



COMPARATIVE STUDY OF ETHEREUM AND BITCOIN USING BLOCKCHAIN TECHNOLOGY

Shivkumar R. Chandey, Assistant Professor, Department of Computer Science & Information Technology, Nirmala Memorial Foundation College of Commerce and Science, Mumbai – 400101.

Abstract: Bitcoin was introduced in the year 2009, after the launch several new cryptocurrencies have been seen with variations to Bitcoin's original creation. Bitcoin still remains the most prominent actor in the digital world. The ideal of the exploration paper is to determine whether the newer cryptocurrencies solves the problem arises in the digital world, rather of assessing several cryptocurrencies for this comparison, the crypto currency Ethereum has been chosen as a deputy for the others. Ethereum was started in 2014, is extensively backed in the community and is alternate in line to Bitcoin when it comes to market capitalization. As a base for the relative analysis a rigorous study of the Bitcoin and Ethereum protocols have been performed, and resemblant descriptions of the systems have been considered. Three major problems have shaped the focus of the study such as computational waste, attention of power and nebulosity of deals.

Keywords: Cryptocurrency, Security, Blockchain, Bitcoin, Internet, Ethereum, Digital Signature, etc.

1. Introduction

Traditionally, our financial systems depends on physical exchange of money and digital credit. In the world of online transactions the only way of exchanging value is by utilizing trusted third parties, such as banks or intermediate payment systems – for instance,

PayPal to relay the transaction. A weakness of these kinds of online systems is that you have to trust the mediating third party to act in your interest. Even fiat currencies, i.e. the physical money system, have their weaknesses – trust needs to be placed in the institution issuing such currencies, that they will not act in ways that may cause unreasonable levels of inflation or financial crises.

Cryptocurrencies gives an alternate solution to the various existing systems. By utilizing a Peer-to-Peer transaction system – where identities and ownership can be validated using cryptographic means – the users of the system do not have to rely on trust in third parties to exchange value online. Most cryptocurrencies mint their own coin to create value within the system. This is an essential part of their functionality that decouples the value in the cryptocurrency from any fiat currency that relies on governments or organizations for issuance. It also means that cryptocurrencies can be exchanged globally – independently of what currency is native to a region.

When Bitcoin emerged in 2009 it was just a small group of early adopters that saw the potential in the technology and made use of it. Since then a growing ecosystem of different cryptocurrencies has emerged. It becomes increasingly interesting to notice the differences and challenges of the several systems as they grow in popularity and value.

1.1 Problem Description

The Bitcoin is extensively honored as the first successful attempt at a distributed cryptocurrency, with bitcoins being accepted as payment in a growing number of cases. Despite its popularity,

central problems remain with the system design. These issues can be categorized into three major categories such as: wastefulness of computational resources, tendency to centralization over time and ambiguity of transaction finalization. After the launch of bitcoin many alternatives to it have been designed, with many trying to combat these issues. First among the alternatives, in terms of market value and popularity, is the Ethereum system. The developers claim that it provides a wider scope of functionality and higher levels of effectiveness compared to Bitcoin, all the while maintaining the same levels of security.

This paper will put a light on a comparative analysis of Bitcoin and Ethereum by considering on the above mention parameters. Our goal is to determine if Ethereum suffers from the same problems, and attempts to offer some insight into the future of this technology in general. The study will use the published technical descriptions of both systems as well as statistics from the live blockchains of each where appropriate.

1.2 Research Objective

Over the past few years, Bitcoin has been thoroughly reviewed, and technical issues for the system have been identified:

Computational Waste

Large amounts of computation and energy is wasted in the validation process of Bitcoin. This is because nodes – i.e. Bitcoin system participants – are investing in expensive hardware to get an advantage when competing to receive rewards for validating the transactions of peers. Combined with the dynamic adjustment of the difficulty of the validation process to fit the expected time of ten minutes between each set of transactions, it creates a situation where unnecessarily large amounts of computation are expended.

Concentration of Power

The validation is concentrated in a few centrally organized groups, and not spread out in the distributed manner as it was intended. For the validation process to be profitable for nodes in the peer-to-peer network regarding costs related to the process, nodes join together and split rewards received from successful validation. In a group like this, the cost of specialized validation equipment and power expenses is split between the nodes in the group, and any reward for a successful validation is shared with the others.

Ambiguity

Because of the underlying architecture of Bitcoin, transactions take time to process. Knowing exactly when a transaction can be trusted or not is the matter of variance, causing the validity of the transactions to remain ambiguous for a period of time after they have been relayed to the network.

The main objective of this research work is to determine if the later cryptocurrencies have avoided the known problems of Bitcoin, by performing a comparative analysis of Bitcoin and Ethereum.

Newer cryptocurrencies have the advantage of the knowledge of the problems of Bitcoin before development; comparing these cryptocurrencies to Bitcoin therefore seems like the natural choice when reviewing how well these challenges are being met and handled by the newcomers. Rather than try to answer this by examining multiple instances of cryptocurrencies the main focus has been put on Ethereum.

There are many reasons for selecting Ethereum as a proxy for the other cryptocurrencies. Firstly, the currency is relatively recent, Ethereum was launched in the summer of 2015, the developers of the system will likely be aware of the current research in the field. Secondly, the system is explicitly aimed at fixing the shortcomings of Bitcoin, which means that we can assume they have had these problems in mind when designing the protocol. Lastly, although Bitcoin is still the biggest of the cryptocurrencies in terms of adoption and value, Ethereum comes next in line as the second most popular alternative and is widely backed in the community. To give a quantifiable measure of the two

systems, the website coinmarketcap.com values the current Bitcoin market capitalization as being over 561 billion US dollars. After this, Ethereum comes next with more than 229 billion US dollars. However, it should be noted that these values are highly volatile and subject to change on a daily basis.

1.3 Methodology

As a methodology for this research paper consists of deriving parallel technical descriptions for Bitcoin and Ethereum to detail both systems in a scientifically rigorous manner to accurately compare and contrast them. Especially, while Bitcoin has recently been described well in the literature, information on Ethereum is dispersed over online platforms which is subject to edits and changes by the different authors sporadically – making the task of detailing Ethereum significantly.

Furthermore, the technical problems of Bitcoin have been elaborated in terms of the protocol detail, and Ethereum has been analyzed to evaluate whether it exhibits the same problems. The two descriptions are placed in contrast to each other, highlighting their similarities and differences. The comparative study will also consider data available from the live systems when this is appropriate. This data has been gathered and synthesized to enlighten the discussion and to determine if the findings from the comparison align with the data.

2. What is Bitcoin?

An entirely P-2-P interpretation of electronic cash would allow online deals to be transferred directly from one party to another without going through a fiscal association. Digital signs are used as a part of the overall result, but the key benefits are lost if a third party is still need to help double- spending. The network instants deals by mincing them into an ongoing chain of hash- grounded evidence- of- work, forming a record that can not be changed without redoing the evidence- of- work. The longest chain not only serves as evidence of the sequence of events witnessed, but evidence that it came from the largest pool of CPU power. As long as a maturity of CPU power is controlled by bumps that aren't cooperating to attack the network, they'll induce the longest chain and outpace bushwhackers. The network itself requires minimum structure. dispatches are broadcast on a stylish trouble base, and bumps can leave and return the network at will, accepting the longest evidence- of- work chain as evidence of what happed while they were gone.[6]

3. The Blockchain

Blockchain is a new technology that has surfaced with the appearance of the Bitcoin, which has added a new way of dealing financially. Grounded on the success of this fashion with the idea of Bitcoin, the fashion has been reckoned upon and applied gradationally in colorful conditioning, whether governmental or private and entered the confidence and satisfaction of guests. The paper highlights the challenges ahead and openings in this ultramodern technology that's all set to develop our digital world.[4]

Blockchain technology is one of the approaches that has the possibility to enhance decentralization, translucency, equivalency, and responsibility on the internet[1]. Blockchain is a distributed database of records that can be either public tally of digital issues or deals that got achieved and have been participated among sharing parties across a large network of untrusted actors. It stores data in blocks that can corroborate information which are veritably delicate to hack. It avoids the demand of a third-party verification and therefore deactivates any sector that leverages it traditionally.[2]. Using blockchain can give advanced security compared to storing all data in a central database. The use of these technologies in Bitcoin “mining” was ground-breaking in the data storehouse and operation side, detriment from attacks on a database can be averted. Further, since the blockchain has an openness trait, it can give translucency in data when applied to an area taking the exposure of data [3].

4. What is Ethereum?

Ethereum is an open source project first introduced in 2013, initially described as a “Next-Generation Smart Contract and Decentralized Application Platform”. At first glance Ethereum is a peer-to-peer network and an exchangeable cryptocurrency that allows nodes to share computing resources for the execution of programmable smart contracts on the blockchain. There are however multiple different ways to describe Ethereum depending on ones point of view. In the official guides Ethereum is also described as a ‘World Computer’, in the sense that it can be seen as a single computing platform which anyone in the world is able to use. In this computer world any number of programs can be encoded and executed, and any participating code can interact and have access to the state of each one of these programs.

In other words, with Ethereum any user can have access to a cheap, zero-infrastructure, global platform that provides a very interesting set of features:

- User authentication will be validated by the use of cryptographic signatures.
- Easily deployable payment logic. A payment system can be setup on Ethereum very quickly with no third party reliance.
- Total DDoS resistance. Each application on Ethereum is not executed on any single node; rather it is executed on each and every node on the system. As long as there is one node maintaining the blockchain the application will run perpetually and will be able to be interfaced by any joining node.
- Limitless interoperability. Each Ethereum contract can seamlessly interact with any other contract instance via the provided interfaces in the Ethereum ecosystem
- No server infrastructure. As mentioned before Ethereum is completely built on top of a Peer-to-Peer network with no central server infrastructure involved. Thus, the deployment of an application on the blockchain does not require the setup and the costs of setting and maintaining servers. Having said this, we can understand that Ethereum strives to provide a platform where anyone can easily deploy and run Internet services.[5]

5. Conclusion: Comparative Analysis of Bitcoin and Ethereum

Comparison of Bitcoin and Ethereum is shown in the following Table.

Sr. No.	Parameters	Bitcoin	Ethereum
01	Maximum block size	1 MB	Flexible Limit
02	Target block time	10 min	13 sec
03	State	Stateless	Stateful
04	Consensus mechanism	Proof of work	Proof of work
05	Consensus Protocol	Nakamoto consensus	GHOST
06	Mining algorithm	Hashcash	Ethash

Table 1: Comparative Analysis of Bitcoin and Ethereum.

Among the cryptocurrencies available moment, Bitcoin is the more well- known, but Ethereum has been gaining ground in recent times. Both have their unique benefits and downsides. Bitcoin is the original bone and remains the most well- known. It's also the most precious, with a high market cap. Bitcoin is frequently used as a store of value, and it's seen as a more dependable investment than Ethereum.

Ethereum, on the other hand, is a platform that allows for the creation of decentralized operations. These operations can be deployed on top of the Ethereum blockchain, and they run on Ethereum's native currency, Ether. Ethereum also has a much lower transaction charges as compared to Bitcoin.

Both Bitcoin and Ethereum have their strengths and drawbacks. Bitcoin is more precious and is seen as a more dependable investment, but Ethereum has lower transaction charges and allows for the creation of decentralized operations.

6. References

- [1] Walid A., Nicolas S., 2017, "Blockchain technology for social impact: opportunities and challenges ahead", available : <https://doi.org/10.1080/23738871.2017.1400084>
- [2] Arijit C., Ashesh K., 2017, " Blockchain and its Scope in Retail" available: <https://irjet.net/archives/V4/i7/IRJET-V4I7616.pdf>
- [3] Ketki R., Sheetal Y., 2018, " Blockchain Technology in Cloud Computing : A Systematic Review" , available : <https://www.irjet.net/archives/V5/i4/IRJET-V5I4428.pdf>
- [4] <https://www.irjet.net/archives/V5/i5/IRJET-V5I5659.pdf>
- [5] <https://delaat.net/rp/2015-2016/p53/report.pdf>
- [6] <https://bitcoin.org/bitcoin.pdf>