VIZET Matthieu
Academic Director: PETITJEAN Mikael
Master in Finance Asset & Risk Management
2020-2021

MASTER'S THESIS

Modeling bitcoin returns based on supply and demand drivers

June 15th, 2021

Abstract

This thesis examines the significance of microeconomic supply and demand drivers of bitcoin returns over the period 2013-2021. Also, to control additional factors, this paper includes exogenous security and macroeconomic variables. The effects of supply and demand are studied on bitcoin returns, with variables extracted from Bitcoin's blockchain. Such variables include daily active addresses, hodl waves, the percent of supply in profit, coin days destroyed and exchange net flows. Simple linear regressions are first applied to look at these effects and then VAR models are developed to give insights on how returns, supply, and demand interact with each other. Empirical evidence is found that demand, supply, and security are key determinants of bitcoin returns. Causality is also revealed between returns and daily active addresses, as a bidirectional relationship, while a liquid portion of the supply and the percent of supply in profit both Granger cause returns. This study clearly demonstrates the relevance of using on-chain data.

Table of contents

Acknowledgement

I would like to thank Dr. Mikael Petitjean, Associate Professor at IÉSEG School of Management who supervised this thesis. His precious insights and advice substantially guided my work and successfully helped me complete this paper.

I would also like to dedicate my master's thesis to my friends and family in appreciation for their encouragement and unconditional support.

1 Introduction

Bitcoin is an alternative form of money not officially recognized as a legal tender in any country invented in 2008, by an anonymous person or entity called Satoshi Nakamoto. According to the Bitcoin whitepaper, it is an electronic payment system based on cryptography instead of trust. Like Napster, or BitTorrent, it is a peer-to-peer (P2P) system with no intermediaries and no central bank. The Bitcoin protocol relies on proof-of-work (PoW) to issue coins and secure the network, and a shared state of all transactions in Bitcoin's history commonly called a blockchain.

Bitcoin was the first cryptocurrency and possess the biggest adoption as a store of value (it is the largest cryptocurrency by market capitalization), as a unit of account (other cryptocurrencies are frequently traded against bitcoin) and as a mean of exchange. What is differencing Bitcoin from fiat currencies is its monetary policy, which is fixed and capped at a maximum of 21 million bitcoins. However, Bitcoin is not backed by anything unlike fiat currencies in the past with gold, or a central authority or the legal obligation to accept a currency. But it could change very soon at least in one country, since Nayib Bukele, president of El Salvador announced a bill to make Bitcoin legal tender in the country. In the meantime, it has only a subjective value which is tested through demand and supply on exchanges.

1.1 Problem statement

Since the mysterious birth of the Bitcoin network in 2009 and the mining of the genesis block, there is no consensus on the fair and intrinsic value of bitcoin, its native asset. The question of what is determining the value of Bitcoin is becoming more important in a time where publicly listed companies purchase one-billion-dollar worth of bitcoins as a hedge against inflation (MicroStrategy, 2020), insurance companies as exposure to the digital world, famous fund managers like Paul Tudor Jones or Druckenmiller as a store of value and Tier 1 banks see it as a digital gold. The macroeconomic conditions are also currently favorable to the cryptoasset with algorithmic-enforced scarcity, as monetary inflation is being propelled to the world following the COVID crisis. The recent favorable developments around Bitcoin have also been accompanied with positive price action for its native asset and new all-time highs. However, whereas for stocks it is widely recognized to use discounted cash flow models, for cryptoassets such as bitcoin there are no earnings. Bitcoin has also no underlying use unlike commodities.

Finally, bitcoin is not a legal tender anywhere. That is the reason why it is only possible to identify the determinants of the bitcoin price and not use models.

1.1.1 Motivation

This study will examine the determinants of bitcoin price using the data offered by the Bitcoin protocol. Indeed, it offers a level of transparency never seen in any other assets or markets thanks to the data of the blockchain. With all transactions registered in blocks and cryptographically linked on the ledger, it is possible to track the movements of coins on the blockchain, and even associate public addresses with behaviors or labels, like exchanges. This data is referred to as on-chain data or on-chain metrics in this paper.

On-chain data and metrics allow to analyze both supply and demand dynamics. For instance, the Net Flow between deposits and withdrawals of bitcoins on exchanges is one such metric: it shows the flows of bitcoins in and out of exchanges. Large deposits of bitcoins on exchanges could potentially add sell-side pressure. While withdrawals of bitcoins out of exchanges' custody could indicate accumulation. Other metrics that can be tracked are for instance the evolution of the number of whales (holders of more than 1000 bitcoins) or the percentage of bitcoin addresses in profit and so on.

1.1.2 Perimeter

This thesis will focus its study of determinants on on-chain data and metrics only to proxy supply and demand. Control variables commonly used in previous studies will also be included. Macroeconomic variables will be added, especially monetary inflation, which is a reason often quoted by investors for the rationale behind buying bitcoin. Another control determinant to bitcoin price to consider is security, since dozens of millions of dollars are spent each day by the Bitcoin network to pay miners (at a rate of 900 bitcoins mined per day with one block every 10 minutes and a reward of 6.25 bitcoins), which can be defined as the security budget, named by Jordan McKinney (2018).

1.1.3 Contribution

If the question of the determinants of bitcoin price has already been addressed by the literature, the combination of supply and demand both proxied by blockchain data has been developed very little. This requires further analysis, and this study will do so to find the determinants of bitcoin returns by analyzing supply and demand dynamics.

1.2 Research questions

In light to the recent developments around blockchain data and related on-chain metrics, and to the novel approach proposed in this paper, the general research question of this thesis is:

- How does supply and demand determine bitcoin price?

Other subsidiary research questions will be also discussed in this paper:

- What is the relationship between supply and bitcoin returns?
- What is the relationship between demand and bitcoin returns?
- Does security spending/budget affect bitcoin returns?
- Are there macroeconomic determinants of bitcoin returns?

This study will try to answer these research questions by conducting an empirical analysis of bitcoin determinants.

2 Literature Review

2.1 Introduction

Many empirical scientific research studies previously discussed the determinants of bitcoin price. This thesis will review the existing literature and explore it by the lens of groups of determinants such as supply and demand, security, and macroeconomic factors.
Then, the hypotheses of this study will be established and discussed.

2.2 Review of the literature

2.2.1 Supply

Supply has been discussed in the literature has a possible determinant of bitcoin and has been measured in different ways such as the number of circulating bitcoins, coin days destroyed, or metrics based on blockchain analytics such as flows of bitcoins in or out of exchanges.

Huhtinen (2014) discovers that an increase in the circulating supply causes a decrease in bitcoin price (inflationary effect), suggesting that supply plays a role in determining bitcoin price. Bartos (2015) employing an Error Correction model (ECM) confirms Huhtinen results that supply has an important role in determining bitcoin prices.

Michael and William (2014) study the effects of coin days destroyed as well as other determinants in a multivariate model. Smith (2018) defines Bitcoin days destroyed are transactions measured in bitcoin multiplied by the number of days passed since these were last spent. Smith also demonstrates that dormancy is a better variable to understand the behavior of Bitcoin users compared to coin days destroyed and can be considered as the inverse of velocity. Michael and William (2014) found that coin days destroyed significantly affect bitcoin price.

Sukamulja and Sikora (2018) use a vector error correction model (VECM) to look for the determinants of bitcoin price. The supply is proxied by the total number of bitcoins mined (circulating supply). Variance decomposition and Impulse Response Function (IRF) are used to study the effect on a variable when there is a shock on other variables. The authors found that in the short-run supply affects price (negative effect).

Using an ARDL model, Li and Wang (2016), find that in the early market (before the fall of Mt. Gox exchange) in the long-term, the price is affected by the number of bitcoins in circulation.

2.2.2 Demand

Demand is a determinant studied a lot in the literature. It has been proxied in several ways: attractiveness and behavior (Google and Wikipedia queries, social media activity), direct activity on the Bitcoin protocol (daily active addresses) and indirect activity such as the number of wallets created on the service provider blockchain.com.

2.2.2.1 Investor behavior

Michael and William (2014) in a multivariate model show a positive effect on bitcoin returns from Google trends.

Polasik et al. (2014) empirically study the determinants of bitcoin fluctuations. The variables used include monthly bitcoin returns, the number of articles with the word bitcoin and the google searches (both to proxy popularity). They find that popularity or investor attractiveness is a significant driver of bitcoin returns.

Bartos (2015) using an ECM model finds that demand plays a crucial role in determining bitcoin returns and is even more significant than supply effects. To capture other demand determinants, Wikipedia queries are used to measure the interest of investors and thus demand but there is no significant effect.

Bouoiyour and Selmi (2015) use an ARDL bounds testing approach to find the drivers of Bitcoin price. The proxy of demand tested is investor's attractiveness (bitcoin views on Google). The ARDL approach allows to estimate the cointegration relationship with an OLS estimator when the lag order of the model is known. It also allows to study both the short run and long run relationships and does not require to test variables for unit roots unlike Johansen cointegration. The model is built with all variables as first differences. The critical bounds allow to determine cointegration which happens if the F-statistic is higher than the upper bound. The authors affirm that Granger causality is less accurate to identify causal links in case of shocks and use instead an innovative accounting approach by simulating variance decomposition and impulse response function. After descriptive statistics, the ADF and Philippe-Perron tests are performed to test the integration of variables which are at level or first difference. So, the ARDL model can be used to test the cointegration. The optimal lag of the model is selected using AIC criterion. With this model, they find that investor attractiveness is positively correlated with bitcoin price. The F-statistic is significant at the 10% level, implying a long-run relationship among variables. Innovative variance decomposition shows that 69% of bitcoin price can be explained by its own innovative shocks. The impulse response function shows the impacts of shocks of the independent variable on dependent variables in a VAR system. According to the study bitcoin responds to its own shocks and investor attractiveness.

Li and Wang (2016) conduct an empirical study on the determination of bitcoin price and some of the variables are the number of bitcoin transactions, search intensity and social media attention. The variables of their data being both stationary and non-stationary, they use an autoregressive distributed lag (ARDL) model. The data is separated in two parts to consider the rise and fall of Mt. Gox exchange. The data presents co-integration and there are I(0) and I(1) variable so the ARDL model is more suitable, and a bounds test approach is adopted. They conclude that investor behavior is more significant in the short-term and Google searches have also a positive impact in the long-term.

Kjaerland et al. (2018) look at the drivers of bitcoin fluctuations using ARDL models. Weekly variables include Google searches. Variables have been first differenced to make them stationary. The ARDL models are estimated with AIC and BIC to find the best lags. The first model has all variables while the second one only has the variables that are significant in the previous model. Multicollinearity is tested and one variable is removed. The Durbin-Watson (DW) test allow to confirm the absence of autocorrelation in the models. The results of the first model show a positive relationship with Google searches volume. In the second model, Google searches are also significant.

Panagiotidis et al. (2018) use Google trends to proxy demand within a LASSO regression framework and they find that this is the largest determinant of bitcoin price.

Panagiotidis et al. (2019) confirm the results of Bartos (2015) and Panagiotidis et al. (2018) using VAR models and generalized impulse response functions because they find that

Wikipedia queries have no effect while shocks in Google queries affect bitcoin when its price is above its trend.

2.2.2.2 Bitcoin network users

Bitcoin network users are proxied in the literature in a direct way with the number of transactions, or the daily number of active addresses but also in an indirect way such as the number of wallets created on specific service providers like blockchain.com.

First, Ciaian et al. (2014) use the number of daily active bitcoin addresses as a proxy for bitcoin demand. Indeed, if the network is more used, the number of unique addresses interacting with the protocol should rise. Using VAR and VECM models, they find that in the long run, demand plays a significant role along with supply. Michael and William (2014) in a multivariate model also show a positive effect from the number of transactions on bitcoin price. Using an ECM model, Bartos (2015) confirm the impact of active addresses. Aalborg et al. (2019) also use active addresses to measure demand and the change of bitcoin users, and they find that this driver is correlated to bitcoin returns on both daily and weekly timeframes.

Polasik et al. (2014) find that the number of transactions is a driver of bitcoin returns, indicating network effect. Li and Wang (2016) find that in the later market, after the fall of Mt. Gox exchange, the price is affected by the number of bitcoin transactions.

Sukamulja and Sikora (2018) use a vector error correction model (VECM) to study the determinants of bitcoin price. The number of wallets created on blockchain.com is used a as a proxy for demand. The Granger’s causality test is performed to test the mutual relationship between the drivers. A two-way relationship is found between the price and the demand. The VECM model allows to study time series with cointegration, and the standard coefficient describes the short-run relationship while residual lags of the regression describe the long-run relationship. Variance decomposition (quantify relationship) and Impulse Response Function (IRF) are used to study the effect on a variable when there is a shock on other variables. The authors found that in the long run, the bitcoin price is affected by changes in demand. Demand has also a positive effect in the short run.

2.2.3 Security

Using an ARDL bounds testing approach, Bouoiyour and Selmi (2015) find that hash rate has a significant but minor correlation with bitcoin price fluctuations. Kjaerland et al. (2018) find that hash rate has not a significant effect in their ARDL models. Kei et al. (2019) use an Impulse response function to see that hash rate has a positive relationship with bitcoin but is insignificant in the long run. The VAR Granger causality shows that hash rate and velocity cause each other. Mining difficulty has a positive effect on price. Variance decomposition analysis shows that hash rate has a minor role.

Adjei (2019) study the relationship between drivers related to the Bitcoin mining industry and bitcoin returns using a GARCH-M model. Hash rate, mining difficulty and block size are the studied variables. Control variables are the volatility and the number of transactions. With no independent variables, the model presents GARCH effects. Results show a clear positive relationship between hash rate and returns, while difficulty and block size have a negative relationship. Using the Fama and French forecasting model and GMM estimator for predictability regressions, the author found that all mining variables have forecasting power over the returns of bitcoin.

Security is therefore a significant driver of bitcoin price and will be analyzed in this thesis.

2.2.4 Macroeconomic factors

Macroeconomic variables are often used in the models of the literature, both as a subject of study itself or as control variables. Drivers studied include commodities (gold, oil), stock indices (or volatility of stocks), unemployment numbers, inflation, money supply, and uncertainty indices.

The gold effect has been extensively studied because it is a commodity with no fundamentals like bitcoin. It is also a store of value, like what is trying to be bitcoin as part of its use as a possible form of money and therefore is a speculative form of store of value. Gold is also considered as a hedge against inflation, an argument often used by bitcoin proponents. Panagiotidis et al. (2018) examine the determinants of bitcoin returns within a LASSO approach, with two different LASSO methods used. The LASSO regression allows to consider all variables and keep only the most relevant by automating the selection of the model. They find that the largest determinants are Google trends and gold. Bitcoin is indeed positively affected by gold according to the authors. Sukamulja and Sikora (2018) have found with a VECM model that in the long run, the bitcoin price is affected by changes in gold price. Panagiotidis et al. (2019) confirm their previous study with VAR and FAVAR models and conclude that gold and bitcoin seem to have similarities in their behavior and gold has a positive effect on bitcoin.

Other macroeconomic determinants than gold are also studied in the literature. Polasik et al. (2014) empirically study the determinants of bitcoin fluctuations. The variables include macroeconomic drivers such as growth in industrial production, unemployment, and inflation. However, they find that macro variables are not significant. Ciaian et al. (2014) also find that macroeconomic drivers are not statistically significant.

Panagiotidis et al. (2018) find that Bitcoin is negatively affected by uncertainty indices, positively by oil and unclearly from stock markets.

Panagiotidis et al. (2019) study the effects of markets, uncertainty and searches on bitcoin returns using VAR and Factor-Augmented VAR (FAVAR) models. Variables employed are all on a weekly timeframe and include oil price, gold price, FED funds effective rate, ECB deposit facility rate, currency exchange rates (EUR, GBP, CNY, JPY against USD), Dow Jones index, Nasdaq, Nikkei225, S&P350, Shanghai composite index, CBOE DJIA volatility index, US, Europe and China policy uncertainty. The first model is a classic VAR. This model is reduced to 11 variables with Granger causality, and shocks are introduced with generalized impulse response functions and local projections to see how bitcoin responds. The second model is a FAVAR one with two-step principal component estimation, the third model uses Bai and Ng criteria to reduce the number of variables in the VAR model and the last one uses principal components analysis before VAR estimation. Results show considering only statistically significant variables that Dow Jones and Nasdaq stocks have positive effects. China uncertainty has negative effects.

Sukamulja and Sikora (2018) in their vector error correction model (VECM) include a macroeconomic determinant, the Dow Jones Industrial Average (DJIA). The authors found that in the long run, the bitcoin price is affected by changes in DJIA (negative influence) and in the short run.

Li and Wang (2016), in their ARDL model found that in the later market (after the closure of Mt. Gox exchange), bitcoin price is affected in the short-term by changes in US inflation, money supply and interest-rate.

Bouoiyour and Selmi (2015) in their ARDL bounds testing approach find in the impulse response function which shows the impacts of shocks of the independent variable on dependent variables that bitcoin responds to its own shocks and the Shanghai market index.

Kjaerland et al. (2018) also using ARDL models, include macroeconomic weekly variables (S&P500, S&P500 volatility index, oil price, and two dummy variables for positive and negative incidents). Variables have been first differenced to make them stationary. An ADF test is performed to confirm stationarity with MAIC criterion, except for hash rate which has a structural break. A Zivot Andrews (ZA) test is performed to take this break into account and the stationarity of hash rate is confirmed. The ARDL models are estimated with AIC and BIC to find the best lags. The first model has all variables while the second one only has the variables that are significant in the previous model. Multicollinearity is tested and one variable is removed. The Durbin-Watson (DW) test allow to confirm the absence of autocorrelation in the models. The results of the first model show a negative relationship of bitcoin with oil price. However, volatility is not significant. In the second model the dummy variable for negative incidents is statistically significant.

2.3 Conceptual framework

The Law of Supply and Demand is the theory explaining the interactions between the buyers and sellers of an economic resource. The law of demand interacts with the law of supply to create an equilibrium at which the price is determined. Many previous studies use supply and demand interactions as their theoretical foundation, like Ciaian et al. (2014).

Supply is usually a function of multiple factors, including the cost of production and the number of sellers. A naive and fundamentally flawed approach would be basing a study on the cost of production model. Indeed, the competition between miners to earn bitcoin rewards that increases the circulating supply involves fixed and marginal costs of production. Electricity is the biggest, since it is needed to power the specialized hardware (ASICs) that are trying to find a valid hash to produce a block. However, the cost of production follows the bitcoin price. In fact, the cost of production reacts to the price and the difficulty adjustments. For instance, if the bitcoin price largely drops, it will make some miners unprofitable and turn off their machines, which will lower the difficulty adjustment (the protocol will lower it if blocks are mined less than every ten minutes) and finally make easier to find new blocks and therefore reduce the production cost of bitcoin for the remaining miners. And the bitcoin price does not follow the cost of production, or in little proportion, because the emission of new bitcoins by the mining process has a fixed rate and time, and the rate is even reduced every four years. Furthermore, if bitcoin markets follow the Efficient Market Hypothesis, (Fama, 1970) the emission of new bitcoins should be already priced in since it is fixed and known in advance. Thus, the bitcoin supply can be better approached by looking at the flows of bitcoins on-chain and the behavior of bitcoin investors (their tendency to hold or sell), including bitcoin miners that are also bitcoin sellers.

Demand is also a function of multiple factors, including investor preferences or the demand for usage of the Bitcoin network. Regarding the demand for usage, the scarce resource offered by the protocol to consumers is blockspace, which is the limited space composing blocks used to include transactions. Thus, the demand can also be proxied indirectly for instance by the number of transactions or the number of users interacting with the network, such as the active addresses. This last proxy is also supported by Metcalfe’s law, which states that the value of a network is proportional to its number of users.

Security is another foundation that needs to be controlled, because miners offer this valuable and paying service to the network and is defined as security spending or budget. This service is responsible for bitcoin unique properties like resistance against censorship or attacks. Indeed, Proof Of Work (PoW), the Bitcoin consensus mechanism is vulnerable for example to 51% attacks, that have a quantifiable economic cost according to Yang et al. (2019) and others (Crypto51, 2021).

2.4 Hypotheses development

A. Hypothesis 1

The demand dynamics for Bitcoin is positively correlated with bitcoin log returns. Indeed, if the demand rises to use the network with everything else remaining constant, the price of bitcoin should rise.

B. Hypothesis 2

The supply dynamics of Bitcoin should affect bitcoin returns. If the supply of liquid bitcoins rises with everything else remaining constant, the sell-side added pressure should make the bitcoin price fall. If the supply is held and removed of circulation (for instance out of exchanges), with everything else remaining constant, this should create a supply shock and make the bitcoin price rise.

C. Hypothesis 3

Security should affect bitcoin price, because the security of a network is a valuable service, and the level of security spending directly makes the protocol more or less secure.

2.5 Conclusion

In this section, the literature has been reviewed to look at the potential determinants of bitcoin prices for demand and supply, based on the supply and demand conceptual framework. Control factors have been also explored, especially security and macroeconomics.

The review shows that blockchain data has only been used a little in supply and demand interactions, and this paper proposes to fill the gap between the literature findings and the opportunity that represents the transparency of the Bitcoin protocol by developing hypotheses.

3 Methodology

This paper aims to determine the drivers of bitcoin price, focusing on data obtained from the Bitcoin blockchain. This section describes the datasets and methods used in this study.

3.1 Data sources

This study uses log returns derived from bitcoin price changes, from 2013 to 2021. The excess returns have not been used because there is no risk-free interest as there is no equivalent in the cryptocurrency ecosystem, even with decentralized finance or stablecoins since there is always a risk of counterparty or smart-contract hack. Bitcoin price has been extracted on CoinGecko, a leading aggregator of cryptocurrency prices. All variables based on on-chain data or metrics have been extracted from Glassnode, a blockchain data and intelligence provider. Federal surplus or deficit and M2 money stocks both have been extracted from the database of the Federal Reserve Bank of St Louis. The data analysis is based on 2811 observations, collected from 30th April 2013 to 11th January 2021.

3.2 Variables

Some variables have been transformed to returns, such as bitcoin and gold prices. Others have been transformed into percent changes to make them stationary. Finally, the Federal surplus or deficit has been first differenced. Moreover, macroeconomic variables (Gold, Federal surplus or deficit and M2 money stock) have been extracted as monthly series and have been transformed in daily series by using each monthly value as the daily values of the month. Thus, each daily value of a particular month is the same.

3.2.1 Bitcoin log returns

The exchange price of bitcoin has been obtained from CoinGecko because its data goes back to 2013, which is old in the cryptocurrency industry (many exchanges are born later) and it reflects the price of bitcoin on multiple exchanges at the same time and avoid relying on the prices of a single exchange which can be dislocated for any reason (for instance, a flash krach, or a technical maintenance). Furthermore, some exchanges are not regulated and even practice wash trading as reported by Bitwise (2019).

After being extracted, the price of bitcoin has been transformed in log returns. Log returns are continuously compounded returns and are traditionally used by finance researchers and practitioners according to Brooks (2019). Log returns are also time additive, meaning they can be added to compute lower frequency returns for instance.

3.2.2 Demand

Daily active addresses

Demand is difficult to proxy for bitcoin. As shown in the literature, it is often proxied by investor behavior (social media attention, queries on Google, etc). But since the purpose of this study is to use on-chain data, the variable chosen is daily active addresses. It is a proxy for the number of users on the Bitcoin network. Indeed, if more people use the Bitcoin protocol to exchange value, more addresses should be active (meaning sending or receiving bitcoins) and vice-versa.

3.2.3 Security

Hash rate

Hash rate is the average number of estimated hashes per second powered by miners with the goal to find valid blocks and earn rewards in bitcoins. It measures the computing power of the network.

The term comes from the word hash, which is the value below the target hash miners are competing to produce by changing the nonce (a random number). Finding a valid hash is the condition to win the mining competition and produce a valid block that can be accepted by the network consensus. Indeed, the hashing function of Bitcoin (SHA-256) is a one-way function which renders a hash, and changing a slight detail makes a completely different hash. Therefore, it can take millions of trials for a miner to find a valid hash. Today, hash rate is measured in EH/s, or exa hashes per second, with one exa hash equal to one quintillion hashes.

Hash rate is an imprecise measure, because it is computed based on block count and average daily difficulty, leading to values that can differ from one provider to another and can even create controversy according to a report from Kraken Intelligence (2020).

Fee Ratio Multiple

Fee Ratio Multiple (FRM) is the total miner revenue (block rewards and transaction fees) divided by transaction fees. This on-chain metric was created by Matteo Leibowitz (2018). FRM measures security of the Bitcoin network in the long run, because since the supply of bitcoins is fixed, one day block rewards will disappear. Only transaction fees will remain to provide an incentive to miners to secure the network. A low FRM indicates that the network has a good security budget and does not need to rely on block rewards (inflation). A high FRM indicates a network with a low security budget that needs inflation to maintain its security budget. In the case of bitcoin in the long run, FRM should go to 1 because block rewards get halved every 4 years and, in the future, they should be negligible compared to transaction fees to keep the same security.

3.2.4 Supply and related on-chain metrics

Addresses with balance > 1000 BTC

This variable is the number of unique Bitcoin addresses holding at least 1000 BTC. This paper uses this on-chain metric to track the increase or decrease in whales (large holders of bitcoin). Indeed, if the number of such addresses increases, there is less supply available and possibly indicates accumulation, while a decrease could signify those large holders are selling their bitcoins.

Coin days destroyed

Coin day destroyed (CDD), as defined by Smith (2018), are computed by taking the number of coins in a transaction and multiplying it by the number of days it has passed since those coins were last spent.

Several studies have used coin days destroyed as a proxy for analyzing supply dynamics, and are even a significant driver of bitcoin price, as showed by Michael and William (2014). A low CDD value could indicate movements of young coins (possibly selling) while a high CDD value could show that old Bitcoin holders are moving their coins, possibly selling. It is linked to supply dynamics because young coins being sold can be restricted to short-term selling while old coins moving can be more concerning and indicating that old Bitcoin market participants want to sell.

Liveliness

Liveliness is the ratio between the total coin days destroyed and the total of coins created (circulating supply). It was created by Tamas Blummer (2018) and gives insights into holding behavior. Indeed, it indicates changes in long-term investor behavior (holding when liveliness decreases or selling when liveliness increases).

Dormancy

Dormancy is the average number of days destroyed per coins transacted. It is the ratio between coin days destroyed and transfer volume. High dormancy indicates that old coins are coming back to circulation while low dormancy describes those coins moved are recent.

Exchange Balance (Percent)

This variable represents the percentage of supply held by centralized exchanges. A growing percentage indicates high selling activity while a decreasing percentage indicates that bitcoins are moved out from exchanges, for instance to be held in cold storage. Exchanges used by Glassnode to create this metric are: Binance, Bitfinex, Bitmex, Bitstamp, Bittrex, Coinbase, Coincheck, Gate.io, Gemini, Hitbtc, Huobi, Kraken, Luno, Okex and Poloniex.

Exchange Net Flow Volume

It measures the net flows between deposits and withdrawals on exchanges. If there are more deposits, prices are expected to drop, since there is more selling pressure, while if there are more withdrawals, there should be less selling pressure and can also indicate accumulation of coins moved out from exchanges. Exchanges spotted by Glassnode to create this metric are: Binance, Bitfinex, Bitmex, Bitstamp, Bittrex, Coinbase, Coincheck, Gate.io, Gemini, Hitbtc, Huobi, Kraken, Luno, Okex and Poloniex.

Circulating supply last active 1 year plus

This is the percentage of the circulating supply that has not moved since at least one year. If this metric rises, there is less circulating supply and thus less potential selling pressure (accumulation). However, if it decreases, the behavior of market participants can be oriented towards spending.

Hodl waves

Hodl waves represent the distribution of bitcoins in age bands (last moved since x time). Large age bands can indicate illiquid supply (lost), while recent age bands can have a significant impact on supply dynamics. For instance, a sudden decrease in the hodl wave 1-2 years old is possibly bearish for bitcoin price since relatively old bitcoin holders are spending their coins. While a gradual increase in age bands shows accumulation of bitcoins.

Huber and Sornette (2020) analyze the role of speculative bubbles in bitcoin adoption. They show that bubble-fueled adoption cycles can be visually represented with bitcoin age bands (Hodl waves).

Percent UTXOs in profit

This metric is tracking the number of bitcoins in profit based on the last movement of UTXOs (unspent transaction outputs). UTXOs represent on the blockchain ownership of a balance of bitcoins associated to a public key (bitcoin address) and are timestamped at the transaction or block they were created.

Percent supply in profit

This metrics tracks the percentage of the circulating supply in profit based on the price at which coins last moved. If a coin last moved at a price below the current price, it is considered in profit and in loss if higher than the current price.

3.2.5 Macroeconomics

Gold

Gold prices are transformed to returns. Gold returns are interesting to use as a macro variable because Bitcoin is often referred as a form of digital gold. Thus, gold and bitcoin returns should behave in the same ways and be at least correlated.

Deficit

The Federal Surplus or Deficit is the budget deficit or surplus of the United States government. Surplus occurs when income exceeds spending and vice-versa for deficit.

Money supply (M2)

The money supply is the M2 money stock. It is first made of M1, the most liquid forms of money: physical currency and coins, demand deposits, traveler's checks, other checkable deposits, and negotiable order of withdrawal accounts. Then, M2 is also made of small-denomination time deposits at depositary institutions, and balances in retail MMFs (money market funds).

3.2.6 Summary of variables and comparison

The Table I is a summary of variables used in this thesis and compares them with the variables used in the literature.

TABLE I

VARIABLES SUMMARY

Variables	Literature	Thesis
Demand	-Google searches -Number of articles with "bitcoin" -Wikipedia queries -Social media attention -Number of transactions -Daily active addresses -Number of blockchain.com wallets	-Daily active addresses
Supply	-Circulating supply -Coin days destroyed -Dormancy	-Addresses with balance > 1000 BTC* -Coin days destroyed -Liveliness* -Dormancy -Exchanges balance* -Exchange Net Flows* -Supply last active 1 year plus* -Hodl waves* -Percent supply in profit* -Percent UTXO in profit*
Security	-Hash rate -Mining difficulty -Block size	-Hash rate -Fee Ratio Multiple (FRM)*
Macroeconomics	-Gold -Growth in industrial production -Unemployment -Inflation (CPI) -Oil -Uncertainty indexes -FED Funds effective rate -ECB deposit facility rate -Currency exchange rates -Stock indexes -Volatility -Money supply	-Gold returns -Federal Deficit or Surplus -Money supply

* denotes a novel variable, not used in the literature.

3.3 Methods

3.3.1 Descriptive analysis

This method allows us to draw summary statistics on large datasets. First, the measure of central tendency will be applied to each dataset (variable) to see the central position of this dataset. Two measures of central tendency will be computed, the mean and the median. The mean is the sum of all values divided by the number of values n. The median is value in the middle of the dataset.

Other basic statistics include the minimum and the maximum, which are respectively the smallest and the largest observations of the dataset.

Then, the measure of statistical dispersion will be utilized to see how the data is dispersed and spread out. The standard deviation is the square root of the variance. Skewness will be also determined and is the extent at which a distribution varies from a normal distribution. It also shows the extremes values of one tail against another. Indeed, a distribution following a normal law has a zero skewness. Finally, Kurtosis is another measure to describe how the tails of a distribution differ from the normal distribution, while showing the extreme values of either tail.

3.3.2 Unit roots

Testing for the presence of unit roots is crucial in an empirical study and allows to determine if a time series has stationarity or not. According to Brooks (2019), a stationary time series is one with a constant mean, variance and autocovariance for any lag. Stationarity influences the properties of a time series (for instance, with stationarity shocks die slowly away) and avoid spurious regressions. However, if a time series is non-stationary, it is said to have a unit root.
The order of integration is the statistic used to describe a unit root process. Specifically, it shows the number of differences needed to get a stationary time series. For instance, a stationary series is I(0). Moreover, it is important to have stationary variables in a VAR model to use hypothesis tests or look at the significance of coefficients in the opinion of Brooks (2019).

This paper will use the Augmented Dickey-Fuller test (ADF) to test for stationarity in the variables. The null hypothesis of this test is that there is a unit root in the time series (not stationary):

H_0: The time series has a unit root, $\phi = 1$.

H_1: The time series is stationary, $\phi < 1$.

The ADF statistic is a negative number that depending on how negative its value is, allows to reject the null hypothesis.

3.3.3 Linear regression

Linear regression is a method to model the relationship between a dependent variable Y and one or more explanatory variables X by fitting a linear line to the data. Linear regression is not an indication of causality but implies a significant relationship between variables. This regression is linear because its equation is in the form of $Y_t = \beta_0 + \beta_1 \cdot X_t + \varepsilon_t$. The intercept of the equation is β_0 and the slope is β. ε_t is the error term, or the variation in Y that is not captured by the linear regressor.

The multiple regression model is defined as:

$$Y_t = \beta_0 + \beta_1 \boldsymbol{X}_{1,t} + \cdots + \beta_i \boldsymbol{X}_{i,t} + \varepsilon_t$$

The parameters of the equation are estimated using the OLS estimator (ordinary least squares). It consists of minimizing the sum of the squares of the differences between the observed Y and the values predicted by the linear function.

Statistical measures such as the R^2 are computed to evaluate the level of variance in the dependent variable that can be predicted with the independent variables. Its value ranges from 0 to 1. The adjusted R^2 is adjusted from the number of predictors (independent variables) in the model. For instance, it will decrease if a new variable is added that improves less the model that expected by chance and vice-versa when increasing. The p-values of the model indicate the significance at which a dependent variable can predict Y_t.

There are assumptions behind the linear regression model. According to Brooks (2019), the errors must have a mean of zero, the variance of errors must be constant, errors must be independent from one another, there should be no relationship between the errors and the explanatory variables and errors should be normally distributed.

3.3.4 Vector autoregression

A Vector Autoregressive (VAR) model is a systems regression model, as an extension of the univariate autoregressive model, with multiple dependent variables. It is useful to model multiple variables in a single model. A VAR model is regressing a vector of time series against lagged vectors of these variables. The particularity of this model is that each variable influences each other. Indeed, each variable is modeled as a linear combination of lagged values of itself and lagged values of the other variables. This makes variables endogenous. This is perfect from a theoretical point of view to model bitcoin returns and supply and demand effects in VAR approach.

Each coefficient on each equation is estimated using OLS, like in a classical linear regression. A VAR model is defined by p its lag order and k the number of time series regressions. u_t is the white noise disturbance term. This is what looks like the equation of a simple VAR(1) model with k = 2:

$$Y_{1,t} = \beta_{10} + \beta_{11}Y_{1,t-1} + \beta_{12}Y_{2,t-1} + u_{1,t}$$
$$Y_{2,t} = \beta_{20} + \beta_{21}Y_{1,t-1} + \beta_{22}Y_{2,t-1} + u_{2,t}$$

3.3.5 Granger causality

Proposed by Granger (1969), the concept of Granger causality determines if a time series is sufficient to predict another one, by testing the ability to predict the values of a time series Y_t using the lagged values of another time series X_t. Indeed, regressions are not sufficient because they reflect correlation, but not causal effects. The Granger causality is based on the assumptions that a cause happens before its effect and that the cause has statistically significant information about the future values of its effect. This method is used to empirically test the direction of causality when two variables are related. It is testing the null hypothesis that the coefficients α_p of the X_t lagged values are zero combined:

H_0: $\alpha_1 = \alpha_2 = a_p = 0$; where X_t does not Granger cause Y_t

H_1: at least one of α is different from 0; where X_t Granger causes Y_t

3.3.6 Diagnostic tests

Several diagnostic tests are used in this paper to check the assumptions of the models and their quality.
The normality assumption of models such as the classical linear regression are tested with the Shapiro-Wilk and Jarque-Bera tests. The Shapiro-Wilk computes a W statistic that determines if a sample comes from a normal distributed population. If the p-value is greater than the significance level (alpha), the null-hypothesis cannot be rejected.

H_0: The population is normally distributed.
H_1: The population is not normally distributed.

The Jarque-Bera tests normality by checking if a sample has the skewness and kurtosis of a normal distribution.

H_0: The skewness and excess kurtosis are zero.
H_1: The skewness and excess kurtosis are different from zero.

Testing heteroscedasticity allows to determine if the variance of errors in a regression is caused by independent variables or not. It is required because OLS has the homoscedasticity assumption (constant variance). The Breusch-Pagan and Portmanteau Q tests have the following hypotheses:

H_0: The skewness and excess kurtosis are zero.
H_1: The skewness and excess kurtosis are different from zero.

Serial correlation happens when a variable and lagged values of itself are correlated over time. In fact, in time series it is defined when error terms are correlated with lagged error terms. The Breusch-Godfrey tests serial correlation. The null hypothesis states the absence of serial correlation in the model.

H_0: The skewness and excess kurtosis are zero.
H_1: The skewness and excess kurtosis are different from zero.

3.3.7 Variable and model selection

Variable selection is key to build a good model. To select the relevant variables for the general model, forward selection and stepwise regression are used as methods to select them.
First, forward selection starts by building a model with only an intercept. Then, variables are joined to this model one by one. When no more variables improve the model according to a criterion it is done.

Stepwise regression combines backward elimination with forward selection. Indeed, variables are added one by one but when a variable is added, this method verifies all variables and can delete one if needed (no improvement to the model).

The criterion chosen in this study to select variables with forward selection and stepwise regression is the Akaike Information Criterion (AIC). It is an estimator of the quality of a model and allows to choose the best model between multiple ones. The AIC is computed based on the number of independent variables and the maximum likelihood estimate (how well the model fits the data). The AIC formula is:

$$AIC = 2K - 2\ln(L);$$

where K is the number of independent variables and L the log-likelihood estimate (probability that the model produces the observed values). Thus, the AIC will choose the model with the least number of explanatory variables and the most explanatory power over the variations of dependent variable. The lower the AIC score, the better the model is.

The models will be selected and evaluated according to the adjusted R^2 and the AIC, both previously defined.

3.4 Empirical model

As an introductory step, this study aims then to determine the effect of demand on bitcoin log returns using the following linear model:

$$r_t = \beta_0 + \beta_1 \cdot \Delta ACTADD_t + \varepsilon_t;$$

where demand is proxied by the variable chosen in section 3.2.2, the changes in the number of daily active addresses, defined as $\Delta ACTADD_t = (\frac{ACTADD_t - ACTADD_{t-1}}{ACTADD_{t-1}})$.

Next, this paper will look at supply effects on bitcoin log returns, using a linear multivariate model:

$$r_t = \beta_0 + \beta_1 \cdot \sum_{i=6} \beta_i \cdot S_{i,t} + \varepsilon_t$$

where $S_{i,t}$ are the supply variables, which are defined in section 3.2.4.

To control additional factors, macroeconomics will be added to the models previously described. Security variables will also be included for controlling the security level and spending of the Bitcoin network:

$$r_t = \beta_0 + \sum_{i=k} \beta_i \cdot X_{i,t} + \sum_{j=5} \beta_i \cdot C_{i,t} + \varepsilon_t$$

where $X_{i,t}$ are the independent variables (supply or demand) and $C_{i,t}$ are the control variables, grouping both security and macroeconomics. *i* and *j* are the number of candidates per category.

Then, a general linear multivariate model has been developed to model bitcoin log returns with supply, demand, security, and macroeconomics:

$$r_t = \beta_0 + \beta_1 \cdot D_{1,t} + \sum_{i=5} \beta_i \cdot S_{i,t} + \sum_{j=1} \beta_i \cdot H_{i,t} + \sum_{k=1} \beta_i \cdot M_{i,t} + \varepsilon_t;$$

where r_t is the bitcoin log-returns of bitcoin, defined as r_t= log $(\frac{P_t - P_{t-1}}{P_{t-1}})$.

$D_{1,t}$, $S_{i,t}$, $H_{i,t}$ and $M_{i,t}$ represent respectively the groups of variables demand, supply, security, and macroeconomics. And *i*, *j*, *k* the candidates in each category respectively. These variables are defined in section 3.2.

Finally, the following VAR(p) model is created to simultaneously model bitcoin log returns, demand, and supply:

$$
\begin{aligned}
r_{1,t} = {} & \beta_{10} + \beta_{11} r_{1,t-1} + \cdots + \beta_{1p} r_{1,t-p} \\
& + \gamma_{11} D_{2,t-1} + \cdots + \gamma_{1p} D_{2,t-p} + \gamma_{11} S_{3,t-1} + \cdots + \gamma_{1p} S_{3,t-p} + u_{1,t} \\
D_{2,t} = {} & \beta_{20} + \beta_{21} D_{2,t-1} + \cdots + \beta_{2p} D_{2,t-p} \\
& + \gamma_{21} r_{1,t-1} + \cdots + \gamma_{2p} r_{1,t-p} + \gamma_{21} S_{3,t-1} + \cdots + \gamma_{2p} S_{3,t-p} + u_{2,t} \\
S_{3,t} = {} & \beta_{30} + \beta_{31} S_{3,t-1} + \cdots + \beta_{3p} S_{3,t-p} \\
& + \gamma_{31} r_{1,t-1} + \cdots + \gamma_{3p} r_{1,t-p} + \gamma_{31} D_{2,t-1} + \cdots + \gamma_{3p} D_{2,t-p} + u_{3,t}
\end{aligned}
$$

where $r_{1,t}$ is the bitcoin log returns equation, while $D_{2,t}$ and $S_{3,t}$ are respectively the demand and supply equations. The lags are denoted by p.

4 Data Analysis

4.1 Descriptive analysis

4.1.1 Descriptive statistics

There are 25 variables in the dataset with each one containing 2811 daily observations.

We can see in the descriptive statistics tables that there is high volatility in bitcoin returns but it does not come as a surprise since it is a speculative asset with no quantifiable intrinsic value. The best bitcoin log return is around 20% while the worst is 26%. The returns have fat tails and are moderately skewed.

The variable $\Delta ACTADD$ has a high standard deviation, indicating that it is a very volatile series. It can be understood by the fact that when there are large bitcoin price movements, the number of active addresses usually spikes (to deposit to sell, withdraw after buying or move coins between exchanges to profit from price discrepancies for instance) and is correlated to both prices and the level of excitedness of investors.

Hash rate is also very volatile, and it is due to the mining mechanism and particularly the difficulty adjustment. Indeed, every two weeks the difficulty to mine bitcoins increases or decreases depending on blocks that are mined too quickly or too slowly. It can be caused by macro events of the mining industry, such as electricity usage limitations in the Sichuan region of China where many miners are located (Zhao, 2021).

In aggregate, the mean number of bitcoins deposited to exchanges every day is 843, with a maximum of 96773. The highest number of bitcoins pulled out of exchanges in aggregate is 69789.

In average, 10,97% of the bitcoin supply held is aged between 1 and 3 months, while the fresh coins (less than 24h) represent only 1 to 4% of the bitcoin supply.

TABLE II
DESCRIPTIVE STATISTICS

	Mean	Median	Max	Min	S.D	Skewness	Kurtosis	n
r_t	0.0019	0.0016	0.2042	-0.2652	0.0345	-0.4416	6.4201	2811
$\Delta ACTADD$	0.0009	-0.0083	0.6508	-0.4623	0.1269	0.4679	1.0928	2811
$\Delta ADD1K$	0.0002	0.0000	0.0765	-0.0658	0.0044	1.7692	66.1642	2811
$\Delta SPLY1Y$	0.0001	0.0000	0.0280	-0.0426	0.0025	-2.0276	59.3698	2811
CDD	9081423	5417514	397106800	723058.4	15078634	11.37181	213.3764	2811
DORM	9.7298	6.6095	219.2539	0.0824	12.5327	7.0307	81.1951	2811
$\Delta EXBAP$	0.0015	0.0003	0.3635	-0.4458	0.0203	0.3683	142.859	2811
EXNETF	843.4012	521.3513	96773.47	-69789.45	8249.5872	1.3604	21.1733	2811
HO24H	0.0145	0.0136	0.0407	0.0044	0.0056	0.8967	1.2502	2811
HO1D1W	0.0358	0.0333	0.1095	0.0165	0.0121	1.4216	3.0512	2811
HO1W1M	0.0723	0.0666	0.1745	0.0365	0.0242	1.4632	2.5102	2811
HO1M3M	0.1097	0.0989	0.2460	0.0543	0.0379	1.5415	2.1683	2811
$\Delta HO3M6M$	0.0000	-0.0003	0.1527	-0.1617	0.0183	0.1513	16.9005	2811
$\Delta HO6M12M$	0.0000	-0.0002	0.1333	-0.1210	0.0118	0.1461	21.2122	2811
$\Delta HO1Y2Y$	-0.0001	-0.0003	0.0786	-0.1827	0.0085	-3.8534	96.1361	2811
$\Delta HO2Y3Y$	0.0000	-0.0001	0.1319	-0.1739	0.0104	-0.8524	71.5327	2811

The descriptive statistics are as follows: Mean, Median, Maximum (Max), Minimum (Min), Standard Deviation (S.D), the third moment of each variable distribution (Skewness), the fourth moment of the variable distribution (Kurtosis), and the number of observations (n). rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. ADD1K is the number of addresses with a balance ≥ 1000. SPLY1Y is the percent of supply last active one year plus ago. CDD is the number of coin days destroyed. DORM is the dormancy. EXBAP is the number of bitcoins on exchanges in percent. EXNETF are the exchange net flows. Variables beginning by HO are the Hodl waves. LIVE is bitcoin's liveliness. SUPROFIT is the percent of supply in profit. UTPROFIT is the percent of UTXOs in profit. HASH is the hash rate. FRM is the Fee Ratio Multiple. GOLD are gold price returns. M2 is the money supply. DEFICIT is the federal surplus or deficit. Data was collected from 30th of April 2013 to 11th January 2021.

TABLE III DESCRIPTIVE STATISTICS								
	Mean	Median	Max	Min	S.D	Skewness	Kurtosis	n
Δ*HO3Y5Y*	0.0000	-0.0001	0.1337	-0.1734	0.0069	-5.8494	249.2803	2811
Δ*LIVE*	0.0001	-0.0001	0.0217	-0.0011	0.0011	9.6204	142.3852	2811
Δ*SUPROFIT*	0.0000	0.0009	0.2404	-0.3298	0.0410	-0.1881	4.5502	2811
Δ*UTPROFIT*	0.0000	0.0006	0.3133	-0.5318	0.0408	-1.1452	24.2529	2811
Δ*HASH*	0.0052	0.0046	0.5999	-0.4902	0.1148	0.1727	0.9600	2811
Δ*FRM*	-0.0009	0.0079	2.2753	-1.8090	0.2730	-0.0901	7.1767	2811
Δ*GOLD*	0.0023	-0.0032	0.1037	-0.1172	0.0429	0.0968	-0.0648	2811
Δ*M2*	0.0064	0.0048	0.0625	0.0005	0.0084	4.9309	26.2492	2811
Δ*DEFICIT*	-2345.78	1703.94	801082.33	-618725.44	209335.03	0.3090	1.5925	2811

The table reports descriptive statistics of the times series on a daily basis. The descriptive statistics are as follows: Mean, Median, Maximum (Max), Minimum (Min), Standard Deviation (S.D), the third moment of each variable distribution (Skewness), the fourth moment of the variable distribution (Kurtosis), and the number of observations (n). rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. ADD1K is the number of addresses with a balance ≥ 1000. SPLY1Y is the percent of supply last active one year plus ago. CDD is the number of coin days destroyed. DORM is the dormancy. EXBAP is the number of bitcoins on exchanges in percent. EXNETF are the exchange net flows. Variables beginning by HO are the Hodl waves. LIVE is bitcoin's liveliness. SUPROFIT is the percent of supply in profit. UTPROFIT is the percent of UTXOs in profit. HASH is the hash rate. FRM is the Fee Ratio Multiple. GOLD are gold price returns. M2 is the money supply. DEFICIT is the federal surplus or deficit. Data was collected from 30th of April 2013 to 11th January 2021.

4.1.2 Correlation matrix

The correlation matrix is available in Appendix 1. There is high correlation between *CDD* (coin days destroyed) and *DORM* (dormancy), so the two variables should not ultimately be included in the same model to avoid multicollinearity.

4.2 Stationarity tests

TABLE IV
RESULTS OF THE UNIT ROOT TESTS

	Augmented Dickey Fuller statistic
r_t	-11.66***
Δ*ACTADD*	-17.02***
Δ*ADD1K*	-13.28***
Δ*SPLY1Y*	-9.66***
CDD	-9.96***
DORM	-8.89***
Δ*EXBAP*	-15.06***
EXNETF	-11.29***
HO24H	-5.03***
HO1D1W	-6.57***
HO1W1M	-5.70***
HO1M3M	-5.31***
Δ*HO3M6M*	-10.40***
Δ*HO6M12M*	-10.11***
Δ*HO1Y2Y*	-9.51***
Δ*HO2Y3Y*	-10.41***
Δ*HO3Y5Y*	-9.14***

The table reports the Augmented Dickey-Fuller statistic of the variables included in this study. We test for the presence of a unit root in the variables. The presence of a unit root is not consistent with OLS assumptions.
***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

TABLE V

RESULTS OF THE UNIT ROOT TESTS

	Augmented Dickey Fuller statistic
$\Delta LIVE$	-10.05***
$\Delta SUPROFIT$	-15.14***
$\Delta UTPROFIT$	-13.95***
$\Delta HASH$	-16.05***
ΔFRM	-13.96***
$\Delta GOLD$	-8.29***
$\Delta M2$	-4.08***
$\Delta DEFICIT$	-10.84***

The table reports the Augmented Dickey-Fuller statistic of the variables included in this study. We test for the presence of a unit root in the variables. The presence of a unit root is not consistent with OLS assumptions.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

The results of the Augmented Dickey-Fuller (ADF) tests show that all variables are either stationary at level, at first difference or at percent change (log returns for bitcoin).

4.3 Linear regressions

Demand regression with robust standard errors

Table VI

DIAGNOSTIC TESTS DEMAND

	Test statistic			P-value		
Models	(1)	(2)	(3)	(1)	(2)	(3)
Shapiro-Wilk	0.90	0.90	0.90	0.00***	0.00***	0.00***
Breusch-Pagan	6.23	25.34	28.26	0.01**	0.00***	0.00***
Breusch-Godfrey	187.86	187.72	186.93	0.00***	0.00***	0.00***

This table reports the statistics of diagnostic tests with their respective p-values. Shapiro-Wilk tests normality, Breusch-Pagan tests heteroscedasticity and Breusch-Godfrey tests serial correlation.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

The diagnostic tests show the violation of normality assumptions, but this is expected since the dataset has a large size. And Gaussian models are robust to many non-normality situations (Knief and Forstmeier, 2021). Due to the presence of heteroscedasticity, to avoid biased and inconsistent standard errors, robust standard errors have been estimated.

The demand model demonstrates the significance of the impact of demand on bitcoin returns, as displayed in the table below. However, the explanatory power is low (4%) but can be slightly improved when controlling for security. Macroeconomics do not have an impact. The AIC scores show that adding security and macroeconomics do not improve the model significantly.

TABLE VII DEMAND AND BITCOIN RETURNS			
Dependent var: r_t	(1)	(2)	(3)
ΔACTADD	0.018*** (0.005)	0.011* (0.006)	0.011* (0.007)
ΔHASH		0.005 (0.006)	0.005 (0.006)
ΔFRM		-0.007** (0.003)	-0.007** (0.003)
ΔGOLD			0.010 (0.020)
ΔM2			-0.012 (0.105)
ΔDEFICIT			-0.000* (0.000)
AIC	-10953	-10955	-10952
Adjusted R^2	0.004	0.005	0.005

The table reports the OLS regression coefficients estimates with their respective robust standard errors. The dependent variable rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. ADD1K is the number of addresses with a balance ≥ 1000. SPLY1Y is the percent of supply last active one year plus ago. CDD is the number of coin days destroyed. DORM is the dormancy. EXBAP is the number of bitcoins on exchanges in percent. EXNETF are the exchange net flows. Variables beginning by HO are the Hodl waves. LIVE is bitcoin's liveliness. SUPROFIT is the percent of supply in profit. UTPROFIT is the percent of UTXOs in profit. HASH is the hash rate. FRM is the Fee Ratio Multiple. GOLD are gold price returns. M2 is the money supply. DEFICIT is the federal surplus or deficit. Data was collected from 30th of April 2013 to 11th January 2021.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

Supply regression with robust standard errors

Table VIII DIAGNOSTIC TESTS SUPPLY						
	Test statistic			P-value		
Models	(1)	(2)	(3)	(1)	(2)	(3)
Shapiro-Wilk	0.89	0.89	0.89	0.00***	0.00***	0.00***
Breusch-Pagan	292.22	298.00	307.12	0.00***	0.00***	0.00***
Breusch-Godfrey	34.69	34.11	33.87	0.00***	0.00***	0.00***

This table reports the statistics of diagnostic tests with their respective p-values. Shapiro-Wilk tests normality, Breusch-Pagan tests heteroscedasticity and Breusch-Godfrey tests serial correlation.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

The diagnostic tests have the same results as the demand model. The data exhibits non-normality, heteroscedasticity, and serial correlation.

The supply model is built using variables selected with stepwise regression (combining backward and forward selection). The model has a very good explanatory power, 10.4%, much better than the demand model.

The results reveal that the impact on the percent of supply in profit on bitcoin fluctuations is significant at the 1% level. Exchange net flows (bitcoins moving in and out of exchanges) and the most liquid portions of the supply, represented by the 24h and 1 day to 1 week bitcoin age bands (coins last moved in the last 24 hours and between 1 day to 1 week ago) are also significant at the 10% level.

Controlling for security is significant for both hash rate and the Fee Ratio Multiple (FRM). Like the previous model, adding macroeconomics does not improve it significantly.

TABLE IX

SUPPLY AND BITCOIN RETURNS

Dependent var: r_t	(1)	(2)	(3)
Δ*SUPROFIT*	0.261*** (0.014)	0.259*** (0.014)	0.260*** (0.014)
EXNETF	-0.000* (0.000)	-0.000* (0.000)	-0.000* (0.000)
Δ*LIVE*	-0.926 (0.845)	-0.863 (0.846)	-0.845 (0.837)
HO24H	0.331* (0.200)	0.226 (0.196)	0.218 (0.196)
HO1D1W	0.132* (0.070)	0.166** (0.070)	0.166** (0.070)
Δ*HO1Y2Y*	-0.130 (0.084)	-0.137 (0.084)	-0.136 (0.083)
Δ*HASH*		0.012** (0.005)	0.012** (0.005)
Δ*FRM*		-0.008*** (0.002)	-0.008*** (0.002)
Δ*GOLD*			0.007 (0.017)
Δ*M2*			-0.026 (0.082)
Δ*DEFICIT*			-0.000* (0.000)
AIC	-11244	-11252	-11249
Adjusted R^2	0.104	0.107	0.107

The table reports the OLS regression coefficients estimates with their respective robust standard errors. The dependent variable rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. ADD1K is the number of addresses with a balance ≥ 1000. SPLY1Y is the percent of supply last active one year plus ago. CDD is the number of coin days destroyed. DORM is the dormancy. EXBAP is the number of bitcoins on exchanges in percent. EXNETF are the exchange net flows. Variables beginning by HO are the Hodl waves. LIVE is bitcoin's liveliness. SUPROFIT is the percent of supply in profit. UTPROFIT is the percent of UTXOs in profit. HASH is the hash rate. FRM is the Fee Ratio Multiple. GOLD are gold price returns. M2 is the money supply. DEFICIT is the federal surplus or deficit. Data was collected from 30th of April 2013 to 11th January 2021.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

General multivariate linear model with robust standard errors

TABLE X DIAGNOSTIC TESTS GENERAL MODEL		
	Test statistic	P-value
Shapiro-Wilk	0.89	0.00***
Breusch-Pagan	224.06	0.00***
Breusch-Godfrey	32.38	0.00***

This table reports the statistics of diagnostic tests with their respective p-values. Shapiro-Wilk tests normality, Breusch-Pagan tests heteroscedasticity and Breusch-Godfrey tests serial correlation.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

The tables X and XI display the OLS coefficients and results of the general multivariate linear model as specified in section 3.4. This model analyzes the relationship of bitcoin returns with demand, supply, security, and macroeconomics.

The variables have been selected using both stepwise regression and forward selection and these methods lead to the same choice of variables.

The OLS coefficients indicate that demand has a significant positive effect on bitcoin returns at the 1% confidence level. The percent of the supply in profit has also a significant impact on bitcoin at the 1% confidence level. If the percent of bitcoins last moved 1 week to 1 month ago (relatively liquid portion of the supply) rises by 1%, the price of bitcoin will rise 0.21% in average at the 1% confidence level. The 1 year – 2 years age band is also relevant. The optimal level of the security budget (Fee Ratio Multiple) also negatively impacts bitcoin at the 10%

confidence level. Other variables like exchange net flows and the federal deficit are significant but negligible.

This model shows with a 10.8% adjusted explanatory power that demand, supply and security spending have a significant effect on bitcoin returns.

TABLE XI

GENERAL MODEL

Dependent var: r_t	Estimates
Δ*ACTADD*	0.015*** (0.006)
Δ*SUPROFIT*	0.259*** (0.014)
HO1D1W	0.206*** (0.071)
HO1M3M	-0.026 (0.018)
Δ*HO1Y2Y*	-0.137* (0.082)
EXNETF	-0.000* (0.000)
Δ*FRM*	-0.005* (0.003)
Δ*DEFICIT*	-0.000* (0.000)
AIC	-11257
Adjusted R^2	0.108

The table reports the OLS regression coefficients estimates with their respective robust standard errors. The dependent variable rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. ADD1K is the number of addresses with a balance ≥ 1000. SPLY1Y is the percent of supply last active one year plus ago. CDD is the number of coin days destroyed. DORM is the dormancy. EXBAP is the number of bitcoins on exchanges in percent. EXNETF are the exchange net flows. Variables beginning by HO are the Hodl waves. LIVE is bitcoin's liveliness. SUPROFIT is the percent of supply in profit. UTPROFIT is the percent of UTXOs in profit. HASH is the hash rate. FRM is the Fee Ratio Multiple. GOLD are gold price returns. M2 is the money supply. DEFICIT is the federal surplus or deficit. Data was collected from 30th of April 2013 to 11th January 2021.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

Additional regressions with robust standard errors:

This study develops two additional models to confirm the impact of control variables, security, and macroeconomics. Tables XII to XV are included in the appendix 3.

The regression of security on bitcoin returns shows a significant positive impact on bitcoin returns from hash rate and a negative one from FRM respectively at the 10 and 1% levels of confidence. Notwithstanding the significant effects, the low explanatory power of the model suggests these are not key determinants of bitcoin.

The macroeconomic regression confirms the previous results: macroeconomics does not have a significant effect on bitcoin returns. At least for the three chosen proxies: gold returns, M2 money supply and the Federal Deficit or Surplus. The model like previous ones does not hold normality assumptions, except for homoscedasticity.

4.4 Vector Autoregressions

The objective of the Vector Autoregressive model of this paper is to model at the same time bitcoin returns, supply and demand. Each VAR model has 3 equations, one for bitcoin log returns, one for demand and one for supply. The equation of bitcoin returns is always the same, along the demand one since there is only one demand variable, the number of daily active addresses. However, to account for the 17 different supply variables and find the best models, 17 models have been developed.

Modelling bitcoin log returns

TABLE XVI

DIAGNOSTIC TESTS VAR MODEL 1

	Test statistic	P-value
Jarque-Bera	6615.60	0.00***
Portmanteau Q	1313.80	0.00***
Breusch-Godfrey	222.73	0.00***

This table reports the statistics of diagnostic tests with their respective p-values. Jarque-Bera tests normality, Portmanteau Q tests for residual heteroscedasticity and Breusch-Godfrey tests serial correlation.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

The tables XVI and XVII display the results of a VAR model that best predict bitcoin log returns, as a function of lagged returns, supply, and demand. This VAR has 8 lags, chosen after the AIC criterion, which is an estimator of prediction error and of the relative quality of statistical models.

The equations of bitcoin returns and demand have both good explanatory power, but not for the supply equation.

Bitcoin returns seem to be significantly affected by lags of returns (1,2,4,5 and 6), the daily active addresses (lags 1 and 2) and the percent of supply in profit for the first three lags. Together, these variables explain 26.3% of the bitcoin fluctuations, which is a better result than the general multivariate model.

TABLE XVII VAR MODEL 1			
VAR(8)	(1)	(2)	(3)
r_{t-1}	0.059***	0.162**	−0.013
	(0.022)	(0.070)	(0.030)
$\Delta ACTADD_{t-1}$	0.012**	-0.607***	-0.020
	(0.006)	(0.019)	(0.008)
$\Delta SUPROFIT_{t-1}$	0.403***	0.116**	-0.170***
	(0.016)	(0.0508)	(0.021)
r_{t-2}	-0.054**	0.235***	-0.009
	(0.022)	(0.070)	(0.030)
$\Delta ACTADD_{t-2}$	0.012*	-0.530***	0.003
	(0.007)	(0.022)	(0.009)
$\Delta SUPROFIT_{t-2}$	0.059***	-0.022	-0.043*
	(0.019)	(0.061)	(0.026)
r_{t-3}	0.022	0.229***	0.036
	(0.022)	(0.070)	(0.030)
$\Delta ACTADD_{t-3}$	0.012	-0.484***	-0.001
	(0.007)	(0.023)	(0.010)
$\Delta SUPROFIT_{t-3}$	0.051***	-0.087	-0.073***
	(0.019)	(0.060)	(0.026)
r_{t-4}	0.070***	0.010	-0.009
	(0.022)	(0.070)	(0.030)
$\Delta ACTADD_{t-4}$	0.008	-0.428***	0.009
	(0.007)	(0.024)	(0.010)
$\Delta SUPROFIT_{t-4}$	-0.006	-0.041	-0.080***
	(0.019)	(0.060)	(0.026)
r_{t-5}	0.046**	-0.035	-0.011
	(0.021)	(0.069)	(0.030)
$\Delta ACTADD_{t-5}$	0.007	-0.442***	0.010
	(0.007)	(0.024)	(0.010)
$\Delta SUPROFIT_{t-5}$	-0.023	0.032	-0.034
	(0.019)	(0.060)	(0.025)
r_{t-6}	0.068***	0.108	-0.028
	(0.021)	(0.069)	(0.030)
$\Delta ACTADD_{t-6}$	0.005	-0.308***	0.002
	(0.007)	(0.023)	(0.010)
$\Delta SUPROFIT_{t-6}$	-0.006	0.050	0.010
	(0.018)	(0.060)	(0.025)
r_{t-7}	0.023	-0.076	-0.070**
	(0.021)	(0.069)	(0.030)
$\Delta ACTADD_{t-7}$	0.008	0.172***	0.007
	(0.007)	(0.022)	(0.009)
$\Delta SUPROFIT_{t-7}$	-0.009	0.073	0.011
	(0.018)	(0.059)	(0.025)
r_{t-8}	-0.018	-0.028	-0.059**
	(0.017)	(0.057)	(0.024)
$\Delta ACTADD_{t-8}$	-0.003	0.098***	-0.012
	(0.006)	(0.019)	(0.008)
$\Delta SUPROFIT_{t-8}$	-0.004	-0.010	0.032
	(0.017)	(0.055)	(0.023)
R^2	0.269	0.446	0.044
Adjusted R^2	0.263	0.441	0.036

The table reports the OLS regression coefficients estimates with their respective standard errors. The dependent variable rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. ADD1K is the number of addresses with a balance ≥ 1000. SPLY1Y is the percent of supply last active one year plus ago. CDD is the number of coin days destroyed. DORM is the dormancy. EXBAP is the number of bitcoins on exchanges in percent. EXNETF are the exchange net flows. Variables beginning by HO are the Hodl waves. LIVE is bitcoin's liveliness. SUPROFIT is the percent of supply in profit. UTPROFIT is the percent of UTXOs in profit. HASH is the hash rate. FRM is the Fee Ratio Multiple. GOLD are gold price returns. M2 is the money supply. DEFICIT is the federal surplus or deficit. Data was collected from 30th of April 2013 to 11th January 2021, from various data providers and are daily observations. (1) is the first equation of the VAR model, bitcoin log returns. (2) is the second equation of the VAR model, demand. (3) is the third equation of the VAR model, supply.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

TABLE XVIII DIAGNOSTIC TESTS VAR MODEL 2		
	Test statistic	P-value
Jarque-Bera	21525.00	0.00***
Portmanteau Q	1200.10	0.00***
Breusch-Godfrey	120.86	0.00***

This table reports the statistics of diagnostic tests with their respective p-values. Jarque-Bera tests normality, Portmanteau Q tests for residual heteroscedasticity and Breusch-Godfrey tests serial correlation.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

The VAR(8) modelling best supply and demand presents interesting results on the supply equation. Indeed, 99.6% of supply fluctuations as proxied by the bitcoin age band of 1 month to 3 months (relatively liquid portion of the supply) are explained by lagged values of itself, lagged values of active addresses (significant effect at lags 2,3,4,7 and 8) and lagged values of returns (1 and 8). This demonstrates that the supply is affected by the demand and that they interact with each other, as expected in the conceptual framework and especially by the Law of Demand and Supply.

Furthermore, the returns themselves seem to significantly affect the supply and demand equations, which could be explained by investor behavior: large increases of bitcoin price attract more buyers and large decreases attract more sellers.

The demand equation has also the best explanatory power of all VAR models with 44.4%. Lagged demand, returns and supply have a significant impact on demand.

TABLE XIX

VAR MODEL 2

VAR(8)	(1)	(2)	(3)
r_{t-1}	0.261***	0.212***	-0.002*
	(0.019)	(0.055)	(0.001)
$\Delta ACTADD_{t-1}$	0.009	-0.614***	-0.000
	(0.006)	(0.019)	(0.000)
	0.096	-1.477**	1.254***
$HO1M3M_{t-1}$	(0.259)	(0.746)	(0.019)
r_{t-2}	-0.097***	0.158***	-0.000
	(0.020)	(0.057)	(0.001)
$\Delta ACTADD_{t-2}$	0.008	-0.537***	0.001*
	(0.008)	(0.022)	(0.000)
	-0.293	0.673	-0.203***
$HO1M3M_{t-2}$	(0.416)	(1.198)	(0.030)
r_{t-3}	0.034*	0.179***	0.001
	(0.020)	(0.057)	(0.001)
$\Delta ACTADD_{t-3}$	0.014*	-0.480***	0.002***
	(0.008)	(0.024)	(0.001)
	0.468	0.840	-0.010
$HO1M3M_{t-3}$	(0.419)	(1.207)	(0.030)
r_{t-4}	0.033*	0.024	-0.001
	(0.020)	(0.057)	(0.001)
$\Delta ACTADD_{t-4}$	0.008	-0.414***	0.001**
	(0.008)	(0.024)	(0.001)
	-0.481	0.823	0.027
$HO1M3M_{t-4}$	0.419	(1.207)	(0.030)
r_{t-5}	0.012	-0.019	-0.000
	(0.020)	(0.057)	(0.001)
$\Delta ACTADD_{t-5}$	0.014*	-0.421***	0.001
	(0.008)	(0.024)	(0.001)
	0.361	1.415	-0.050
$HO1M3M_{t-5}$	(0.419)	(1.206)	(0.030)
r_{t-6}	0.058***	0.165***	0.001
	(0.020)	(0.056)	(0.001)
$\Delta ACTADD_{t-6}$	0.010	-0.292***	-0.001
	(0.008)	(0.024)	(0.000)
	-0.004	-1.578	0.011
$HO1M3M_{t-6}$	(0.418)	(1.205)	(0.030)
r_{t-7}	0.002	-0.059	0.001
	(0.019)	(0.056)	(0.001)
$\Delta ACTADD_{t-7}$	0.009	0.172***	-0.002***
	(0.009)	(0.022)	(0.000)
	-0.831**	-2.830**	0.051*
$HO1M3M_{t-7}$	(0.415)	(1.195)	(0.030)
r_{t-8}	-0.039**	-0.048	-0.005***
	(0.019)	(0.054)	(0.001)
$\Delta ACTADD_{t-8}$	0.001	0.093***	-0.001***
	(0.006)	(0.019)	(0.000)
	0.673***	2.106***	-0.084***
$HO1M3M_{t-8}$	(0.259)	(0.745)	(0.019)
R^2	0.080	0.449	0.996
Adjusted R^2	0.072	0.444	0.996

The table reports the OLS regression coefficients estimates with their respective standard errors. The dependent variable rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. ADD1K is the number of addresses with a balance ≥ 1000. SPLY1Y is the percent of supply last active one year plus ago. CDD is the number of coin days destroyed. DORM is the dormancy. EXBAP is the number of bitcoins on exchanges in percent. EXNETF are the exchange net flows. Variables beginning by HO are the Hodl waves. LIVE is bitcoin's liveliness. SUPROFIT is the percent of supply in profit. UTPROFIT is the percent of UTXOs in profit. HASH is the hash rate. FRM is the Fee Ratio Multiple. GOLD are gold price returns. M2 is the money supply. DEFICIT is the federal surplus or deficit. Data was collected from 30th of April 2013 to 11th January 2021, from various data providers and are daily observations. (1) is the first equation of the VAR model, bitcoin log returns. (2) is the second equation of the VAR model, demand. (3) is the third equation of the VAR model, supply.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

4.5 Testing Granger causality

TABLE XX GRANGER CAUSALITY				
VAR MODEL	Variables	F statistic	P-value	Interpretation
1	$r_t \rightarrow \Delta ACTADD_t$	3.128	0.000***	Granger causality
	$\Delta ACTADD_t \rightarrow r_t$	1.250	0.221	No Granger causality
	$\Delta SUPROFIT_t \rightarrow r_t + \Delta ACTADD_t$	46.009	0.000***	Granger causality
2	$r_t \rightarrow \Delta ACTADD_t$	4.729	0.000***	Granger causality
	$\Delta ACTADD_t \rightarrow r_t$	5.473	0.000***	Granger causality
	$HO1M3M_t \rightarrow r_t + \Delta ACTADD_t$	2.090	0.006***	Granger causality

This table reports the Granger causality test statistics. The null hypothesis states that Xt does not Granger cause Yt. The variable rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. SUPROFIT is the percent of supply in profit. Variables beginning by HO are the Hodl waves.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

The results of the causality tests clearly show causality and confirm the significance of supply and demand effects on bitcoin returns, as previously explored in the VAR models. In the first VAR model, the log returns of bitcoin Granger cause the number of daily active addresses while the percent of supply in profit and the active addresses Granger cause the bitcoin returns. The second VAR model shows the same results. Therefore, this paper demonstrates the causality between bitcoin returns and demand/supply. Furthermore, there is evidence of a bidirectional causal relationship between bitcoin returns and demand, as proxied by active addresses.

4.6 Summary of significant determinants

The table XXI reports the variables that have been found as significant drivers of bitcoin returns, across the entire data analysis.

TABLE XXI BITCOIN RETURNS DETERMINANTS		
Categories	Variables	Granger causality
Demand	*ΔACTADDt-p*	*Yes*
Supply	*ΔSUPROFITt-p* *HO24H* *HO1D1W* *HO1M3Mt-p* *ΔHO1Y2Y* *EXNETF*	*Yes* *Yes*
Control variables	*ΔHASH* *ΔFRM* *ΔDEFICIT*	
Others	*rt-p*	
The dependent variable rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. Variables beginning by HO are the Hodl waves. SUPROFIT is the percent of supply in profit. EXNETF are the exchange net flows. HASH is the hash rate. FRM is the Fee Ratio Multiple. DEFICIT is the federal surplus or deficit. Data was collected from 30th of April 2013 to 11th January 2021.		

4.7 Discussion of findings

This research paper attempts to find the supply and demand determinants of bitcoin fluctuations, first by estimating linear models and then by estimating two VAR models that model simultaneously bitcoin returns, supply and demand.

The general multivariate model showed that demand is a significant driver of bitcoin, along with supply (percent of supply in profit and some bitcoin age bands) and security. Macroeconomics is not a significant determinant.

The demand and supply linear regressions confirmed the results of the first model and revealed that the security control variables are also significant but only have a minor impact.

The VAR models have much better results compared to the linear models, since the first VAR(8) explains 26.3% of bitcoin fluctuations compared to 10.8% of the general model.

The statistically significant determinants behind this model are the daily active addresses, the lagged returns, and the percent of the supply in profit. The rationale behind this last driver is probably linked to the fact that when a large portion of the supply is profitable, sophisticated investors sell and thus affect returns. The second VAR(8) also modeled the supply and demand, with significant and powerful results. Modelling supply using the bitcoin returns, the demand and supply (a bitcoin age band) demonstrates that the law of supply interacts with the law of demand.

The first hypothesis of this paper can be validated based on the empirical findings. As a matter of fact, the demand is positively correlated with bitcoin returns on all models. The demand is a significant driver of bitcoin returns in the general multivariate model and this is also confirmed both in the demand regression and the VAR models. The second hypothesis of this study can also be validated because the supply dynamics affect bitcoin returns. Interestingly, this relationship is not unidirectional since bitcoin returns also affect supply. The third and last hypothesis is consistent with the empirical results although in a smaller extent. Indeed, the level of security affect bitcoin returns significantly. An increase in the hash rate, which is a proxy for the level of security corresponds to an increase in bitcoin returns. An increase in the Fee Ratio Multiple (FRM) leads to a decrease in bitcoin returns, which is consistent with the ratio itself because a higher FRM indicates less security of the network in the long run. Surprisingly, macroeconomics does not affect bitcoin fluctuations, even the money supply, which contradicts that bitcoin is a hedge against inflation and is digital gold.

This paper goes further than validating the hypotheses and demonstrate causality effects between bitcoin returns, demand and supply. More specifically, the bitcoin log returns, and demand (daily active addresses) exhibit a bidirectional relationship. Supply, as proxied by the percent of supply in profit or the portion of the bitcoin supply aged from 1 to 3 months also Granger cause bitcoin returns.

These results are consistent with the conceptual framework developed for this research. Indeed, the theory of supply and demand is empirically confirmed for Bitcoin since demand and supply both affect bitcoin log returns. Furthermore, it is demonstrated with a Vector Autoregressive (VAR) approach that supply and demand interact with each other. Bitcoin returns themselves impact supply and demand. This is expected and can be explained by investor behavior: for instance, a higher bitcoin price attracts new investors. The level of security and the security budget are also linked to bitcoin returns, confirming the fact that Proof Of Work (PoW) and therefore mining is a valuable service to the users of the protocol and giving Bitcoin unique properties. The findings are also consistent with the literature: demand, supply and security are key drivers of bitcoin price.

5 Conclusion

There is no consensus on the fair and intrinsic value of bitcoin, explaining its high volatility. Therefore, bitcoin has a subjective value, dictated by supply and demand interactions on bitcoin markets (exchanges). With no models, it is however possible to identify determinants of the bitcoin price. The Bitcoin's blockchain being transparent and auditable (in a pseudonymous way), it is possible to track the movements of bitcoins and identify behavior of selling or holding for instance.

This paper used on-chain data to examine the supply and demand effects on bitcoin returns, while controlling for security spending and macroeconomic factors. Empirical evidence has been found about the demand and supply effects on bitcoin returns, as well as for security. The daily active addresses (demand) are a significant determinant and have a causal bidirectional relationship with returns. Supply is also a statistically significant driver and Granger causes bitcoin returns. This answers the research questions of this paper.
Most importantly, this paper showed the relevance of blockchain data, and why it can be used as a tool to get insights about price movements.

This study used only one variable to proxy demand, and it can be argued that increasing the number of demand variables could improve the models. The literature uses other proxies beyond the scope of this study that blockchain data is, such as the number of Bitcoin wallets created, queries on Bitcoin, or social media attention. The potential number of supply variables is also extendable, and more drivers could be tested.

There are also only three proxies for controlling macroeconomics, and future research could use many other variables, such as stock indices. Recently, the Covid crisis caused a market meltdown in risk-on assets like equities and Bitcoin. This is possibly indicating correlation between stock indices and Bitcoin.

Finally, after demonstrating that on-chain data drives bitcoin returns, it can be asked how this knowledge can be transformed into actionable insights. Indeed, a systematic trading strategy could be built based on on-chain metrics as trading indicators, since some market participants are already using them (Maddrey and CoinMetrics, 2020).

Bibliography

Scientific articles and books

Adjei, F., 2019. Determinants of Bitcoin Expected Returns. Journal of Finance and Economics, 7, pp.42-47.

Bartos, J., 2015. Does Bitcoin follow the hypothesis of efficient market? International Journal of Economic Sciences, IV(2), pp.10-23.

Bouoiyour, J. and Selmi, R., 2015. What Does Bitcoin Look Like? Annals of Economics and Finance, 16, pp.449-492.

Brooks, C., 2019. Introductory econometrics for finance. 4th ed. Cambridge: Cambridge University Press.

Ciaian, P., Rajcaniova, M. and Kancs, d., 2014. The economics of BitCoin price formation. Applied Economics, 48(19), pp.1799-1815.

Fama, E., 1970. Efficient Capital Markets: A Review of Theory and Empirical Work. Journal of Finance, 25(2), pp.383–417.

Granger, C., 1969. Investigating Causal Relations by Econometric Models and Cross-spectral Methods. Econometrica, 37(3), pp.424-438.

Huhtinen, T., 2014. Bitcoin as a monetary system: Examining attention and attendance. [online] Available at: <https://aaltodoc.aalto.fi/handle/123456789/13667> [Accessed 10 June 2021].

Kei, B., Jin, C., Yi, N., Sin, W. and Ling, W., 2019. The determinants of crypto currency price: the case of Bitcoin. [online] Available at: <https://www.semanticscholar.org/paper/The-determinants-of-crypto-currency-price%3A-the-case-Woo-Boon/d48acb9ba99109ee529b7c4f5277766f3ba1c89d> [Accessed 10 June 2021].

Kjærland, F., Meland, M., Oust, A. and Øyen, V., 2018. How can Bitcoin Price Fluctuations be Explained? International Journal of Economics and Financial Issues, 8(3), pp.323-332.

Knief, U. and Forstmeier, W., 2021. Violating the normality assumption may be the lesser of two evils. Behavior Research Methods, [online] Available at: <https://doi.org/10.3758/s13428-021-01587-5> [Accessed 10 June 2021].

Li, X. and Wang, C., 2016. The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin. [online] Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0167923616302111?via%3Dihub> [Accessed 10 June 2021].

Panagiotidis, T., Stengos, T. and Vravosinos, O., 2018. On the determinants of bitcoin returns: A LASSO approach. Finance Research Letters, 27, pp.235-240.

Panagiotidis, T., Stengos, T. and Vravosinos, O., 2019. A Principal Component-Guided Sparse Regression Approach for the Determination of Bitcoin Returns. SSRN Electronic Journal.

Peterson, T., 2018. Metcalfe's Law as a Model for Bitcoin's Value. Alternative Investment Analyst Review, Q2 2018, 7(2), pp.9-18.

Polasik, M., Piotrowska, A., Wisniewski, T., Kotkowski, R. and Lightfoot, G., 2014. Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry. SSRN Electronic Journal.

Smith, R., 2018. Bitcoin Average Dormancy: A Measure of Turnover and Trading Activity. Ledger, 3.

Sukamulja, S. and Sikora, C., 2018. The new era of financial innovation: the determinants of Bitcoin's price. Journal of Indonesian Economy and Business, 33(1), p.46.

William, S. and Michael, D., 2014. Does the Velocity of Bitcoins Effect the Price Level of Bitcoin? [online] Available at:

<https://www.academia.edu/8210293/Does_the_Velocity_of_Bitcoins_Effect_the_Price_Level_of_Bitcoin> [Accessed 10 June 2021].

X. Yang, Y. Chen and X. Chen, "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information," *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 261-265, doi: 10.1109/Blockchain.2019.00041.

Web resources

Bitwise Asset Management. 2019. Analysis of Real Bitcoin Trade Volume. [online] Available at: <https://static.bitwiseinvestments.com/Research/Bitwise-Asset-Management-Analysis-of-Real-Bitcoin-Trade-Volume.pdf> [Accessed 10 June 2021].

Blummer, T., 2018. Liveliness of Bitcoin. [online] Medium. Available at: <https://medium.com/@tamas.blummer/liveliness-of-bitcoin-174001d016da> [Accessed 10 June 2021].

Crypto51, 2021. PoW 51% attack cost. [online] Available at: <https://www.crypto51.app> [Accessed 10 June 2021].

Kharif, O., 2020. 169-Year-Old MassMutual Invests $100 Million in Bitcoin. Bloomberg, [online] Available at: <https://www.bloomberg.com/news/articles/2020-12-10/169-year-old-insurer-massmutual-invests-100-million-in-bitcoin> [Accessed 10 June 2021].

Kraken Intelligence. 2020. Bitcoin's True Hashrate. [online] Available at: <https://kraken.docsend.com/view/gvyiece7hzwvds94> [Accessed 10 June 2021].

Leibowitz, M., 2018. Introducing: Fee Ratio Multiple (FRM). [online] Medium. Available at: <https://medium.com/coinmonks/introducing-fee-ratio-multiple-frm-1eada9ac9bec> [Accessed 10 June 2021].

Maddrey, N. and Coin Metrics, 2020. Bitcoin On-Chain Indicators Primer. [online] Coin Metrics. Available at: <https://f.hubspotusercontent00.net/hubfs/5264302/The%20Coin%20Metrics%20Bitcoin%20On-Chain%20Indicators%20Primer.pdf> [Accessed 10 June 2021].

McKinney, J., 2018. Bitcoin Security Part I: A Negative Exponential. [online] jordanmmck. Available at: <https://www.jordanmmck.com/crypto/bitcoin-security> [Accessed 10 June 2021].

McSweeney, M., 2021. El Salvador's president announces legislative proposal to declare bitcoin legal tender. The Block, [online] Available at: <https://www.theblockcrypto.com/linked/107381/el-salvador-bitcoin-legal-tender> [Accessed 10 June 2021].

MicroStrategy, 2020. MicroStrategy Announces Over $1B in Total Bitcoin Purchases in 2020. [online] Available at: <https://www.microstrategy.com/en/company/company-videos/microstrategy-announces-over-1b-in-total-bitcoin-purchases-in-2020> [Accessed 10 June 2021].

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. [online] Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 10 June 2021].

Sinclair, S., 2020. Citibank Analyst Says Bitcoin Could Pass $300K by December 2021. Coindesk, [online] Available at: <https://www.coindesk.com/citibank-bitcoin-gold-318k-2021> [Accessed 10 June 2021].

Zhao, W., 2021. Bitcoin hash rate drops as Sichuan miners face short-term power cap. The Block, [online] Available at: <https://www.theblockcrypto.com/post/105464/bitcoin-hash-rate-sichuan-miner-power-limit> [Accessed 10 June 2021].

Appendix

Appendix 1: Correlation matrix

	RT	CDD	EXNETF	HO24H	HO1D1W	HO1W1M	HO1M3M	DORM	ΔSUPROFIT	ΔACTADD	ΔADD1K	ΔHASH	ΔFRM	ΔEXBAP	ΔLIVE	ΔSPLY1Y	ΔHO3M6M	ΔHO6M12M	ΔHO1Y2Y	ΔHO2Y3Y	ΔHO3Y5Y	ΔGOLD	ΔM2	ΔDEFICIT
RT	1																							
CDD	-0.005	1																						
EXNETF	-0.050	0.167	1																					
HO24H	0.053	0.400	0.145	1																				
HO1D1W	0.055	0.214	0.063	0.439	1																			
HO1W1M	0.020	0.123	0.054	0.290	0.544	1																		
HO1M3M	-0.022	0.006	0.029	-0.013	0.146	0.410	1																	
DORM	-0.016	0.832	0.076	0.140	0.060	0.031	-0.012	1																
ΔSUPROFIT	0.310	-0.049	-0.031	-0.024	-0.022	-0.022	-0.014	-0.036	1															
ΔACTADD	0.066	0.085	0.091	0.131	-0.068	-0.004	-0.004	0.058	0.015	1														
ΔADD1K	-0.001	0.095	-0.033	0.026	-0.014	-0.025	-0.001	0.096	-0.016	0.006	1													
ΔHASH	0.005	0.000	0.034	0.022	0.009	0.023	0.026	-0.002	-0.029	0.235	0.040	1												
ΔFRM	-0.064	-0.071	-0.041	-0.154	0.084	0.011	0.014	-0.039	-0.049	-0.347	0.015	0.384	1											
ΔEXBAP	-0.031	0.048	0.510	0.093	0.030	0.052	0.027	0.023	-0.005	0.058	-0.045	0.021	-0.026	1										
ΔLIVE	-0.011	0.553	0.132	0.411	0.301	0.153	0.019	0.391	-0.050	0.011	0.033	0.011	-0.015	0.081	1									
ΔSPLY1Y	-0.030	-0.607	-0.069	-0.298	-0.213	-0.137	-0.070	-0.498	0.024	-0.050	-0.054	-0.011	0.022	-0.037	-0.458	1								
ΔHO3M6M	-0.022	-0.068	-0.037	-0.061	-0.014	0.035	0.171	-0.074	0.004	0.022	0.069	-0.022	-0.029	-0.050	-0.059	0.017	1							
ΔHO6M12M	0.012	-0.123	-0.035	-0.185	-0.053	-0.009	0.071	-0.092	0.010	-0.011	-0.034	0.010	0.035	0.003	-0.135	-0.289	-0.378	1						
ΔHO1Y2Y	-0.041	-0.157	-0.007	-0.173	-0.132	-0.098	-0.016	-0.139	0.006	-0.013	0.038	-0.018	-0.020	-0.030	-0.144	0.585	0.008	-0.273	1					
ΔHO2Y3Y	-0.007	-0.225	-0.012	-0.093	-0.081	-0.034	-0.047	-0.190	0.008	-0.005	-0.069	0.004	0.006	-0.003	-0.214	0.287	0.017	-0.011	-0.360	1				
ΔHO3Y5Y	0.017	-0.455	-0.072	-0.079	-0.033	-0.044	-0.039	-0.333	-0.002	-0.058	-0.062	0.015	0.047	-0.007	-0.151	0.208	0.016	0.006	0.004	-0.237	1			
ΔGOLD	0.013	0.039	0.029	0.015	0.001	-0.045	-0.055	0.027	0.021	0.012	0.006	0.005	-0.008	-0.010	-0.002	0.011	0.023	-0.045	0.010	0.010	-0.018	1		
ΔM2	0.004	-0.028	-0.080	-0.061	-0.067	-0.079	-0.117	0.042	0.018	0.002	-0.011	-0.005	-0.013	-0.022	-0.040	0.008	-0.013	-0.011	-0.003	0.009	0.039	0.169	1	
ΔDEFICIT	-0.033	0.007	0.013	-0.022	-0.005	0.043	-0.050	0.001	-0.006	-0.006	0.010	0.001	0.005	-0.016	0.007	0.014	0.002	-0.030	0.013	0.009	0.009	0.008	-0.115	1

Appendix 2: R code

The empirical analysis of this paper has been realized in R, a programming language designed for statistical computing and graphics. The source code is publicly accessible on the following link: https://rstudio.cloud/project/238096.

Appendix 3: additional linear regressions

TABLE XII

DIAGNOSTIC TESTS SECURITY

	Test statistic	P-value
Shapiro-Wilk	0.90	0.00***
Breusch-Pagan	26.15	0.00***
Breusch-Godfrey	189.15	0.00***

This table reports the statistics of diagnostic tests with their respective p-values. Shapiro-Wilk tests normality, Breusch-Pagan tests heteroscedasticity and Breusch-Godfrey tests serial correlation.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

TABLE XIII

SECURITY AND BITCOIN RETURNS

Dependent var: r_t	Estimates
ΔFRM	-0.010*** (0.003)
$\Delta HASH$	0.010* (0.005)
AIC	-10953
Adjusted R^2	0.004

The table reports the OLS regression coefficients estimates with their respective robust standard errors. The dependent variable rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. ADD1K is the number of addresses with a balance ≥ 1000. SPLY1Y is the percent of supply last active one year plus ago. CDD is the number of coin days destroyed. DORM is the dormancy. EXBAP is the number of bitcoins on exchanges in percent. EXNETF are the exchange net flows. Variables beginning by HO are the Hodl waves. LIVE is bitcoin's liveliness. SUPROFIT is the percent of supply in profit. UTPROFIT is the percent of UTXOs in profit. HASH is the hash rate. FRM is the Fee Ratio Multiple. GOLD are gold price returns. M2 is the money supply. DEFICIT is the federal surplus or deficit. Data was collected from 30th of April 2013 to 11th January 2021.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

TABLE XIV

DIAGNOSTIC TESTS MACROECONOMICS

	Test statistic	P-value
Shapiro-Wilk	0.90	0.00***
Breusch-Pagan	2.69	0.44
Breusch-Godfrey	190.48	0.00***

This table reports the statistics of diagnostic tests with their respective p-values. Shapiro-Wilk tests normality, Breusch-Pagan tests heteroscedasticity and Breusch-Godfrey tests serial correlation.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.

TABLE XV

MACROECONOMICS AND BITCOIN RETURNS

Dependent var: r_t	Estimates
$\Delta GOLD$	-0.011 (0.015)
$\Delta M2$	-0.010 (0.080)
$\Delta DEFICIT$	-0.000* (0.000)
AIC	-10940
Adjusted R^2	0.000

The table reports the OLS regression coefficients estimates with their respective robust standard errors. The dependent variable rt is the log returns of bitcoin. ACTADD is the number of daily active addresses. ADD1K is the number of addresses with a balance ≥ 1000. SPLY1Y is the percent of supply last active one year plus ago. CDD is the number of coin days destroyed. DORM is the dormancy. EXBAP is the number of bitcoins on exchanges in percent. EXNETF are the exchange net flows. Variables beginning by HO are the Hodl waves. LIVE is bitcoin's liveliness. SUPROFIT is the percent of supply in profit. UTPROFIT is the percent of UTXOs in profit. HASH is the hash rate. FRM is the Fee Ratio Multiple. GOLD are gold price returns. M2 is the money supply. DEFICIT is the federal surplus or deficit. Data was collected from 30th of April 2013 to 11th January 2021.

***, ** and * denotes statistical significance at the 1%, 5% and 10% level respectively.