CZECH TECHNICAL UNIVERSITY IN PRAGUE

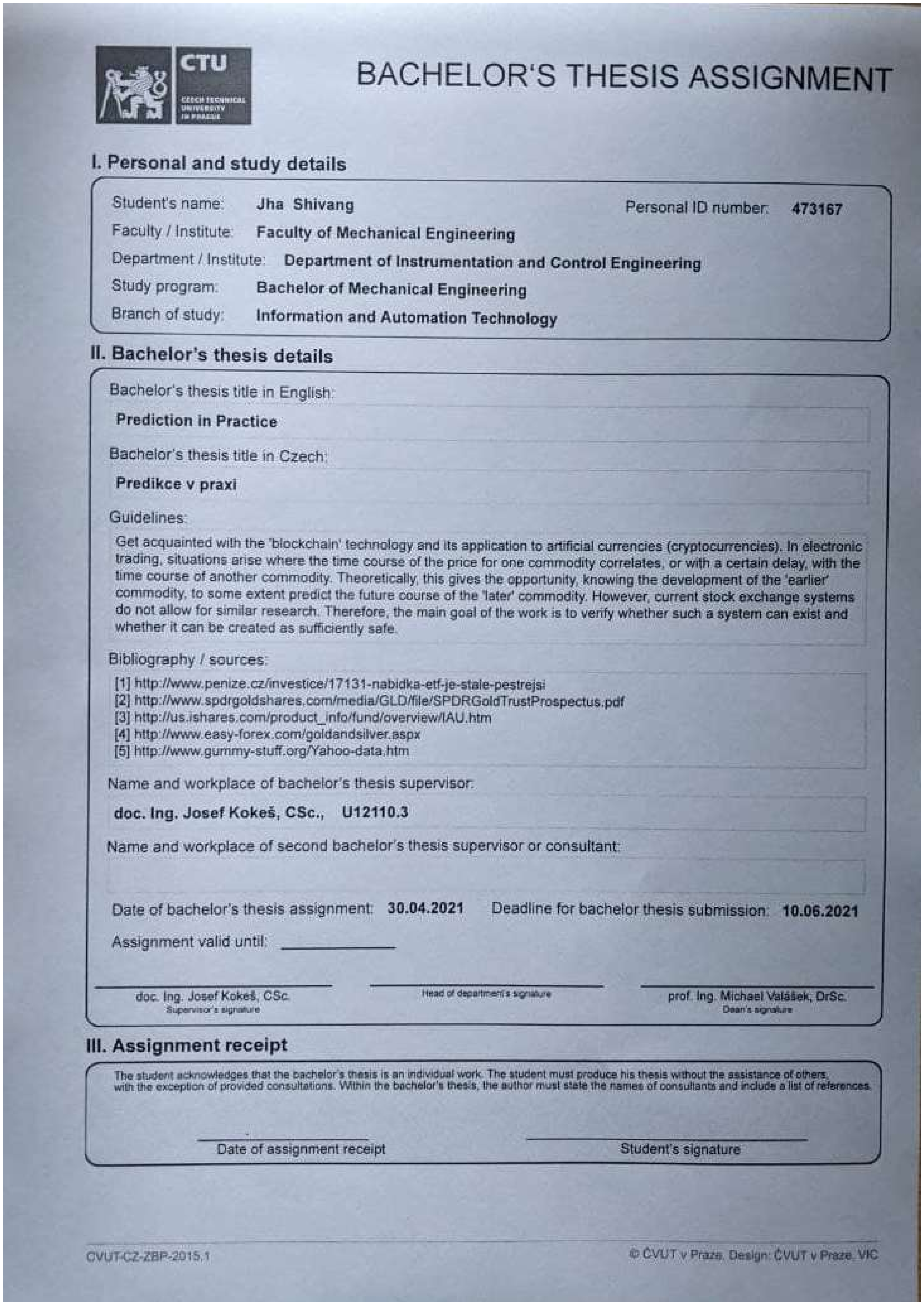
FACULTY OF MECHANICAL ENGINEERING

INFORMATION AND AUTOMATION TECHNOLOGY

PREDICTION IN PRACTICE

BACHELOR THESIS

SHIVANG JHA 24-08-2021



CTU
CZECH TECHNICAL UNIVERSITY IN PRAGUE

BACHELOR'S THESIS ASSIGNMENT

I. Personal and study details

Student's name: **Jha Shivang** Personal ID number: **473167**

Faculty / Institute: **Faculty of Mechanical Engineering**

Department / Institute: **Department of Instrumentation and Control Engineering**

Study program: **Bachelor of Mechanical Engineering**

Branch of study: **Information and Automation Technology**

II. Bachelor's thesis details

Bachelor's thesis title in English:

Prediction in Practice

Bachelor's thesis title in Czech:

Predikce v praxi

Guidelines:

Get acquainted with the 'blockchain' technology and its application to artificial currencies (cryptocurrencies). In electronic trading, situations arise where the time course of the price for one commodity correlates, or with a certain delay, with the time course of another commodity. Theoretically, this gives the opportunity, knowing the development of the 'earlier' commodity, to some extent predict the future course of the 'later' commodity. However, current stock exchange systems do not allow for similar research. Therefore, the main goal of the work is to verify whether such a system can exist and whether it can be created as sufficiently safe.

Bibliography / sources:

[1] http://www.penize.cz/investice/17131-nabidka-etf-je-stale-pestrejsi
[2] http://www.spdrgoldshares.com/media/GLD/file/SPDRGoldTrustProspectus.pdf
[3] http://us.ishares.com/product_info/fund/overview/IAU.htm
[4] http://www.easy-forex.com/goldandsilver.aspx
[5] http://www.gummy-stuff.org/Yahoo-data.htm

Name and workplace of bachelor's thesis supervisor:

doc. Ing. Josef Kokeš, CSc., U12110.3

Name and workplace of second bachelor's thesis supervisor or consultant:

Date of bachelor's thesis assignment: **30.04.2021** Deadline for bachelor thesis submission: **10.06.2021**

Assignment valid until: ____________

doc. Ing. Josef Kokeš, CSc. Supervisor's signature	Head of department's signature	prof. Ing. Michael Valášek, DrSc. Dean's signature

III. Assignment receipt

The student acknowledges that the bachelor's thesis is an individual work. The student must produce his thesis without the assistance of others, with the exception of provided consultations. Within the bachelor's thesis, the author must state the names of consultants and include a list of references.

Date of assignment receipt	Student's signature

CVUT-CZ-ZBP-2015.1 © ČVUT v Praze, Design: ČVUT v Praze, VIC

DECLARATION

I hereby declare that I have prepared my bachelor thesis entitled "Prediction in Practice" independently, under the guidance of my supervisor Doc. Ing. Josef Kokes, CSc., using the literature and material listed at the end, in the bibliography.

In Prague …………… ……………………

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude toward my supervisor doc. Ing. Josef Kokes, CSc. for his valuable and expert guidance throughout the course of researching and writing this thesis.

I would like to thank my wonderful family and friends for providing all their help and support.

And lastly, I would like to thank the anonymous identity of Satoshi Nakamoto, the inventor of Bitcoin, for exposing us to the brilliant world of blockchains.

SYNOPSIS

The objective of this thesis was to get acquainted with blockchain technology and its application to artificial currencies, also known as, cryptocurrencies, and to determine if a system can exist where two distinct commodities (here: cryptocurrencies or crypto assets) can be compared to check if their behavior is independent of each other or not.

The Hilbert Huang Transform is an unconventional mathematical model that has had promising results in fields similar to the behavior of cryptocurrencies.
Hence, it has been considered and portrayed in this thesis as a potential candidate of a model that we seek to find.

Keywords: BTC, ETH, HHT, EMD, ESA, IMF

Table of Contents

List of Figures

Links to the figures:

1. https://www.researchgate.net/figure/The-block-structure-of-Bitcoin-blockchain_fig2_341189041
2. https://cryptoast.fr/qu-est-ce-qu-un-soft-hard-fork/amp/
3. https://medium.com/@markusgebhardt/does-iota-solve-the-blockchain-trilemma-importance-for-the-future-6fca45d6d960
4. to 14. Huang et al., [Interdisciplinary Mathematical Sciences] Hilbert Huang Transform and Its Applications_ 2nd Edition (2014, World Scientific Publishing Company), pp. 5 – 11, 87 – 95

15. & 16. Exodus Desktop Wallet Application

1. Cryptography

Ever since the start of time, humans have had the need to hide or withhold information from their peers. This could be for personal privacy, strategical surprise or sometimes even deceit. For any of such reasons, or countless others that may not come to mind on the first instance, being cryptic has been popular since a long time.

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages [1].

One of the most important examples of cryptography in the recent history was done by the world-famous mathematician Alan Turing that helped the Allies win World War II: The Enigma.

2. Blockchain Technology

The most modern application of cryptography brings us what is widely known as “The Blockchain Technology”.

In today’s world, Blockchain Technology is synonymous to “Bitcoin (BTC)” and a few other cryptocurrencies, but this technique was invented years ago, in 1990, by a young cryptographer known as Stuart Haber, at the Bell Communications Research in New Jersey, USA [2].

As the name suggests, in the simples of terms, Blockchain technology builds up as fragments of information join one after the other in the form of *Blocks.*

Technically, it can be described as a timestamped append only log that is secured by cryptography.

The blocks carry vital information that can either be computer code or an item with some monetary value.

Blockchain technology uses the help of *Cryptographic Primitives* to function securely and cryptically .

Cryptographic primitives protect communication and computation by having them verified on both ends, i.e., from the receiver and the transmitter/sender.

In blockchain, the two fundamental cryptographic primitives are

- Hashfunctions, &
- Digital Signatures

2.1 Technical Features of Blockchain

The one and only element of the blockchain technology, the blocks, contain all the necessary information within itself to ensure the continued growth of a chain.

A block consists of:

- A block header
- Merkle root
- Cryptographic hashfunction
- Transaction list
- Asymmetric cryptography & Digital signatures

Cryptographic hashfunctions can be considered as digital fingerprints of the carried data. It has a few key characteristics:

i. It maps any input (say x) of any given size to an output of a fixed magnitude. This is known as a *hash*.

ii. It is deterministic. This guarantees that it will always return the same hash for the same input (x).

iii. Highly efficient and fast, as it generally takes not more than a few nanoseconds.

<u>A block header</u> has a set number of elements:

i. Version number

ii. Hash of the previous block: to ensure continuity

iii. Merkle root: creates a hash of all the transactions that are posted on the bottom of the block

iv. Timestamp

v. Difficulty index: how hard the block is to find, and

vi. Nonce: a random number used once for unique identification

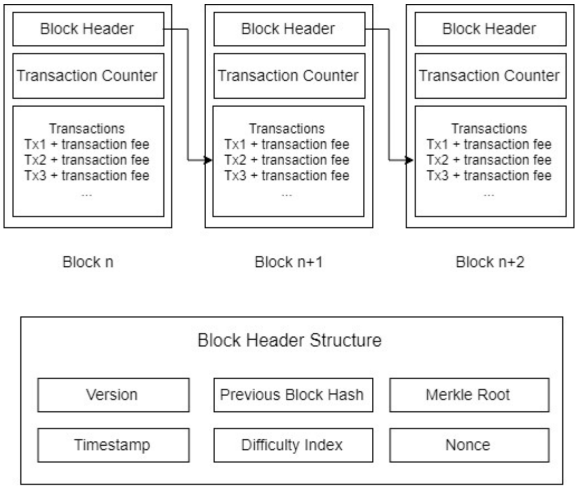


Fig.1: Structure of a block and the blockchain

All these characteristics work towards the following objectives:

- Ensuring Preimage resistance. This makes it infeasible to determine the original x from its hash.

- Collision resistance. To ensure its infeasible to find inputs x and y where hash(x) = hash(y).
- Avalanche effect. A slight change in x significantly changes hash(x).
- Puzzle Friendliness. Even if hash(x) and a part of the input x is found out, it still is close to impossible to determine the rest of the original input.

3. Bitcoin

Bitcoin is a transaction ledger-based cryptocurrency working on the principles of the blockchain technology, launched in 2009 by an anonymous person or a group of people going by the name of **Satoshi Nakamoto.**

It was world's first cryptocurrency, or as Mike Carney, the ex-governor of Bank of Canada & the Bank of England suggested calling it, "crypto-asset".

It was invented after the infamous financial crisis of 2008 as a peer-to-peer payment system, in order to essentially eliminate the so called "middle-man".

At the time of its invention, Bitcoin was one of a kind of a payment substitute. Ever since, there have been thousands of other cryptocurrencies launched, where most of them were not successful, unlike Bitcoin.

3.1 Technical Features

- **Hash functions**:
  Bitcoin uses not one but two hash functions- SHA 256 & RIPEMD 160. Satoshi Nakamoto used these two instead of just one to

warrant highest level of security. They claimed that in any way if one of them were to break, the other would still be working, ensuring safety and protection.

- **Asymmetric Cryptography and Keys:**
  In cryptography, there exist two keys – Public and Private. The private key is chosen as a random number between 0 and 255. It is then exponentiated by another number. The resulting one-way output function becomes the public key. Thus, with a given public key, it is not possible to obtain the private key as that would be disastrous and fail the entire objective of cryptography. This is exponentiation.
  Instead of exponentiation, Bitcoin uses a more intricate method of elliptic curve cryptography.

- **Digital Signatures:**
  Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA).

  Consider two users, A & B, that need to send a message to one another. When A send a message, it is run through a hash function to generate a hash, which is the encrypted with their private key. User B uses the same hash function with the message to generate the hash with the public key of user A.

  This is done to decrypt A's signature. If B obtains the same hash function as A's, the users know that the message is intact and secure and hasn't been tampered with.

The algorithm is as follows:

1. Generate Key Pair – Public and Private Key that are obtained from a random number
2. Creation of a Digital Signature
3. Hash Verification

3.2 Mining & Proof of Work

- Proof of Work is the mechanism that allows the decentralized network to come to consensus or agree on things like account balances and the order of transactions. This prevents users "double spending" their coins and ensures that the chain is incredibly difficult to attack or overwrite. [3]
- Mining is the process of creating a block of transactions to be added to the Ethereum blockchain. Mining is the lifeblood of proof-of-work. Miners - computers running software - use their time and computation power to process transactions and produce blocks. [4]
- When created, back in 2009, the reward was 50 Bitcoins per block. This reward is halved every 210,000 blocks. The current reward is at 6.25 Bitcoins per block, while the next halving is set to take place somewhere around the Spring of 2024 to 3.125.
- The consensus of Blockchains is on the fact that only the longest chain will be the one on which other miners will build upon.
- In Bitcoin, there is a software embedded that prevents miners from cashing out their block reward / output before 100 additional blocks are added onto the chain.
- This is to ensure that the chain is legitimate, and the reward has not been obtained via dubious and illegal methods.

- The average time per each block production is 10 minutes. The difficulty is defined by the number of leading zeroes that are required to solve proof of work/obtain reward. It is adjusted every 2 weeks. The time frame of block production is inversely proportional to the difficulty.
- The aggregate electricity consumed annually mining bitcoin globally has been compared to the annual electricity consumption of countries like Ireland and Denmark.

4. Blockchain Network

One of the main reasons why Blockchain technology is becoming a lot more prevalent among the up-and-coming digital currencies is due to the fact that it is based on a decentralized network.

This means that unlike most of the rest of the networks spread across the current world, a decentralized network does not grant most of its authority to just one particular person, group, or entity.

Instead, the power, responsibility, and most importantly, the ability to be secure is spread equally among all its members and partners.

The Network encompasses three main types of nodes:

a) Full nodes – These nodes store the entire blockchain up to the current moment and are thus able to validate all of its transactions to date.
b) Pruning nodes – As it says in the name, these nodes prune their transactions after validation and a certain aging.
c) Lightweight nodes – Also known as Simplified Payment Verification (SPV) nodes, contain only the block headers of the chain up to the current moment.

One key element of the networks are miners, given the fact that they perform proof of work through general consensus and give rise and growth to the blockchain. Miners need not function just on full nodes but can also exist via Pruning or SPV nodes.

Some other elements include wallets, mining, and memory pools.

5. Permissioned Blockchains

Mostly, all of the network systems before the advent of cryptocurrencies were (and most of them still are) permissioned blockchains.

To become a member of such a blockchain, a governing body or authority needs to grant the user access before making it a part of that blockchain. Thus, membership is restricted only to authorized nodes. This gives rise to the fact that the number of members or participants is always known.

A common example can be banks and their databases.

Permissioned blockchains are more secure from a single point of few, rather than being “decentralized”. Thus, they are centralized and a single or a small collective are responsible for most of its functioning and security.

Consequently, they are highly efficient on one hand but do not offer transparency, on another.

6. Permissionless Blockchain

Permissionless blockchains have been on the rise in the past few years. They act host to all the cryptocurrencies, that started off with Bitcoin back in 2009.

As the name suggests, a potential member does not need to get authorized from a central governing entity before becoming a partner.

Such central governing entities just do not exist for Permissionless blockchains. Thus, every joining member acts as a node that can hold equal say and power in any matter regarding the blockchain. Hence, it is "Decentralized".

Due to this, the number of participants is not always known. However, it is more secure.

7. Bitcoin Cash & its Hard Fork

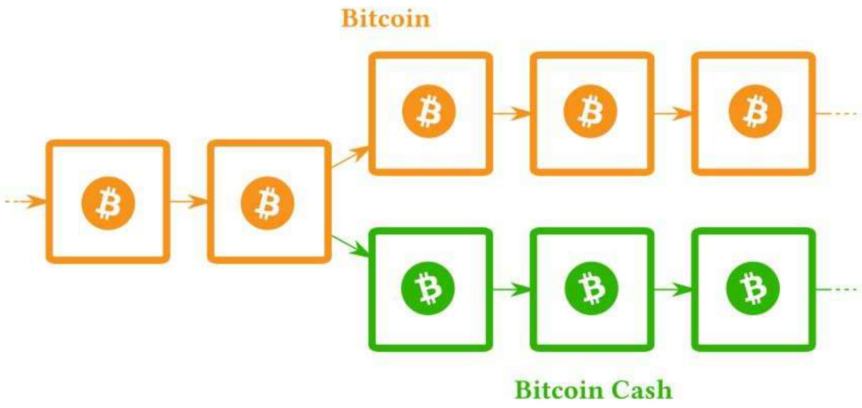


Fig. 2

In August of 2017, Bitcoin Cash was created when the main Bitcoin blockchain branched out and created a hard fork. A simple schematic is shown in figure 2. This occurred due to differences in opinion between some of Bitcoin's developers on the upcoming technology and protocols that the update was going to bring through. Though, Bitcoin XT was the first hard fork in the history of cryptocurrencies, as of date Bitcoin Cash has been the most successful one.

8. Alternate Consensus Protocols

Instead of the conventional consensus that occurs through Proof of Work, Alternate Consensus Protocol licenses randomized or delegated selection of nodes to validate the next block.

While the delegated selection may be based on the tier of nodes, randomized selection is based on the following alternatives:

- Proof of Stake – Stake in the native currency (predominantly USD)
- Proof of Activity – A combination of Proof of Work & Proof of Stake
- Proof of Burn – Validation achieved upon successful expenditure of the crypto-asset
- Proof of Capacity – dependent on hardware storage[5].

9. Unspent Transactions Output (UTXO) Set

It is defined as the set of all unspent Bitcoin transactions output at any given moment. The main purpose of the UTXO set is to speed up the transaction validation process.

Ironically, ever since the inception of Bitcoin and in all of the later versions that developers have released since 2009, the UTXO set has been kept not on the blockchain but on a separate database of the type "levelDB" named *Chainstate.*

10. Bitcoin Script

Since Bitcoin is the first and the leading cryptocurrency of the current modern world, transactions are a very important, if not most, aspect of it.

Bitcoin runs on a simple, stack-based script that is not Turing complete, and thus has no loops.[6]

The purpose of the script is to supply the blockchain with protocols for transaction validation and signature authentication. There are four most common types of scripts in the UTXO set :-

- Transaction sent to hash of Bitcoin Address: *Pay-to-Pubkeyhash*. This covers a majority share of the scripts in UTXO: a massive 81%.
- Transactions sent to hash of Conditional Script: *Pay-to-ScriptHash.* This covers about 18%.
- Transactions subject to multiple signatures. Covers a mere 0.7%.
- Transactions sent to Bitcoin Address: *Pay-to-Pukey* (0.1%).[7]

11. Initial Coin Offering (ICO)

Initial Coin Offering can be considered as the crypto equivalent of the Initial Public Offering that a company or a firm goes through.

While still in development phase, some cryptocurrency developers may offer a few units or *Tokens* of their cryptocurrency in order to raise investment into their project. These proceeds largely go into building networks before the cryptocurrency, or crypto asset, is released and launched to the general public. However, those tokens might not be functional to the user up until the proper launch. The offer is just to reel in investors and offer them stake or value and also for developers to promote their projects and build up a hype.

In most of the cases, the developers announce that they themselves will be holding onto a particular portion of all the tokens that will be mined or later be in circulation.

Two prime examples of this were:

- Satoshi Nakamoto, the anonymous creator of Bitcoin, is said to hold about 1 million Bitcoins.
- Vitalik Buterin, the co-founder of Ethereum, is said to hold 333,521 Ether.[8]

12.Challenges

For blockchains, similar to any other technology, the point of perfection is not easily achieved. And it definitely isn't when the technology is just in its starting phase with hardly about a decade's worth of experience.

A few major challenges still act as a hurdle between cryptocurrencies and their widespread acceptance.

Performance and Efficiency:

While cryptocurrencies like Bitcoin and Ether provide users with various advantages over the current centralized financial systems, they still are far behind when it comes to transaction efficiency. While companies like VISA & The Depository Trust & Clearing Corporation handle over 24,000 and 100,000 transactions per second, Bitcoin can only manage 7-10 transactions per second while Ethereum also is not that far ahead with 20 transactions per second. [9]

Privacy & Security:

Some issues that arise are that while much of the user pool are enticed by the decentralization of data and control, law enforcement agencies and regulators demand more privacy. Financial institutions and a few of their customers also agree with this and object with such a high level of transparency.

Interoperability:

To bring fruition to the idea of blockchains and to incorporate them into many more aspects of the daily life, they need to be linked with the legacy databases, infrastructures and existing technologies that have always been centralized up until this point.

This brings in the issue of trust amongst the joining parties on coordinating the transfer of their own assets and information on a decentralized network where basically every user can hold access to their data.

Other noted challenges that need to be addressed are:

- Governance
- Collective Action
- Commercial Use
- Public Policies
- Legal Frameworks

Vitalik Buterin, the cofounder of Ethereum, aptly described the foremost issue in the form of a trilemma between Decentralization, Scalability and Security stating that as of today with the current technology, a user or a developer can only choose 2 out of these three.

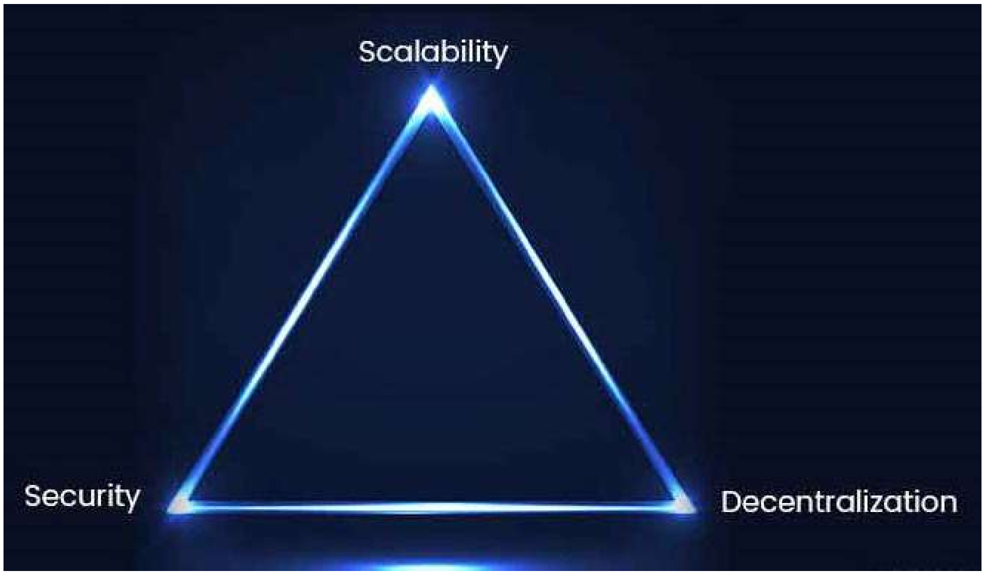


Fig.3.: Vitalik Buterin's Trilemma

13. Data Analysis of Cryptocurrencies

Analyzing the behavior of cryptocurrencies, one can immediately notice that they have anything but a linear pattern over any certain time frame.

However, if you were to magnify to the highest resolution, you would notice that they do in fact have linear changes between the smallest of any two consecutive points. But that would not be feasible in analyzing in the same way as a circle is composed of infinitesimally small straight lines.

Thus, the behaviors of different cryptocurrencies can be very safely termed as non-linear.

Moreover, since their behavior depends on a lot of financial and political factors and that their means, variance and covariances change over time, they cannot be predicted either, making them nonstationary.

For the longest part in the history of data analysis, all models that are used are based on linear and stationary assumptions. However, there have been examples in the past where data analysis was done either for combinations of either linear and non-stationary data or nonlinear and stationary data. But never for a certain combination of nonlinear and nonstationary data, what resembles most of the real-life data.

One example of such kind of system would be the model defining the tides and waves of the ocean.

One major reason why conventional models cannot be used to evaluate nonlinear and nonstationary models is due to the fact that their basis is predefined. This predefined basis would not adjust itself if the model would suddenly change its behavior, thus causing harmonic distortions via the imposing of a linear model onto a nonlinear system (for instance, in the case of waves).

A nonlinear and nonstationary model, that is prone to change at any instant would thus require an adaptive basis. A basis that is data dependent, something very unconventional from the point of mathematics.

14. Hilbert Huang Transform

The Hilbert Huang Transform (HHT), by Huang et al. (1996) tackles such problematic, real world models via such unconventional methodology.

It is an empirically based data-analysis method. Its basis of expansion is adaptive, so that it can produce physically meaningful representations of data from nonlinear and non-stationary processes. [10]
Having been tested thoroughly and empirically validated, HHT gives much more promising results in the field, especially for time-frequency-energy representations.

An important feature by which nonlinear systems can be defined physically is their intra-wave frequency modulation. It is their instantaneous frequency change over any given oscillation cycle.

HHT offers the calculation of the instantaneous frequency change by the help of the Hilbert Transform:

$$\mathcal{H}[x(t)] = \frac{1}{\pi}\,\mathrm{PV}\int_{-\infty}^{\infty} \frac{x(\tau)}{t-\tau}\,d\tau\,,$$ [a]

where,

x(t): real value function

PV: principal value of the singular integral

$$z(t) = x(t) + iy(t) = a(t)e^{i\theta(t)}$$

$$a(t) = \sqrt{x^2 + y^2}, \quad \theta(t) = \arctan\left(\frac{y}{x}\right)$$ [b]

where,

z(t): analytic signal,

y(t): complex conjugate of the function x(t),

a(t): instantaneous amplitude,

θ(t): phase function as a function of time

We then obtain the instantaneous frequency as:

$$\omega = \frac{d\theta}{dt}$$ [c]

The Hilbert Huang Transform consists of two parts:

A. The Empirical Mode Decomposition (EMD), &
B. The Hilbert Spectral Analysis (HSA)

14.1 The Empirical Mode Decomposition (EMD)

The empirical mode decomposition, also known as the *Sifting Process,* was introduced by Norden E. Huang in 1996. The intention behind it was to present a new, intuitive, adaptive, and direct method for the evaluation of nonlinear and nonstationary models.

An assumption of EMD was that every data set consists of varied simple intrinsic modes of oscillation, and it would have the following characteristics:

- The intrinsic mode representing a single oscillation could be either linear or nonlinear.
- It would have the same number of extrema and zero crossings.
- The oscillation would be symmetric to the local mean.
- At any instance, the data may have coexisting oscillation modes. On some instances, they might be superimposed on one another.[11]

All these oscillation modes are represented by an *Intrinsic Mode Function (IMF)* that can be defined as follows:

- In the entire dataset, the number of extrema and zero-crossing must either be equal or differ at most by one,
- At any point, the mean value of the envelope defined by all the local maxima and the envelope defined by all the local minima must be zero. [12]

Thus, an IMF need not just have a definite amplitude and frequency but even amplitudes and frequencies as functions of time.

Following is the test data provided by Huang et al. (1998) describing the procedure of the HHT via the use of empirical mode decomposition (EMD) and intrinsic mode functions (IMF).

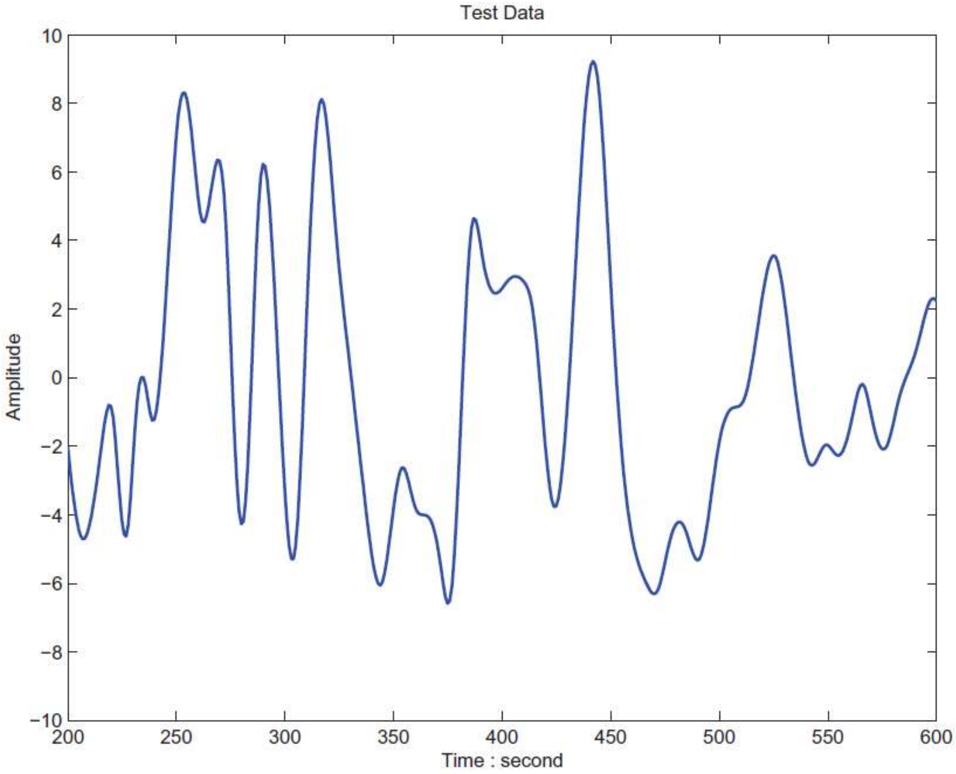


Figure 4. Test Data

Consider the above test data x(t) in figure 4, represented by the blue line.

Step 1 : Identify all the local maxima. Connect them all with a cubic spline (represented by the light green line in figure 5).

Step 2: Identify all the local minima. Connect them all with a cubic spline (represented by the dark green line in figure 5).

This should form an upper and lower envelope encompassing all the plotted data between them.

Step 3: Compute the mean of the upper and lower splines (represented in red in figure 5)

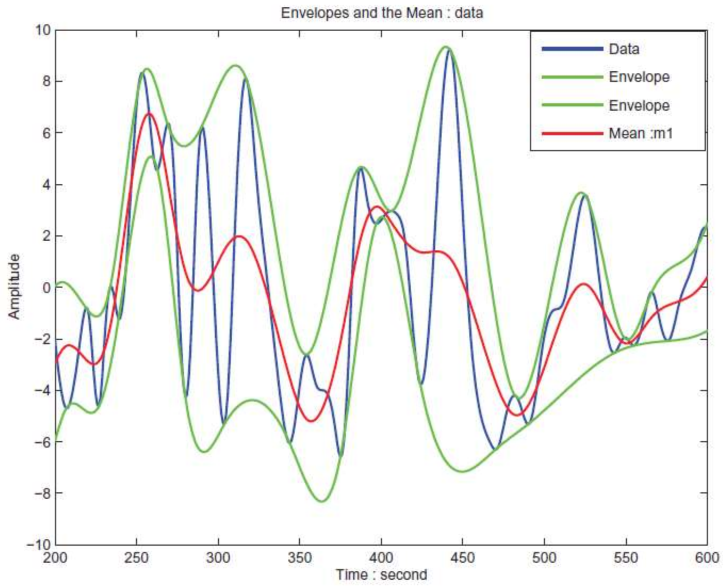


Figure 5 The upper and lower envelope, and their mean along with the original data.

Let the mean be designated by m_1, and the first component as h_1.Then, the first component is defined as the difference between the original data and the computed mean of the two envelopes/splines, as:

$h_1 = x(t) - m_1$, (as shown in figure 6)

In an ideal case, this would give an h that would satisfy all the conditions of an IMF:

- Be symmetric,
- Have all maxima values positive,
- Have all minima values negative.

Steps 1 to 3 are considered as one round of sifting. The purpose was to eliminate riding waves to obtain a meaningful instantaneous frequency and to make the wave profiles as symmetric as possible [13].

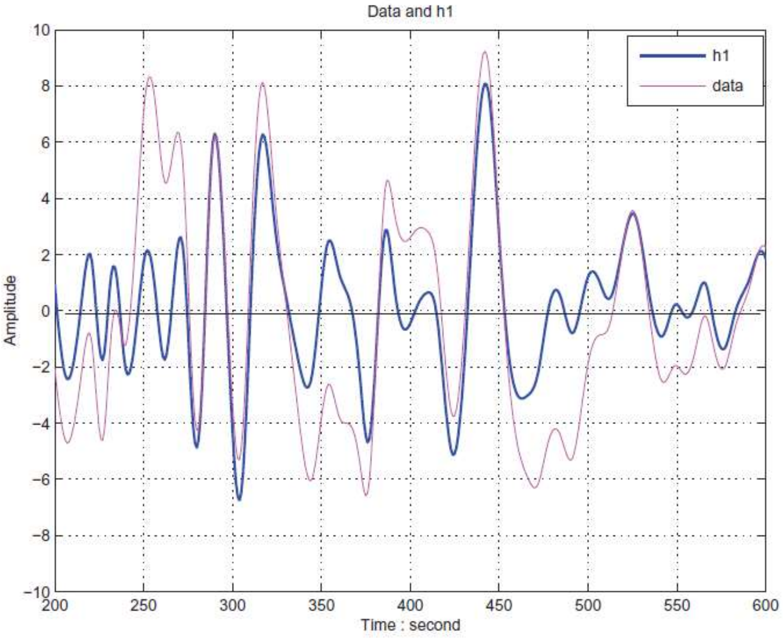


Figure 6

The sifting process (steps 1 to 3) are repeated till the extracted signal is reduced to an IMF fulfilling the conditions above (figures 7&8).

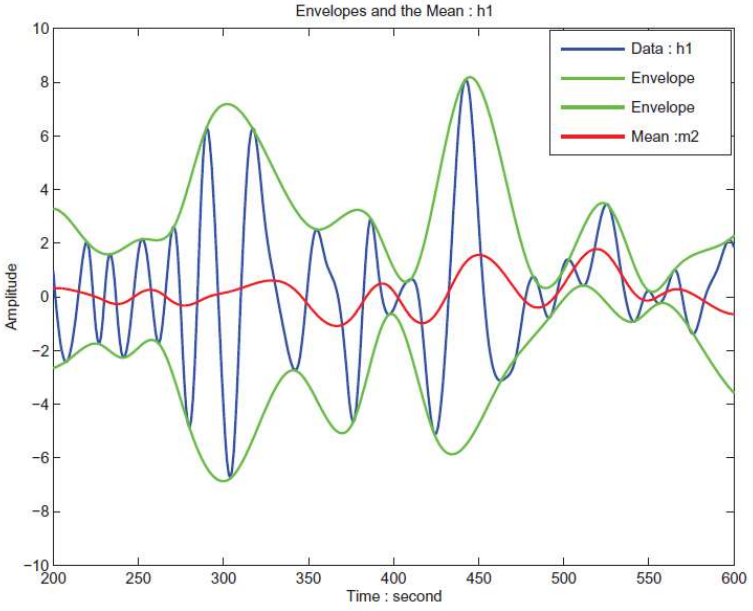


Figure 7: $h_2 = h_1 - m_2$

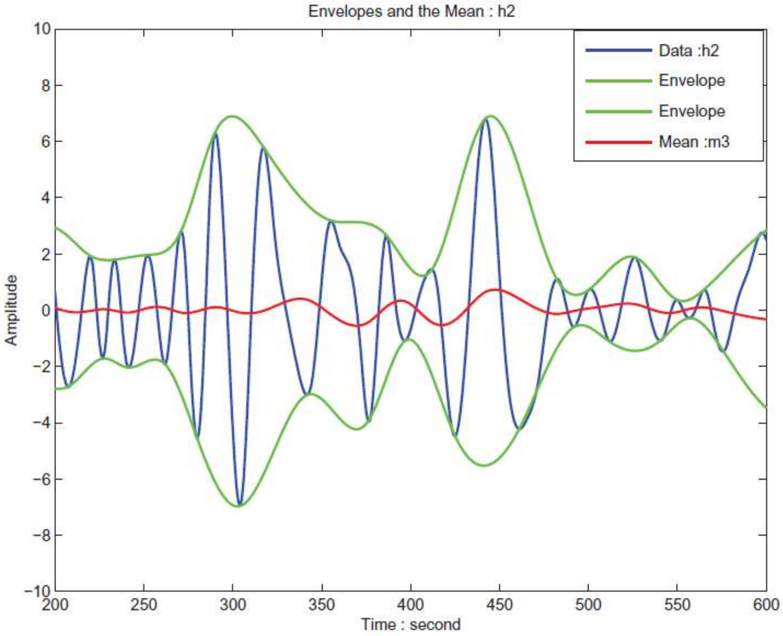


Figure 8: $h_3 = h_2 - m_3$

After performing the sifting process 12 times, the first IMF component c_1 was obtained. (Figure 9)

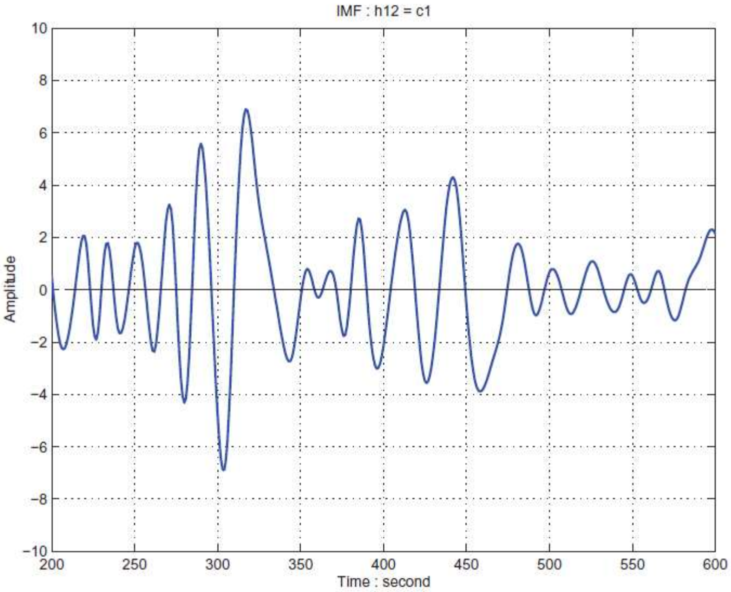


Figure 9: The first IMF component c_1

As it can be seen from figure 9, the IMF produced after 12 rounds of sifting fulfills all the three conditions for it to be an ideal IMF: it is symmetric, has all local maxima positive and local minima negative.

Hence, for siftings done up to k times, the formula can then be generalized to:

$$h_{1k} = h_{1(k-1)} – m_{1k},$$

and the IMF component is designated as: $c_1 = h_{1k}$

Stoppage Criteria: Huang et al. (1999, 2003) came up with an efficient way to determine when to stop the sifting process, based on the definition of the IMFs. An *S* number is to be selected beforehand. For optimal sifting, it should be between 4 – 8. The selection of the S number should be on the basis of the fact that, after sifting S times the obtained component should fulfill the IMF definition that the modulus of the difference between the number of extrema and zero crossings should either be 0 or 1 at most.

Once the S value has been chosen and the component c is not a monotonic function, the following steps take place:

The IMF component c_1 is subtracted from the original data x(t) giving, the first residue (r_1)of the data set:

$r_1 = x(t) - c_1$ (as it can be seen in figure 10)

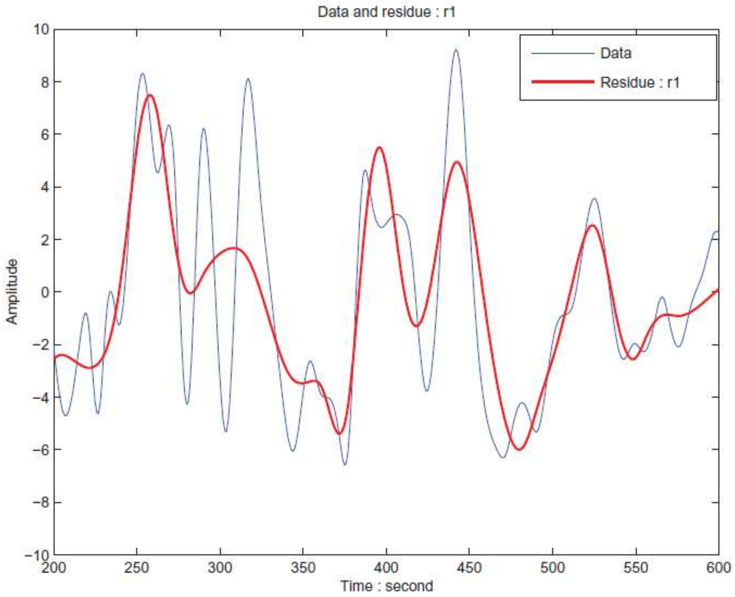


Figure 10

Since, the obtained residue (r_1) is neither periodic nor symmetric and does not have evenly spaced distribution of its curves and peaks, it can be referred to as a new data set and the same sifting process can be repeated all over again.

The sifting process is thus repeated until either the IMF component c_x or residue r_x

a) have become of the magnitude too low to have any importance, or
b) have become a monotonic function or a constant from which no more intrinsic mode functions can be developed.

Note: the residue would never be computed if the IMF component c_x had already become a monotonic function or a constant.

Finally, along with the IMF components and the residue, the test data set can be represented as

$$x(t) = \sum_{j=1}^{n} c_j + r_n.$$

[d]

14.2 Hilbert Spectral Analysis (HSA)

Obtaining the intrinsic mode functions from the original data, Hilbert Transform is applied to all the IMF components in order to obtain their instantaneous frequencies.

The original data set is then represented by its real part as :

$$x(t) = \Re\left\{\sum_{j=1}^{n} a_j(t)\exp\left[i\int \omega_j(t)\,dt\right]\right\}.$$

[e]

where, both the amplitude and the instantaneous frequency are mentioned as functions of time and not constants, thus accommodating nonlinear and nonstationary data. [14]

This frequency-time dependence and distribution is known as the “Hilbert Spectrum” and designated as H (ω,t).

Another important term can be defined: Marginal spectrum h(ω). It is the measure of the total amplitude contributed from each frequency value [15].

$$h(\omega) = \int_0^T H(\omega,t)\,dt$$

[f]

An example provided by Huang, to show how intricate data can be decomposed down to a simple, readable graph is given by the following: The following graph (figure 11) shows the deviation of the length of the day from the standard 24 hours in milli-seconds plotted against the years from 1960 to 2005:

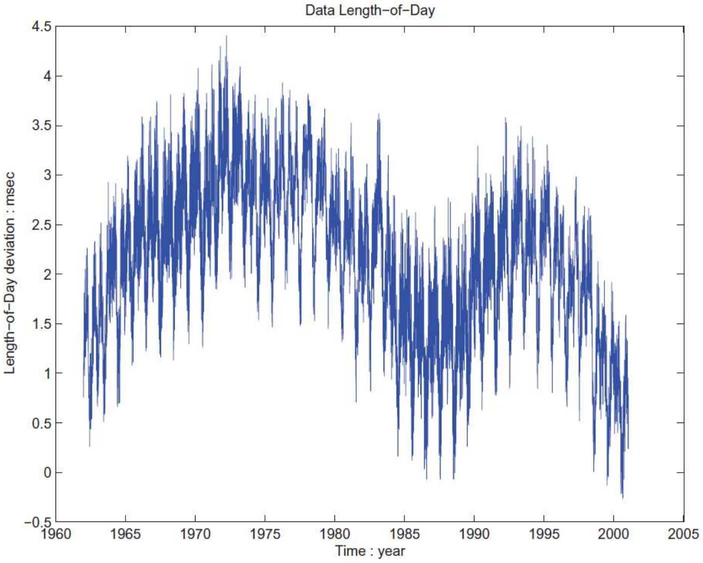


Figure 11

The results shown under figure 12 were obtained from repeating the sifting process, as it was done in the previous example. It can be clearly seen that after obtaining 12 IMF components, the graph was monotonic.

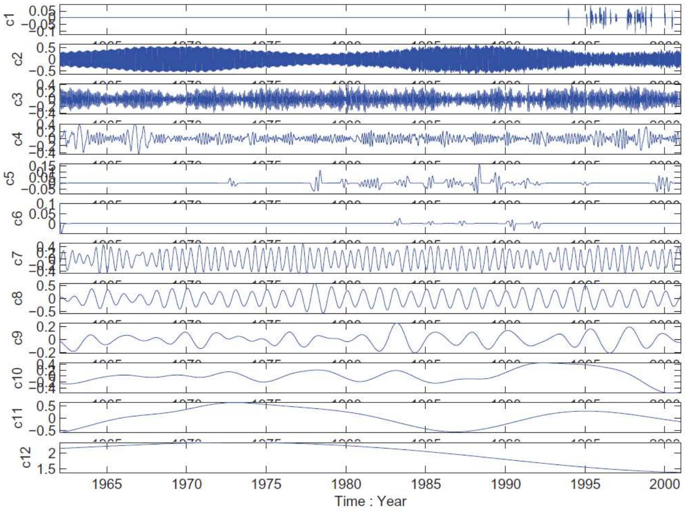


Figure 12

15. Case Study

This case study was presented by S. Braun in “Mechanical Signature Analysis” (1986). The objective was to diagnose the presence of any localized failure present on a rolling bearing. The parameters of the bearing that was tested were given in advance [16]:

- It consisted of 8 rolling elements,
- Diameter of the rolling elements were 15mm with medium diameter of 65 mm and contact angle of 0 °,
- Dimple defect on the inner race was of 1 mm diameter and of 0.1 mm depth,
- Inner ring rotated at a constant speed of 1900 rpm,
- The vibration signals (Figure 13) picked up at the inner race were lowpass-filtered at 9 kHz and digitized at the sampling rate of 20 kHz.

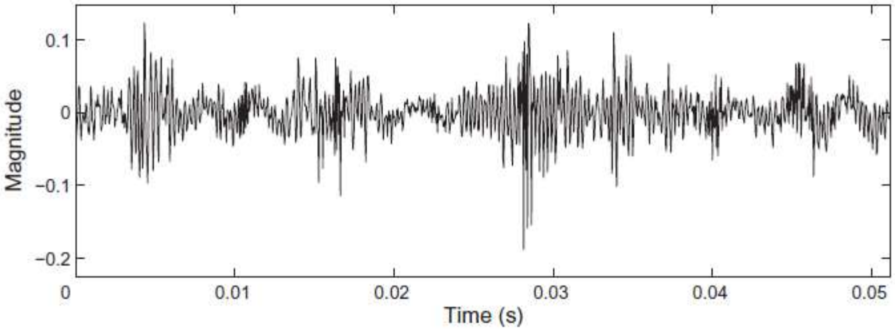


Figure 13: Vibration signal collected from the bearing

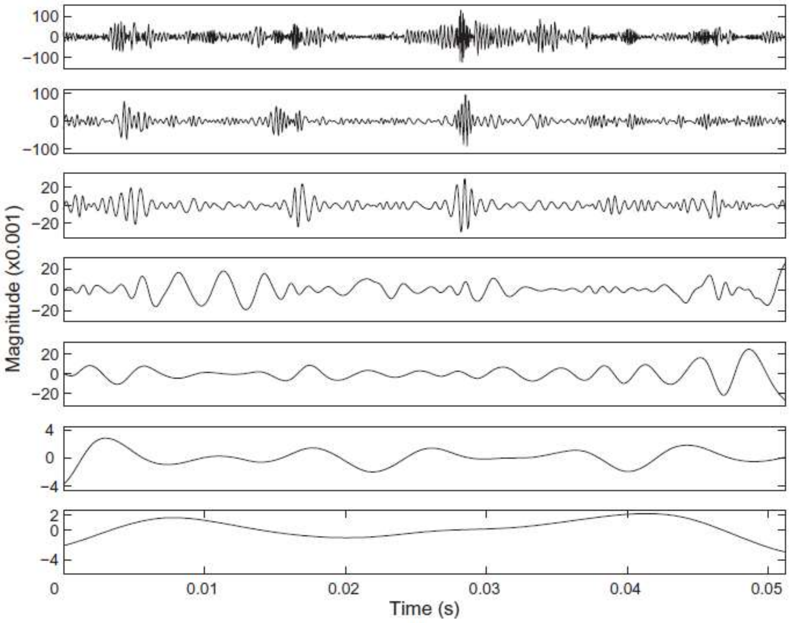


Figure 14: IMFs produced from the data of Fig. 13

From Figure 14, it can be seen that the sifting process produced a monotonic function from the data set of vibration signals (Figure 13).

16. Findings & Conclusion

The following graphs have been obtained from **Exodus Desktop Crypto Wallet:**

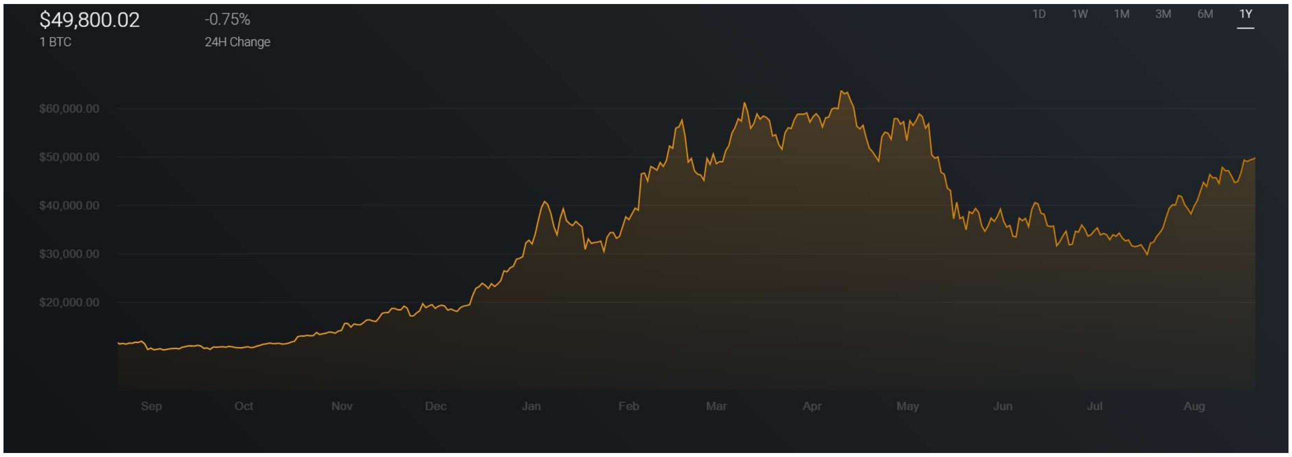


Figure 15: Behavior of BTC over the past one year

(Aug 24th, 2020 to Aug 24th, 2021)

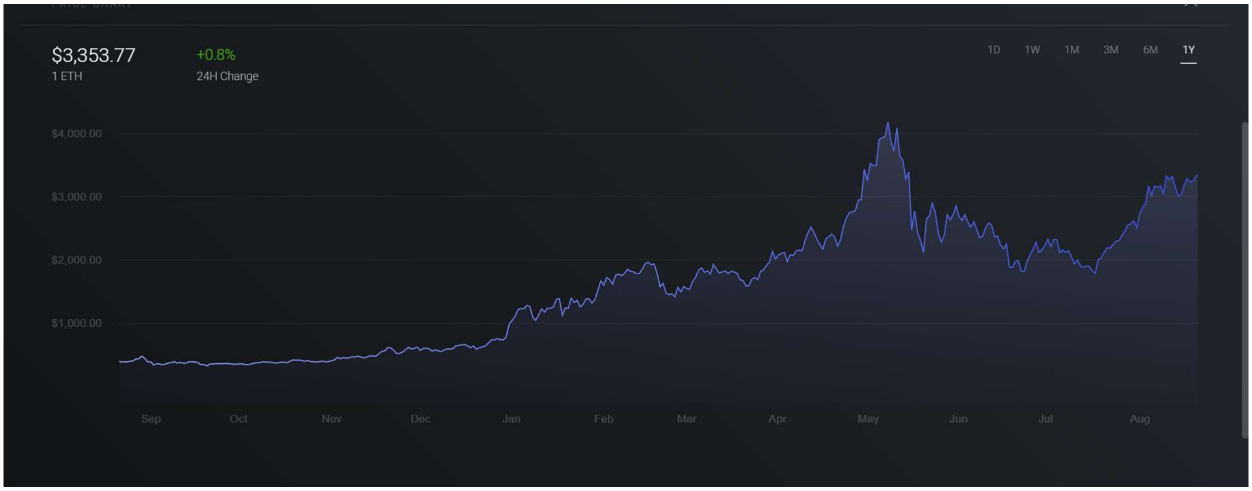


Figure 16: Behavior of ETH over the past one year

(Aug 24th, 2020 to Aug 24th, 2021)

As it has been shown in the sections above, Hilbert Huang Transform exhibits high effectiveness when dealing with systems that have nonlinear and nonstationary data points, by the help of computing Intrinsic Mode Functions (IMFs) via the Empirical Mode Decomposition (EMD) and finding the instantaneous frequencies for the systems that do not have constant amplitude and frequency with the change of time, via the Hilbert Spectral Analysis (HAS).

Figures 15 & 16 depict an annual behavior of two leading cryptocurrencies: Bitcoin (BTC) and Ethereum (ETH). The graphs share key characteristics with the examples and case study discussed above: nonlinearity, and the quality of being non-stationary.

With the help of Empirical Mode Decomposition, the sifting process can be performed on such graphs of the cryptocurrencies in order to generate Intrinsic Mode Functions.

For instance, on BTC, after a successful number of siftings, the IMFs would produce either a monotonic function or a constant from the original data, data that would very closely be of the type displayed in figure 15.

When the same process is repeated for another cryptocurrency, ETH, at the same moment, the final IMF that is generated shall be compared with that of BTC generated on the same time frame at the same time.

If there is a similarity in the behavior of the two IMFs, theoretically, it is possible to state that the two cryptocurrencies have been behaving the same way, at that very instance.

Thus, using the Hilbert Huang Transform, it is theoretically possible to analyze the behavior of two (or more) distinct cryptocurrencies, decomposing their intricately plotted data and determining whether they have any sort if interdependency in their instantaneous behavior.

However, to test out this thesis in practicality, I was not able to find a software or a platform that would help me perform the Hilbert Huang Transform on the data sets that would resemble closely to the figures 15 &16.

Thus, as per my findings and observation, upon the attainment of a proper platform that could perform the sifting process on the behavioral graphs of the cryptocurrencies, the resulting IMF component could very well be used to compare the behavior of that particular cryptocurrency with the same of another such commodity.

17. Bibliography

5. “Cryptography | Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/Cryptography
6. “Stuart Haber |Ted x Beacon Street”. [Online]. Available: https://tedxbeaconstreet.com/speakers/stuart-haber/
7. “Proof of Work | Ethereum.” [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/
8. “Mining | Ethereum.” [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/mining/
9. “Blockchain basics and consensus | MIT OCW.” [Online]. Available: https://ocw.mit.edu/courses/sloan-school-of-management/15-s12-blockchain-and-money-fall-2018/video-lectures/session-4-blockchain-basics-and-consensus/
10. “Script | Wikipedia. “ [Online]. Available: https://en.bitcoin.it/wiki/Script\
11. “ Blockchain basics and transactions, UTXO, and Script code | MIT OCW”, [Online]. Available: https://ocw.mit.edu/courses/sloan-school-of-management/15-s12-blockchain-and-money-fall-2018/video-lectures/session-5-blockchain-basics-transactions/
12. “ Ether Breaks Past $4,000, Adding More Than $300 Million To Vitalik Buterin’s Wealth | Forbes.” [Online]. Available: https://www.forbes.com/sites/ninabambysheva/2021/05/10/ether-breaks-past-4000-adding-more-than-300-million-to-vitalik-buterins-wealth/?sh=28fa86531bb2
13. “Technical Challenges | MIT OCW.” [Online]. Available: https://ocw.mit.edu/courses/sloan-school-of-management/15-s12-blockchain-and-money-fall-2018/video-lectures/session-7-technical-challenges/
14. Huang et al., [Interdisciplinary Mathematical Sciences] Hilbert Huang Transform and Its Applications_ 2nd Edition (2014, World Scientific Publishing Company), pp. 1
15. Huang et al., [Interdisciplinary Mathematical Sciences] Hilbert Huang Transform and Its Applications_ 2nd Edition (2014, World Scientific Publishing Company), pp. 5

16. Huang et al., [Interdisciplinary Mathematical Sciences] Hilbert Huang Transform and Its Applications_ 2nd Edition (2014, World Scientific Publishing Company), pp. 5
17. Huang et al., [Interdisciplinary Mathematical Sciences] Hilbert Huang Transform and Its Applications_ 2nd Edition (2014, World Scientific Publishing Company), pp. 7
18. Huang et al., [Interdisciplinary Mathematical Sciences] Hilbert Huang Transform and Its Applications_ 2nd Edition (2014, World Scientific Publishing Company), pp. 12
19. Huang et al., [Interdisciplinary Mathematical Sciences] Hilbert Huang Transform and Its Applications_ 2nd Edition (2014, World Scientific Publishing Company), pp. 14
20. Huang et al., [Interdisciplinary Mathematical Sciences] Hilbert Huang Transform and Its Applications_ 2nd Edition (2014, World Scientific Publishing Company), pp. 87 - 95