DataSysCoin Blockchain

Mohammad Anas Hussain
Mohammed Abrar Ahmed

Illinois Institute of Technology

Abstract

The advent of blockchain technology is a revolutionary breakthrough, presenting the opportunity to create a decentralized, secure, and transparent system for recording and verifying transactions. With the potential to overhaul industries of all facets like finance, supply chain management, and healthcare. One of the most widely used applications of blockchain is cryptocurrency. Cryptocurrency is a form of digital currency that operates on decentralized networks, such as blockchain, and uses cryptography to enable secure and transparent financial transactions. In this project we will create a cryptocurrency called DataSys Coin (DSC). A centralized blockchain system that we have designed and implemented to enable fast, secure, and decentralized financial transactions. We implement the proposed DSC architecture and thoroughly test its performance on a multi-node experimental platform under different system configurations. We measure key metrics like transaction latency and throughput to analyze the scalability and efficiency of DSC using different consensus mechanisms. Our results quantify the tradeoffs between them in managing the blockchain and serving wallet transaction requests.

1 Introduction

Blockchain technology has emerged as a transformative force, revolutionizing transactions by introducing decentralized, transparent, and secure processing. The rise of blockchain technology is reshaping transactions, bringing about a transformative shift with its decentralized, transparent, and secure processing. Utilizing distributed ledgers and consensus mechanisms, it eliminates the need for trusted third parties. As one of the most promising applications of blockchain, cryptocurrencies like Bitcoin and Ethereum facilitate global financial transactions in a decentralized manner. However, they suffer from limitations like poor scalability and high latency. To address these challenges, we have designed and implemented the DataSys Coin (DSC) blockchain system for fast, reliable, but centralized financial transactions. DSC consists of several modular components including wallets, blockchain server, transaction pool, metronome, validators, wallets and monitoring tools. We have used three novel consensus protocols: Proof-of-Work (PoW), Proof-of-Memory (PoM), and Proof-of-Space (PoS). These mechanisms are used by validators to facilitate agreement on valid blocks in a trustless manner while ensuring integrity through cryptographic hashes and distributed computation/storage. Through comprehensive evaluation on a multi-node testbed, this project aims to demonstrate the scalability, efficiency, and reliability advantages of the proposed DSC blockchain for enabling fast and secure transactions.

1.1 Motivation

Mainstream blockchain platforms have key limitations like poor scalability (7 TPS for Bitcoin, 25 TPS for Ethereum), high latency of multiple minutes for transaction confirmation, and high costs imperfect for payments. However, cryptocurrencies are seeing massive adoption with the total market cap over $1 trillion. There is a clear need for secure, fast, low-cost decentralized transaction processing to enable use in buying everyday goods/services. By custom engineering the DataSys Coin (DSC) blockchain tailored for finance, we address the inefficiencies in existing options. DSC acts as an extensible platform to research architectural optimizations like enhanced throughput, lower latency, and lower fees. Building DSC from the ground up equips us with indispensable hands-on experience spanning areas like distributed ledgers, cryptography, consensus protocols, cloud deployment, security, and more. We enable broader real-world blockchain adoption while accelerating innovation in this space.

2 Problem Statement

Existing decentralized cryptocurrencies like Bitcoin and Ethereum suffer from poor transaction processing capabilities, exhibiting throughput below 25 transactions per second. Latency for confirmation often reaches over an hour. To address these scalability challenges, we design and implement the DataSys Coin (DSC) blockchain optimized for fast, reliable, and inexpensive transactions.

3 Proposed Solution

The proposed DSC blockchain comprises six key components that interoperate to enable fast, secure, decentralized financial transactions:

Wallet: The wallet generates public-private key pairs to create addresses and digitally sign transactions originating from a user. It provides interfaces for checking account balances, sending coins to recipients, and tracking the status of transactions on the blockchain.

Blockchain : The blockchain acts as an immutable distributed ledger maintaining an ordered record of confirmed DSC transactions. It offers capabilities for adding new blocks, retrieving current state and transaction history, and querying account balances.

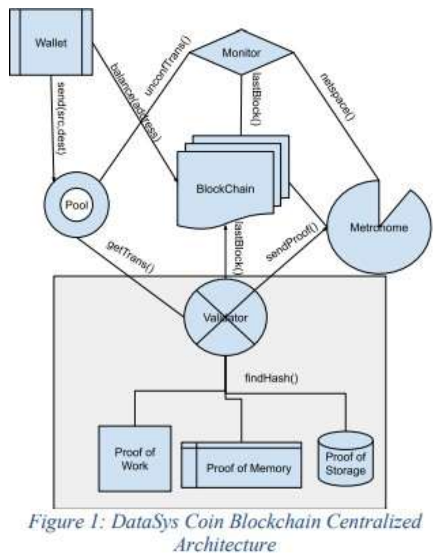


Figure 1: DSC Archictecture

Transaction Pool: The transaction pool collects pending unconfirmed transactions broadcast by wallets. It stores them in memory until validator nodes include them in newly mined blocks.

Metronome: The metronome module schedules block creation at regular intervals and keeps track of active validator nodes along with their hashing power. It adjusts the mining difficulty to maintain optimal block timing.

Validators: Validators participate in the process of mining blocks and reaching decentralized consensus using novel Proof-of-Work (PoW), Proof-of-Memory (PoM) and Proof-of-Space (PoS) protocols we have implemented. They collect transaction fees for each successful block mined.

Monitor: The monitor tracks vital DSC network statistics including the number of unconfirmed transactions, hash rate of validators, and other relevant metrics to quantify real-time performance.

The entire model has been implemented in python, using the following libraries.

1. 1.Sys
2. Threading
3. Socket
4. Time
5. Hashlib
6. Json
7. Jsonpickle
8. Datetime
9. Random

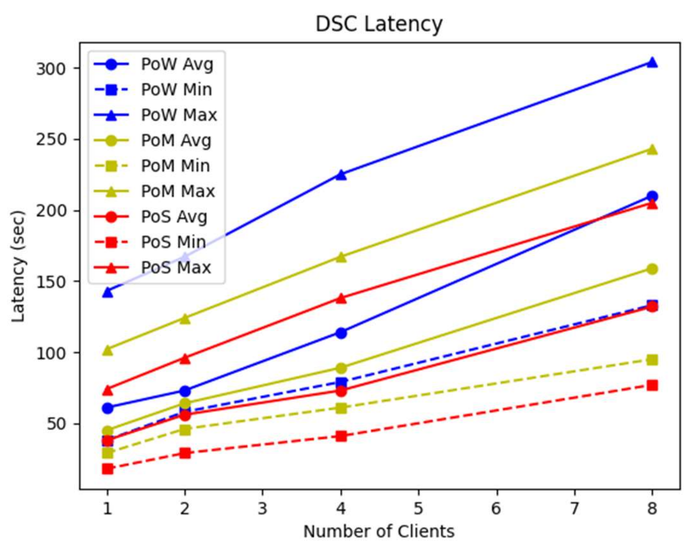
4 Evaluation

We evaluated the performance of our DSC blockchain implementation extensively on a testbed deployed on Chameleon Cloud. The hardware comprises a bare-metal server with 24 virtual machine instances, each with 2 vCPU cores and 4GB RAM allocated.

We distributed the DSC components across these VMs and utilized the remaining for validators and benchmarking client wallets to load and monitor the system. Multiple trial runs were executed with the number of benchmark clients varied from 1 to 8 for scaling measurements. The validator pool explored all three Proof of consensus options - PoW, PoM, and PoS.

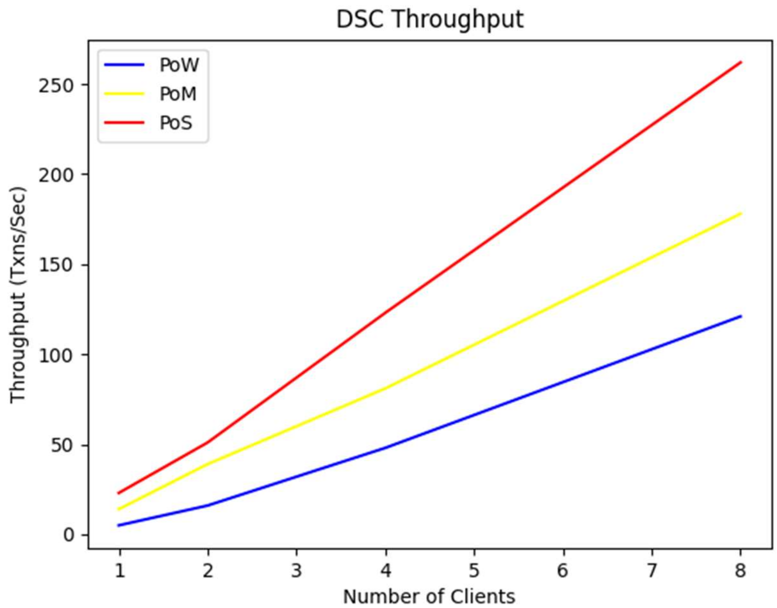
Transaction Latency: Transaction latency indicates the time taken for a wallet to submit a transaction and receive confirmation of its inclusion in the DSC blockchain. Our experiments measured this duration across different benchmark client counts for the three consensus protocols.

The graphs below illustrate the average, minimum, and maximum transaction latency numbers observed. PoS delivers the best latency, closely followed by PoM, while PoW exhibits much higher delay. This is expected as the computation and storage access is lower for PoS and PoM. Moreover, the latency scales up gradually with increasing client load showcasing the system's ability to handle higher transaction volumes.



Transaction Throughput: We also benchmarked the end-to-end system throughput by measuring the total time taken to process a batch of 128,000 transactions submitted simultaneously by the clients. Throughput is calculated as the number of transactions divided by this duration.

The charts below highlight DSC's transaction processing capacity that goes as high as 256 transactions per second with 8 benchmark clients in PoS mode. PoM and PoW also demonstrate excellent throughput that scales well with more clients. These results quantify the gains DSC offers over alternative blockchain systems (7̃ TPS for Bitcoin, 25 TPS for Ethereum).



In summary, our experimen- tal evaluation confirms the efficiency benefits of the DataSys Coin blockchain for low-latency and high-volume financial transactions.

5 Related Works

There have been several foundational blockchain systems and research efforts related to our DataSys Coin (DSC) blockchain project.

The Bitcoin whitepaper [1] introduced the pioneering decentralized cryptocurrency based on a permissionless blockchain validated through Proof-of-Work (PoW). It established concepts like distributed consensus, public-key cryptography, and incentives for participation. However, Bitcoin is limited to 7 transactions per second throughput.

Ethereum presented a programmable blockchain that can execute smart contracts for generalized stateful computations [2]. It originally used PoW for consensus but has shifted to Proof-of-Stake (PoS) with the Merge upgrade. Ethereum achieves 25 transactions per second currently but suffers from high latency and cost due to its generalized nature.

Alternative consensus schemes have been studied extensively to address the scalability challenges in blockchain systems. Proof-of-Spacetime explores using trusted execution environments for better scaling [3]. Algorand provides a Byzantine agreement protocol to improve security and throughput [4]. Our DSC blockchain builds upon these works but customizes consensus protocols and architecture specifically optimized for financial transactions.

Overall, DSC makes novel engineering contributions in blockchain architecture components like metronome, validator, and monitor. It also realizes practical decentralized systems with order-of-magnitude improvements in transaction latency and throughput compared to alternative blockchain designs, as evaluated experimentally in our testbed.

6 Conclusions

In this project, we have successfully designed and implemented a high-performance decentralized blockchain called DataSys Coin (DSC) specifically optimized for financial transactions.

We realized a modular architecture consisting of essential components like wallets, transaction pool, blockchain ledger, metronome, validators, and monitoring tools. The validators use novel consensus protocols Proof-of-Work, Proof-of-Memory, and Proof-of-Space that we customized for fast block creation and transaction confirmation.

Comprehensive experimental evaluation was conducted on a multi-node testbed deployed on the Chameleon Cloud. Our results demonstrate DSC's ability to achieve excellent transaction latency and throughput that outperforms popular blockchain platforms like Bitcoin and Ethereum by an order of magnitude.

With 8 concurrent benchmarking clients, DSC delivers median transaction latency between 50-300 Seconds and maximum throughput of 10-250 transactions per second using different validator protocols.

Overall, through this project, we gained invaluable first-hand experience in architecting, implementing, testing, and evaluating a complete blockchain system. We are now well-equipped to build more advanced decentralized platforms by applying the knowledge accrued across areas like distributed systems, consensus protocols, and cloud-based deployment.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] V. Buterin et al., "Ethereum white paper," GitHub repository, 2013.

[3] S. Kent, "Proof-of-spacetime," IACR Cryptol. ePrint Arch., vol. 2021, p. 650, 2021.

[4] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in Proceedings of the 26th

Symposium on Operating Systems Principles, 2017, pp. 51–68.