UNIVERSIDAD AUTÓNOMA DE MADRID

FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

TRABAJO FIN DE GRADO

Disentangling Tangle: A Statistical Analysis on the In(efficiency) of IOTA

Oscar Eizaguirre Madère

Grado en Economía y Finanzas (4º)
2017-2021

TUTORA
Beatriz De Blas Pérez

MADRID
Mayo 2021

Abstract

There is a race in the cryptocurrency domain to be considered a widely accepted means of payment and supplant conventional 'government money' in the global monetary order. As of today, it is impossible to pronounce with certainty which cryptocurrencies will achieve universal adoption. Nonetheless, we examine a promising cryptocurrency (IOTA), and the rationale behind the possibility that this cryptocurrency succeeds in being implemented as a distributed ledger for global transactions (especially in the Internet of Things ecosystem). Furthermore, we contribute to the literature of IOTA by analysing IOTA's economic attributes. In particular, those related to market efficiency in the context of Fama (1970). We use Urquhart (2016) and Aslaksen and Wiersdalen (2019) as a mould for searching for evidence of weak-form efficiency in the IOTA market by employing a battery of statistical tests. The results we obtain are ambiguous; some of the tests performed suggest that the IOTA market is inefficient, while others point towards the possibility of it being weak-form efficient. Overall, there is slightly more evidence of inefficiency in the data, and therefore our conclusion is that the IOTA market is inefficient within the meaning of the Efficient Market Hypothesis. Urquhart (2016) and Aslaksen and Wiersdalen (2019) show that Bitcoin may be becoming more efficient with time as some of the tests performed suggest that more recent observations are somewhat more random. We do not find this to be true for our study, perhaps owing to the fact that IOTA's market is less mature and developed than Bitcoin's.

Key Words: post-quantum cryptography, efficient market hypothesis, cryptocurrency.

JEL Classification: G12, G14, E42.

Table of Contents

List of Figures

List of Tables

1 Introduction

Currencies and means of payment have evolved continuously over the past millennia. Modern payment systems have adapted to the technological innovations of the 21st century and many revolve around electronic payments for e-commerce and internet banking. The most prominent innovation, arguably, of the last 15 years has been cryptocurrencies (digital currencies secured by cryptography[1]). These digital currencies aim to achieve widespread adoption and consolidate themselves as a secure, fast and low-cost means of payment for the digital future that is to come. However, there is still a long way to go until this happens, mainly because our modern lives do not yet require the use of cryptos, and even if they did, most cryptocurrencies are not yet ready to be used by society as a whole.

The 'Blockchain Trilemma' states that current cryptocurrencies fail at being scalable, secure and decentralised (explained in further sections) simultaneously. For this reason, we focus on a particular cryptocurrency that has the potential to resolve the aforementioned trilemma, IOTA.

Prior literature on IOTA has mainly focused on the underlying mechanisms of the technology it uses and on its applications. We propose an alternative area of study for the IOTA literature—the economic, and analyse the possible price predictability of the cryptocurrency. Similar research on price predictability has been done for other cryptocurrencies (mainly Bitcoin). The existence of price predictability allows for opportunities to beat the market. In contrast, the absence of it is evidence of random prices and efficient markets, and therefore the impossibility to beat the market.

This paper builds on earlier research, in particular the findings of Urquhart (2016) and Aslaksen and Wiersdalen (2019) regarding Bitcoin's market efficiency. Both papers suggest that even though the initial stages of the Bitcoin market showed substantial signs of inefficiency, the more recent stages provided some evidence for an evolution towards weak-form efficiency and randomness in the returns series. This paper aims to follow the previously mentioned research's methodology and analysis applied to IOTA instead of Bitcoin. We are especially interested in finding out whether the move towards efficiency detected in Bitcoin can also be observed in IOTA, since the cryptocurrency that we analyse was developed seven years later.[2]

[1] Cryptography is the method of providing security for information and communication through the use of coding and encryption.
[2] Bitcoin was created in January 2009 whereas IOTA was released in July 2016.

Even though we perform six statistical tests, we do not find concrete evidence of efficiency (or lack of) in the IOTA market. Although, we do believe that overall there is slightly more evidence to suggest that historical prices may have explanatory power in future IOTA prices (i.e., that the IOTA market is inefficient). An inefficient market within the meaning of Fama (1970) allows for the possibility of investors to use technical analysis to beat the market.

This paper is structured as follows. Sections 2 and 3 explain briefly the history of money and cryptocurrencies, and Blockchain and Tangle technologies. The fourth section of this study introduces the cryptocurrency IOTA and the Efficient Market Hypothesis. Section 5 is dedicated to explaining what data we use and why, and perform a brief analysis to portray the descriptive statistics of our data. The following two sections (6 and 7) are intended to define the statistical tests we employ and analyse their results. Section 8 provides a conclusion for the results we obtain in the context of the Efficient Market Hypothesis and provides some ideas for further research regarding the factors that may be driving IOTA's price. Given the novelty of the topics being dealt with in this paper, we provide definitions for some of the most recurrent terms in Appendix A. Finally, in order to facilitate further research, we have included all the R code we have used to create our figures and compute the statistical tests employed in this study in Appendix B.

2 Background

Human beings rely on exchanging goods and services, and trade is the backbone of our societies. It promotes economic growth, benefits employment and raises living standards[3]. Payment methods have evolved constantly to make trading faster, more efficient, and secure. In the last decade, there has been significant progress regarding creating currencies adapted to a more technological future.

2.1 Functions of Money

The invention of money was a revolutionary event in the development of the human race. Prior to the inception of the earlier forms of money, societies relied on barter-like methods to trade amongst them. Money completely reshaped these societies' economies. It made trading goods and services much more manageable because people were willing to accept money as payment since they knew exactly what that value of money equated to. It is difficult to price certain goods in a barter economy and even more difficult for people to remember prices. If one goat equals 50 stacks of hay, 25 stacks of hay equal one chicken, one chicken equals 15 pots of honey, how many pots of honey is one goat equal to? Apart from being a cumbersome process to keep track of all the prices, what happens if you want to acquire something from someone but do not possess anything that is of value to your trading partner? Money solves this issue and many more, and it does so because of the three functions that economists have long said money performs: being a medium of exchange, a unit of account, and a store of value.

The fact that money is a medium of exchange means that it is widely accepted, and its value is recognised by everyone in an economy. Because of this, it is not necessary to search for a coincidence of wants between a seller and a buyer. Instead of offering a specific good in return for buying another good or service, money can be used in lieu, as a seller would gladly accept it as a payment method.

Money can be viewed as a yardstick used to measure value in economic transactions. In the problem previously mentioned, it may be difficult to calculate the value of a goat in terms of pots of honey, especially when dealing with indivisible assets. Because money is widely accepted and divisible, fungible and

[3] Office of the United States Trade Representative (viewed 07/06/2021) https://ustr.gov/about-us/benefits-trade

countable, it is used to measure, amongst others, value, profits, losses, income, debt and expenses. As such, it is said to be a unit of account.

Apples, cars, and clothes are valuable goods, but like most assets, they either perish or lose value relatively quickly. Money, on the other hand, is a good store of value. If you sell a good or service and get paid in money, in principle, it does not matter how much time passes by. You could hold on to that money indefinitely and potentially exchange it for something in the future for the same amount of money that it would have cost you today (negating the effects of inflation). Initially, money was made of precious metals such as gold and silver or other durable objects like cowry shells because of their almost perpetual shelf lives.

2.2 Conventional Money and Differences with Cryptocurrencies

In order to describe how our usage of money has changed over the past millennia, it is imperative to explain the difference between money and currency. Both terms are often used interchangeably, but they have important economic dissimilarities. The following table outlines their key differences:[4]

Table 2.1: Key Differences Between Money and Currency

Money	Currency
A store of value, intangible in nature	Not a store of value, tangible in nature
The actual value goods and services are traded for	A medium of payment that represents an amount of money
Has intrinsic value	Does not have intrinsic value
Performs three primary functions	Any form of money that is circulated in public

Source: EDUCBA[5]

The coins and bills we use in our everyday life are technically not considered money but currency[6]. This is because they do not actually have intrinsic value (the value one would obtain from melting the coins and selling them is significantly inferior to the value those coins represent). Thus, they are not the actual value for which one would like to exchange goods and services for, but rather the medium of payment that represents an amount of money with which one can buy said goods and services. This comes to say that the

[4] There may be other differences between money and currency not included in Table 2.1, but we include the main ones.
[5] EDUCBA https://www.educba.com/money-vs-currency/
[6] WallStreetMojo.com https://www.wallstreetmojo.com/money-vs-currency/

utility a seller may get from receiving a payment in coins and bills is equivalent to the value of the good or service they would have bartered the sold good for, if and only if the amount of currency they receive is able to purchase the good or service they desire.

Our means of payments have evolved greatly since our departure from barter systems. Currencies developed from precious objects (such as cowry shells[7] in Southern Asia and miniature replicas of animals in Ancient China) into coins representing exchangeable goods, coins minted from precious metals, fiduciary notes and paper representing coins, and finally into modern digital currency proposals. Digital currencies encompass central bank reserves, currency deposits at banks and cryptocurrencies, amongst others (Bech and Garratt, 2017). As explained in the Introduction, a cryptocurrency is a digital medium of exchange that uses cryptography to secure transactions, control the creation of additional units and verify asset transfers amongst its users.

Cryptocurrencies aim to become a widely accepted means of payment and replace regular fiat money. They differ from modern central bank-backed money in three primary aspects: decentralisation[8], lack of intermediaries[9] and programmability[10]. Central banks dictate the monetary policy of an economy. In contrast, there is no central authority that controls the demand, supply or price of cryptocurrencies. Defenders of cryptocurrencies posit that this quality (decentralisation) would improve our current financial sector by democratising it[11]. Furthermore, the fact that cryptocurrencies allow for the elimination of intermediaries suggests that transactions should be fairer (but not necessarily less costly). The peer-to-peer nature of these digital currencies means that there is absolute transparency whenever a transaction is completed. Finally, being programmable (meaning that they have an innate logic) could make cryptocurrencies extremely useful in certain aspects. For example, they can be programmed to be compliant with laws and regulations, have an inherently fixed inflation rate, or to be spent only on certain goods and services.

[7] National Geographic https://www.nationalgeographic.com/culture/article/money-human-origins-journey-humankind
[8] Investopedia.com https://www.investopedia.com/terms/c/cryptocurrency.asp
[9] Fox Business https://www.foxbusiness.com/money/what-are-the-benefits-of-cryptocurrency
[10] LSE Business Review https://blogs.lse.ac.uk/businessreview/2020/09/14/do-we-need-programmable-money/
[11] Finextra https://www.finextra.com/blogposting/20082/how-cryptocurrency-is-democratising-our-financial-system

3 Introducing Blockchain and Tangle

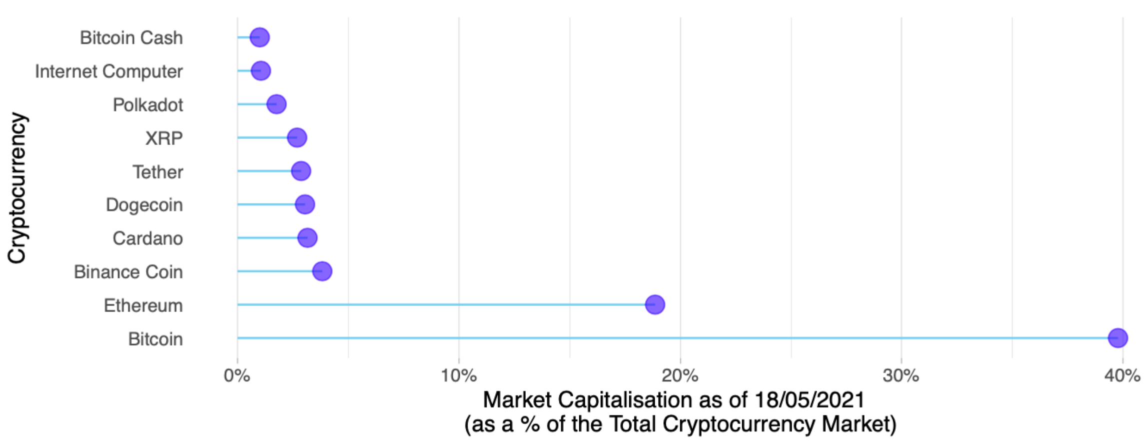
Cryptocurrencies are making headlines on a daily basis, but why? This section aims to describe how the cryptocurrency market looks like currently and why the underlying technology of cryptocurrencies is causing so much expectation.

3.1 Current Landscape in the Crypto Realm

The creation process of most cryptocurrencies has been very open and public. So much so that it is relatively uncomplicated to actually make one. As of May 2021 (when this paper was completed), there are 5175 cryptocurrencies listed on Coinbase.com, and 5336 on Investing.com. The number of coins and tokens has increased significantly over the last couple of years; in 2019, there were 2817 cryptocurrencies, and back in 2016, a mere 644 existed.[12]

At the moment of writing this paper, the cryptocurrency market is completely dominated by Bitcoin and Ether (Ethereum's cryptocurrency). Between them, they hold around 40% and 19% of the total market capitalisation of the cryptocurrency market, which is currently around $2.03 trillion. The rest of the top-ten cryptocurrencies hold 19.5% amongst them. Figure 3.1 displays the market capitalisation of the most representative cryptocurrencies.

Figure 3.1: Top Ten Cryptocurrencies by Market Capitalisation



Source: Own elaboration, CoinMarketCap.com https://coinmarketcap.com/

[12] Statista https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

Figure 3.1 contains the top ten cryptocurrencies by market capitalisation and clearly portrays the existing Bitcoin-Ethereum supremacy. Amongst them, the first ten coins and tokens represent 78% of the whole global market. Those ranked 11-30 merely account for approximately 10.5% at the time of writing. Keeping in mind that there are more than 5000 coins and tokens, wealth is evidently not distributed equally amongst the thousands of different cryptocurrencies.

Bitcoin was founded in 2008 by a programmer (or group of programmers) under the pseudonym Satoshi Nakamoto, and has been leading the market ever since, in part by virtue of its advantageous head-start. Another reason for Bitcoin's utter dominance in the cryptocurrency realm is its mainstream acceptance. The first transaction ever recorded dates back to 2010, and today an increasing number of companies are beginning to accept payments in Bitcoin. Furthermore, it counts with the popular vote. In the years following its inception, Bitcoin was infamous for its lack of transparency and connections to illicit operations, but the public perception has changed since then, mainly due to its colossal returns and increasingly recurrent references in pop culture.

Ethereum has been chipping away at Bitcoin's market capitalisation for the last few years, but even though it has many more potential uses and applications, it currently cannot compete with Bitcoin's popularity. Ether can not only be used as a digital currency and store of value (like Bitcoin), but the Ethereum network also makes it possible to create and run myriad decentralised applications and smart contracts (unlike Bitcoin). Ethereum supports Decentralised Finance (DeFi), smart contracts and Non-Fungible Tokens (NFT), amongst others. These terms will not be discussed in this paper in further detail, but they are the main reasons why Ether is at the top of the cryptocurrency hierarchy.

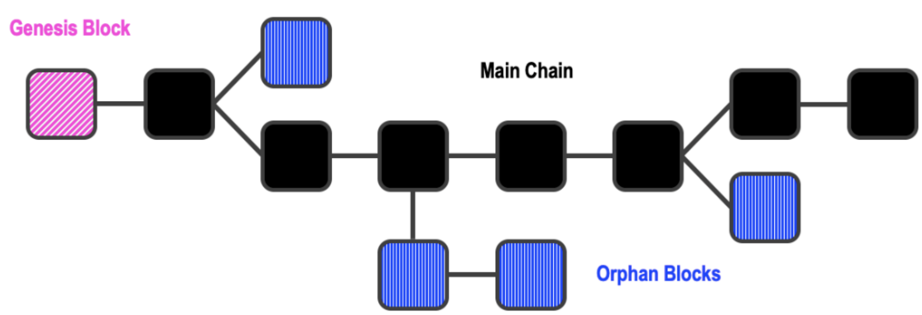
It is debatable whether or not we are in a cryptocurrency bubble at the moment. Those who argue against the existence of a bubble suggest that cryptocurrencies are outperforming conventional 'government money', in the sense that virtual currencies secured by cryptography have created a new and misunderstood economy that is slowly gaining pace towards attaining dominance in the global monetary order (Forbes, 2021). Oppositely, cryptocurrency bears posit that even though there has been an influx of institutional money lately in the crypto market, the recent boom in prices should be looked askance, for the current landscape is reminiscent of the 2017 cryptocurrency bubble. Either way, what is undeniable is that the underlying technology in cryptocurrencies is here to stay. Said technology is commonly referred to as Blockchain.

3.2 Blockchain

Cryptographer David Chaum introduced the first known blockchain-like protocol proposal in his 1982 dissertation project on “Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups”. Haber and Scornetta (1991) provided further research on preventing the possibility of tampering with timestamps in documents. A year later, Bayer et al. (1992) improved the efficiency of the then-nascent Blockchain technology by introducing Merkle trees, thus enabling many document certificates to be collected into a single block. Since then, there have been many contributions to the field, but none of them as groundbreaking as Satoshi Nakamoto’s 2008 “Bitcoin: A Peer-to-Peer Electronic Cash System”.

A blockchain can be viewed as a special type of database, where information is stored in blocks that are connected (chained) to other blocks. To store more information on a blockchain, data is entered in a new block which is then linked to the last block of the blockchain. Thus, blocks are chained in chronological order, the first of them being the genesis block. Because these chains are decentralised, they are both public and immutable, anyone can access the information, but no one can tamper with it.

Figure 3.2: Simplified Blockchain Network



Source: Compiled by authors

Figure 3.2, shown above, portrays the classical representation of a blockchain, including a genesis block, the main chain and orphan blocks at the sides. Conventional blockchains start from a genesis block, pink (diagonal texture) block in Figure 3.2, whose properties define the following blocks in the chain and thus the system itself. The subsequently validated blocks are included in chronological order by their validation date and form the main chain. Orphan (blue or vertical texture) blocks exist mainly due to a situation where two miners solve the same block almost simultaneously. However, it is also possible for them to be created after a hacker attempts to reverse a few transactions in the blockchain.[13]

Cryptocurrencies like Bitcoin and Ethereum are blockchains, where transactions made with said currencies are recorded in blocks. These new blocks have to be validated and registered in the chain. Bitcoin's whitepaper stipulates that these new blocks must be validated by Proof-of-Work (PoW), whereas in other cryptos like Ethereum, Proof-of-Stake (PoS) is used. In a PoW system, participants compete to validate the new block by trying to be the first at solving a mathematical problem. He who first obtains the correct answer will then notify all other participants and validate the new block. On the other hand, in a PoS environment, the opportunity to validate blocks is granted to participants on the sole basis of their stake in the chain. This means that those who own more blocks (and thus a larger stake) have greater opportunities of being chosen to validate a new transaction. Apart from PoW and PoS, there are other systems of new block validation for blockchain cryptocurrencies. The process of verifying new information in the context of cryptocurrencies is called mining, and the participants who engage in said activity are referred to as miners.

There is a financial incentive to mine. Miners receive two types of rewards for their contribution to the network. Firstly, they receive a block reward whenever it is they who are the first to resolve the mathematical problem (in PoW) or when they have been selected by the network based on their stake (PoS). Bitcoin rewards halve every 210,000 blocks mined. In the early days of bitcoin, the reward for mining was 50 BTC. The latest halving occurred in May 2020, which leaves rewards for mining at 12.5 BTC. The other reward miners receive are transaction fees, which are paid directly to them by those taking part in the actual transaction.

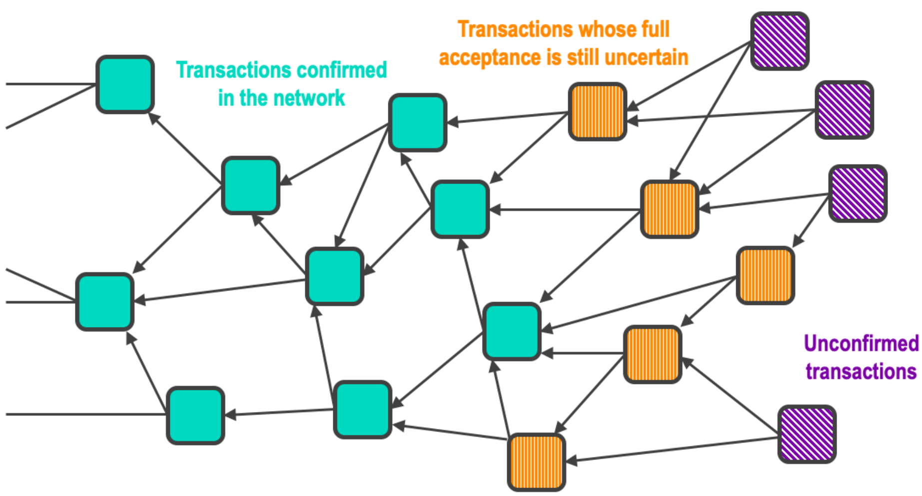
3.3 Tangle Technology

Blockchain-like systems have sequential blocks, with each block storing many transactions. In 2015, Popov presented a whitepaper on a novel cryptocurrency for the Internet of Things (IoT) industry whose main feature was the 'Tangle'. Tangle is a less restricted DAG (Directed Acyclic Graph) (Silvano and Marcelino, 2020), where there are no 'blocks'. Instead, every new transaction has to reference two previous transactions.
Figure 3.3 presents an example of a simplified Tangle Network where each transaction has to approve two other transactions (each directed edge (arrow) represents a 'reference' or 'approval'). A new transaction

[13] For a description of each case, see Bit2me Academy https://academy.bit2me.com/en/what-is-an-orphan-block/ and Investopedia.com https://www.investopedia.com/terms/o/orphan-block-cryptocurrency.asp

referencing two previous transactions is equivalent to stating, "I certify that these transactions, which have not been proven before, as well as all their predecessors, and their success is tied to my success" (Silvano and Marcelino 2020). Consensus is not necessarily immediate, but is related to the number of transactions that referenced and approved a specific transaction. The greater the number of approvals a transaction has, the higher the level of confidence of its consensus. As opposed to Bitcoin, where validation is achieved through PoW and only a small subset of the network is responsible for overall consensus, the Tangle's validation process is carried out by the entire network of participants making transactions. Because the 'validators' of the transactions are the network users per se, there is no need for mining; this is analogous to a pay-it-forward economic model where new transactions 'help' prior transactions get validated before being validated themselves. This comes to say that the only cost of making a transaction in Tangle is the computational cost of validating two previous transactions. The cryptocurrency behind the Tangle architecture is called IOTA, and will be discussed further in Section 4.

Figure 3.3: Simplified Tangle Network



Source: Own elaboration

In Figure 3.3, turquoise (no texture) blocks[14] represent transactions that have been successfully confirmed. The Tangle network has reached a consensus on the legitimacy of their transactions, and there is a security guarantee that those blocks indeed represent valid information. This is because they have been confirmed directly or indirectly by all the unapproved transactions (purple, diagonal texture). Orange (vertical texture) blocks are transactions for which the network has not yet reached a consensus on their validity, this means

[14] In a Tangle network, there are no "blocks" as such but for graphical purposes we have used blocks to represent transactions.

that they have not yet been approved by all the unconfirmed transactions. Lastly, purple blocks represent unconfirmed transactions (called 'tips'). This is a simplified example, in reality, as mentioned earlier in this section, transactions generally have a degree (confidence level) of approval calculated by dividing the number of tips that directly or indirectly reference the transaction by the amount of tips in the network.

3.3.1 Scalability

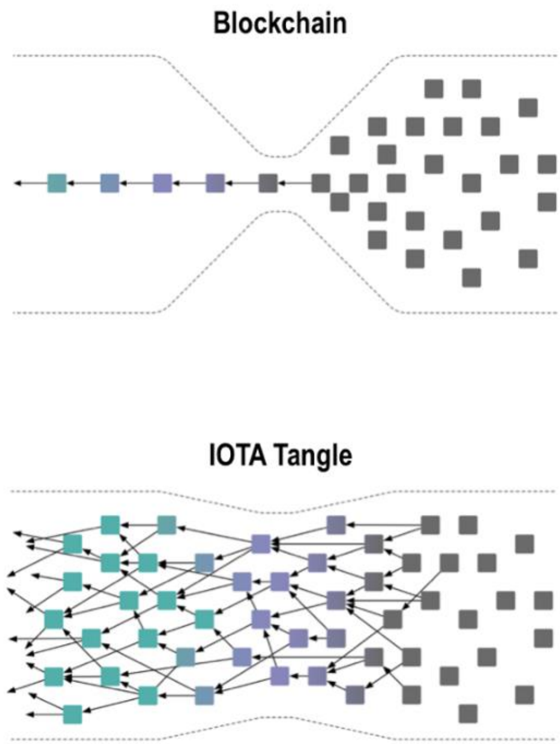
The term 'Scalability Trilemma' or 'Blockchain Trilemma' is a term coined by Ethereum founder Vitalik Buterin. According to him, the trilemma Blockchain has is developing a technology that offers decentralisation, security and scalability. Most blockchain cryptocurrencies at the moment prioritise decentralisation and security but there is yet to exist a cryptocurrency that can perform well in the three categories simultaneously, hence the trilemma. At this moment, our economies and financial system do not rely on digital coins or tokens as a means of payment, so cryptocurrencies are not exposed to high activity (Bitcoin did 3.5 transactions per second[15] (tps) in 2020 whereas Visa processed over 4464 tps,[16] approximately 1275 times more). Cryptocurrencies have to evolve to circumnavigate the scalability issue if we want to use them as regular means of payment.

Regarding scalability, the problem with Blockchain-based protocols is that they (generally) can only have a single path. This means that if the network has more activity because the coin representing the protocol is being used more often, the protocol itself may not be able to keep up with new transactions. In simple terms, more activity in the network equals the same validation rate as before. Conversely, Figure 3.4 shows how Tangle efficiently tackles this problem. In a Tangle network, the more activity there is (that is, the more new tips there are), the more validation there will be in the system because those new tips are obligated to reference two prior transactions.

[15] Blockchain.com (viewed 01/06/2021) https://www.blockchain.com/charts/n-transactions

[16] VISA processed 140.8 billion transactions in the year 2020. VISA Annual Report 2020 (viewed 01/06/2021) https://annualreport.visa.com/financials/default.aspx

Figure 3.4: The Blockchain Bottleneck



Source: Popov (2018)

Figure 3.4 displays the 'Blockchain Bottleneck', which visually portrays the scalability issue Blockchain has and how Tangle succeeds in dealing with it. Instead of having the limitation of only having a single site for attaching new transactions, the Tangle protocol offers myriad sites where the new tips can reference prior transactions. Participants of the network can attach new transactions to different parts of the Tangle without having to wait for their previous transaction to be confirmed.

3.3.2 Costs

The IOTA Tangle does not require mining for the system to work. As such, it offers two big advantages in terms of costs when compared to Blockchain-like cryptocurrencies. The first one is that there are no transaction costs because participants in the Tangle do not have to incentivise others to do PoW on their transaction. The IoT depends on the use of microtransactions, which is why being a feeless cryptocurrency is vital for IOTA's viability in the IoT ecosystem. Blockchain currencies usually have fluctuating average transaction costs. The reason for this is that in times of high activity when the blockchain gets congested and there are many blocks waiting to be included in the chain, miners usually select the ones which are most profitable. Therefore, participants who make transactions in the Bitcoin network will pay higher fees when this happens to incentivise miners to validate their transactions first. Actually, over the last three years, the average Bitcoin transaction fee has been 4.11 USD, but at times of high activity (still relatively low activity when compared to non-cryptocurrency means of payments such as VISA), transaction fees went as high as 62 USD (Blockchain.com).

The second advantage the Tangle has over Blockchain with regards to costs is that IOTA is, essentially, environmentally friendly, whereas Blockchain protocols, especially Bitcoin, require large amounts of energy to run and be maintained. Mining a single bitcoin has a carbon footprint of around 165 tonnes of CO_2 and a single Bitcoin transaction consumes around 680 kg of CO_2 (equivalent to 1,507,857 VISA transactions)[17]. In fact, the Bitcoin network consumes around 0.53% of the total global electricity supply and if it were a country would rank 33 for electricity consumption[18]. In the Tangle, when participants of the network desire to issue a transaction, they must first do some computational work to approve two older transactions. Depending on the user's hardware, this computational work takes a negligible amount of time and energy. Thus, in a world where energy efficiency and low carbon footprints will be kings, IOTA's Tangle is better suited to comply with the energy requirements future generations will ask for.

3.3.3 Quantum Immunity

Computers, even supercomputers, as we know them today, rely on bits (binary digits[19]) to process information. Every tweet, podcast and email is essentially a long string of 1s and 0s. Quantum computers use qubits (quantum bits) instead. Two of the most important quantum properties of qubits are superposition[20] and entanglement[21]. These properties suggest that future quantum computers will have considerably more computing power than even the most powerful supercomputers. A two-bit string can only store one of the following binary arrangements: "00", "01", "11" or "10". On the other hand, owing to the properties of superposition and entanglement, quantum computers are able to record all of the four previously-mentioned

[17] Digiconomist (viewed 28/05/2021) https://digiconomist.net/bitcoin-energy-consumption
[18] Cambridge Center for Alternative Finance (viewed 29/05/2021) https://cbeci.org/cbeci/comparisons
[19] The most basic unit of information in computing, it can only have two values, 0 or 1.
[20] The ability to simultaneously represent numerous possible combinations of 1s and 0s.
[21] When two members of a pair (of qubits) exist in a single quantum state.

strings in a single two-qubit record. Regardless of when we will reach quantum supremacy[22], and its potential benefits to society are realised, it is only natural to suppose that quantum computing could pose a threat to our current security systems. The reason for this threat resides in the fact that cybersecurity depends on the speed of computers, and quantum computers could potentially be millions of times faster than today's supercomputers[23].

Blockchain protocols, although relatively secure against contemporary supercomputers, could also be vulnerable to the superior processing power of quantum computers because quantum computers can break cryptographic keys[24] quickly by means of calculation or simply searching for all secret keys by using Shor's and Glover's Algorithms (Mavroeidis et al., 2018). Shor's Algorithm in Asymmetric Cryptography (Shor, 1994) may render modern asymmetric cryptography[25] useless as it provides proof that quantum computers would be able to factorise large prime numbers (prime number factorisation is the backbone of current asymmetric cryptography). Grover's Algorithm in Symmetric Cryptography (Grover, 1996) can find a certain entry in an unsorted database of N entries in $\sqrt{N}$ tries, whereas conventional current computers need $N/2$ searches. IOTA's Tangle is considered to be quantum immune because it uses Hash-Based Cryptography[26] (specifically Winternitz One Time Signatures[27] – a variation of Lamport Signatures[28]) instead of the Elliptic Curve Cryptography[29] that Blockchain uses. Zentai (2020) and other previous literature suggest that sufficiently large hash functions would make Lamport Signatures (Lamport, 1979) quantum resistant. Thus, the Tangle promises potential immunity to possible attacks from quantum computers (Silvano and Marcelino, 2020).

[22] The point at which quantum computers will surpass supercomputers in the ability to solve complex mathematical problems.
[23] Scientific American viewed (29/05/2021) https://www.scientificamerican.com/article/light-based-quantum-computer-exceeds-fastest-classical-supercomputers/
[24] A key in cryptography is a string of characters within an encryption algorithm. Analogous to physical keys, it enables users to encrypt (lock) information so that only a user with the right key can decrypt (unlock) it.
[25] Asymmetric cryptography is an encryption mechanism which uses two separate keys for encryption and decryption, one public and the other private. It is widely used and has myriad applications in the digital security space.
[26] Hash-based cryptography are algorithms used to build protocols for computer security systems. These algorithms are based on hash functions (functions that take a key and map it to a value of certain length called hash.
[27] Winternitz One Time Signatures are a thought-to-be quantum robust cryptographic method for digital security.
[28] Lamport Signatures are a method to securely construct digital signatures.
[29] Elliptic Curve Cryptography is a method for data encryption and decryption based on public and private keys and uses elliptic curves instead of prime numbers like regular asymmetric encryption methods. It is the method used by most cryptocurrencies for digital signatures to sign transactions.

4. Introducing IOTA

The vast majority of cryptocurrencies use Blockchain to record transactions. The most notable exceptions are IOTA and Hedera Hashgraph, which use Tangle and Hashgraph, respectively, as a transactional ledger. This paper focuses on the former (IOTA) because it is the non-blockchain cryptocurrency with the highest market capitalisation, and the maximum exponent of DAG consensus algorithms. Founded by David Sønstebø, Sergey Ivancheglo, Dominik Schiener and Dr Serguei Popov, and released on the 11th of July 2016, IOTA is an open-source, scalable and feeless distributed ledger that is designed to support frictionless data and value transfer in the IoT ecosystem. The IoT demands a system capable of supporting hundreds of thousands of transactions per second, and as explained in prior sections, current Blockchain cryptocurrencies are not able to do so. Therefore, other technologies have to step in to fill the gap, and at the moment, IOTA's Tangle is at the top of the list of contenders.

Because the Tangle represents such an advancement in the cryptocurrency space, IOTA has the potential to be widely implemented in our daily lives. The literature on IOTA is scarce and heavily focused on its underlying technology and vision, and to a smaller extent, on its applications. Prior studies revolve around IoT, M2M, E-Health, Automotives and Smart Cities. We want to contribute to the literature by analysing IOTA's underlying economic attributes. In particular, those related to market efficiency in the context of Fama (1970). To do this, we employ a battery of statistical tests and analyse our results in a similar fashion to those of Urquhart (2016) and Aslaksen and Wiersdalen (2019). In fact, we provide further empirical analysis on the aforementioned academic papers by examining IOTA and Tangle Technology instead of Bitcoin and Blockchain.

4.1 The Efficient Market Hypothesis (EMH)

The Efficient Market Theory or, as it is alternatively known, Efficient Market Hypothesis (EMH), in its strong form, states that the price of a given security fully reflects all the information in a market, whether public or private (Fama, 1970). Although theoretically plausible, empirical evidence suggests that accepting the EMH in its most pure form is generally quite difficult; this has been corroborated by academia from a logical and theoretical standpoint (Grossman and Stiglitz, 1980). For this reason, apart from the strong form, two other main modifications exist.

On the one hand, there is the semi-strong efficiency hypothesis. This form of EMH distinguishes between private and public information and assumes only the latter is used to assess a given security price. The semi-strong form assumes that an investor would be able to use neither technical nor fundamental analysis to generate abnormal returns in a given market even if they could make use of all publicly available information. In a semi-strong efficient market, investors trade their securities based on newly available public information. For those investors who are interested in beating the market, it would only be possible for them to do so if they accept a higher level of risk. Generating abnormal returns without an increase in risk is not possible in a semi-strong efficient market due to the market's ability to rapidly adjust the prices of securities as new information is made public (Malkiel, 2003).

On the other hand, there is weak-form efficiency. This second form of EMH claims that the price of a security fully reflects all past observations (all security prices up to time $t-1$) at time t. The weak-form efficiency hypothesis implies the random walk hypothesis, which states that future prices are non-predictable due to successive price changes being serially independent and random (Chen, 2011). The underlying principle in the weak-form efficiency element of the EMH is that investors are intelligent (they make the best decisions possible based on the information they possess), capable (they are able to invest and disinvest whenever they want) and rational (their decision process is based on logic). Investors are not able to beat the market using technical analysis, and would only be able to do so in the short run, using fundamental analysis.[30]

Following Urquhart (2016) and Aslaksen and Wiersdalen (2019), we test for the weak-form efficiency hypothesis. The main difference between our paper and the aforementioned papers is that we analyse the IOTA market instead of Bitcoin's. The weak-form efficiency relies upon the premise that the price series follows an unpredictable pattern; hence returns are considered a random walk. As a result, to test for weak-form efficiency, the statistical tests employed in this analysis have the null hypothesis of randomness. The random walk hypothesis requires that the observations are serially independent and that the probability distributions are constant over time (Malkiel, 1989).

[30] Source: eFinanceManagement.com https://efinancemanagement.com/investment-decisions/weak-form-of-market-efficiency

5 Data

This section is dedicated to explaining how and where we gathered our data from, performing a brief analysis on said data and commenting on its descriptive statistics. Furthermore, we describe the reasoning behind the selection of three subsamples. By creating subsamples, in further sections we will test whether there has been an evolution in the underlying economic qualities of the IOTA market.

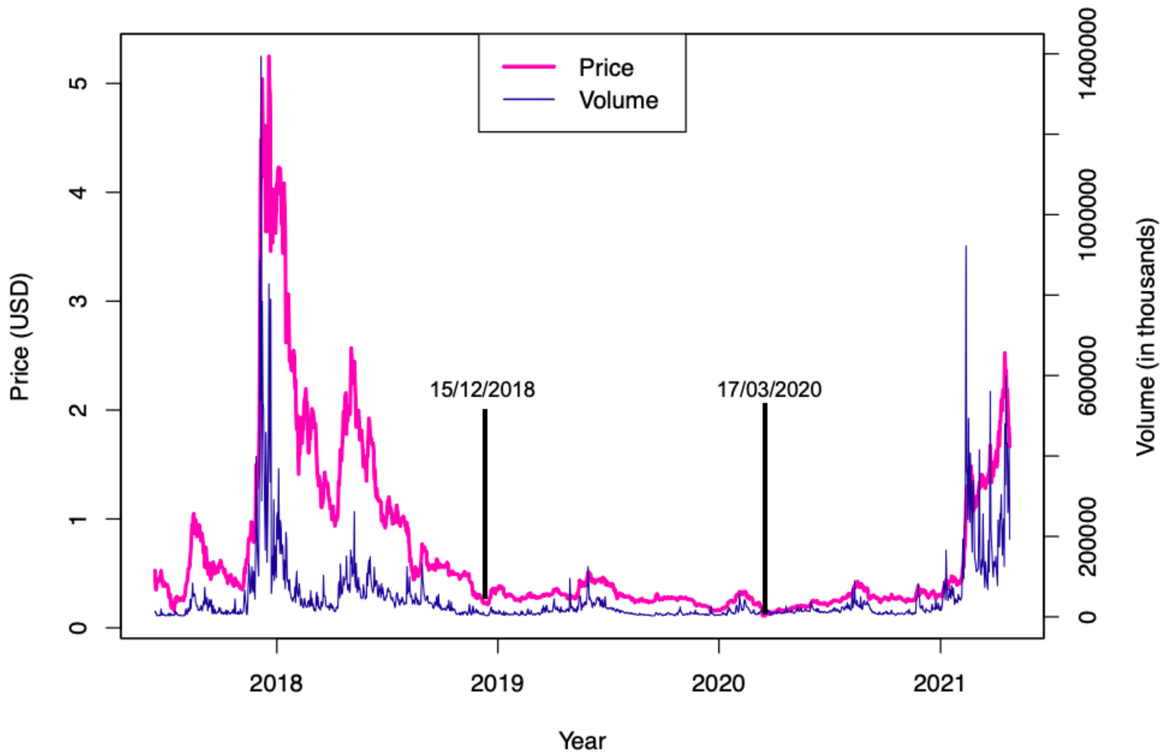
5.1 Data Sources

When gathering data, our primary concern was choosing a crypto price listing website that included downloadable price time series for IOTA and Bitcoin. There are many platforms online that display historical prices, but we used Coin Gecko because it provided the largest historical daily price samples for the aforementioned cryptocurrencies, and all daily observations were available. Having a large sample size was of great importance because we wanted to understand and test different periods to see if IOTA had undergone significant behavioural changes over the last few years. We used the historic price sample available for IOTA in its entirety, including trading volumes for the same time periods. It must be noted that the price series we use for IOTA contains all its historic prices since its inception; it covers all of IOTA's lifespan up until the moment of writing this paper. We used the same time period for Bitcoin's historic price sample as the one we used for IOTA's sample.

5.2 Samples

In order to investigate whether the underlying economic fundamentals of the IOTA market have evolved over time, we follow Urquhart (2016) and Aslaksen and Wiersdalen (2019) in dividing the full sample into subsamples. We cut the full sample at dates: 15/12/2018 and 17/03/2020 based on visual aspects of IOTA's price and trading volume time series.

Figure 5.1: IOTA Price and Trading Volume



Source: Own elaboration, CoinGecko.com https://www.coingecko.com/es

As seen in Figure 5.1, a bubble started in mid-2017 until it burst at the beginning of 2018. We choose 15/12/2018 as the last observation of the first subsample because it is the day IOTA's price reaches a support level and maintains a consistent price for the remaining of the second subsample up to the 17/03/2020 cut-off. Furthermore, this decision is strengthened by the fact that trading volumes are at the lowest levels since before the initial bubble. The justification for the second cut-off point is based on the fact that a new cycle starts in the IOTA market: after a series of days with negative returns, from 18/03/2020 onwards, the price undergoes a continuous upwards trend. Furthermore, we decided to group all the observations for the period of the Covid-19 crisis together in a single subsample. Our subsamples are similar in size and neither of them could be considered small by means of the statistical tests we will employ later on. For comparison purposes, we also work with the full sample of IOTA returns. Thus, we use the following samples in our statistical analysis:

Table 5.1: Samples Used in Statistical Analysis

Full Sample	15/06/2017 – 25/04/2021
First Subsample	15/06/2017 – 15/12/2018
Second Subsample	16/12/2018 – 17/03/2020
Third Subsample	18/03/2020 – 24/04/2021

5.3 Daily Log-Returns

The statistical tests employed in this paper have been applied to the IOTA returns time series. The benefit of using returns instead of prices is that results are normalised and therefore comparable to results from other securities with different price series. We calculate daily returns using logarithms:

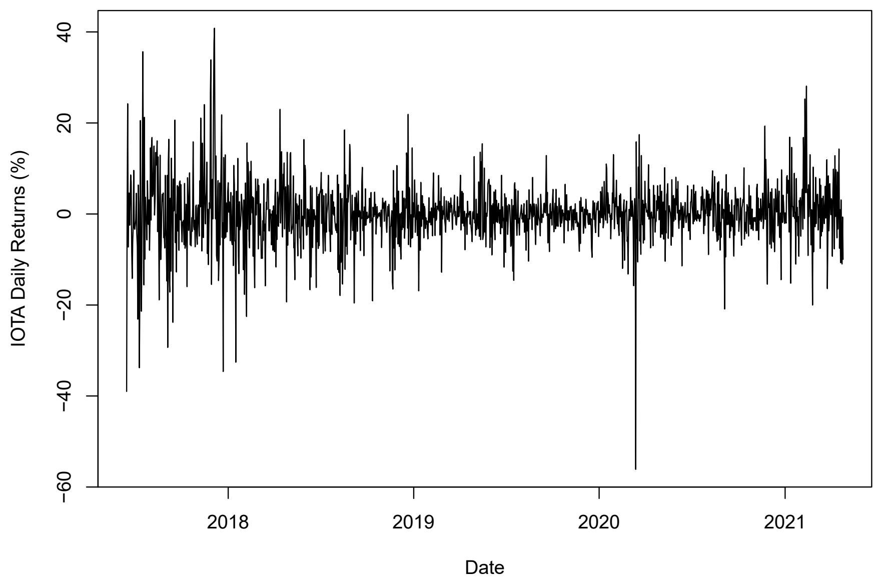
$$R_t = \ln(P_t/P_{t-1}) \cdot 100.$$

Log-returns are an approximation of percentage change when said change is close to 0%. Thus, it can be argued that because cryptocurrencies present atypically high positive and low negative daily returns (see Table 5.2 for IOTA's maximum and minimum daily returns), percentage change could be used instead of log-returns to derive the returns time series. Upon careful examination of the descriptive statistics of the returns time series using both log-returns and percentage change, we determine that both series display the same qualitative properties. As such, we prefer to emulate prior literature, such as Urquhart (2016) and Aslaksen and Wiersdalen (2019), in using log-returns to better compare our results with theirs.

5.4 Data Description

Figure 5.2 below, shows the transformed series resulting from calculating daily returns using logarithms:

Figure 5.2: IOTA Daily Log-Returns Time Series



Source: Own elaboration, CoinGecko.com https://www.coingecko.com/es

As commented in Section 5.3, there are numerous examples over IOTA's lifespan where returns have been relatively high (and low) compared to other asset classes. Figure 5.2 shows the return series has many outliers, the most noteworthy happening on 13/03/2020 when IOTA's price dropped 56% in a single day.

The sample size of each subsample is sufficiently large enough that the statistical tests we employ in Sections 6 and 7 give robust outcomes. Shown below are the descriptive statistics of the IOTA Returns time series.

Table 5.2: IOTA Log-Returns Descriptive Statistics

Sample Period	N	Mean (%)	St. Dev. (%)	Max. (%)	Min. (%)	Kurtosis	Skewness
15/6/2017 – 25/04/2021	1411	0.08	7.10	40.83	-56.13	7.21	-0.17
15/06/2017 – 15/12/2018	549	-0.16	9.03	40.83	-39.00	3.29	0.16
16/12/2018 – 17/03/2020	458	-0.14	5.26	21.89	-56.13	28.66	-2.38
18/03/2020 – 25/04/2021	404	0.67	5.81	28.10	-20.87	2.78	0.32

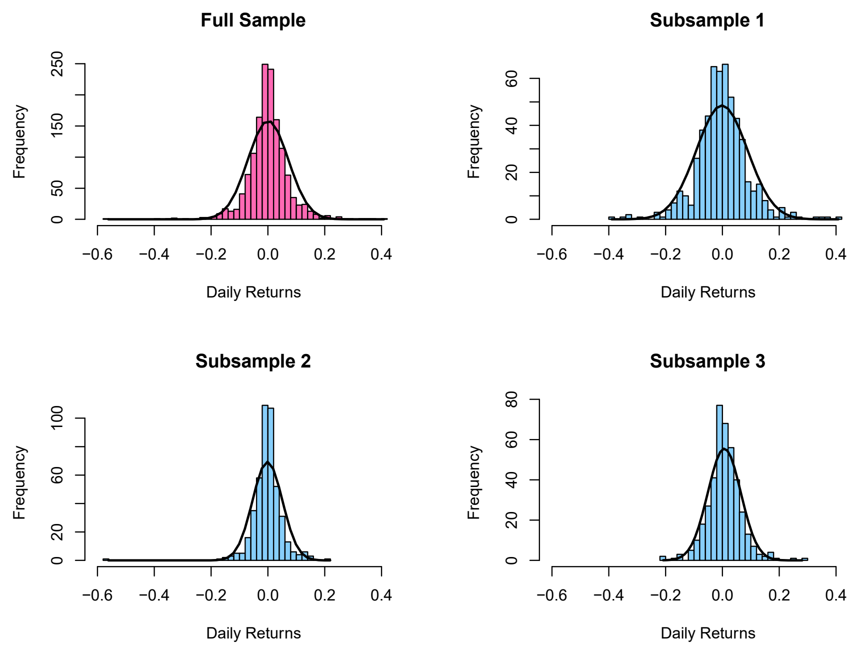
Source: Own elaboration, CoinGecko.com https://www.coingecko.com/es

From Table 5.2, we see that the mean returns are notably higher for the last subsample, perhaps the sign of the possible cryptocurrency bubble mentioned earlier in Section 3.1. The maximum and minimum returns are significantly higher and lower, respectively, than the ones we would encounter in other asset classes such as the stock exchange (the SP500's maximum daily variation in the last 20 years has been 11.5% and the minimum daily variation for the same period has been near to -12%).[31] It should be noted that the coefficients displayed for the kurtosis reflect excess kurtosis over a normal distribution (a normal distribution having a kurtosis coefficient of 0). All samples present a leptokurtic distribution; see Figure 5.3 for a visual representation of each sample's distribution. The second subsample in particular shows a significantly higher kurtosis than the other three samples, owing to the fact that it had most of its observations in the [-0.05 , 0.05] range. For comparison purposes between Table 5.2 and Figure 5.3: the values in the x axis of the histograms are not in percentages. Most samples present a skewness coefficient close to 0, which means the mean, median and mode are close to each other and the shape of the distribution is somewhat symmetrical. The second subsample is inconsistent with this pattern and shows a negative skewness, meaning that the lower (left) tail is longer than the upper (right) tail, and the relationship amongst its mean, median and mode is: $\mathrm{mean}<\mathrm{median}<\mathrm{mode}$.

To aid in visualising the IOTA returns' descriptive statistics, we include histograms of the return series for each sample. The histograms give us an insight into the shape of the distribution of each sample. They have been fitted with a normal distribution with μ equal to the mean of the sample in question and σ equal to the standard deviation of each specific sample.

[31] Source: Investing.com https://es.investing.com/indices/us-spx-500-historical-data

Figure 5.3: IOTA Daily Log-Returns Histograms

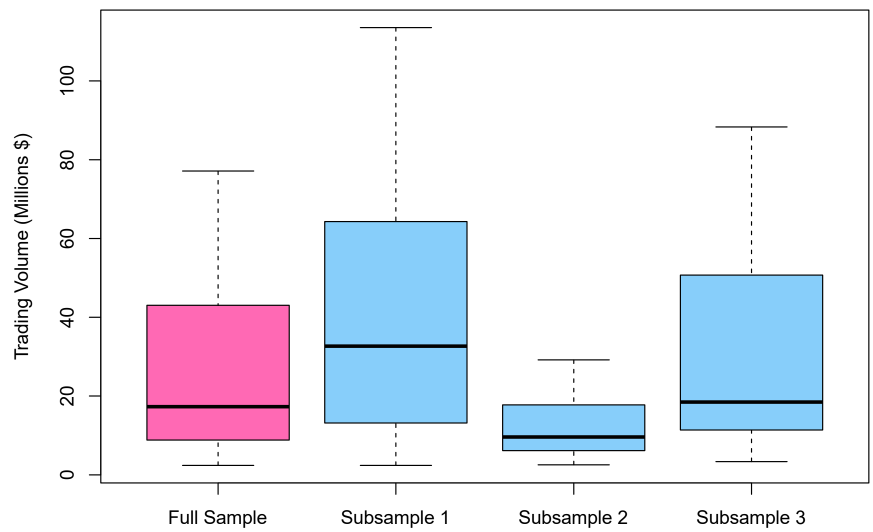


Source: Own elaboration, CoinGecko.com https://www.coingecko.com/es

The fitted normal distribution over the histograms in Figure 5.3 clearly portrays the prominent peaks in excess of the normal distribution, especially for subsample 2, which evidently presents a significant leptokurtic distribution. All samples appear to be relatively symmetric to the naked eye, but subsample 2 has some extreme negative returns in the [-40% , -60%] range that affect the calculation of the skewness coefficient (-2.38). Normal distributions have skewness of 0, so in terms of symmetry, all samples except for subsample 2 are considered normal.

IOTA's trading volume distribution over the four samples is included below in Figure 5.4. These box plots have been plotted in the absence of outliers, as they distorted the visual representation of the distributions of each sample.

Figure 5.4: IOTA Trading Volume Box Plots



Source: Own elaboration, CoinGecko.com https://www.coingecko.com/es

IOTA's trading volume represents the overall activity in the market, and provides an insight into the general interest in the cryptocurrency. Figure 5.4 suggests that there was a greater interest in IOTA in the first subsample (the average trading volume was around 35 million USD) than in the other two subsamples (especially the second subsample). This relatively high interest in IOTA coincides with the crypto bubble of 2017[32] and subsequent crash of 2018. Subsample 3 shows an increase in interest from the prior sample. There may be various reasons behind this surge in trading volume, but it most likely is a similar situation to the one from subsample 1 (most cryptocurrencies seem to have followed the same price and trading volume increases for the year to date, suggesting the possible existence of a bubble).

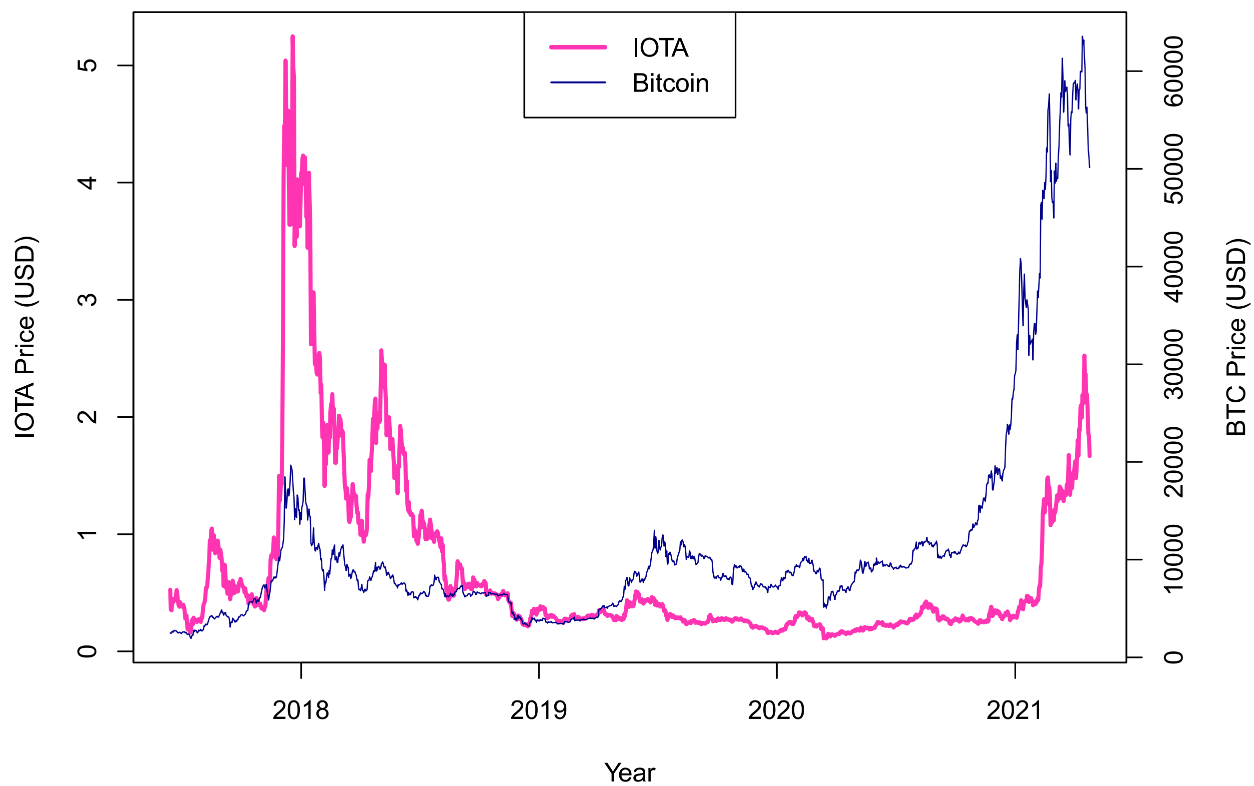
5.5 IOTA Price Bubbles

From Figure 5.1, one may say that even though IOTA's price soared and crashed in 2017-2018, the cryptocurrency is finally taking off, investors are realizing its true potential and thus its price is increasing following a surge in its demand. In part, owing to the law of supply and demand, this is true. But, the recent surge in prices has not been seen exclusively in IOTA, most cryptocurrencies have appreciated considerably from early November 2020 till mid-April 2021. The following figure includes both the price of IOTA and Bitcoin

[32] The crypto bubble of 2017 came about mostly from investors that bought into Initial Coin Offerings (much like regular IPOs), hoping to achieve financial gains similar to those enjoyed by early Bitcoin and Ethereum speculators.

in an attempt to show that the increase in the price of IOTA did not come from an increase in interest relative to other cryptocurrencies but rather an increase in interest in cryptocurrencies as a whole.

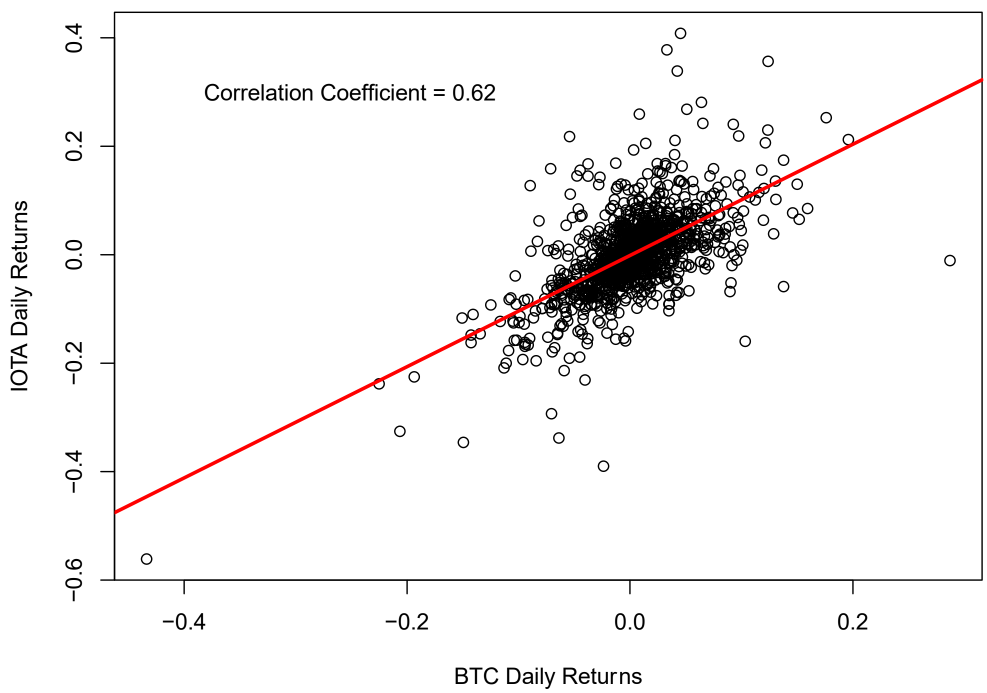
Figure 5.5: IOTA vs Bitcoin Price



Source: Own elaboration, CoinGecko.com https://www.coingecko.com/es

Figure 5.5 clearly shows that both cryptocurrencies share some kind of relation, as they seem to move in the same direction. Even though the tests we will employ in further sections do not take into consideration what factors drive the price of IOTA, we do feel the need to share our findings regarding the correlation between IOTA and Bitcoin for daily returns, as it may create possible inefficiencies and opportunities to beat the market. Because of this, we include a scatter graph with IOTA's returns plotted against Bitcoin's, with a line of best fit calculated from a simple linear regression. Furthermore, we include the correlation coefficient between IOTA and Bitcoin for our sample full sample period (18/03/2020 – 25/04/2021).

Figure 5.6: IOTA and Bitcoin Correlation



Source: Own elaboration, CoinGecko.com https://www.coingecko.com/es

Shown in Figure 5.6 is the correlation between IOTA and Bitcoin, which may suggest that either both cryptocurrencies are driven by similar forces, or one drives the other's price. Further research that could be done regarding the factors that determine IOTA's price is commented in Section 8.

6 Methodology

The statistical tests used in this section allow us to test the Efficient Market Hypothesis in the IOTA market. No single test is reliable enough on its own to provide concrete evidence for the (in)existence of weak-form market efficiency. Therefore, various tests with different methodologies and approaches are needed to evaluate the nature of the IOTA returns series within the context of Fama (1970). They do so by testing for randomness, mainly, and lack of any correlation in the returns that could suggest the possibility of predicting future values using past observations. The selection of these tests is made on the basis of comparing our results with those of the existing literature of Bitcoin (Urquhart, 2016 and Aslaksen and Wiersdalen, 2019).

6.1 Ljung-Box Test

The Ljung-Box test (1978) is widely used in Econometrics to test for the absence of serial autocorrelation. It tests for the overall randomness of a series based on a specified number of lags, where the autocorrelation (ρ) for at least one lag is significantly different from 0. The Ljung-Box is a modification of the Box-Pierce test, and more often than not preferred because of its overall better performance, especially in small samples. The null hypothesis states that there is no serial autocorrelation (the data points are independently distributed, and any observed correlations in the data are a result of the randomness of the sampling process). On the other hand, the alternative hypothesis posits that the data points exhibit serial autocorrelation and are therefore not independently distributed. Statistically, the null and alternative hypothesis are stated in the following way:

$H_0: \rho_1 = \rho_2 = \cdots = \rho_L = 0$

$H_A: \exists \tau. \rho_\tau \neq 0$

H_A comes to say that there is at least one τ that satisfies the condition $\rho_\tau \neq 0$, where τ is the lag being tested and L is the total number of lags being tested. The Ljung-Box test statistic is the following:

$$Q = T(T+2)\sum_{\tau=1}^{L}\frac{\rho_\tau^2}{T-\tau},$$

where T is the sample size or number of observations, L is the total number of lags being tested,[33] and ρ_τ is the estimated autocorrelation at lag τ. Under H_0 the Ljung-Box test statistic (Q) asymptotically follows a chi-squared distribution with h degrees of freedom ($Q \sim \mathcal{X}_h^2$). The null hypothesis is rejected when $Q > \mathcal{X}_{1-\alpha,h}^2$, where $\mathcal{X}_{1-\alpha,h}^2$ is $1-\alpha$ quantile of the chi-squared distribution with h degrees of freedom.

When the test statistic fails to reject the null hypothesis, it means that there is no serial autocorrelation in the IOTA returns, and there is evidence suggesting that the IOTA market is weak-form efficient. This would mean that the IOTA returns are random overall and therefore future prices would not be possible to predict.

6.2 Runs Test

The Wald-Wolfowitz (Runs) test (Wald and Wolfowitz, 1940) is a statistical test that checks if a data sequence of a dichotomous variable fits a randomness hypothesis. The way we obtain a dichotomous variable from the IOTA Daily Returns time series is by doing the following procedure:

Without changing the order of the original series, mark any data point greater than the median with a "$+$" and any data point lower than the median with a "$-$" (values that are equal to the median are omitted). A sequence of the sort is obtained:

$$+++--+-++-+---+-+++--$$

Once converted into a dichotomous variable, we count the number of 'runs' (12 in the aforementioned example) and convert this into a Z-Score using the 'Expected Number of Runs' and the 'Standard Deviation of the Null Hypothesis'. When the number of runs is (statistically considered) small it means the average run is longer than its expected value, which may indicate positive autocorrelation. In contrast, negative correlation is associated with a (statistically speaking) high number of runs. In this test, the null hypothesis states that the series is random and the alternative hypothesis that the elements of the sequence are not independently drawn from the same distribution, meaning there is no randomness in the number of runs.

H_0: the elements of the series are mutually independent

H_A: the elements of the sequence are dependent

The test statistic is the following:

[33] Calculated by selecting the smallest value between $\frac{n}{2} - 2$ and 40.

$$Z = \frac{R - \mathbb{E}[R]}{\sigma[R]},$$

where R is the number of runs, and $\mathbb{E}[R]$ and $\sigma[R]$ denote the expected number and standard deviation of runs respectively.[34] Under H_0, Z follows a normal distribution. The null hypothesis is rejected when $|Z| > Z_{1-\frac{\alpha}{2}}$, where $Z_{1-\frac{\alpha}{2}}$ is the critical value at a given 'α' critical value from a normal distribution (Wald and Wolfowitz, 1940).

If H_0 holds, the observations in the IOTA returns series would be mutually independent. This comes to say that the probability that a certain return (r_t) is positive or negative is not influenced by prior observations. Therefore, if the null hypothesis cannot be rejected, the IOTA market will show signs of being weak-form efficient and all current information will be reflected in the IOTA price.

6.3 Bartels Test

In rank tests, data are replaced by the order in a sample. The highest value in the sample will receive the highest rank. Suppose we have the following randomly generated series: $x_1 = 6,\ x_2 = 1,\ x_3 = 8,\ x_4 = -6,\ x_5 = 0\ and\ x_6 = -9$. If we applied ranks $R(x_t)$ to the previously-mentioned series we would obtain the following:

Table 6.1: Rank Test Example

$\boldsymbol{t}$	1	2	3	4	5	6
$\boldsymbol{x_t}$	6	1	8	-6	0	-9
$\boldsymbol{R(x_t)}$	5	4	6	2	3	1

Source: Author's own elaboration

Rank tests are particularly useful when testing for monotone trends in time series and can be more powerful than runs tests when testing for randomness (Bartels, 1982) as rank tests such as Bartels ignore the

[34] $\mathbb{E}[R] = \frac{2N_+N_-}{N} + 1$, where N_+ is the number of observations larger than the median, N_- those smaller than the median and N is the total number of observations.

$\sigma[R] = \sqrt{\frac{2N_+N_-(2N_+N_- - N)}{N^2(N-1)}}$, where the prior notation of N_+, N_- and N holds.

magnitude of the data points of a series (Cromwell et al., 1994). Furthermore, this type of test is robust against outliers, which is especially useful for our study given that IOTA has many significant outliers (e.g., on the 13/03/2020 IOTA's price dropped 56% in a single day). The aforementioned test statistic is a nonparametric version of a test originally proposed by mathematician John Von Neumann in 1941. In Bartels' version, the test statistic substitutes ranks for observations. This statistical test is defined in the following way:

H_0: the observations are stochastically independent

H_A: the observations are dependent

The test statistic is given by:

$$RVN = \frac{\sum_{i=1}^{T-1}(R_i - R_{i+1})^2}{\sum_{i=1}^{T}(R_i - \bar{R})^2},$$

where R_i is the rank of the i^{th}observation, T is the number of observations and $\bar{R}$ denotes the average rank.

Under H_0, the test statistic follows an asymptotic normal distribution with $\mu = 2,\ \sigma = 4/T$. The critical values for null hypothesis rejection are given in Bartels (1982). Furthermore, Bartels (1982) found that the $N(2, 20/(5n + 7))$ gives an improved distribution.

The Bartels test provides evidence for the IOTA returns being stochastically independent whenever we fail to reject the null hypothesis. This comes to say that the occurrence of any past return does not affect the probability of occurrence of another return. In this regard, past IOTA prices would have no relationship with current market prices so future prices would not be possible to predict.

6.4 AVR Test

Variance Ratio (VR) tests are extensively used when testing for Random Walk Hypothesis, as they have been proven to be quite powerful in this context. In essence, VR tests evaluate whether or not the variance of a series is stationary. Lo and MacKinlay (1988) fashioned the first VR Test based on the property that the variance of increments of a random walk X_t is linear in its data interval (Chen, 2008). This comes to say that the variance of $X_t - X_{t-q}$ is 'q' times the variance of $X_t - X_{t-1}$. An issue with this test is choosing a suitable value for the parameter 'q'. Popular holding periods ('q' values) are $(2, 5, 10, 20, 40)$ for daily returns (Kim, 2009). Nevertheless, the choice of this parameter is completely arbitrary at best; to avoid making unsubstantiated decisions with no statistical justification, we consider the Automatic Variance Ratio Test from Choi (1999). This AVR test eliminates the need of the researcher of inputting a value for the parameter 'q', which is determined using a completely data-dependent procedure based on Andrews (1991). Furthermore, we use the Wild Bootstrapped[35] version of Kim (2009) because it estimates the distribution of the test statistic and allows us to assess the significance of the results. In Kim (2009), the null and alternative Hypothesis, the VR estimator and test statistic are defined as in Choi (1999):

H_0: Δr_t is serially uncorrelated (where $\Delta r_t = r_t - r_{t-1}$)
H_A: Δr_t is serially correlated

The VR estimator is: $VR(k) = 1 + 2\sum_{i=1}^{T-1} h\left(\frac{i}{k}\right)\hat{p}(i)$ [36], where $\hat{p}$ is the autocorrelation function and k is the holding period.

The test statistic is defined as:

$$VR_f = \frac{VR(k) - 1}{\sqrt{2}\left(\frac{T}{k}\right)^{-1/2}} \xrightarrow{d} N(0,1)$$

Under H_0, the VR converges in distribution to a standard normal distribution. When the test statistic is greater than the critical value of a normal distribution for a given significance level 'α', H_0 is rejected.

If $VR(k)$ is close to unity for all horizons of k, the IOTA returns are expected to follow a random walk, whereas if the test statistic is higher (lower) than unity, the IOTA returns would be positively (negatively) correlated (Charles and Darné, 2009). The null hypothesis is not rejected when the test statistic is close to unity, therefore, if we fail to reject H_0 it means that the IOTA market is weak-form efficient and future prices cannot be predicted. The AVR test will suggest that the IOTA returns are mean reverting (averting) if the null hypothesis is rejected due to the test statistic being significantly lower (higher) than unity, at long k horizons (Poterba and Summers, 1988).

---

35 Bootstrapping is a resampling method initially proposed by Efron (1979) that mimics the sampling process by using random sampling with replacement.

36 Where $h(x) = \frac{25}{12\pi^2 x^2}\left[\frac{\sin\left(\frac{6\pi x}{5}\right)}{6\pi x/5} - \cos\left(\frac{6\pi x}{5}\right)\right]$, and $x = \frac{i}{k}$.

6.5 BDS Test

The BDS test was first introduced in Brock et al. (1996) and is a Portmanteau test used in univariate time series analysis used when checking for possible deviation from independence. For this test we consider a pair of points and a given distance ε, which is fixed throughout the whole procedure of the test. If the observations of the time series are independent and identically distributed then, for any set of pairs, the probability that the distance between the two observations of each pair is greater or smaller than ε should be constant for every pair. The notation for this probability is $c_1(\varepsilon)$. To construct the set of pairs, we choose consecutive numbers so that said pairs are ordered chronologically. We denote the number of consecutive points in the set by m. The joint probability of the set of pairs satisfying the distance ε condition is denoted by $c_m(\varepsilon)$. Under the assumption of independence, the following should hold:

$$c_m(\varepsilon) = c_1^m(\varepsilon)$$

However, when working with real data, $c_1(\varepsilon)$ and $c_m(\varepsilon)$ are estimated, so the previous condition is less strict. The larger the deviation from the aforementioned equality is, the less likely it is that said error was caused by random sample variations.

In order to perform the BDS independence test, a value has to be assigned to parameters ε (the fixed distance between observations being tested) and m (the number of consecutive terms or embedded dimensions). We rely on previous literature with similar objectives (testing for weak-form efficiency), “assets” (cryptocurrencies) and sample size to select an appropriate value for the embedding dimension parameter (Aslaksen and Wiersdalen, 2019). Furthermore, Brock et al. (1996) defends using a distance ε in the range of [0.5σ , 1.5σ]. Again, based on Aslaksen and Wiersdalen (2019), we choose to use $\varepsilon = \sigma$.

The test is statistically defined in the following way:

H_0: the data generating processes are iid

H_A: the model may be misspecified.

When H_0 holds, the test statistic (given below) is assumed to follow a normal distribution:

$$w_{m,n}(\varepsilon) = \sqrt{n-m+1} \cdot \frac{c_{m,n}(\varepsilon) - c_{1,n-m+1}^m(\varepsilon)}{\sigma_{m,n}(\varepsilon)},$$

where sigma is the square root of the variance, which is defined in the following way (Belaire-Franch and Contreras, 2002):

$$\sigma_{m,n}^2(\varepsilon) = 4\left[k^m + 2\sum_{j=1}^{m-1} k^{m-j}c^{2j} + (m-1)^2c^{2m} - m^2kc^{2m-2}\right].$$

When H_0 is true, $w_{m,n}(\varepsilon)$ follows a normal distribution. When the test statistic is greater than the critical value of a normal distribution for a given significance level 'α', H_0 is rejected.

When the BDS test statistic fails to reject the null hypothesis it suggests the IOTA market has no memory in the sense that the occurrence of any single return does not provide any information regarding the probability of occurrence of future returns. In this situation, the IOTA market would respond to the characteristics of weak-form efficiency and future prices would be impossible to predict using past observations.

6.6 Hurst Exponent and R/S Analysis

In 1951, engineer and hydrologist Harold Hurst developed the Rescaled Range Analysis (R/S Hurst) as a result of his wanting to check if the accumulation of water in the river Nile above and below average values was random. Hurst got his inspiration from Einstein's (1905) brownian motion (random process definition) research paper. Since then, many authors have added to Hurst (1951), some even suggesting the Hurst exponent (H) could be used in financial analysis to predict future prices (Qian and Rasheed, 2004). To estimate the Hurst exponent using the Rescaled Range (R/S) as in Hurst (1951), we use Tzouras et al. (2015):

1. Assume a time series, $X = X_1, X_2 \dots X_N$

2. Calculate the mean of said time series, $\mu = \frac{1}{N}\sum_{i=1}^{N} X_i$

3. Create a mean adjusted series (Y), $Y_t = X_t - \mu,\quad t = 1, 2, 3 \dots N$

4. Calculate the cumulative deviation series (Z), $Z_t = \sum_{t=1}^{N} Y_t,\quad t = 1, 2, 3 \dots N$

5. Calculate the range series (R),

$R_t = \max(Z_1, Z_2 \dots Z_N) - \min(Z_1, Z_2 \dots Z_N), \qquad t = 1, 2, 3 \dots N$

6. Calculate the standard deviation series (S),

$S_t = \sqrt{\frac{1}{t}\sum_{i=1}^{t}(X_i - u)^2}\,, \qquad t = 1, 2, 3 \dots N, \qquad$ where u is the mean value from X_1 to X_t.

7. Calculate the Rescaled Range Series $(R/S)_t = \dfrac{R_t}{S_t}, \qquad t = 1, 2, 3 \dots N$

Hurst Exponent (H) is related to $(R/S)_t$ in the following way:

$$(R/S)_t = c_\alpha t^H$$

Where c_α is a constant. H is estimated by plotting (R/S) against t in a $log - log$ axis and using Ordinary Least Squares (OLS) to estimate the curve of the slope (which would be the Hurst Exponent).

The R/S Hurst Analysis is statistically defined in the following way:

$H_0: H = {}^1\!/_2$

$H_A: H \neq {}^1\!/_2$

The R/S Hurst Analysis does not provide any p-values as no asymptotic distribution has been derived for the Hurst Exponent statistic. Mandelbrot (1969) developed a method where the null hypothesis is rejected both when $H > 1/2$ due to the series showing signs of persistence and trend reinforcing behaviour, and when $H < 1/2$ because the Hurst exponent in that situation suggests anti-persistence and mean reverting behaviour. When $H \approx 1/2$, the return series is said to show signs of following a random walk. For values of the Hurst Exponent close to 0.5, we turn to Mitra (2012) that accepts any value of H in the range [0.45 , 0.55] to qualify as a random process.

If H_0 is close to 0 and the null hypothesis cannot be rejected, the R/S Hurst Analysis provides evidence for the IOTA market being weak-form efficient. This comes to say that the IOTA returns would follow a random walk and investors would not be able to earn excess returns in IOTA based on historical data and past performance.

7 Results

In this section we display the results from the tests mentioned in Section 6. We choose a significance level of 5% for all statistical tests, except for the R/S Hurst analysis for which we turn to previous literature (Mitra, 2012) and (Aslaksen and Wiersdalen, 2019) to select [0.45 , 0.55] as a suitable range that is consistent with a random series. The p-values and Hurst Exponent (H) are presented in tables for each test.

The tests included in this paper have been computed using programming language R. In order to facilitate further research, we have incorporated all the code we use for these tests in the Appendix B.

7.1 Ljung-Box Test

To obtain a test statistic with its corresponding p-value, the «Box.test» command is used in R. In said command, we stipulate that the number of lags is 40 («lag = 40») for all the samples being studied, and we indicate the type of box test we want to perform, in this case we want the Ljung-Box test («type = "Ljung-Box"»), as opposed to the Box-Pierce test. As mentioned in Section 7.1, H_0 states that there is no autocorrelation up to a specific lag L.

Table 7.1: Ljung-Box Test p-values

Sample Period	p-values
15/6/2017 – 25/04/2021	(0.0763)
15/06/2017 – 15/12/2018	(0.2009)
16/12/2018 – 17/03/2020	(0.6852)
18/03/2020 – 24/04/2021	(0.5096)

Table 7.1 displays the p-values from the Ljung-Box test performed in the full sample and three subsamples. We fail to reject the null hypothesis of no autocorrelation for all the samples. The p-values do not show any evidence of sample autocorrelation and therefore all the periods are consistent with the weak-form of EMH. These results suggest that the historical prices of IOTA do not have explanatory power for current or future prices, as the price series seems to follow a random process.

7.2 Runs Test

For the Runs test application in R, we used the «runs.test» command from the «randtests» package in R. H_0 specifies that the data is identically and independently distributed (iid). The smaller the difference between the expected and observed number of runs, the closer the Runs test statistic gets to 0. This is due to the nature of the statistic itself (a Z-score).

Table 7.2: Runs Test p-values

Sample Period	p-values
15/6/2017 - 25/04/2021	(0.0000)
15/06/2017 - 15/12/2018	(0.0261)
16/12/2018 - 17/03/2020	(0.0015)
18/03/2020 - 24/04/2021	(0.0903)

H_0 is rejected for all samples except for the third subsample, for which we fail to reject the null hypothesis of iid IOTA daily returns. These results show a significant sign of the returns being dependent, although it is worth noting that the last subsample showed evidence of weak-form market efficiency. The results we obtain from the Runs test appear to provide evidence for an evolution in the IOTA market towards weak-form efficiency, which would suggest that more recent observations follow a random, non-predictable process. If that were to be the case, investors could have benefitted in the past from using technical analysis to generate excess returns, but not anymore.

7.3 Bartels Test

To obtain results for the Bartels test, we used the command «bartels.rank.test» from the «randtests» package in R. As mentioned in Section 6.3, the null hypothesis of the Bartels test specifies that the returns are stochastically independent.

Table 7.3: Bartels Test p-values

Sample Period	p-values
15/6/2017 - 25/04/2021	(0.0001)
15/06/2017 - 15/12/2018	(0.1618)
16/12/2018 - 17/03/2020	(0.0098)
18/03/2020 - 24/04/2021	(0.0019)

Table 7.3 clearly shows that there is significant evidence for rejecting the null hypothesis in all samples except for the first subsample, for which the null hypothesis of stochastically independency in the returns cannot be rejected. This comes to say that the full sample and the second and third subsample present signs of autocorrelation in the returns thus indicating the existence of inefficiency in the IOTA market. Bartels test results suggest a possible deviation from market efficiency. According to this test, it seems that at the earlier stages of IOTA's lifespan, its market was efficient, and it has become more inefficient as time has passed.

7.4 AVR Test

To conduct the AVR test we use the «AutoBoot.test» command in R, from the package «vrtest». This specific function is a wild bootstrapped version of Choi (1999) AVR («Auto.VR» command in R). The reason for using the «AutoBoot.test» command is that «Auto.VR» does not provide p-values. Both functions return the same test statistic. To obtain reliable and robust results, we use 10,000 bootstrap iterations («nboot = 10000»). Because this test is two tailed, to make sure, we should specify in our command that the area at the critical region of each tail must be $\frac{\alpha}{2} = 2.5\%$ («prob=c(0.025 , 0.975)»).

Table 7.4: AVR Test p-values

Sample Period	p-values
15/6/2017 - 25/04/2021	(0.8434)
15/06/2017 - 15/12/2018	(0.5757)
16/12/2018 - 17/03/2020	(0.1741)
18/03/2020 - 24/04/2021	(0.2258)

We fail to reject the null hypothesis that the price follows a random walk. The results obtained for the AVR test for all samples overall provide strong evidence of the existence of weak-form efficiency in the IOTA market. This would suggest that there is no benefit in projecting the series to obtain future values using historical prices over doing so without any knowledge of past observations.

7.5 BDS Test

To conduct the BDS test we used the «bdsTest» command from the «fNonlinear» package in R. To use the aforementioned package it is required that the packages «timeDate», «timeSeries» and «fBasics» are also installed and loaded in the R workspace. In the BDS test, H_0 states that the returns are independent and identically distributed. Rejection of the null hypothesis indicates the possibility that the market may be inefficient. Previous literature on cryptocurrencies with similar sample sizes (namely Aslaksen and Wiersdalen) suggests that a sensible value for m is 8. As for ε, Brock et. Al (1996) suggests choosing a distance in the range [0.5σ , 1.5σ] so we used $\varepsilon = \sigma$ for our analysis.

Table 7.5: BDS Test p-values

Sample Period	Embedding dimensions (*m*)	p-values
15/6/2017 - 25/04/2021	2	(0.0000)
	3	(0.0000)
	4	(0.0000)
	5	(0.0000)
	6	(0.0000)
	7	(0.0000)
	8	(0.0000)
15/06/2017 - 15/12/2018	2	(0.0000)
	3	(0.0000)
	4	(0.0000)
	5	(0.0000)
	6	(0.0000)
	7	(0.0000)
	8	(0.0000)
16/12/2018 - 17/03/2020	2	(0.0003)
	3	(0.0000)
	4	(0.0000)
	5	(0.0000)
	6	(0.0000)
	7	(0.0000)
	8	(0.0000)
18/03/2020 - 24/04/2021	2	(0.0014)
	3	(0.0000)
	4	(0.0000)
	5	(0.0000)
	6	(0.0000)
	7	(0.0000)
	8	(0.0000)

The null hypothesis of independent and identically distributed results is rejected for all samples and embedding dimensions. There is no indication, as per the BDS test, that the IOTA returns are iid and therefore there is strong evidence of the market being inefficient. Based on the results for this test, any investor wishing to generate excess returns could potentially due so using technical analysis.

7.6 Hurst Exponent and R/S Analysis

To compute the Hurst Exponent (H) we use the «hurstexp» command in R, from the Practical Numerical Math Functions («pracma») package. The aforementioned command returns five H coefficients, and we choose the Simple R/S Hurst estimation. Results for the other approaches: corrected R/S method, an empirical and corrected empirical method, and an attempt at a theoretical Hurst exponent[37] can vary significantly so one must be cautious when using them for reaching conclusions on the long-term memory of the time series.

Table 7.6: R/S Hurst Exponents (H)

Sample Period	H
15/6/2017 - 25/04/2021	0.5788
15/06/2017 - 15/12/2018	0.5899
16/12/2018 - 17/03/2020	0.5085
18/03/2020 - 24/04/2021	0.5456

From Table 7.6 we see that the full sample and first subsample show evidence for mild persistence in the IOTA returns series. Mitra (2012) accepts any value of H in the range [0.45 , 0.55] to qualify as evidence for the data following a random process, thus the second and third subsample, according to Mitra (2012), do not have a sufficiently high enough H to be considered as evidence for existing persistence. A useful characteristic of H is that when it is above 0.5 (significantly), it means that an observation will have the same sign as the one directly before it, with a probability equal to H itself. For example, in the full sample, if an observation at $t-1$ (for any given t) is positive, then the probability that the observation at t is positive is 57.88% (Peters, 1991, s. 76). The results from the second and third subsample are not consistent with the first subsample but overall, the IOTA returns series does show evidence for persistence and trend reinforcing behaviour and is thus not consistent with the weak-form efficiency hypothesis. Based on Mitra (2012), there

[37] Source: RDocumentation https://www.rdocumentation.org/packages/pracma/versions/1.9.9/topics/hurstexp

is evidence to suggest there has been an evolution towards weak-form efficiency in the IOTA market. Nevertheless, the Hurst Exponent for the last subsample is very close to the upper limit of the range Mitra provides and therefore may suggest a possible deviation towards inefficiency in more recent observations.

7.7 Discussion

The weak-form efficiency element from the Efficient Market Hypothesis states that past prices cannot predict future prices, and investors cannot benefit from any form of technical analysis to outperform the market. Following Urquhart (2016) and Aslaksen and Wiersdalen (2019), in order to detect possible weak-form efficiency in the IOTA market, we have run six statistical tests. The corresponding p-values to each test (and the H exponent) are included in the following table:

Table 7.7: Summary of Results (p-values and Hurst Exponent)[38]

Sample Period	Ljung-Box	Runs	Bartels	AVR	BDS	R/S Hurst
15/6/2017 - 25/04/2021	(0.0763)	(0.0000)*	(0.0001)*	(0.8434)	(0.0000)*	0.5788
15/06/2017 - 15/12/2018	(0.2009)	(0.0261)*	(0.1618)	(0.5757)	(0.0000)*	0.5899
16/12/2018 - 17/03/2020	(0.6852)	(0.0015)*	(0.0098)*	(0.1741)	(0.0000)*	0.5085
18/03/2020 - 24/04/2021	(0.5096)	(0.0903)	(0.0019)*	(0.2258)	(0.0000)*	0.5456

The results obtained, for all samples as a whole, are open to interpretation, as the outcome of the tests do not provide overall solid evidence of inefficiency or efficiency. All samples fail to reject the null hypothesis of iid returns and absence of serial correlation when computing the Ljung-Box and AVR tests, respectively, suggesting the possibility of weak-form efficiency in the IOTA market. However, all samples have statistically significant p-values which indicate strong evidence against H_0 for the BDS test, pointing to a possible deviation from independence and contradicting to a certain extent the results obtained for the Ljung-Box test. Furthermore, all samples except the third subsample reject the null hypothesis of randomness of the Runs test. For the Bartels test, the only sample that does not present significant p-values is the first subsample. The R/S Hurst results are especially interesting because the full sample and first subsample show evidence for persistence and trend reinforcing behaviour whereas the last two subsamples seem to suggest the IOTA returns follow a random process.

[38] Note: Asterisks indicate statistically significant p-values (for $\alpha = 5\%$).

Urquhart (2016) and Aslaksen and Wiersdalen (2019) arrive at similar ambiguous overall results. For that reason, both pay particular attention to the possibility of there being an evolution in the Bitcoin market over time. In this regard, we do not achieve any auspicious results as the evidence we find for an evolution towards weak-form efficiency over the three subsamples is weak, at the very least. Although it is true that the third subsample fails to reject the null hypothesis of the Runs test, it rejects the one of the Bartels test. As mentioned earlier in Section 6.3, the Bartels test is considered to be more powerful than the Runs test, since it accounts for the magnitude of the observations (Cromwell et al, 1994). Because of this, we give greater importance to the results obtained in Bartels. The only test, apart from the Runs test, that may show an evolution towards weak-form efficiency is the R/S Hurst. As stated previously in Section 6.6, even though the H exponent of the third subsample is larger than 0.5, according to Mitra (2012) a Hurst exponent of 0.5456 can be considered random. Nonetheless, this value is close to the upper limit proposed in the aforementioned paper. Therefore, it would be far-fetched to posit a reliable conclusion in connection to the point previously mentioned regarding the possibility of an evolution in IOTA towards a more efficient market.

The Ljung-Box and AVR tests are the only ones that fail to reject the null for all samples. The BDS test rejects H_0 for all samples and Bartels and Runs reject the null for most of them. Half of the Hurst exponents reject the null hypothesis, but if we factor into account that the last subsample is in the limit proposed by Mitra (2012) and we were to call for a stricter range (say [0.475 , 0.525]), three out of four samples would reject the null hypothesis. Therefore, four out of six tests either reject the null hypothesis of efficiency totally or partially. As a result, based on our findings, our overall conclusion is that the IOTA market is inefficient and there is no evidence strong enough to suggest that with time it is becoming more efficient. This means, in terms of the Efficient Market Hypothesis that IOTA's historical prices have information that can be used to predict future prices, to a certain extent. Because of this, apart from being able to use fundamental analysis to generate excess returns (which is also possible in a weak-form efficient market), investors could potentially outperform the market by using technical analysis.

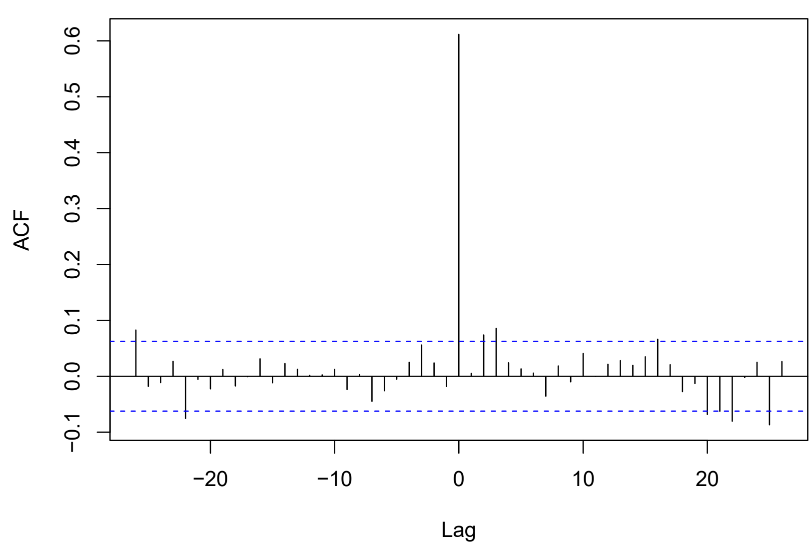
8 Conclusion

In this section we provide our conclusions as to wₕat degree the IOTA market can be considered weak-form efficient. Moreover, we provide potentially interesting further areas of study regarding IOTA.

Even though we have computed six different statistical tests, it is not possible to determine with complete certainty if the IOTA price follows a random process, although we do believe there is more evidence to suggest that historical prices may have explanatory power in future IOTA prices. This potential lack of randomness in the IOTA market means that in terms of the Efficient Market Hypothesis proposed by Fama (1970), IOTA's market is not weak-form efficient. Consequently, our findings point to the existence of inefficiency, enabling investors to beat the IOTA market (generate excess returns) using technical analysis.

In this paper we have discussed some of the underlying economic qualities of IOTA and what they mean for potential investors in terms of market efficiency within the meaning of Fama (1970). Future research could explore the factors that influence the price of IOTA to find out if other cryptocurrencies could be used to predict IOTA prices. We mention earlier in Section 5.5 that IOTA and Bitcoin are positively correlated. The correlation coefficient that we calculate is using daily frequency. The following figure shows a cross correlation function between IOTA and Bitcoin daily returns for the period 15/6/2017 - 25/04/2021 (our full sample period).

Figure 8.1: IOTA and Bitcoin Cross Correlation



Source: Own elaboration, CoinGecko.com https://www.coingecko.com/es

It would be interesting to run an autocorrelation function for higher frequency data to see if the correlation coefficients hold (only the correlation at lag 0 for daily frequency is significant) or maybe IOTA takes some time (minutes or hours) to respond to changes in the price of Bitcoin. Furthermore, it could be the case that IOTA does not follow Bitcoin and that the price of both cryptocurrencies is affected simultaneously by an unknown factor. Either way, we believe it is an interesting area of further research that could shed some light into what drives altcoins' prices.

Bibliography

Andrews, D. W. (1991). Heteroskedasticity and Autocorrelation Consistent Covariance Matrix Estimation. *Econometrica, 59*(3), 817.

Aslaksen, K., & Wiersdalen, A. L. B. (2019). *Statistical Analysis of the (In)efficiency of Bitcoin : A comparison of the weak form efficient market hypothesis in the Us and Venezuela* (dissertation).

B. Lee, T. (2017, October 5). *Explaining the new cryptocurrency bubble-and why it might not be all bad.* Ars Technica. https://arstechnica.com/tech-policy/2017/10/explaining-the-new-cryptocurrency-bubble-and-why-it-might-not-be-all-bad/.

Bartels, R. (1982). The Rank Version of von Neumann's Ratio Test for Randomness. *Journal of the American Statistical Association, 77(*377), 40–46.

Bayer, D., Haber, S., & Stornetta, W. S. (1992). Improving the Efficiency and Reliability of Digital Time-Stamping. *Sequences II,* 329–334.

Bech, M. L., & Garratt, R. (2017). Central bank cryptocurrencies. *BIS Quarterly Review,* 55–70. https://doi.org/https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

Belaire-Franch, J., & Contreras, D. (2002). How to compute the BDS test: a software comparison. *Journal of Applied Econometrics, 17*(6), 691–699.

Brock, W. A., Scheinkman, J. A., Dechert, W. D., & LeBaron, B. (1996). A test for independence based on the correlation dimension. *Econometric Reviews, 15*(3), 197–235.

Brockwell, P. J., & Davis, R. A. (2016). *Introduction to time series and forecasting.* Springer.

Charles, A., & Darné, O. (2009). Variance Ratio Tests of Random Walk: An Overview. *Journal of Economic Surveys, 23*(3), 503–527.

Charles, A., Darné, O., & Kim, J. H. (2011). Small sample properties of alternative tests for martingale difference hypothesis. *Economics Letters, 110*(2), 151–154.

Chen, J.-H. (2011). Variance Ratio Tests Of Random Walk Hypothesis Of The Euro Exchange Rate. *International Business & Economics Research Journal (IBER), 7*(12), 97-106.

Choi, I. (1999). Testing the random walk hypothesis for real exchange rates. *Journal of Applied Econometrics, 14*(3), 293–308.

Cromwell, J. B., Hannan, M. J., Labys, W. C., & Terraza, M. (1994). *Multivariate tests for time series models.* Sage.

Efron, B. (1979). Bootstrap Methods: Another Look at the Jackknife. *The Annals of Statistics, 7*(1), 1-26. https://doi.org/10.1214/aos/1176344552

Einstein, A. (1905). Investigations on the Theory of Brownian Motion. https://www.maths.usyd.edu.au/u/UG/SM/MATH3075/r/Einstein_1905.pdf

Fama, E. F. (1970). Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance, 25*(2).

Gross, J. (2020, September 29). Programmable money and programmable payments. Retrieved June 2, 2021, from https://jonasgross.medium.com/programmable-money-and-programmable-payments-c0f06bbcd569

Grossman, S. J., & Stiglitz, J. E. (1980). On the Impossibility of Informationally Efficient Markets. *The American Economic Review, 70*(3), 393–408.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC '96.* https://doi.org/10.1145/237814.237866

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology, 3*(2), 99–111.

Hurst, H. E. (1951). Long-Term Storage Capacity of Reservoirs. *Transactions of the American Society of Civil Engineers, 116*(1), 770–799.

Kim, J. H. (2009). Automatic variance ratio test under conditional heteroskedasticity. *Finance Research Letters, 6*(3), 179–185. https://doi.org/10.1016/j.frl.2009.04.003

Lamport, L. (1979). Constructing digital signatures from a one-way function. *SRI International Computer Science Laboratory.* Available at the following site: https://doi.org/https://www.microsoft.com/en-us/research/uploads/prod/2016/12/Constructing-Digital-Signatures-from-a-One-Way-Function.pdf

Ljung, G. M., & Box, G. E. (1978). On a measure of lack of fit in time series models. *Biometrika, 65*(2), 297–303.

Lo, A., & MacKinlay, A. C. (1988). Stock Market Prices Do Not Follow Random Walks: Evidence From a Simple Specification Test. https://doi.org/10.3386/w2168

Malkiel, B. G. (1989). Efficient Market Hypothesis. *Finance,* 127–134. https://doi.org/10.1007/978-1-349-20213-3_13

Malkiel, B. G. (2003). The Efficient Market Hypothesis and Its Critics. *Journal of Economic Perspectives, 17*(1), 59–82.

Mandelbrot, B. B., & Wallis, J. R. (1969). Robustness of the rescaled range R/S in the measurement of noncyclic long run statistical dependence. *Water Resources Research, 5*(5), 967–988. https://doi.org/10.1029/wr005i005p00967

Mavroeidis, V., Vishi, K., D. Zych, M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications, 9*(3).

Mitra, S. K. (2012). Is Hurst Exponent Value Useful in Forecasting Financial Time Series? *Asian Social Science, 8*(8), 111–120.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://doi.org/https://bitcoin.org/bitcoin.pdf

Peters, E. E. (1996). *Chaos and order in the capital markets: a new view of cycles, prices, and market volatility.* John Wiley.

Popov, S. (2015). The Tangle. Manuscript available at the following site: https://doi.org/https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

Popov, S. (2018, June 29). On the Tangle, White Papers, Proofs, Airplanes, and Local Modifiers [web log]. https://blog.iota.org/on-the-tangle-white-papers-proofs-airplanes-and-local-modifiers-44683aff8fea/.

Poterba, J., & Summers, L. (1988). Mean Reversion in Stock Prices: Evidence and Implications. https://doi.org/10.3386/w2343

Qian, B., & Rasheed, K. (2005). Hurst Exponent and Financial Market Profitability. https://doi.org/https://www.semanticscholar.org/paper/HURST-EXPONENT-AND-FINANCIAL-MARKET-PREDICTABILITY-Qian-Rasheed/0816a5a989c8d2431a6d20076d27c4295c00fb77

Rizzo, P. (2021, March 4). *The Bitcoin Bubble Myth.* Forbes. Article can be found in the following link: https://www.forbes.com/sites/peterizzo/2021/03/04/the-bitcoin-bubble-myth/?sh=67cb07be37c1.

Rueda, M. (2018, June 14). *¿Qué son las 'smart cities'?* BBVA NOTICIAS. https://www.bbva.com/es/las-smart-cities/.

Raimundo, M.S., & Okamoto Jr, J. (2018). Application of Hurst Exponent (H) and the R/S Analysis in the Classification of FOREX Securities. *International Journal of Modeling and Optimization, 8*(2), 116–124.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science.* https://doi.org/10.1109/sfcs.1994.365700

Silvano, W. F., & Marcelino, R. (2020). Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future Generation Computer Systems, 112,* 307–319.

Singer, A. (2020, September 16). Programmable money: How crypto tokens could change our entire experience of value transfer. Retrieved June 1, 2021, from https://cointelegraph.com/magazine/2020/09/16/programmable-money-crypto-tokens

Tzouras, S., Anagnostopoulos, C., & McCoy, E. (2015). Financial time series modeling using the Hurst exponent. *Physica A: Statistical Mechanics and Its Applications, 425,* 50–68.

Unknown. (2011, February 21). *Why Log Returns.* Quantivity. Available at the following site: https://quantivity.wordpress.com/2011/02/21/why-log-returns/.

Unknown. (2019, October 23). *What is the difference between Coins and Tokens?* Ledger. https://www.ledger.com/academy/crypto/what-is-the-difference-between-coins-and-tokens.

Urquhart, A. (2016). The Inefficiency of Bitcoin. *Economics Letters, 148,* 80–82*.* Paper available at: https://doi.org/10.2139/ssrn.2828745

Wald, A., & Wolfowitz, J. (1940). On a Test Whether Two Samples are from the Same Population. *The Annals of Mathematical Statistics, 11*(2), 147–162.

Zentai, D. (2020). On the Efficiency of the Lamport Signature Scheme. *Land Forces Academy Review, 25(*3), 275–280.

Appendix

Glossary

Altcoin	**Any cryptocurrency different to Bitcoin (and Ethereum according to some definitions).**
Coin (Cryptography)	**Any cryptocurrency that has a unique and independent distributed ledger.**
Cryptocurrency	**Digital currencies that are built on a distributed ledger and are secured by cryptography.**
Cryptographic Hash Function	**An algorithm that maps a message to a fixed-size compressed-array of data.**
Cryptography	**The methods of securing data through the use of encryption and encodement.**
Decentralised (Cryptocurrency)	**When a system enables investors (participants of the network) to deal and transact directly with each other without the presence of an intermediary or central figure.**
Decentralised Finance (DeFi)	**A system where financial products are not offered by intermediaries such as banks or brokerage firms, instead these products are available on a public decentralised blockchain network.**
Directed Acyclic Graph (DAG)	**A graph made up by directed edges (from one vertex to another) in which there is never a closed loop.**
Distributed Ledger	**Synchronised databases across multiple sites where any change is reflected and copied to all participants, essentially having public witnesses.**
E-Health	**A healthcare practice that makes use of emerging information and technology (such as the Internet) to address and solve health problems.**
Genesis Block	**The block cryptocurrencies are 'born' from, it is the template for all subsequent blocks of the chain.**

Hashgraph	**A distributed ledger based on a DAG (like IOTA). It is a patented technology that focuses on the needs of the private corporate sector.**
Internet of Things (IoT)	**A concept that refers to the system of digital objects that are internet-connected and able to collect and transfer data over a wireless network, without human intervention.**
Machine to Machine (M2M)	**A concept that refers to the exchange of information between devices.**
Market Capitalisation	**Refers to the total value of a cryptocurrency, calculated by multiplying the total supply of coins or tokens a cryptocurrency has by their market value.**
Merkle Trees	**A ramified data structure used in blockchain that is used for outlining and verifying the integrity of a database.**
Microtransactions	**Financial transactions conducted over the Internet that have a value so small that if they were to be done using conventional means of payments, processing the transaction would cost more than the transaction itself**.
Non-Fungible Tokens (NFTs)	**Digital assets that represent a unique tangible or intangible item and are generally created using the same underlying technology as cryptocurrencies.**
Open-Source	**Software that is produced as a collaboration, shared at no cost, published transparently, and created for the benefit of the community rather than a private good for a certain company or individual.**
Smart Cities	**Complex and interconnected systems that detect the needs of citizens of a particular city or town and react to these demands by managing the interactions between its citizens and its public services in a more efficient manner.**
Smart Contract	**Self-executing programmes stored in a blockchain, that run when some specific predetermined conditions are met.**
Token (Cryptography)	**Cryptocurrencies that use the distributed ledger technology of another cryptocurrency and are therefore derivatives of said original distributed ledger.**

R Code

```
###########################
#IMPORT DATA
###########################
#Insert Full Sample Data
library(readxl)
IOTA_Daily_Returns_FS <- read_excel("miota-usd-max (1).xls",
                         sheet = "IOTA.returns.fullsample", col_types = c("date",
                                                                           "numeric"))
View(IOTA_Daily_Returns_FS)
###########################
#Insert First Subsample Data
library(readxl)
IOTA_Daily_Returns_S1 <- read_excel("miota-usd-max (1).xls",
                         sheet = "sample1.ret", col_types = c("date",
                                                                "numeric"))
View(IOTA_Daily_Returns_S1)
##########################
#Insert Second Subsample Data
library(readxl)
IOTA_Daily_Returns_S2 <- read_excel("miota-usd-max (1).xls",
                         sheet = "sample2.ret", col_types = c("date",
                                                                "numeric"))
View(IOTA_Daily_Returns_S2)
##########################
#Insert Third Subsample Data
library(readxl)
IOTA_Daily_Returns_S3 <- read_excel("miota-usd-max (1).xls",
                         sheet = "sample3.ret", col_types = c("date",
                                                                "numeric"))
```

```
View(IOTA_Daily_Returns_S3)
##########################
#Insert IOTA Prices and Trading Volume
library(readxl)
Price_VS_Volume <- read_excel("miota-usd-max (1).xls",
                              sheet = "price.vs.volume", col_types = c("date",
                                                                       "numeric", "numeric"))
View(Price_VS_Volume)
##########################
library(readxl)
BTC_vs_IOTA <- read_excel("miota-usd-max (1).xls",
                        +    sheet = "iota vs btc", col_types = c("date",
                                                                  +        "numeric", "numeric"))
View(BTC_vs_IOTA)
##########################
library(readxl)
Absolute_Market_Cap    <-    read_excel("~/Desktop/Oscar/UAM/Cuarto/Segundo    Semestre/TFG/Market
Cap/Market Cap.xlsx",
                              +    sheet = "Absolute", col_types = c("text",
                                                                     +        "numeric"))
View(Absolute_Market_Cap)
##########################

library(readxl)
Relative_Market_Cap    <-    read_excel("~/Desktop/Oscar/UAM/Cuarto/Segundo    Semestre/TFG/Market
Cap/Market Cap (18.05.2021).xlsx",
                              +    sheet = "Relative", col_types = c("text",
                                                                     +        "numeric"))
View(Relative_Market_Cap)
##########################
library(readxl)
```

```
Relative10_Market_Cap <- read_excel("~/Desktop/Oscar/UAM/Cuarto/Segundo Semestre/TFG/Market Cap/Market Cap (18.05.2021).xlsx",
                                    +     sheet = "Relative top 10", col_types = c("text",
                                                                                   +        "numeric"))
View(Relative10_Market_Cap)
##########################
library(readxl)
percentage_IOTA_Daily_Returns_FS <- read_excel("miota-usd-max (1).xls",
                                               +     sheet = "percentage.IOTA.returns.FS",
                                               +     col_types = c("date", "numeric"))
View(percentage_IOTA_Daily_Returns_FS)
##########################
#START CODE
##########################
#Lollipopp Market Cap TOP 10 ONLY

install.packages("tidyverse")
install.packages("hrbrthemes")
install.packages("kableExtra")
install.packages("ggplot2")
install.packages("dplyr")
library(dplyr)
library(ggplot2)
library(tidyverse)
library(hrbrthemes)
library(kableExtra)
options(knitr.table.format = "html")


x1 <- Relative10_Market_Cap$Cryptocurrency
y1 <- Relative10_Market_Cap$`Market Capitalisation`
```

```
# Horizontal version
ggplot(Relative10_Market_Cap, aes(x=x1, y=y1)) +
  geom_segment( aes(x=x1, xend=x1, y=0, yend=y1), color="skyblue") +
  geom_point( color="blue", size=4, alpha=0.6) +
  theme_light() +
  coord_flip() +
  scale_x_discrete(limits=Relative10_Market_Cap$Cryptocurrency) +
  xlab("Cryptocurrency") +
  ylab("Market Capitalisation as of 18/05/2021 \n (as a % of the Total Cryptocurrency Market)") +
  scale_y_continuous(labels = scales::percent_format(accuracy = 1)) +
  theme(
    panel.grid.major.y = element_blank(),
    panel.border = element_blank(),
    axis.ticks.y = element_blank()

  )

##################
#Price vs Trading Volume Graph
date_iota_time <- Price_VS_Volume$Date
iota_price <- Price_VS_Volume$`IOTA Price`
iota_volume <- Price_VS_Volume$`Total Trading Volume`

iota_new_volume <- iota_volume *(1/1000) #Quiero el volumen en miles

op <- par(mar = c(5,4,4,4) + 0.1)
plot(date_iota_time, iota_price, col="maroon1", type = "l", xlab = "Year", ylab = "Price (USD)", lwd=2.5)
mtext("Volume (in thousands)", side = 4, line=3)
par(new=TRUE)
```

```
plot(date_iota_time, iota_new_volume, yaxt="n", xaxt="n", ylab="", xlab = "", col="darkblue", type="l",
lwd=0.8)
axis(side=4)
legend("top", c("Price", "Volume"), col=c("maroon1", "darkblue"), lty = c(1,1), lwd = c(2.7,1.2))

#################
#BTC vs IOTA Price Graph
date_iota_time1 <- IOTA_vs_BTC_Price$Date
iota_price1 <- IOTA_vs_BTC_Price$`IOTA Price`
btc_price1 <- IOTA_vs_BTC_Price$`BTC Price`

op <- par(mar = c(5,4,4,4) + 0.1)
plot(date_iota_time, iota_price1, col="maroon1", type = "l", xlab = "Year", ylab = "IOTA Price (USD)", lwd=2.5)
mtext("BTC Price (USD)", side = 4, line=3)
par(new=TRUE)
plot(date_iota_time, btc_price1, yaxt="n", xaxt="n", ylab="", xlab = "", col="darkblue", type="l", lwd=0.8)
axis(side=4)
legend("top", c("IOTA", "Bitcoin"), col=c("maroon1", "darkblue"), lty = c(1,1), lwd=c(2.7, 1.2))

#################
#IOTA vs BTC Returns Scatterplot
BTC_returns <- BTC_vs_IOTA$`BTC Returns`
IOTA_returns <- BTC_vs_IOTA$`IOTA Daily Returns`
cor(IOTA_returns, BTC_returns)
plot(BTC_returns, IOTA_returns, ylab = "IOTA Daily Returns", xlab = "BTC Daily Returns")
abline(lm(IOTA_returns ~ BTC_returns), col = "red", lwd=2.5)
text(-0.25, 0.3, "Correlation Coefficient = 0.62")

#################
#IOTA Returns plotted
par(mfrow=c(1,1))
```

```
plot(percentage_IOTA_Daily_Returns_FS, type = "l", ylab="IOTA Daily Returns (%)", lwd=1)

#################
#IOTA vs BTC correlation
ccf(BTC_returns, IOTA_returns, plot = TRUE, main = "")

#################
#Returns Histograms
full_sample_returns <- IOTA_Daily_Returns_FS$`IOTA Daily Returns`
sample1_returns <- IOTA_Daily_Returns_S1$`IOTA Daily Returns`
sample2_returns <- IOTA_Daily_Returns_S2$`IOTA Daily Returns`
sample3_returns <- IOTA_Daily_Returns_S3$`IOTA Daily Returns`

par(mfrow=c(2,2))
h1 <- hist(full_sample_returns, main="Full Sample", xlab="Daily Returns",xlim=c(-0.6,0.5),col="hotpink",breaks=40)
xfit <- seq(min(full_sample_returns), max(full_sample_returns), length = 40)
yfit <- dnorm(xfit, mean = mean(full_sample_returns), sd = sd(full_sample_returns))
yfit <- yfit * diff(h1$mids[1:2]) * length(full_sample_returns)
lines(xfit, yfit, col = "black", lwd = 2)

h2 <- hist(sample1_returns, main="Subsample 1", xlab="Daily Returns",xlim=c(-0.6,0.5),col="lightskyblue",breaks=40)
xfit <- seq(min(sample1_returns), max(sample1_returns), length = 40)
yfit <- dnorm(xfit, mean = mean(sample1_returns), sd = sd(sample1_returns))
yfit <- yfit * diff(h2$mids[1:2]) * length(sample1_returns)
lines(xfit, yfit, col = "black", lwd = 2)

h3 <- hist(sample2_returns, main="Subsample 2", xlab="Daily Returns",xlim=c(-0.6,0.5),col="lightskyblue",breaks=35)
xfit <- seq(min(sample2_returns), max(sample2_returns), length = 40)
```

```
yfit <- dnorm(xfit, mean = mean(sample2_returns), sd = sd(sample2_returns))
yfit <- yfit * diff(h3$mids[1:2]) * length(sample2_returns)
lines(xfit, yfit, col = "black", lwd = 2)

h4 <- hist(sample3_returns, main="Subsample 3", xlab="Daily Returns",xlim=c(-0.6,0.5),col="lightskyblue",breaks=30)
xfit <- seq(min(sample3_returns), max(sample3_returns), length = 40)
yfit <- dnorm(xfit, mean = mean(sample3_returns), sd = sd(sample3_returns))
yfit <- yfit * diff(h4$mids[1:2]) * length(sample3_returns)
lines(xfit, yfit, col = "black", lwd = 2)

#################
#Histogramas Trading Volume
full_sample_tradingvolume <- (Full_Sample_Volume$`Total Trading Volume`)*(1/(1000*1000))
sample1_tradingvolume <- (sample1_volume$`Total Trading Volume`)*(1/(1000*1000))
sample2_tradingvolume <- (sample2_volume$`Total Trading Volume`)*(1/(1000*1000))
sample3_tradingvolume <- (sample3_volume$`Total Trading Volume`)*(1/(1000*1000))

par(mfrow=c(2,4))
hist(full_sample_tradingvolume, main="Full Sample", xlab="Daily Trading Volume (Millions $)", col="hotpink", breaks = 50, xlim=c(0,300))
hist(sample1_tradingvolume, main="Subsample 1", xlab="Daily Trading Volume (Millions $)", col="lightskyblue", breaks = 50, xlim=c(0,300))
hist(sample2_tradingvolume, main="Subsample 2", xlab="Daily Trading Volume (Millions $)", col="lightskyblue", breaks = 5, xlim=c(0,300))
hist(sample3_tradingvolume, main="Subsample 3", xlab="Daily Trading Volume (Millions $)", col="lightskyblue", breaks = 40, xlim=c(0,300))
yfit <- dnorm(xfit, mean = mean(g), sd = sd(g))

#################
#Trading Volume Box Plot
```

```
#OUTLIERS NOT INCLUDED!! (outline=FALSE)
par(mfrow=c(2,2))
boxplot(full_sample_tradingvolume, horizontal = TRUE, outline = FALSE, col = "hotpink")
boxplot(sample1_tradingvolume, horizontal = TRUE, outline = FALSE, col = "lightskyblue")
boxplot(sample2_tradingvolume, horizontal = TRUE, outline = FALSE, col = "lightskyblue")
boxplot(sample3_tradingvolume, horizontal = TRUE, outline = FALSE, col = "lightskyblue")

#################
#FINAL Boxplot
#OUTLIERS NOT INCLUDED!! (outline=FALSE)
par(mfrow = c(1,1))
colores <- c("hotpink", "lightskyblue", "lightskyblue", "lightskyblue")
variables <- c("Full Sample", "Subsample 1", "Subsample 2", "Subsample 3")
boxplot(full_sample_tradingvolume, sample1_tradingvolume, sample2_tradingvolume,
sample3_tradingvolume,
    col = colores, main = "Trading Volume Boxplots", ylab = "Trading Volume (Millions $)", names =
variables, horizontal = FALSE,
    outline = FALSE, boxwax = 1, range = 1)


#################
#Statistical Analysis
#################

####Ljung Box####
#Number of lags: min( T/2 -2 or 40)

#Full Sample
Box.test(full_sample_returns, lag = 40, type = "Ljung-Box")

#First Subsample
```

```
Box.test(sample1_returns, lag = 40, type = "Ljung-Box")

#Second Subsample
Box.test(sample2_returns, lag = 40, type = "Ljung-Box")

#Third Subsample
Box.test(sample3_returns, lag = 40, type = "Ljung-Box")

##################
####Runs Test####

#Full Sample
library(randtests)
runs.test(full_sample_returns, plot=FALSE )

#First Subsample
runs.test(sample1_returns)

#Second Subsample
runs.test(sample2_returns)

#Third Subsample
runs.test(sample3_returns)

##################
####Bartels Test####

#Full Sample
bartels.rank.test(full_sample_returns)

#First Subsample
```

```
bartels.rank.test(sample1_returns)

#Second Subsample
bartels.rank.test(sample2_returns)

#Third Subsample
bartels.rank.test(sample3_returns)

#################
####AVR Test####
install.packages("vrtest")
library(vrtest)

#Choi 2009 AVVR Test, does not give p-values but test statistic is the
#same as in Kim 2009

#Full Sample
Auto.VR(full_sample_returns)

#First Subsample
Auto.VR(sample1_returns)

#Second Subsample
Auto.VR(sample2_returns)

#Third Subsample
Auto.VR(sample3_returns)

#Wild Bootstrapped AVR Test
##Careful when running, high nboot (>500) may take a long time to give output
#The test can be run with low nboot but results are less reliable
```

```
#Full Sample
#prob=c(0.025,0.975)
AutoBoot.test(full_sample_returns, nboot=100,wild="Normal")

#First Subsample
AutoBoot.test(sample1_returns, nboot=100,wild="Normal")

#Second Subsample
AutoBoot.test(sample2_returns, nboot=100,wild="Normal")

#Third Subsample
AutoBoot.test(sample3_returns, nboot=10000,wild="Normal")

#################
####BDS Test####

install.packages("timeDate")
install.packages("timeSeries")
install.packages("fBasics")
install.packages("fNonlinear")
library(timeDate)
library(timeSeries)
library(fBasics)
library(fNonlinear)

#Full Sample
x_full <- full_sample_returns
sd(x_full) #I use: (eps = sd(x))
bdsTest(x_full, m=8, eps = seq(0.5*sd(x_full), 2*sd(x_full), length = 4))
```

```
#First Subsample
sd(sample1_returns)
bdsTest(sample1_returns, m=8)

#Second Subsample
sd(sample2_returns)
bdsTest(sample2_returns, m=8)

#Third Subsample
sd(sample3_returns)
bdsTest(sample3_returns, m=8)

#################
####Hurst Exponent#### #To run this test, it is best to
#not have run the other tests
install.packages("pracma")
library(pracma)

#Full Sample
hurstexp(full_sample_returns)

#First Subsample
hurstexp(sample1_returns)

#Second Subsample
hurstexp(sample2_returns)

#Third Subsample
hurstexp(sample3_returns)
```