Duke CS+ Summer 2021: Decentralized Finance: Cryptocurrency and Blockchain on the Internet Computer: https://ic.pubpub.org/pub/7ms2ilwh/

Impact of Gas: a Comparative Study for Transaction Fee Mechanisms on Blockchains

by Dylan Paul
Project Leads: Profs. Luyao Zhang, Yulin Liu, Kartik Nayak, Fan Zhang
Graduate mentor: Derrick Adam

Project Summary

The proposed research is aimed at analyzing and comparing transaction fee mechanisms/models on two blockchains: the gas model on Ethereum and the reverse gas model on the Internet Computer, and then determining how these models affect efficiency, scalability, and sustainability of applications on these blockchains. To do this, we created a decentralized lending protocol, called 'ICy', on the Internet Computer that works with the reverse gas model. ICy will be a simplified fully functional protocol, providing us with a product to run experiments on to effectively compare to the gas model on the Ethereum blockchain.

Through ICy, we will measure the throughput of the Internet Computer in terms of transactions per second, as well as the transaction costs for users and developers on this specific application, which analyzes efficiency. Additionally, we will specifically test how many transactions it will take until the developer must pay more gas to fuel the application. This will determine the scalability potential and sustainability of the ICy platform and thus the reverse gas model. Then, through simulation, we can attempt to mathematically scale this to as many users as are seen on Ethereum's popular AAVE lending protocol and draw direct comparisons of transaction costs, throughput, and scalability of both gas models.

Intellectual Merit

Although there are other blockchains such as EOS that have provided ways to remove or mitigate the transaction fees of users, there haven't been studies analyzing the effects these models have on overall transactional costs, speeds, and scalability of applications on these networks. In effectively creating a product on the Internet Computer that mimics the basic functionality possessed by a lending protocol, we will be able to analyze the economic differences that the gas models have on lending protocols and expand that to all DeFi apps. This can better equip the nascent DeFi field with key information on gas models, and perhaps guide the field to the model that can best serve millions of users in an exponentially growing field.

Table of Contents

Abstract

Ethereum's popularity as a DeFi platform has resulted in extreme congestion, which has increased the costs of making DeFi transactions and significantly decreased the speed of the network. These changes in the transaction costs and speeds are primarily due to the Ethereum blockchain architecture and gas model. When the costs get too high and the transactions too

slow, users refrain from utilizing the platform, effectively making this permissionless application inaccessible. Other blockchains such as DFINITY's Internet Computer realized this problem and introduced the concept of the 'reverse gas model' which alleviates the economic pressure on the user and places the cost of the transaction fees on the developer. We would like to analyze and compare Ethereum's current gas model with the Internet Computer's 'reverse gas model' and ultimately determine the impact of these contrasting approaches on efficiency, scalability, and sustainability for applications on their respective platforms. In order to effectively analyze the economic impacts of the models, we will create an operating application of a decentralized lending protocol on the Internet Computer that works with the reverse gas model, and then compare it to Ethereum's network. We will then analyze metrics such as the transaction speeds, transaction costs (for users and developers), and the potential for scalability of these platforms. In doing so, we will be equipped with data to determine the most efficient and scalable gas model which can provide the ever-growing DeFi field with a recommended direction in terms of allowing for the best user and developer experience.

DeFi Background

Decentralized Finance (DeFi) represents global virtual financial infrastructures built upon blockchain technology. Decentralized finance applications are permissionless, interoperable, borderless, transparent, and secure due to being built on blockchains' distributed ledger technology (Chen and Bellavitis 2020). Blockchain technology enables the development of these DeFi applications by essentially replacing centralized architectures and intermediaries with smart contracts or software canisters built on the distributed peer-to-peer networks (Chen and Bellavitis 2019). Smart contracts, which are inherent to Ethereum's blockchain, and software canisters, which are part of the DFINITY Internet Computer (Granström 2020), allow for building software services that scale cheaply and enable the development of these DeFi applications by mimicking existing financial services (Schär 2021). Therefore, DeFi presents a way to improve existing financial services by increasing transparency, scalability, and interoperability as well as making investing more accessible to individuals who may not have been able to participate within the current system. DeFi applications have recently exploded in popularity as there are over 2 million unique addresses compared to around 500 thousand in October of 2020, signifying increased adoption of these protocols by investors who are putting more and more of their money into these protocols and leading to an estimated 128-billion-dollar market cap for DeFi (Dale 2021). These investors are attracted to the increased control over their funds, high returns, and new use cases that the field has to offer. Currently, the DeFi space is dominated by Ethereum with AAVE being one of the most well used decentralized applications (ByteTree, 2021). AAVE is a decentralized lending protocol on the Ethereum blockchain, which allows users to lend, borrow, and earn interest on Ethereum crypto assets without an intermediary's involvement. The potential of decentralized lending protocols is immense as they are permissionless so there is no ID verification or KYC, thereby increasing accessibility of its uses to all members on its platform, which comes in direct contrast to centralized institutions, while also providing security. Unfortunately, the growth of these decentralized lending protocols is constricted by the Ethereum blockchain that they are built on, as high transaction costs and slow transaction speeds inhibit even more widespread use.

Gas Model

Gas in Ethereum is the transaction cost necessary to perform a transaction on the network. Gas fees are payments made by users to compensate for the computing energy required to process and validate transactions on the Ethereum blockchain (Frankenfield 2021). The exact price of the gas is determined by supply and demand between the network's miners, who can decline to process a transaction if the gas price does not meet their threshold, and the demand by users of the network who seek processing power. On Ethereum, anybody can become a miner and validate transactions as it is POW (proof of work consensus) at the present, and miners can choose which transaction to validate based on the gas price offered by a user. Additionally, space is limited currently due to the network demand and the block gas limit, thereby creating a sort of supply/demand equilibrium for how much users must pay in gas to ensure that their transaction is bundled up by a validator into a block that is lacking space (Conner 2019). This creates pressure on the users to pay higher fees to ensure their transaction goes through faster due to the low scalability of the network and the high demand for DeFi apps on Ethereum. It appears Layer-2 scaling solutions, and Ethereum 2.0, will be necessary to reduce the transaction fees by increasing scalability and increasing the number of transactions that can be processed per block.

Reverse Gas Model

In contrast to Ethereum's gas model, the reverse gas model on the Internet Computer puts the onus on the developer as the one required to pay the transaction fees and thus makes it easier for the users to use the applications (Walters 2021). This is only possible on the Internet Computer because of the structure of their blockchain. Unlike traditional layer 1 solutions such as Ethereum, 'mining' doesn't exist for every user as it is the structure of the data centers, node machines, subnets, chain key, and the consensus protocol that ensures the security of the system. The developers must pay for ICP tokens, the utility token on the Internet Computer, from data centers or neuron holders (users who stake ICP tokens to take part in governance) who are given these as rewards for upholding the system, and the developers must use the ICP tokens to convert to cycles to run their apps so that users don't have to pay (DFINITY 2020b). Cycles reflect the real costs of operations for applications hosted on the Internet Computer's platform (DFINITY 2021). The amount a developer pays or 'gas' in cycles is easy to predict because cycles have a stablecoin mechanism not dependent on the price of the ICP. Also, scalability is not a problem thanks to the ability to add more node machines as is necessary and determined by the NNS (self-governing body of the Internet Computer), so congestion isn't an issue (DFINITY 2020b). However, a developer may need to deploy many software canisters, or scalable smart contracts which hold the executable code, to serve their user base which can cost them many cycles. The differences in the structures of the Ethereum blockchain and the Internet Computer is what creates the differences in gas models and determines how much users and developers pay in transaction fees.

General Aims

Duke CS+ Summer 2021: Decentralized Finance: Cryptocurrency and Blockchain on the Internet Computer: https://ic.pubpub.org/pub/7ms2ilwh/

The goal of this research will be to address the current problems faced by Ethereum by directly comparing the Ethereum gas model to the reverse gas model implemented on DFINITY's Internet Computer. We want to determine these models' impacts on efficiency, scalability, and sustainability for applications on their respective platforms. In order to do so, we will first have to analyze and give a more comprehensive overview of how both layer 1 blockchains are structured (i.e. consensus mechanisms, validators, NNS, tokenomics) which will give even greater insight and understanding into how their gas models are structured. This will be done by constructing models of the 'life cycle' of a transaction from a user's wallet to the protocol and then to the network.

Then, we will implement a decentralized lending protocol on the Internet Computer, called 'ICy' (Internet Computer Yield), to collect the necessary data of transaction throughput, transaction costs, and scalability potential, and use this to compare to Ethereum's network. Transaction throughput will be calculated for each network in terms of maximum, minimum, median, and mean number of transactions possible per second. Transaction costs will be measured for users and developers on 'AAVE' and 'ICy' which will naturally compare the costs for users and developers on Ethereum and the Internet Computer respectively. Lastly, scalability potential will be discussed when comparing the maximum and mean number of transactions per second, but we will also model the amount of users/activity on the application to the projected transaction costs, which will investigate which gas model can handle user volume more effectively and thus measure the sustainability of the models.

	Efficiency	**Scalability**	**Sustainability**
Metrics to Collect	Projected Transaction Costs for Users and Developers	Throughput on Network: max/median/mean/min tps (transactions per second)	The Number of Users on Lending Protocol
Current data for AAVE and Ethereum	Ranging anywhere from 4-45 dollars for users	Ranges from 15-45 tps	88,388 addresses and growing on AAVE ~1.5K active per day

Data to be Collected for ICy and IC			

Table 1: Data Comparison of AAVE (Ethereum) to ICy (Internet Computer)

ICy

We implemented a simplified version of a decentralized lending protocol on the Internet Computer, 'ICy' (Internet Computer Yield), which has lending and borrowing features for arbitrary tokens representing the Internet Computer's native tokens, called cycles and ICP. ICy enables users to lend to the protocol and receive interest in return for their liquidity, or provide collateral to borrow another token to be paid back in the future with interest. With a few more modifications and help from a DFINITY engineer it can be converted to a fully functional decentralized lending platform for users with real cycles and ICP, and it can help us to start visualizing how the reverse gas model works in action.

At the present, ICy is structured with the product and reserve canisters which are responsible for the functionality of the protocol, and the additional user canisters and treasury canister which are used to run tests on the protocol. Each user canister represents a 'user' on the platform and the treasury canister's role is to supply the 'user' with funds to play around with in the product canister. Users who are interacting with the application are interacting with the code in the product canister. Users must first create an account through the product canister which connects to a database that holds the user's ID and balance of tokens and thus supports potentially many users. Users must then add funds to their account to have access to all the desired functionality of lending and borrowing of tokens representing ICP and cycles that the product canister has to offer. Meanwhile, the reserve canister works quietly in the background to keep track of the liquidity of each token in an artificial liquidity pool. Improvements with ICy will be continuously made as the Internet Computer becomes more mature and has increased documentation.

Methodology with ICy

We will first have to tweak the code of ICy to successfully create a fully functional decentralized lending platform, with the reverse gas model of no user gas fees, for as many users as possible. We will then manually test the size of transactions users can make as well as measure how fast transactions are processed. Therefore, we will measure transaction costs and throughput as discussed before. Additionally, we will test how many transactions a canister can handle before being depleted of its cycles which will require more developer transaction fees or gas. This will determine the scalability potential and the costs associated with increased users on the ICy platform. Then, through simulation, we can attempt to mathematically scale this to as many users as are seen on Ethereum's AAVE and draw direct comparisons of transaction costs, throughput, and scalability of both gas models. With this information, we can fill out 'Table 1' and have enough data to determine these gas models' impacts on efficiency, scalability, and sustainability as well as draw conclusions as to which model provides for a better user and developer experience.

Novelty and Contribution to Literature

This proposed research presents the unique opportunity to be the very first to build a lending protocol on DFINITY's Internet Computer and moreover conduct research on how the reverse gas model can change how lending protocols could be built out. In effectively creating a product on the Internet Computer that mimics the basic functionality possessed by AAVE, we will be able to analyze the key economic impacts and differences that the gas models have on lending protocols and expand that to all DeFi apps, information that isn't provided by current literature. This can better equip the nascent DeFi field with key information on these two gas models and perhaps guide the field to the model that can best serve millions of users in an exponentially growing field (Behrens 2021).

Bibliography

aave. 2020. “Aave-Protocol/Aave_Protocol_Whitepaper_v1_0.Pdf at Master · Aave/Aave-Protocol · GitHub.” GitHub. AAVE. 2020. https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf.

Behrens, Alex. 2021. “The Growth of DeFi.” Circle | Payments Infrastructure for Internet Businesses. June 16, 2021. https://www.circle.com/blog/the-growth-of-defi.

ByteTree.com. 2021a. “Ethereum’s DeFi Domination: Understanding the Size and Role of Ethereum’s Largest DApps.” Medium. Medium. February 5, 2021. https://bytetree.medium.com/ethereums-defi-domination-understanding-the-size-and-role-of-ethereum-s-largest-dapps-a6063505b2d3.

Chen, Yan, and Cristiano Bellavitis. 2019. “Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System.” Search ELibrary :: SSRN. Stevens Institute of Technology School of Business Research Paper. July 3, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3418557.

Chen, Yan, and Cristiano Bellavitis. 2020. “Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models.” Journal of Business Venturing Insights, no. Volume 13. https://doi.org/e00151.

Conner, Eric. 2019. “Understanding Ethereum Gas, Blocks and the Fee Market.” Medium. Medium. September 26, 2019. https://medium.com/@eric.conner/understanding-ethereum-gas-blocks-and-the-fee-market-d5e268bf0a0e.

Dale, Brady. 2021. “DeFi Is Now a $100B Sector - CoinDesk.” CoinDesk. CoinDesk. April 29, 2021. https://www.coindesk.com/defi-100-billion-dolla.

DFINITY. 2020a. “A Technical Overview of the Internet Computer.” Medium. The Internet Computer Review. September 18, 2020. https://medium.com/dfinity/a-technical-overview-of-the-internet-computer-f57c62abc20f.

DFINITY. 2020b. “The Internet Computer’s Token Economics: An Overview.” Medium. The Internet Computer Review. October 6, 2020. https://medium.com/dfinity/the-internet-computers-token-economics-an-overview-29e238bd1d83.

DFINITY. 2021b. “Cycles.” DFINITY Foundation | Internet Computer. 2021. https://dfinity.org/faq/cycles.

Duke CS+ Summer 2021: Decentralized Finance: Cryptocurrency and Blockchain on the Internet Computer: https://ic.pubpub.org/pub/7ms2ilwh/

Frankenfield, Jake. 2021. “Gas (Ethereum).” Investopedia. 2021. https://www.investopedia.com/terms/g/gas-ethereum.asp.

Granström, Johan. 2020. “A Closer Look at Software Canisters, an Evolution of Smart Contracts.” Medium. The Internet Computer Review. October 7, 2020. https://medium.com/dfinity/software-canisters-an-evolution-of-smart-contracts-internet-computer-f1f92f1bfffb.

Schär, Fabian. 2021. “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets.” Review, no. 2. https://doi.org/10.20955/r.103.153-74.

Walters, Steve. 2021. “Internet Computer (ICP) Review: The Global Internet Computer.” Coin Bureau. June 6, 2021. https://www.coinbureau.com/review/dfinity-icp/.