IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Comparative Study Of Ethereum And Bitcoin Using Blockchain Technology

Shivkumar R Chandey
Assistant Professor
{Nirmala Memorial Foundation College of Commerce and Science}

Abstract. : Bitcoin was launched in 2009, several new cryptocurrencies have been initiated with variations to Bitcoin's original design. Bitcoin still remains the most prominent actor in the market. The objective of the research paper is to determine whether the newer cryptocurrencies solves the problem arises in the digital world, Instead of evaluating several cryptocurrencies for this comparison, the crypto currency Ethereum has been chosen as a proxy for the others. Ethereum was started in 2014, is widely backed in the community and is second in line to Bitcoin when it comes to market capitalization. As a basis for the comparative analysis a rigorous study of the Bitcoin and Ethereum protocols have been performed, and parallel descriptions of the systems have been devised. Three problem have shaped the focus of the analysis: computational waste, concentration of power and ambiguity of transactions.

Keywords: Cryptocurrency, Security, Blockchain, Bitcoin, Internet, Ethereum

1 Introduction

Traditionally, financial systems are based on physical 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 provide an alternate solution to the 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 [Nak08] emerged in 2009 it was just a small group of early adopters that saw the potential in the technology and made use of it [NBF+16]. 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 widely recognized as the first successful attempt at a distributed cryptocurrency, with bitcoins being accepted as payment in a growing number of instances. Despite its popularity, central problems remain with the system design. These issues can be classified into three major groups: wastefulness of computational resources, tendency to centralization over time and ambiguity of transaction finalization. Since its launch several alternatives to Bitcoin have been developed, 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 thesis will provide a comparative analysis of Bitcoin and Ethereum with a focus on the three aforementioned issues. Our goal is to determine if Ethereum suffers from – or will suffer 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 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. This defeats the original purpose of Bitcoin, which is to be

Ambiguity Because of the underlying architecture of Bitcoin, transactions take time to process. Knowing exactly when a transaction
can be trusted or not is subject to variance, causing the validity of the transactionsto remain ambiguous for a period of time after they have been relayed to the network.
The main research objective of this thesis 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 several reasons for choosing Ethereum as a proxy for the other cryptocurrencies. Firstly, the currency is relatively recent, Ethereum was launched 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 (30. May 2017) Bitcoin market capitalization as being over 32 billion US dollars. Ethereum comes next with over 20 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 thesis 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. Importantly, while Bitcoin has recently been described well in the literature, information on Ethereum is dispersed over online wikis, blogs, and forums, subject to edits and changes by the different authors sporadically – making the task of detailing Ethereum non-trivial.

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 analysis will also include 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?

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.
The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest
proof-of-work chain as proof of what happened while they were gone.[6]

What is Blockchain?

Blockchain is a new technology that has emerged with the appearance of the Bitcoin, which has added a new way of dealing financially. Based on the success of this technique with the idea of Bitcoin, the technique has been relied upon and applied gradually in various activities, whether governmental or private and received the confidence and satisfaction of customers. The paper highlights the challenges ahead and opportunities in this Modern technology that is all set to develop our digital world. [4]

Blockchain technology is one of the approaches that has the possibility to enhance decentralization, transparency, equality, and responsibility on the internet [1]. Blockchain is a distributed database of records that can be either public ledger of digital issues or transactions that got achieved and have been shared among participating parties across a large network of untrusted participants. It stores data in blocks that can verify information which are very difficult to hack. It avoids the requirement of a third-party verification and thus deactivates any sector that leverages it traditionally. [2]. Using blockchain can provide higher security compared to storing all data in a central database. The use of these technologies in Bitcoin "mining" was ground-breaking in the data storage and management side, harm from attacks on a database can be prevented. Further, since the blockchain has an openness attribute, it can provide transparency in data when applied to an area requiring the disclosure of data [3].

What is Ethereum?

Ethereum is an open source project first introduced in2013, 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 once 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 world computer 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, verified 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.

Comparative analysis of Bitcoin and Ethereum

Comparison of bitcoin and Ethereum is shown in the following Table 1.

Table 1. Comparative analysis of Bitcoin and Ethereum.

Parameters	**Bitcoin**	**Ethereum**
Maximum block size	1 MB	Flexible Limit
Target block time	10 min	13 sec
State	Stateless	Stateful
Consensus mechanism	Proof of work	Proof of work
Consensus Protocol	Nakamoto consensus	GHOST
Mining algorithm	Hashcash	Ethash

References

1. Walid A., Nicolas S., 2017,"Blockchain technology for social impact: opportunities and challenges ahead",available
2. Arijit C., Ashesh K., 2017, " Blockchain and its Scope in Retail"available
3. Ketki R., Sheetal Y., 2018, " Blockchain Technology in Cloud Computing: A Systematic Review", available
4. Blockchain Technology : Classification, Opportunities, and Challenges, Nadir Abdelrahman Ahmed Farah, Dept. of Information Systems, Arts and Science College, University of Bisha, Saudi Arabia, e-ISSN: 2395-0056, p-ISSN: 2395-0072
5. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER, BERLIN VERSION 8fea825 – 2022-08-22, DR. GAVIN WOOD, FOUNDER, ETHEREUM & PARITY, GAVIN@PARITY.IO
6. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, satoshin@gmx.com, www.bitcoin.org