Ethereum vs. Bitcoin: A Comparative Analysis of Two Preeminent Blockchain Technologies

Zhirui Li

CSCI1951L

Brown University

May 17, 2023

Table of Contents

Table of Contents..... 2

Introduction..... 3

Purpose, Goals, and Philosophy..... 3

Consensus Algorithm..... 4

Scalability, Security, and Resource Efficiency..... 5

Cryptocurrency Structure: Blocks, Hashes, etc..... 5

Token Issuance..... 6

Conclusion..... 7

References..... 8

Introduction

Blockchain technology, an ingenious invention by a person or group using the pseudonym Satoshi Nakamoto, is now utilized in myriad ways beyond its initial application - Bitcoin (Nakamoto, 2008). Ethereum, another significant blockchain innovation, is a fundamental technology whose impact resonates through many applications and sectors. This comparative analysis highlights the similarities and differences between Bitcoin and Ethereum, focusing on their purpose, consensus algorithms, token issuance, and other aspects.

Purpose, Goals, and Philosophy

Bitcoin, the first application of blockchain technology, emerged in 2009 against the backdrop of the global financial crisis. It was introduced by an anonymous entity or group of individuals under the pseudonym Satoshi Nakamoto (Nakamoto, 2008). The Bitcoin White Paper articulated a clear vision: to enable "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" (Nakamoto, 2008, p.1). Bitcoin aimed to deliver a decentralized, peer-to-peer digital cash system free from the control of any central authority. The underlying philosophy of Bitcoin was to challenge the status quo of the traditional financial system, thereby creating a more inclusive, efficient, and democratized monetary system (Narayanan et al., 2016).

On the other hand, Ethereum, proposed by Vitalik Buterin in 2013 and officially launched in 2015, was built with a distinct purpose (Buterin, 2013). While Bitcoin's blockchain was essentially a ledger for BTC transactions, Ethereum aimed to be a "world computer" – a decentralized, global platform for creating and running smart contracts (Buterin, 2013). These self-executing contracts, with the terms of the agreement directly written into lines of code, extended the functionality of blockchain from a mere transaction ledger to a platform capable of executing arbitrary stateful computations (Mücke, 2020). Ethereum's philosophy was, thus, not just about enabling decentralized money but about fostering decentralized applications (dApps), thereby paving the way for the "decentralized web" or "Web 3.0."

Although Bitcoin and Ethereum both leverage blockchain technology and are inherently decentralized, their philosophical underpinnings diverge significantly. While Bitcoin was conceived as an alternative to traditional money, Ethereum was envisioned as a platform for decentralizing all applications, not just currency. These differing purposes

have led to distinct developmental trajectories, functionalities, and communities around these two preeminent blockchain technologies.

Consensus Algorithm

Consensus algorithms are integral to blockchain technology. They validate and verify the information added to the blockchain, ensuring that all nodes in the network agree on the current state of the distributed ledger. This consensus is crucial in maintaining these blockchain networks' decentralized and secure nature (Mukhopadhyay et al., 2020).

Bitcoin and Ethereum initially employed the Proof-of-Work (PoW) consensus algorithm (Nakamoto, 2008; Buterin, 2013). In PoW, nodes, known as miners, solve complex mathematical problems to validate transactions and add new blocks to the chain. The first miner to solve the problem is rewarded with new tokens and transaction fees, a process known as mining.

Bitcoin's use of PoW provides network security and helps prevent double-spending, a scenario where a Bitcoin owner could spend the same coins twice. Nakamoto (2008) explains that PoW requires a miner to expend computational resources. It would be prohibitively expensive for a malicious actor to take over 50% of the network's hashing power (the so-called 51% attack) and manipulate the transaction history, thus ensuring the validity of Bitcoin transactions.

Ethereum also started with the PoW consensus algorithm (Buterin, 2013), but, unlike Bitcoin, Ethereum's leadership decided to transition to Proof-of-Stake (PoS) via the Ethereum 2.0 upgrade (Ethereum Foundation, 2020). PoS is a consensus algorithm where validators replace miners in validating transactions and creating new blocks. Validators are chosen to propose a block based on their economic stake in the network – how many tokens they hold and are willing to 'lock up' as collateral. In Ethereum's case, this collateral is Ether (ETH), the native token of the Ethereum network.

While the PoW consensus mechanism has proven secure and effective, it faces criticisms due to its high energy consumption and potential centralization risks as mining operations consolidate (Mora et al., 2018). Ethereum's shift to PoS seeks to address these issues by providing a more energy-efficient approach to maintaining consensus across its vast network and adding disincentives for any potential misbehavior by validators (Buterin, 2021).

However, it is crucial to note that Ethereum's shift to PoS is not without its potential drawbacks and critics. Concerns have been raised about the possibility of centralization, as those who can afford to stake more ETH have a higher chance of being chosen as validators (Kokoris-Kogias et al., 2018).

Scalability, Security, and Resource Efficiency

Scalability, security, and resource efficiency represent critical challenges in blockchain technologies like Bitcoin and Ethereum. Bitcoin's scalability is limited by its block size and the time between blocks, causing restrictions on transaction throughput. This has led to forks such as Bitcoin Cash to increase the block size and, thus, transaction capacity (Croman et al., 2016). Similarly, Ethereum also grapples with scalability constraints due to the complexity of executing smart contracts, limiting its throughput to approximately 15 transactions per second as of 2021. Ethereum aims to address these scalability issues with proposals like sharding and transitioning to a Proof-of-Stake consensus mechanism (Buterin, 2020).

Security-wise, Bitcoin and Ethereum deploy cryptographic techniques for transactions and block creation but are still exposed to possible attacks like a 51% attack, where an entity with over half of the network's hashing power can disrupt the network (Nayak et al., 2016). Additionally, Ethereum's smart contracts can present unique security issues, demonstrated by the infamous DAO hack, which resulted in the theft of $50 million worth of Ether (Siegel, 2016).

Resource efficiency is a significant concern due to the Proof-of-Work consensus algorithms employed by Bitcoin and Ethereum (as of 2021). These algorithms necessitate high computational power, resulting in substantial energy consumption. Bitcoin, in particular, has been criticized for its energy usage, which is comparable to the consumption of entire countries (Krause & Tolaymat, 2018). Ethereum's planned transition to Proof-of-Stake in Ethereum 2.0 aims to alleviate these concerns by making block creation less energy-intensive and environmentally friendly (Buterin, 2020).

Cryptocurrency Structure: Blocks, Hashes, etc.

Bitcoin and Ethereum employ similar fundamental structures in creating their respective blockchains. This structure consists of blocks that house transactions or contract computations. These blocks are linked to their predecessors via cryptographic hashes,

creating an immutable chain of blocks - hence the term "blockchain" (Nakamoto, 2008; Buterin, 2013).

In Bitcoin, a block contains a series of transactions. When Bitcoin users send digital currency to each other, miners group their transactions into a block (Nakamoto, 2008). Each block contains the previous block's hash, forming a chain of blocks from the genesis block to the current block. This chain's immutability is provided by the block header's hash, which includes the Merkle root - a data structure used to summarize all the transactions in the block efficiently (Bonneau et al., 2015).

In contrast, Ethereum's blockchain stores a list of transactions and the most recent state of each smart contract (Buterin, 2013). Ethereum's block structure is more complex due to the added information needed for brilliant contract execution and storage. While the Ethereum block also references the parent block's hash, it also stores the state root, a hash of the entire system state, including account balances and contract states (Wood, 2014).

This structural difference is due to Ethereum's added functionality of executing smart contracts. Whereas Bitcoin's blockchain is primarily a ledger for BTC transactions, Ethereum's blockchain acts as a ledger for Ether transactions and a computational engine for running intelligent contracts (Zamyatin et al., 2018).

Despite the structural differences, Bitcoin and Ethereum use cryptography to secure their blockchains. Cryptographic hashes provide tamper evidence, as changing any transaction would require re-computing all subsequent block headers, which is computationally infeasible due to the Proof-of-Work algorithm (Nakamoto, 2008; Buterin, 2013).

Token Issuance

Bitcoin's token issuance model is pre-set and follows a predictable curve. New bitcoins are minted as rewards for miners who successfully append new blocks to the blockchain, a process known as mining (Nakamoto, 2008). Initially, the reward for each block was 50 bitcoins, but this reward halves every four years in an event aptly named "halving." As of September 2021, the reward stands at 6.25 bitcoins per block. The halving mechanism ensures the total number of bitcoins will never exceed 21 million, introducing an aspect of digital scarcity that has led some to liken Bitcoin to "digital gold" (Franco, 2014).

Ethereum, conversely, does not have a maximum cap on its token supply. Like Bitcoin, Ethereum initially employed mining and block rewards as its primary means of token issuance. However, the recent transition to Ethereum 2.0 and its shift to the Proof-of-Stake (PoS) consensus algorithm have altered this approach (Ethereum Foundation, 2020). In Ethereum 2.0, validators must lock up a substantial amount of Ether to participate, propose and validate blocks. These validators receive rewards for their contributions to the network, forming the primary mechanism for new Ether issuance (Buterin, 2021).

The stark divergence in token issuance methods between Bitcoin and Ethereum derives from their distinct monetary policies and approaches to network security. While Bitcoin's finite supply emulates the scarcity of precious commodities, Ethereum's more flexible issuance policy encourages network security and stakeholder engagement without provoking excessive inflation.

Conclusion

In conclusion, while Bitcoin and Ethereum were groundbreaking in their inception, their fundamental difference lies in their scope. Bitcoin is designed to be an alternative to traditional money, while Ethereum is a platform for decentralized applications. Their differing consensus algorithms, scalability solutions, security features, and token issuance methods further distinguish these remarkable yet divergent manifestations of blockchain technology.

References

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In 2015 IEEE Symposium on Security and Privacy.

Buterin, V. (2013). Ethereum White Paper.

Buterin, V. (2020). A rollup-centric Ethereum roadmap. Ethereum Blog.

Buterin, V. (2021). A brief update on PoS security philosophy. Ethereum Foundation Blog.

Buterin, V. (2021). An update on Ethereum's issuance schedule. Ethereum Foundation Blog.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Song, D. (2016). On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security (pp. 106-125). Springer, Berlin, Heidelberg

Ethereum Foundation. (2020). Ethereum 2.0 Introduction.

Franco, P. (2014). Understanding Bitcoin: Cryptography, Engineering and Economics. John Wiley & Sons.

Kokoris-Kogias, E., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., & Ford, B. (2018). Enhancing Bitcoin security and performance with strong consistency via collective signing. In 25th USENIX Security Symposium (USENIX Security 16).

Krause, M. J., & Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. Nature sustainability, 1(11), 711-718.

Mora, C., Rollins, R. L., Taladay, K., Kantar, M. B., Chock, M. K., Shimada, M., & Franklin, E. C. (2018). Bitcoin emissions alone could push global warming above 2°C. Nature Climate Change, 8(10), 931–933.

Mücke, M. (2020). Smart Contracts. In Blockchain Basics (pp. 75-85). Apress.

Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2020). A brief survey of cryptocurrency systems. In 2016 14th Annual Conference on Privacy, Security and Trust (PST), 745-752.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

Nayak, K., Kumar, S., Miller, A., & Shi, E. (2016). Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 305-320). IEEE.

Siegel, D. (2016). Understanding The DAO Attack. CoinDesk.

Vranken, H. (2017). Sustainability of bitcoin and blockchains. Current Opinion in Environmental Sustainability, 28, 1-9.

Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Yellow Paper.

Zamyatin, A., Harz, D., Lind, J., Panayiotou, P., Gervais, A., & Knottenbelt, W. J. (2018). A Wild Velvet Fork Appears! Inclusive Blockchain Protocol Changes in Practice. In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT).