparently alive as of 12th, July 2014.

Last but not least, some coins are dead due to the bad listed timing, usually too early. For instance, Global Denomination (GDN) is unwisely initially listed on exchanges while its market cap was still under $5000. Muniti (MUN) went for exchanges way too quickly, even before there was any market capitalization to distinguish them from the thousands of dead coins.

16.6 Conclusion

In the paper, we are trying to figure out what characteristics are necessary for a cryptocurrency to be a good alternative investment. To be more specific, first, we believe that for a coin to survive and gain popularity, achieving a Pareto optimal distribution is absolutely helpful. Hence we start looking at the wealth distribution and characterizing it by fitting a Power-Law model. To verify the hypothesis, we consider two Cryptocurrencies in two situations – one with the whole sample size and the other with the truncated sample size by optimally selecting the right tail of the wealth distribution. We find that for Auroracoin market, although the fitted parameter α using the truncated sample size has significant predicting power on both the price movement, changes of market cap, and the other fundamental variables posted on Blockchain web. It doesn't follow Power-Law suggested by Clauset's goodness of fit. While in terms of Bitcoin market, it becomes a little tricky. We find that using the whole sample size, it doesn't follow Power-Law model at all and the fitted parameter α has no predicting power on those fundamental variables. After that, we fit the truncated sample size and find that the Power-Law fits the wealth distribution very well. Nevertheless, the parameter, α, still shows no predicting power over those fundamental variables. After further looking into the Bitcoin market, we relax the hypothesis by considering whether the wealth distribution which follows Power-Law has significant predicting power over the market and instead of using parameter α. We choose Clauset's goodness of fit which is more appropriate to measure the whole market. As expected, the predicting power is significant and the closer the wealth distribution approaches the Power-Law, the more stable of the Bitcoin market will be.

In addition, a better crypto-currency usually entails the following characteristics.

i. Known creator;
ii. Some work is required to get the coin;
iii. Coins are not distributed for free;
iv. Attains Pareto-distribution;
v. Appropriate reward scheme;
vi. Good credit of developer;
vii. Uniqueness;
viii. Good launching time.

With this knowledge in mind, countries can use this information to create a successful cryptocurrency when they ever desire to make use of digital currency in the future. Our preliminary study of two digital currencies needs to be expanded to more digital and crypto currencies in order to draw a firmer conclusion. Nevertheless, while Clauset's goodness of fit can be used and has some predictive power over the fundamental variables of a cryptocurrency, it may not be sufficient enough. We may need to combine the indicator with other explanatory variables to yield more accurate predictions. In the future, we could continue to monitor the goodness of fit in order to verify the results obtained in this research paper and to expand the study to other coins. Furthermore, weekly instead of monthly data could be used for Auroracoin in order to further validate the significant level of goodness of fit in relation with the Bitcoin market. Finally, we would compare more density functions to fit the wealth distribution instead of using only the Power-Law model.

References

Clauset, A., Shalizi, C. R., & Newman, M. E. J. (2009). Power-law distributions in empirical data. *SIAM Review*, *51*(4), 661–703.

Ignacio, M., & Lee, D. K. C. (2014). Bitcoin-like Protocols and Innovations. Sim Kee Boon Institute for Financial Economics, Singapore Management University.

Lam, P. N., & Lee, D. K. C. (2014). Introduction to Bitcoin. Sim Kee Boon Institute for Financial Economics, Singapore Management University.

Lee, D. K. C., Ong, B. C. E., Lee, T.M., & Li, G. (2014). Evaluating the Potential of Alternative Cryptocurrencies. Sim Kee Boon Institute for Financial Economics, Singapore Management University.

Li, Xiang Jun, Lee, David K. C., & Teo, Ernie. (2014). Life Cycle of Cryptocurrencies. Sim Kee Boon Institute for Financial Economics, Singapore Management University.