Fundamental Study of Cryptocurrencies

Enwei Liang

Jinan Xinhang Experimental Foreign Language School, Jinan 250102, China
E-mail: enweiliang@163.com

Abstract: *This paper studies cryptocurrency. Firstly, this paper discusses the currency attribute of cryptocurrency. Secondly, this paper analyzes the advantages and disadvantages of cryptocurrency. Thirdly, this paper discusses the impact of cryptocurrency on the currency structure. Finally, this paper constructs the returns according to the daily price and statistically analyzes the yield difference of Bitcoin, Ethereum and Dogecoin. The ARIMA model is used to predict the return of cryptocurrency. This paper also gives the corresponding investment suggestions.*

Keywords: *Cryptocurrency, Time series, Return dynamics*

1. Introduction

With the development of the Internet, a new market has been formed.This market is a virtual market based on cyberspace, in which cryptocurrency becomes a medium of exchange. Cryptocurrency is the non-real money on the Internet, not the real sense of money, and its investment and transaction are not protected by law. The earliest cryptocurrency in the world is bitcoin. On October 31, 2008, a man with an alias of Satoshi Nakamoto published a report entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" on the mailing list of metzdowd.com[1].   In January 2009, Nakamoto released the open source code of bitcoin system software and the first batch of 50 bitcoins. A new virtual currency was born. At this time, the price of bitcoin is only a few cents, approaching zero. However, in the next few years, bitcoin has developed rapidly[2]. On May 11, 2020, bitcoin halved for the third time, and the price of bitcoin was $8821.

Bitcoin is an electronic payment system based on cryptographic proof, instead of traditional trust. Bitcoin does not rely on specific institutions to issue, it is based on a specific algorithm, through a large number of calculations. Based on blockchain technology, digital cryptocurrency adopts Hash encryption algorithm(SHA256) and asymmetric encryption technology (public key and private key) to ensure the security of information[3].After that, the concept of Ethereum was first proposed by programmer Vitalik Buterin inspired by bitcoin. Ethereum is a digital token of Ethereum, a public blockchain platform with smart contract functionality, known as the Bitcoin 2.0 form[4]. It has a similar nature to bitcoin and is traded on an exchange platform. Nowadays, one of the most important components in the latest virtual currency is Dogecoin. This is also an integral part of the virtual marketplace[5]. In addition to various virtual currencies in the virtual currency market, there is also an index like SP500 that is used to measure the overall performance of the whole market, which is the CMC200 index. The CMC200 index is designed to be the most comprehensive index in the market, measuring the performance of the top 200 cryptocurrencies by market capitalization traded in USD.

Based on the brief introduction of the basic principle of cryptocurrency, this paper first analyzes the currency attribute of cryptocurrency, the advantages and disadvantages of cryptocurrency, and the impact of cryptocurrency on currency structure. Secondly, using the data of December 28, 2020 to June 25, 2021, this paper makes descriptive statistics on the return of cryptocurrency. Thirdly, ARIMA model is used to predict the return of digital cryptocurrency. Finally, combined with the previous analysis, relevant suggestions are given.

2. Basic analysis of cryptocurrency

2.1. Is cryptocurrency a real currency?

Under the condition of developed commodity economy, currency has four functions: measure of value, medium of exchange, means of storage and world currency. Is cryptocurrency a real currency? I take

bitcoin as an example. Although Yermack (2015) believes bitcoin largely fails to satisfy these criteria[6], I think bitcoin is reasonable as a currency.

As a value measure, money should have a relatively stable price, but at present, the price of cryptocurrency fluctuates greatly, which affects its function as a value measure. Also, its volatility is greatly higher than the volatilities of widely used currencies, imposing large short-term risk upon users.At present, cryptocurrency has been accepted and recognized by many well-known e-commerce websites all over the world. In addition, bitcoin can be subdivided into 8 digits after the decimal point, that is, 1/100 million. The minimum bitcoin transaction amount can be 0.00000001btc, which meets the needs of some small transactions. Therefore, cryptocurrency has the function of circulation means within a certain range.

Bitcoin has a certain storage function. The public can convert the current cash wealth into bitcoin and save it for future consumption. Since the total amount of bitcoin is fixed(21 million) and has a scarcity similar to gold, it will not cause the phenomenon of wealth dilution caused by excessive issuance of money, which also shows that bitcoin is a good means of wealth storage, so bitcoin can perform the function of storage means.World currency refers to the function of currency as a means of circulation in the world market with the development of international trade. Bitcoin is designed as a decentralized point-to-point payment method without any national and institutional constraints, which determines that the transaction of bitcoin can realize the free circulation of bitcoin around the world without national and regional restrictions. Therefore, bitcoin naturally has the function of world currency, which is also the most prominent advantage of bitcoin as a new currency.

Therefore, this paper holds that although it has certain price volatility, bitcoin is not only a special commodity with value and single use value, but also successfully solves the trust problem of money circulation, which can be regarded as a new special currency.

2.2. Advantages and disadvantages of cryptocurrency

Cryptocurrency has obvious advantages over traditional currency. First, cryptocurrency is easy to use. The issuance and transaction are completely electronic, the transaction security is guaranteed by the cryptographic algorithm, and the social credit cost is very low. The decentralized structure is adopted, all transactions do not need intermediaries, support user to user direct transactions, and real-time transfers can be made under pseudonyms throughout the network. Second, cryptocurrency has high security. The use of modern cryptography, which has been proved safe in theory and practice, can effectively prevent the forgery and repeated spending of bitcoin, and protect the identity privacy of user transactions. In the traditional currency, counterfeit money is difficult to identify, and it costs a lot of human, material and financial resources to crack down on counterfeit money. Third, cryptocurrency makes a programmable digital code into an automatic transaction currency, which can be recorded in a non repudiation manner in time sequence, which can eliminate the risk of credit default and the resulting socio-economic problems to a great extent.

Although cryptocurrency has many advantages, allowing it to grow savagely will inevitably lead to currency invasion and financial pollution. Cryptocurrency seriously erodes the status of legal tender, interferes with the operation and transmission of macroeconomic regulation and financial policies, and provides an underground capital channel for illegal and criminal activities such as money laundering, extortion and extortion[8]. In order to make full use of the advantages of cryptocurrency and reduce or eliminate the risks caused by private issuance of cryptocurrency, the central banks and commercial banks of some countries have actively explored, studied and realized legal digital currency, and gradually formed the trend of competitive research.In 2014, the people's Bank of China set up a special team to conduct special research on digital currency issuance framework, key technologies, issuance and circulation environment and relevant international experience. At the end of 2019, the pilot test of Digital RMB was launched in Shenzhen, Suzhou, xiong'an new area, Chengdu and the future Winter Olympics[7]. On August 1, 2021, Beijing Rail Transit newly supports the application of Digital RMB offline ticket purchase, ticket replenishment and recharge, as well as online ticket purchase.

2.3. The influence of legal digital currency on monetary structure

According to the original currency, M0 = cash in circulation; M1(narrow money) = M0+demand deposits; M2(broad money) = M1+quasi-currency. Base currency(B), also known as monetary base, refers to the sum of cash (C) circulating outside the banking system and deposit reserves (R) (including legal deposit reserves and excess reserves) held by the public and the commercial banking system. Money

supply is determined by money multiplier and base currency.

Because the legal digital currency is directly issued by the Central bank without the participation of commercial banks, compared with the traditional issuance mechanism, the legal digital currency has different characteristics. Holding legal digital currency by the public is equivalent to opening an account in the Central bank. Therefore, the Central bank does not need to adjust the reserve ratio, buy and sell securities in the open market, but can directly adjust the issuance of legal digital currency, which is more direct and effective. Therefore, Base currency (B) = cash (C) + deposit reserves (R) + legal digital currency. M0 = cash in circulation + legal digital currency; M1(narrow money) = M0+demand deposits; M2(broad money) = M1+quasi-currency.

3. Empirical evidence

3.1. Descriptive statistics

In this research, I used the following basic statistics: mean, variance, skewness and histogram. Mean shows the sum of all the values divided by the total number of values. For population variance, it is the average of the sum of squares of deviations between values and their arithmetic mean in a set of data. Sample variance is the estimator of population variance.   Moreover, skewness is a measure of the skew direction and degree of statistical data distribution. In the skewness distribution, when the skewness is positive, the distribution is positive; When the skewness is negative, the distribution is negative. A histogram is a graphical representation of the frequency distribution of a continuous class grouping. It is an area graph that can be defined as a set of rectangles whose base edges are the intervals between class boundaries and whose area is proportional to the frequency in the corresponding class.

This study focuses on four time series variables: return of Bitcoin, return of Ethereum, return of Dogecoin and return of CoinMarketCap Crypto 200 Index (CMC200 hereafter), the full sample period is December 28, 2020 to June 25, 2021. The CMC200 index is designed to be the most comprehensive index in the market, measuring the performance of the top 200 cryptocurrencies by market capitalization traded in USD. These data sets are collected from Coinbase, which is a exchange platform that makes it easy to buy, sell and store cryptocurrency like Bitcoin, Ethereum and more, it is available in over 30 countries worldwide. I use daily close price p_t of each variable to compute the corresponding daily return by $r_t = \ln(p_t / p_{t-1})$. The time series plots are reported in Figure 1 and the descriptive statistics are reported in Table 1.
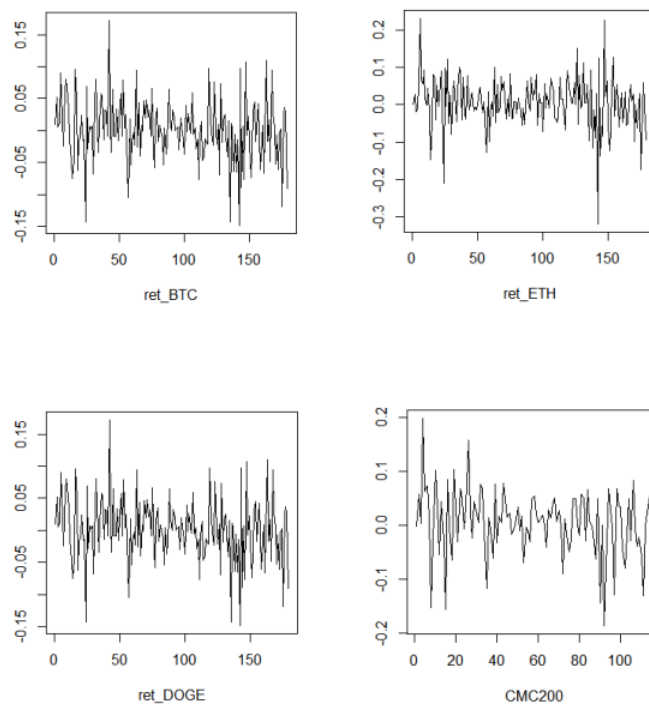

Figure 1. The time series plots of return of Bitcoin, Ethereum, Dogecoin and CMC200.

Table 1. The descriptive statistics

	BIT	ETH	DOGE	CMC200
Mean	0.00087	0.00508	0.02208	0.00370
Variance	0.00240	0.00457	0.03069	0.00371
Min	-0.14811	-0.31746	-0.51511	-0.18545
Max	0.17182	0.23070	1.32347	0.19806

The mean return of four crypto currency are all positive in the data period, the variance of Dogecoin's return is much lager than the other three variables, this means that it has the most unstable return dynamics. From the minimum value and maximum value of the return of Dogecoin, one can find that the maximum loss and earning of holding this crypto currency are 51.511% and 132.347% in one trading day, this is very rare event, or even impossible to happen, in traditional financial market.

In order to capture the information of the distribution of four returns, I employ the histogram. The histogram of four returns are reported in Figure 2. The return of Bitcoin seems to be symmetric about zero, the return of Dogecoin is skew to right, the return of Ethereum and CMC200 are skew to left. I further compute the skewness statistics of four returns to better understand the skewness of the distribution quantitatively. They are -0.07197, -0.51844, 2.75676 and -0.41104 for Bitcoin,Ethereum, Dogecoin and CMC200, respectively. This result is roughly consistent with the result of histogram, the skewness statistics of the return of Bitcoin is close to zero, which implies that it's distribution is the most symmetric in four distributions, a negative value of the statistics means skew to left, and vice versa.
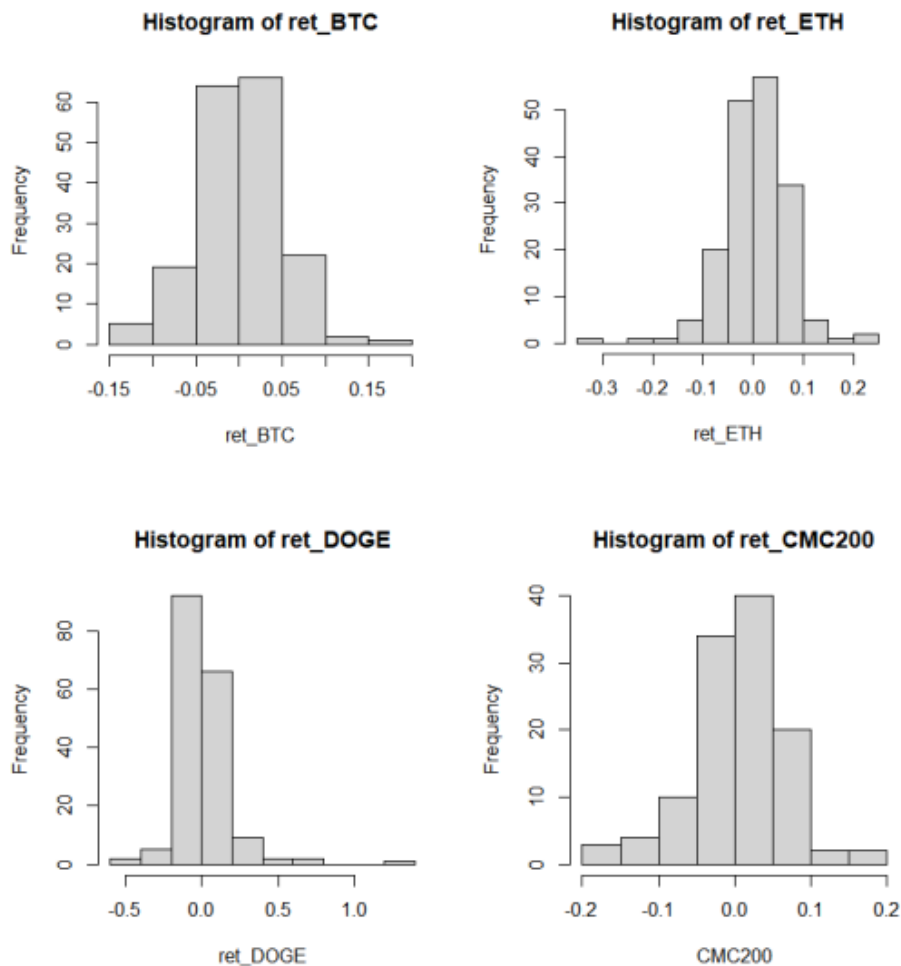

Figure 2. The histogram of four returns.

Base the analysis above, Bitcoin has the most stable return dynamics, the distribution is symmetric about zero, so it would be a suitable investment instrument for risk aversion investor in this market, and risk-seeker might chose Dogecoin to invest because it provides larger return potentially.

3.2. The regression

In time series modeling, we often rely on past data to make estimates about current and future values, a typical example is autoregressive model (AR model). However, sometimes that's not enough. When unexpected events like natural disasters, financial crises, or even wars happen, there can be a sudden shift in values. That's why we need models the time series simultaneously use past data as a foundation for estimates, but can also quickly adjust to unpredictable shocks. From the fundamental of cryptocurrencies, it has not background of any country or government, so the risk capacity of cryptocurrencies is going to be weaker then conventional monetary theoretically. Thus, I use autoregressive integrated moving average model (ARIMA model) to fit the daily return of cryptocurrencies [9].

In general, an ARIMA(p,d,q) model has the form,

$$\alpha(L, p)(1-L)^d r_t = \alpha_0 + \beta(L, q)\varepsilon_t$$

where ε_t is the innovation at time t, L is the lag operator,

$$Lr_t = r_{t-1}$$
$$L^j r_t = r_{t-j}$$

for $j \in \mathbb{Z}^+$, and

$$\alpha(L, p) = 1 - \alpha_1 L - \alpha_2 L^2 - \ldots - \alpha_p L^p;$$
$$\beta(L, q) = 1 + \beta_1 L + \beta_2 L^2 + \ldots + \beta_q L^q.$$

The autoregressive part is based on the idea that current value of the series, r_t, can be explained as a linear combination of p past values, $r_{t-1}, \ldots, r_{t-p}$, together with a random error in the same series. One problem of AR model is the ignorance of correlated noise structures (which is unobservable) in the time series. In other words, the imperfectly predictable terms in current time, ε_t and previous steps, $\varepsilon_{t-1}, \ldots, \varepsilon_{t-q}$, are also informative for predicting observations. For the integrated part $(1-L)^d r_t$, if r_t is stationary time series process, it wouldn't be necessary to take the difference.

The estimation of regression model can be executed by many statistical software, for instance, Matlab, R, Stata and so on. The very first step is one should check the stationarity of the time series process, which is a key requirement for external validity of time series regression. I use augmented Dickey-Fuller test (ADF test). According to Figure 1, there are no significant time trend and the averages are all close to zero, thus the ADF test with no intercept and no time trend in alternative hypothesis is employed in this section. The null hypothesis in ADF test is a nonstationary time series process, to be specific, an unit-root process, the alternative hypothesis means that the time series process is stationary.

Table 2. The ADF test

ADF	BIT	ETH	DOGE	CMC200
Statistics	-9.2178	-8.8683	-9.0939	-7.6410
P-value	<0.01	<0.01	<0.01	<0.01

The results of the ADF tests are reported in Table 2, the p-values are all less then 1%, which implies the rejection of null hypothesises. Since that four returns series are all stationary, I take the value of differences order, d, as zero. The next step is to determine the AR order and MA order (p,q) in each regression model. The autocorrelation function (ACF) and partial autocorrelation function (PACF) are most popular for identifying the order of autoregressive and moving average. The autocorrelation function is the coefficient of correlation between two random variables in a time series, it measure the linear relationship of these two random variables (We usually assume that the r_t and r_{t-k} are two different random variables if no prior information available). Graphical approach can be used here to identify the lag order, they are omitted to save space. Base on the guidance of Akaike information criterion (AIC), autocorrelation function (ACF), partial autocorrelation function (PACF) and principle of parsimonious, four regression models are obtained and the results are reported in Table 3. The value in

the parentheses is the estimated standard deviation the of coefficient estimator. Most of the parameters in the model are significant at 1% significance level, the p-value of the intercept in third model (return of Dogecoin, ARIMA (2,0,2)) is 10.58%, this is close to 10% significance level, I keep it remain in the model to avoid over justification. In the following, I consider the diagnostic of residual by checking the stationarity and correlation coefficient of the residual. The residual is the difference between the real data and estimated value, thus the residual is a time series as well. Table 4 provides the results of ADF test and correlation test to the residuals. One can see that the residual are all stationary and there are not autocorrelation in residuals. This implies that the model used are appropriate.

With the estimated parameters, we can obtain the fitted regression models for each return. These models are actually the prediction model for the conditional mean of return dynamics given the past information. For instance, the regression model for the return of Bitcoin is as follows.

Table 3. The regression results

	BIT ARIMA(1,0,1)	ETH ARIMA(1,0,1)	DOGE ARIMA(2,0,2)	CMC200 ARIMA(1,0,1)
Intercept		0.0051*** (0.0047)	0.0220 (0.136)	
AR1	-0.7101*** (0.2451)	-0.8532*** (0.1096)	1.7166*** (0.404)	-0.8749*** (0.0548)
AR2			-0.9672*** (0.0322)	
MA1	0.6246** (0.2678)	0.7655*** (0.1313)	-1.7357*** (0.0247)	1.0000*** (0.0268)
MA2			1.0000*** (0.0244)	

*"***" means the statistically significant in 1% significance level; "**" means the statistically significant in 5% significance level; "*" means the statistically significant in 10% significance level.*

Table 4. Residual diagnostic

Residual	BIT	ETH	DOGE	CMC200
ADF test	-9.3441 (<0.01)	-9.2479 (<0.01)	-9.4156 (<0.01)	-7.4287 (<0.01)
Pearson's correlation test	-0.0130 (0.9896)	0.2297 (0.8186)	-0.38295 (0.7022)	-0.0955 (0.9241)

$$r_t = \alpha_0 + \alpha_1 r_{t-1} + \beta_1 \varepsilon_{t-1} + \varepsilon_t,$$

and the conditional mean model is

$$E(r_t \mid I_{t-1}) = \alpha_0 + \alpha_1 r_{t-1} + \beta_1 \varepsilon_{t-1},$$

where $I_{t-1} = \sigma\{r_{t-1}, r_{t-2}, \ldots\}$ is the Sigma-field of the past information. We can find that on the right-hand side of the conditional mean model are only about the past information, this simply means that if we have the estimators of unknown parameters, that is $\{\alpha_0, \alpha_1, \beta_1\}$ in this example, then we are able to predict the future value of conditional mean by plug in the values (or estimated value) of $\{r_{t-1}, \varepsilon_{t-1}\}$. The fitted prediction model become,

$$\hat{r}_t = -0.7101 r_{t-1} + 0.6246 \varepsilon_{t-1},$$

for the return of Bitcoin. The prediction model of conditional mean for the other returns can be found as well, and by plugging in the past information, the predictions can be reached.

4. Conclusion

This paper analyzes the origin and development of cryptocurrency. Through analysis, I find that although cryptocurrency has not been rising for a long time, it has the attribute of currency to a certain extent. Cryptocurrency can reduce transaction costs and prevent counterfeiting, but there are still a series of problems in the supervision of cryptocurrency. By analyzing the return of cryptocurrency, I find that

bitcoin has the most stable return dynamics, the distribution is symmetric about zero, so it would be a suitable investment instrument for risk aversion investor in this market, And risk seeker might choose dogecoin to invest because it provides large return potential. ARIMA model can predict the return of cryptocurrency to a certain extent. It is an effective method to analyze the return of cryptocurrency at present.

References

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[J]. 2008.

[2] B ӧhme R, Christin N, Edelman B, et al. Bitcoin: Economics, technology, and governance[J]. Journal of economic Perspectives, 2015, 29(2): 213-38.

[3] Crosby M, Pattanayak P, Verma S, et al. Blockchain technology: Beyond bitcoin[J]. Applied Innovation, 2016, 2(6-10): 71.

[4] Wood G. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum project yellow paper, 2014, 151(2014): 1-32.

[5] Chohan U W. A history of Dogecoin[J]. Discussion Series: Notes on the 21st Century, 2017.

[6] Yermack D . Is Bitcoin a Real Currency? An economic appraisal[J]. Handbook of Digital Currency, 2015:31-43.

[7] Han D. Analysis on risks and Development Countermeasures of Central Bank digital RMB issue[C]//2021 International Conference on Public Management and Intelligent Society (PMIS). IEEE, 2021: 250-254.

[8] Dibrova A. Virtual currency: new step in monetary development[J]. Procedia-Social and Behavioral Sciences, 2016, 229: 42-49.

[9] Sowell F. Modeling long-run behavior with the fractional ARIMA model[J]. Journal of monetary economics, 1992, 29(2): 277-302.