Fundamental and statistical analysis on Bitcoin

Candidate
Manuel Cuberli

Supervisor
Prof. Luca Grassetti

Università degli Studi di Udine
Dipartimento di Scienze Economiche e Statistiche
Corso di Laurea Magistrale in Economics

Academic Year 2018-2019

The aim of the thesis

The thesis is divided into two parts:

- The first part concerns Money and Bitcoin.
- The second part concerns Bitcoin's time series.

The aim of the thesis is to give a comprehensive overview about money and its role inside the society, which is a prerequisite to understand Bitcoin and collocate it correctly in the evolutionary phase of the economy. The analysis should give the fundamental elements to compare different kinds of money, allowing to understand whether the Bitcoin time's series is worth studying.

Part I: Money and Bitcoin

- **Money**. This part will deal with the history of money, its charactertics and its functions. The main references are:
  - *F.A.Hayek. "Denationalization of money"*.
  - *C. Menger. "The Origins of Money"*.
  - *M. N. Rothbard. "What Has Government Done to Our Money?"*.
  - *R. G. Holocombe. "Advanced introduction to the Austrian school of Economics"*.
- **Bitcoin** This part will deal with the mechanics of Bitcoin. The main references are:
  - *E. Felten et all. "Bitcoin and Cryptocurrency Technologies"*.
  - *Andreas M. Antonopoulos. "Mastering Bitcoin, unlocking digital currencies"*.

History of Money

MONEY TYPE	AGE
Gifts	Prehistory
Barter	Prehistory
Food based	3000 BC
Valuable metal	2500 BC
Metal coins	600 BC
Paper money	1300 AD
Double-entry book keeping	1500 AD
Cheque	1700 AD
Fiat Money	1971 AD
Electronic money	1990 AD

Table: Development of different kinds of money in different periods in history.

- Towards the XIX century there is a shift in how money is conveived:
  - **Commodity money** such as Gold (needs to bootstrap value)
  - **Credit/debit money** created by the fractional reserve and money multiplier (needs the trust of the issuing institution)
- The utility of money is given by its positive and negative **attributes**, but also by the circumstances and **limitations** of:
  - Saleability
  - Space
  - Time
  - Independence

The functions of money

Looking to these factors bring us to a complete definition of money through its three basic functions:

- **Medium of exchange**
- **Reserve of value**
- **Unit of account**

The last two are the corollaries of the function of a medium of exchange, indeed, money is a commodity that is exchanged now for goods (and not consumed) to be exchanged in the future.

- Money becomes widely accepeted through a long process of social evolution
- Money has value only if it is expected that it preserves, or increases, that value in the future for other exchanges (purchasing power)
- Establishing prices in commodity money terms allows the comparison of all other goods.

Austrian School of economics

During the XX century there were three currents of economic thought:

- Keynesians
- Monetarists
- Austrian school of economics

The Austrian school make a distinction between **economic cycles** and **monetary cicles**:

- inflation caused by the raising in demand of goods and money
- inflation caused by the manipulation of the monetary base through the fractional reserve system

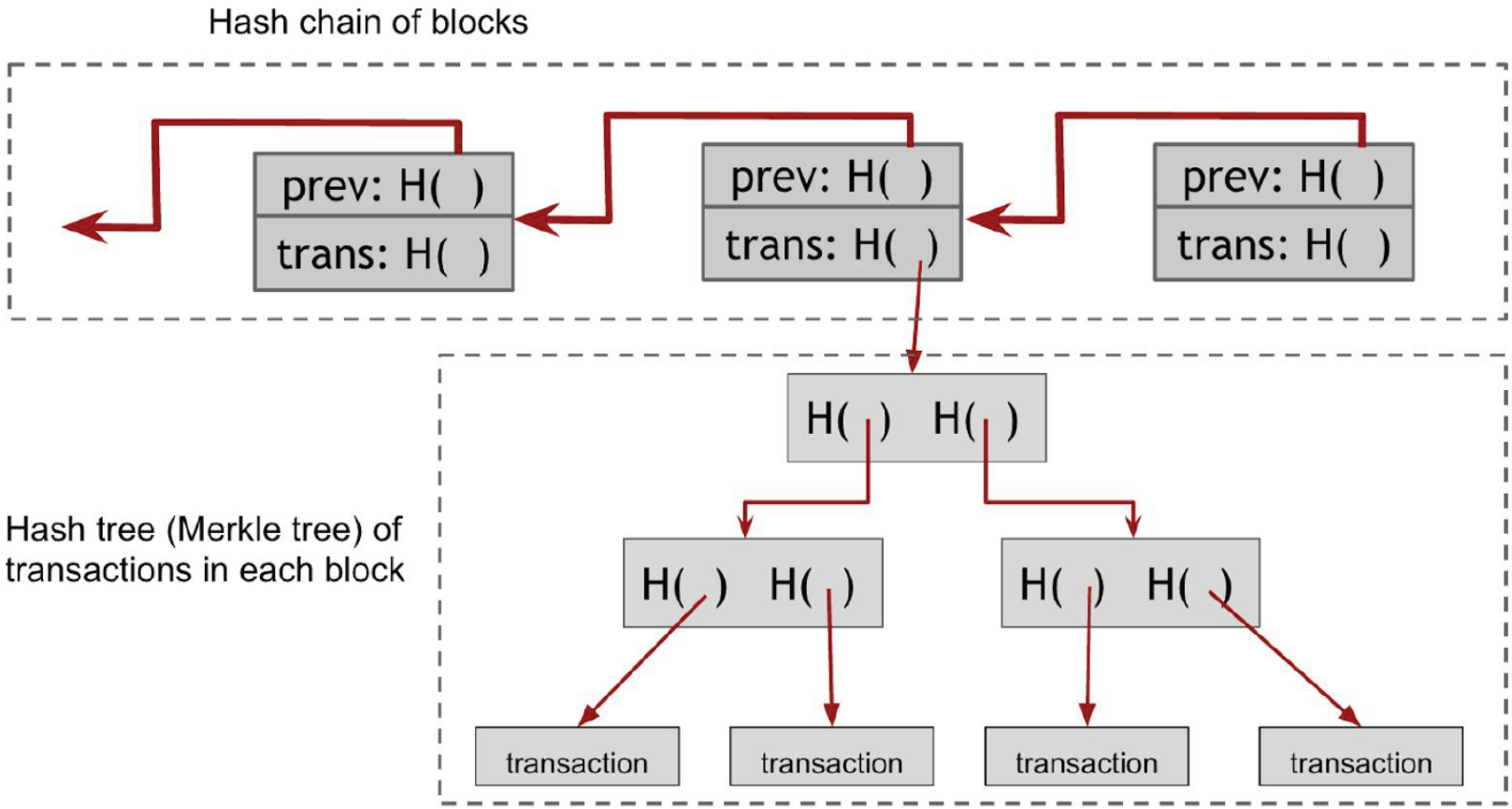
Inflation causes several **problems** in the economic activity:

- Boom and boost cycles with painful adjustments
- uneven distribution of the source of money and polarization of wealth
- distortion of prices on all the production chain (difficult calculation for entrepreneurs)

Bitcoin as protocol bitcoin as currency

- Several attempts were made after the mid-80s, to create a digital currency for the internet, resistant to counterfection and to the problem of **double-spend** (new hard-cash).
- In 2008 Satoshi Nakamoto releases the Bitcoin's *White Paper*, explaining the cryptographic tools used in the protocol, to resolve these problems:
  1. **Hash functions**: is a mathematical hashing algorithm that produces a digital fingerprint that allows to take any input of data, to produce an output of fixed size.
  2. **Digital signatures**: allows to create *commitments* (one cannot change a signed statement in the future).
  3. **Blockchain**: allows to create a data structure which is *tamper-evident log* (changing one hash requires to change all the structure).

The structure of the Bitcoin's blockchain



Bitcoin as protocol Bitcoin as currency

Data structures alone are not sufficient to reach a consensus on:

1. Rules
2. History of transactions
3. Economic value of coins

The **Nakamoto consensus** resolves the problem sociologically and not deterministically thanks to:

- **Incentives** to maintain secure the network through segniorage of issued bitcoins
- True **random distribution** of bitcoins through the competition of miners (poisson distribution)

Mining and Proof of Work

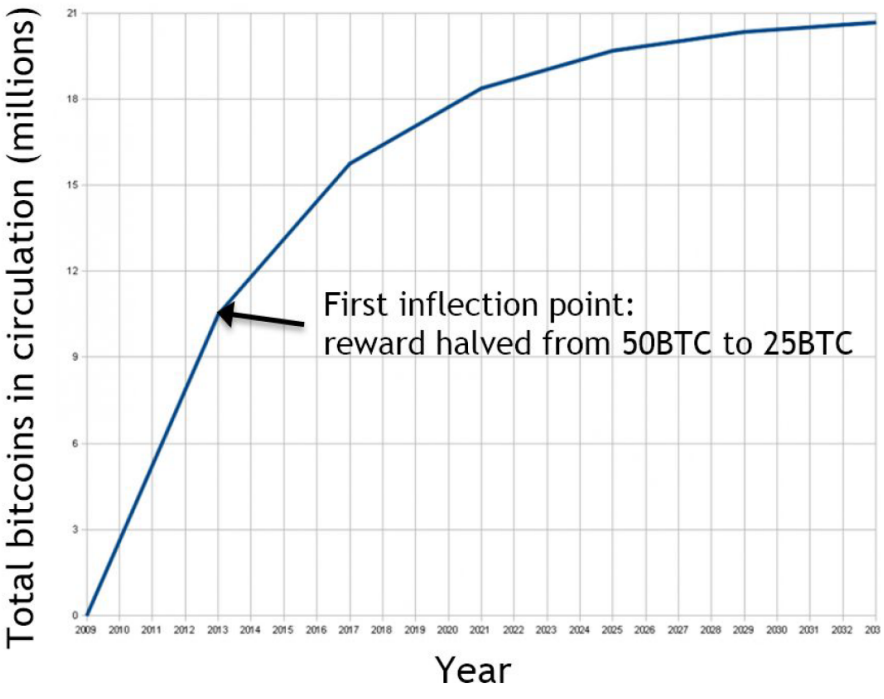


Figure: Emission schedule of bitcoins through years: it halves every 4 years.

- The mechanism design of incentives and randomization is needed to achieve **decentralization**
- The monetary policy of Bitcoin is completely **inelastic** and decided a-priori
- Miners compete with computational resources to extract bitcoins, while at the same time securing the network
- The computational power needed is adjusted to maintain the issuance of blocks of bitcoins every 10 minutes.

Comparison between the main monetary systems

Characteristics	**Bitcoin**
Saleability, acceptance, stability on prices	Not widely accepted, but acceptance depends on the willingness of people. It has a high volatility
Ease to exchange, transportability and borders	The size of the transaction does not matter and an address does not have weight; there are no borders and the market exchange does not close
Speed, capacity and international exchanges	Slow either for nearby transfers or international settlements (60 min); 7 transactions/s. But with payment channels there is no limit on exchanges which are istantaneous
Divisibility, fee and micropayments	Divisible up to satoshis (eight digits after 0), micro-payments can be handled by channels, but using the blockchain fees go up
Verifibility and ease to counterfeit	Verifiable instantaneously through cryptography; practically impossible to counterfeit
Durability, costs of storage	Resilient as internet; there are low costs of storage with some solutions that made costs null
Total stock, rate of inflation, scarcity	21 million units in total with a mathematically programmed inflation that converges to zero
Independence, censurability, privacy, securece	Different interests make it independent, not censurable, partially private (pseudonym) and not hackable

Part II: Statistical Analysis

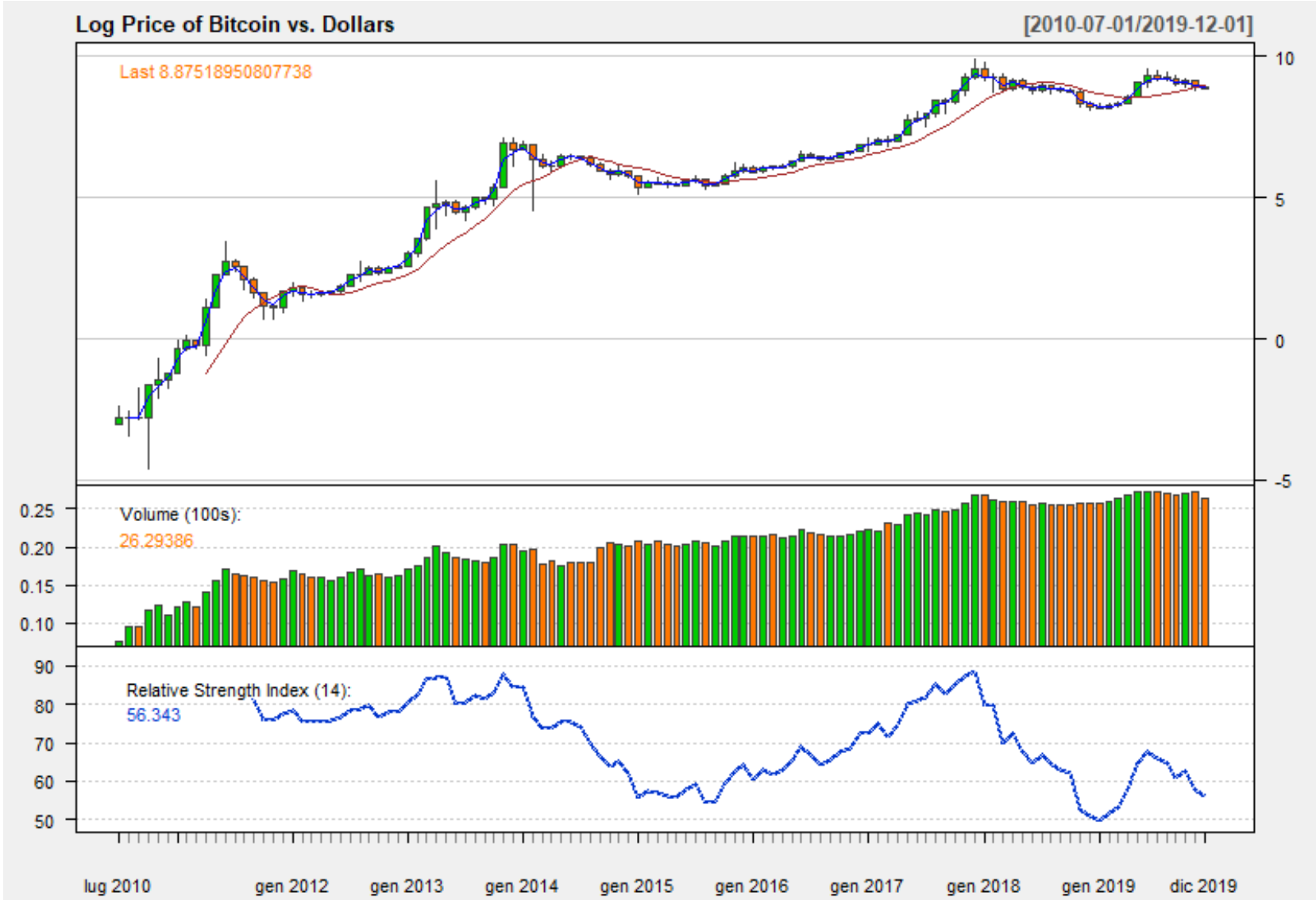
- There is no too much literature on Bitcoin and cryptocurrency's topic yet.
- The main **statistical references** are:
  - *P.H.Franses, Non-linear time series models in empirical finance.*
  - *R.H.Shumway, Time Series Analysis and Its Applications With R Examples.*
  - *A.Ghalanos, Rugarch: Univariate GARCH models.*
- The main references about **Bitcoin time series** are:
  - *B. Radovanov et all. Volatility analysis of four major cryptocurrencies.*
  - *A. Charles et all. Volatility estimation for Bitcoin: Replication and robustness.*
  - *Y. Kurihara1 et all. How Does Price of Bitcoin Volatility Change?*

Exploratory data analysis

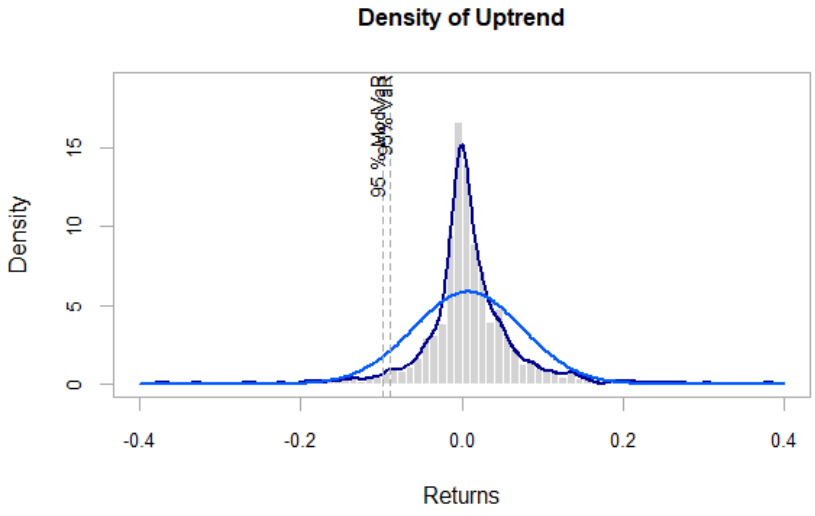
The main dataset is composed by 3230 observations which start from 10/02/2011 to 15/12/2019, where the dependent variable to be explained by the models is the exchange rate between the BTC/USD pair.

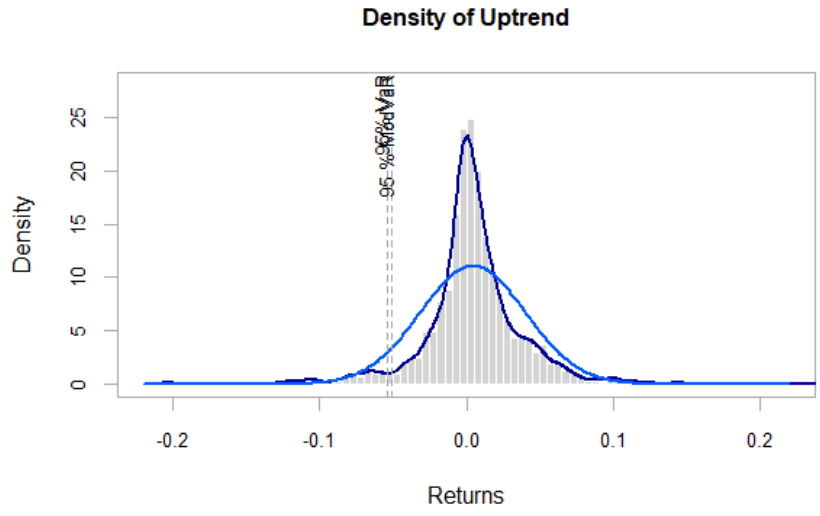
- The vector of prices is transformed in diffirent ways:
  - Logarithmic transformation
  - First difference
  - Log returns
- **Technical and cyclical analysis**: to observe if there are repetitive patterns (4 years cycle)
- **Theory fundamentals**: to build the basis for a statistical model for the conditional mean and conditional variance

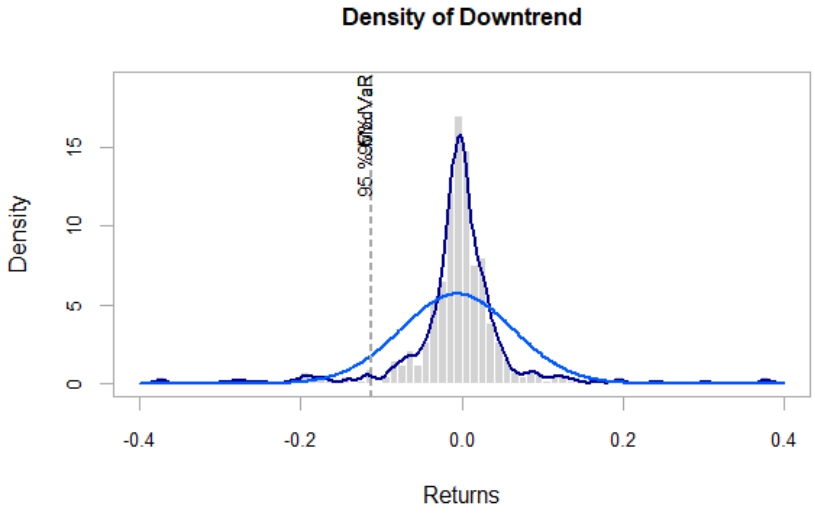
Technical and Cyclical analysis of Bitcoin

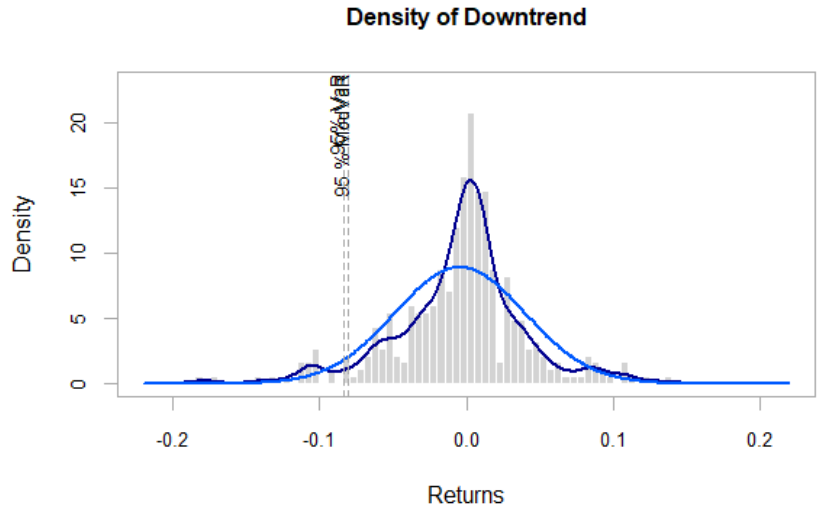


Logarithmic Returns



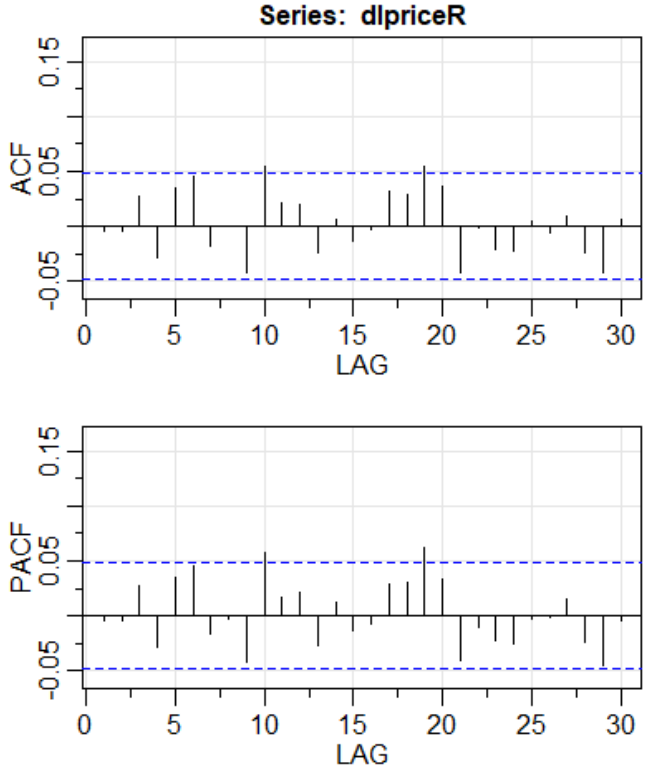






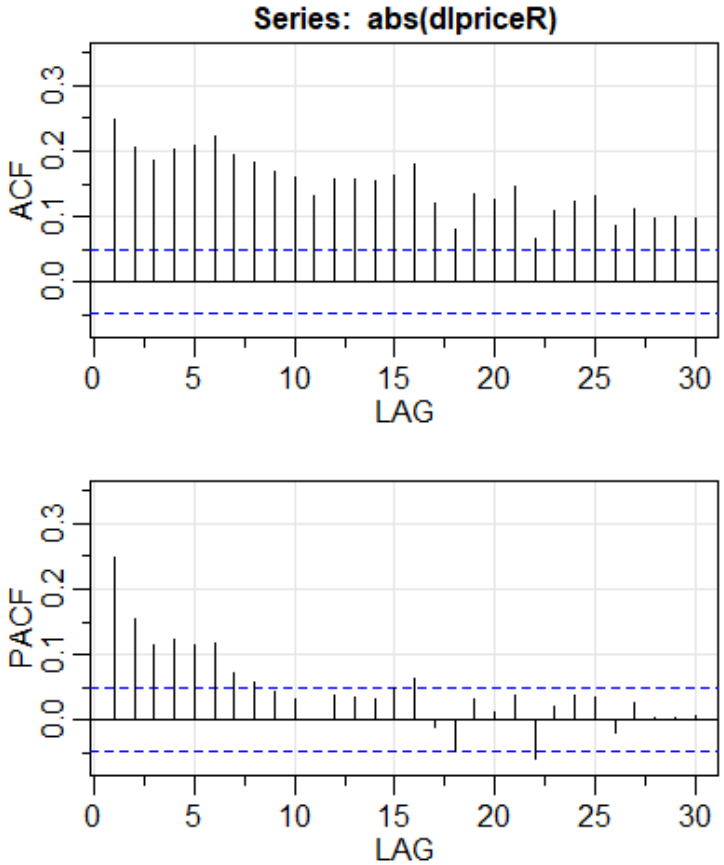
Logarithmic Returns: latest cycles

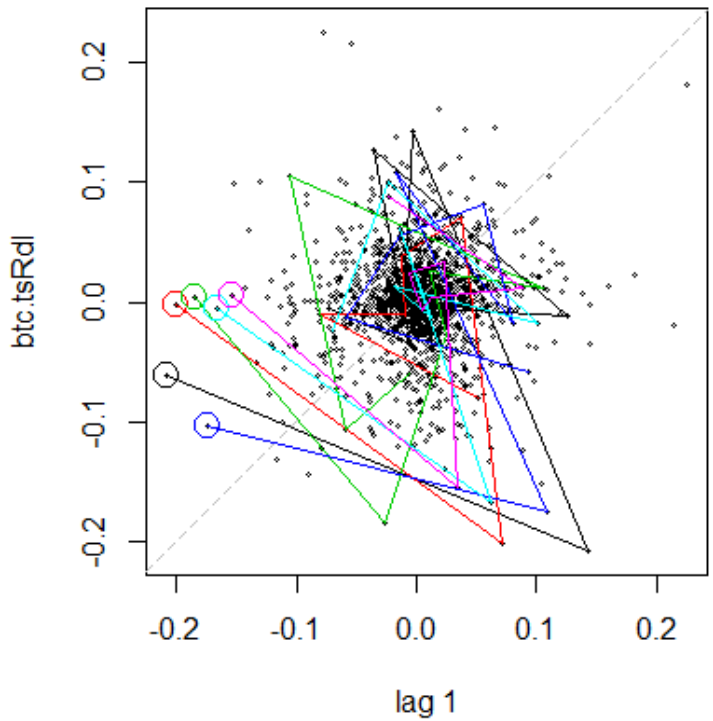
We consider the most recent data as more influential, therefore, to analyze the covariances and correlations of the series we use the period starting from January 2015 and ending in December 2019.



- The lack of autocorrelation and partial autocorrelation implies that measures of linear association and predictability for the conditional mean of linear models will not be useful at all.
- It's more appropriate to analyse the ACF and PACF on the second moment of the series.

Heteroskedasticity





The two graphs show a clear evidence of heteroskedasticity in the Bitcoin's series, which needs to be taken in account for the final model.

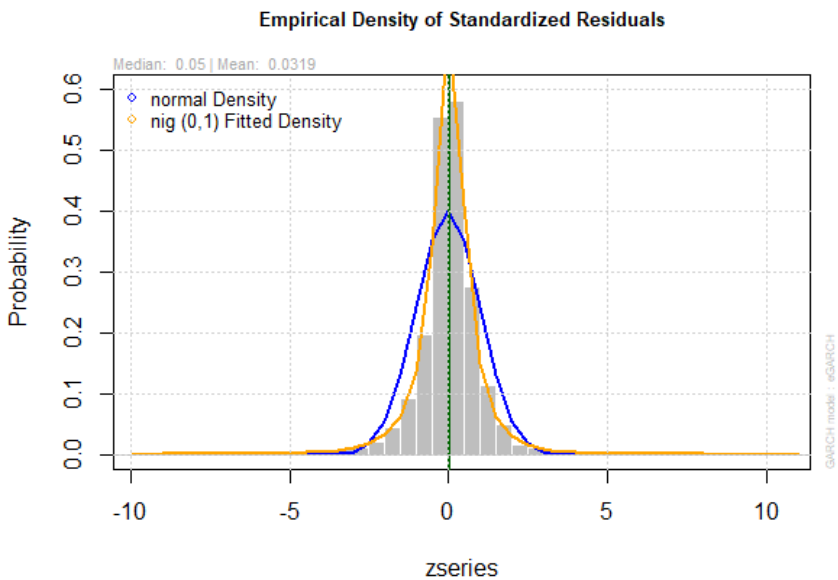
The choice of the model

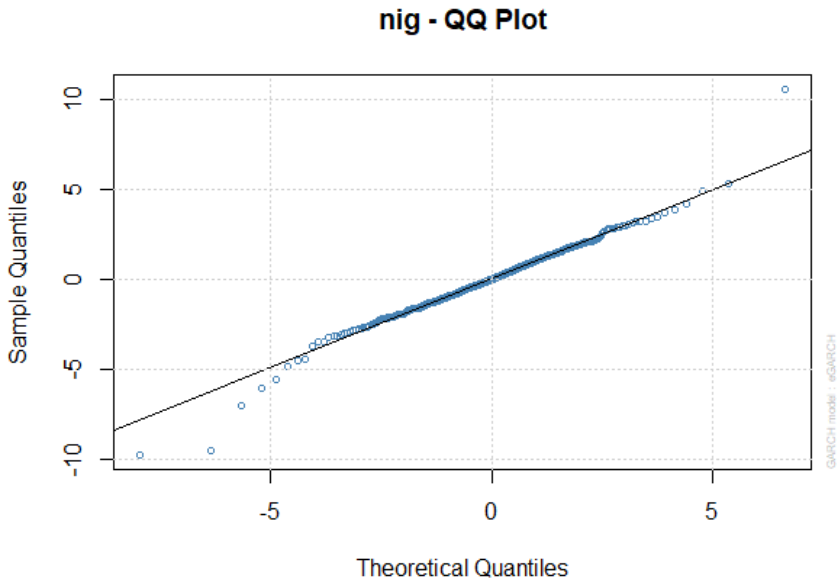
- Non-linear models can be specified considering the following steps:
  1. Look at the ACF and PACF for log returns and absolute log returns.
  2. Estimate the parameters of the several non-linear specifications and different types of distributions chosen.
  3. Select the specification model using diagnostic measures (Maximum likelihood, AIC, BIC, H-Quinn and Shibata).
  4. Jointly estimates the parameters of the non-linear specification chosen, allowing for a variation on the ARMA process (conditional mean).
  5. Evaluate and choose again the best fit using diagnostic measures.
  6. Analyze the estimated parameters to observe the structure of the data generating process and the shape of the distribution.
  7. Test and analyze residuals to see if the model is reliable and then use the model for descriptive or forecasting purposes.
- The final model is then an ARMA(3,2)-eGARCH(1,1) with a nig distribution:

$$
\begin{aligned}
y_t &= 0.00078 - 1.3083\phi_{t-1} - 1.0764\phi_{t-2} - 0.0663\phi_{t-3} + 1.2378\epsilon_{t-1} + 0.9912\epsilon_{t-2} + \epsilon_t \\
ln(h_t) &= -0.095696 + 0.052064 z_{t-1} + 0.272963(|z_{t-1}| - E|z_{t-1}|) + 0.986035 \cdot ln(h_{t-1}) \\
\epsilon_t &= z_t \sqrt{h_t}, \qquad z_t \sim nig(0,1)
\end{aligned}
$$

Analysis of results

Then, we can look at the standardized residuals, to see if the model is able to capture the empirical distribution:





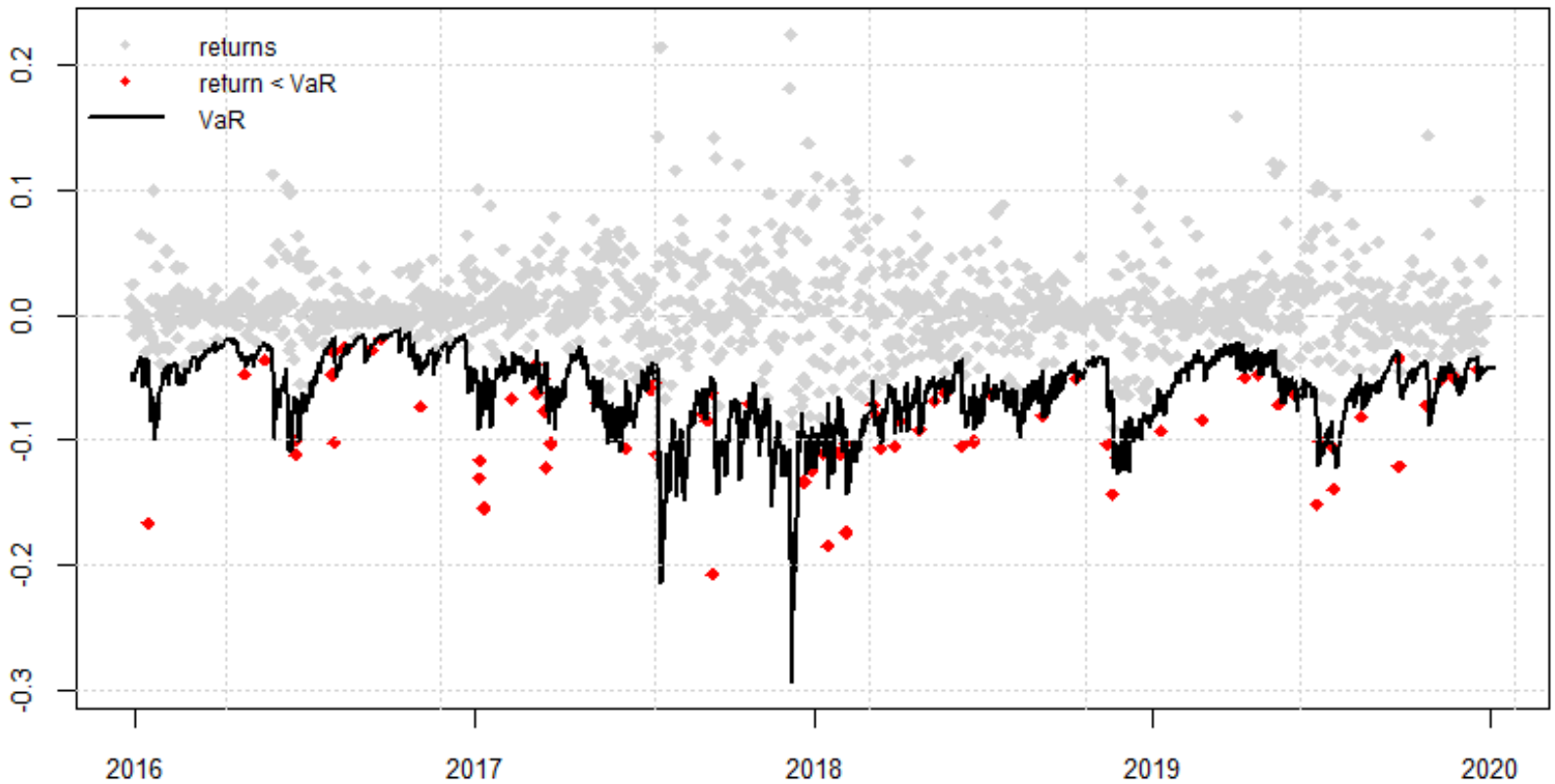
Overall, the two plots show that the nig distribution clearly works better than the normal distribution and that the standardized residual part is well explained by the model, leaving out only a few outliers on the tails.

The utility of the model

With can use the model in different ways:

- Predict the conditional mean and variance of the series.
- Re-estimate the model with expanding and moving windows for backtesting purposes.
- Try other longer term predictions
- Build a model based on the Value at Risk

Value at Risk



Conclusions

- Bitcoin shows to have useful characteristics to be used as sound money.
- Bitcoin can be used also as investment to differentiate a hypotetical porfolio.
- The Bitcoin time series has shown a certain regularity over time.
- Statistical tools can be used in the Bitcoin's time series to take in account for heteroskedasticity, with the aim to decrease risks related to the high volatility.