Seamlessly Transferring Assets through Layer-0 Bridges: An Empirical Analysis of Stargate Bridge's Architecture and Dynamics

Huang, Chuanshan ; Yan, Tao ; Tessone, Claudio J

DOI: https://doi.org/10.1145/3589335.3651964

Originally published at:
Huang, Chuanshan; Yan, Tao; Tessone, Claudio J (2024). Seamlessly Transferring Assets through Layer-0 Bridges: An Empirical Analysis of Stargate Bridge's Architecture and Dynamics. In: WWW '24: The ACM Web Conference 2024, Singapore Singapore, 13 May 2024 - 17 May 2024, 1776-1784.
DOI: https://doi.org/10.1145/3589335.3651964

Seamlessly Transferring Assets through Layer-0 Bridges: An Empirical Analysis of Stargate Bridge's Architecture and Dynamics

Chuanshan Huang
chuanshan.huang@uzh.ch
University of Zurich, Zurich, Switzerland

Tao Yan*
yan@ifi.uzh.ch
University of Zurich, Zurich, Switzerland

Claudio J. Tessone
claudio.tessone@uzh.ch
University of Zurich, Zurich, Switzerland

ABSTRACT

The increasing number of distinct blockchains has led to a growing need for data exchange and asset transfer across various isolated blockchains. To address this, cross-chain bridges have emerged as a critical mechanism for enabling interoperability and facilitating data and asset exchange across diverse blockchains. Among these bridges, the Layer-0 bridge stands out as a scalability solution that enhances blockchain performance at the foundational layer of data transition, without altering the blockchain's structure. Stargate is a notable Layer-0 Lock-and-Unlock cross-chain bridge that supports transactions across various EVM-based blockchains, with the highest Total Value Locked (TVL) among cross-chain bridges of the same kind. While previous cross-chain research has primarily focused on Layer-2 bridges, this study specifically examines Stargate and analyzes its dynamics as well as potential vulnerabilities. We collect transaction data of Stargate on six blockchains including Ethereum, Polygon, Binance Smart Chain, Avalanche, Arbitrum and Optimism. Our findings reveal the transaction patterns and evidence of exploitations of Stargate by investigating its transaction dynamics over time.

CCS CONCEPTS

• **Applied computing → Evidence collection, storage and analysis**.

KEYWORDS

Blockchain, Scalability, Layer-0, Bridge, Stargate

ACM Reference Format:
Chuanshan Huang, Tao Yan, and Claudio J. Tessone. 2024. Seamlessly Transferring Assets through Layer-0 Bridges: An Empirical Analysis of Stargate Bridge's Architecture and Dynamics. In *Companion Proceedings of the ACM Web Conference 2024 (WWW '24 Companion), May 13–17, 2024, Singapore, Singapore.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3589335.3651964

*Corresponding author

WWW '24 Companion, May 13–17, 2024, Singapore, Singapore

ACM ISBN 979-8-4007-0172-6/24/05
https://doi.org/10.1145/3589335.3651964

1 INTRODUCTION

Bitcoin is regarded as the first-generation blockchain, while Ethereum is renowned as the second-generation blockchain with the introduction of smart contracts[27]. Currently, the development and proliferation of the third-generation blockchains [6] are actively taking place. The continuous evolution of blockchain technology has led to the emergence of numerous blockchain platforms, particularly those utilizing the Ethereum Virtual Machine (EVM). However, these different blockchains and protocols have fragmented the blockchain space into isolated islands of information, with a large number of encrypted assets distributed across different blockchains, leading to circumstances where the assets on one blockchain cannot be used directly on another blockchain. For example, Bitcoin, as the most popular and largest cryptocurrency by market capitalization, cannot be used directly on Ethereum. In addition, in the field of Decentralized Finance (DeFi), different DeFi protocols have independent liquidity on different blockchains for the same asset, which not only complicates the process of asset transfers but also has the potential to contribute to token inflation. Therefore, it is essential to achieve a free flow of information and seamless transactions of assets across various blockchains.

The cross-chain bridge is a means of achieving data exchange and asset transfer between different blockchains. It comprises a collection of smart contracts and network nodes. Smart contracts are responsible for managing on-chain data and assets, while network nodes verify transactions. Currently, there are two main approaches to cross-chain bridges: Layer-2 solutions and Layer-0 solutions. While previous research has focused mainly on the Layer-2 solution, specifically exploring the mechanism design[17, 26] and security analysis[19, 31] of cross-chain solutions, this study will empirically investigate the dynamics of the Stargate, a Layer-0 cross-chain bridge, including fund flows, transaction patterns, and potential risks. This work makes the following contributions:

- Providing an analysis of the mechanisms and dynamics of a Layer-0 cross-chain bridge. This analysis sheds light on the performance of six blockchains on the Stargate bridge and offers valuable insights into the collaboration and competition between blockchains.
- Uncovering several significant findings. Notably, it reveals that Layer-2 blockchains which serve as a potential solution for Layer-1, exhibit a strong demand for cross-chain transactions. We find that cross-chain transactions via Stargate bridge mainly occur among Layer-2 blockchains, rather than between Layer-1 and Layer-2 blockchains. This highlights that not only Layer-1 blockchains possess the necessity for

cross-chain capabilities, but also Layer-2 blockchains exhibit a significant demand for asset transfers across blockchains.
- Establishing a foundation for further research on the security of cross-chain transactions by meticulously analyzing cross-chain transaction data for security vulnerabilities. For instance, the discovery of unusually high trading volumes and reward exploitations of Stargate can provide valuable insights into the risks associated with cross-chain activities.

The rest of the paper is structured as follows: Section 2 introduces the mechanisms of cross-chain bridges, with a focus on the implementation of the Stargate protocol, as well as the related work. Section 3 describes the methodology for collecting cross-chain data. Section 4 presents the analysis results of the cross-chain data. Section 5 summarizes the paper and proposes future research directions.

2 BACKGROUND AND RELATED WORK

2.1 Blockchain scalability-improvement solutions

The concept of blockchain layers stems from the different stacks of technologies on which blockchains operate. In most cases, current blockchain technologies can be categorized into three layers according to the architecture and functionalities of blockchain.

- *Layer-1* contains pivotal functions of a blockchain such as consensus mechanism, security and the execution of transactions. Bitcoin and Ethereum are the representatives of Layer-1 blockchains. At the Layer-1 level, the scalability-improvement solutions include optimizing consensus mechanisms, enhancing block capacity, and implementing sharding techniques.
- *Layer-2* technologies are mostly created to scale up Layer-1 blockchains by processing transactions off layer-1 chains and thus reducing the burden of Layer-1[22]. The main Layer-2 blockchains are Polygon, Binance Smart Chain, Optimism, etc. The Layer-2 solutions can be presented in the format of state channels, sidechains and roll-ups.
- *Layer-0* is the underlying network of nodes where a copy of all the data of a blockchain is partially or fully hosted. Layer-0 is usually responsible for data transmission and propagation on which Layer-1 is built[9]. Cosmos and Polkadot are the representatives of Layer-0 solutions. Layer 0 can enhance the interoperability of blockchain systems by offering cross-chain communication protocols that operate beneath Layer-1. For instance, the Cosmos utilizes the Inter-Blockchain Communication (IBC) protocol[5] to facilitate communication among different parallel chains.

LayerZero[30] is a protocol that operates at the Layer-0 level and enables direct communication across different blockchains without the need for intermediary platforms or tokens. Stargate is a cross-chain bridge based on the LayerZero protocol, facilitating the seamless transfer of native assets between multiple EVM-based blockchains. According to DeFiLlama[1], Stargate currently has the highest total value locked (TVL) among all cross-chain bridges.

[1]https://defillama.com/protocols/Cross%20Chain

2.2 Cross-chain Bridges

Cross-chain bridges are mainly defined by the functions of smart contracts that operate on the source chain and the target chain[4]. In addition, Pillai et al. [21] argue that Hashed Timelock Contracts are also a type of cross-chain bridge protocol, despite that it is proposed as an atomic swap [11] and is treated as a different concept in Shadab et al. [23] and Harris's work[10]. The classification varies in the literature, here we present a widely used classification.

Lock-and-Unlock bridges require users to send assets to their bridge contracts on the source chain. The bridge contract will lock these assets, unlock the same amount of desired assets on the target chain, and send them to the user's address on the target chain. These types of bridges usually require strong liquidity support on all involved blockchains [4, 18, 21].

Burn-and-Mint bridges will burn assets when users initiate a cross-chain transaction and send their assets to the bridge contract on the source chain. An equal amount of wrapped assets on the target chain will be minted by the respective token contracts and then sent to the user's address on the target chain [4, 18, 21].

Lock-and-Mint bridges lock a user's asset on the source chain, then mint an equal amount of wrapped asset on the target chain and send to the user' address on the target chain. This architecture is used by bridges between Ethereum and Layer-2 chains, such as the Polygon PoS Bridge[2].

In addition, based on the number of blockchains that a bridge can link together, cross-chain bridges are divided into two types: Chain-to-Chain Bridges and Multi-Chain Bridges. Chain-to-chain bridges only transmit data between two chains, while Multi-Chain bridges can communicate with a network of blockchains.

Stargate is a Lock-and-Unlock, Multi-Chain bridge as per the categorizations mentioned above. Following the definition of the cross-chain bridge in Section 1, a cross-chain transaction on EVM-based blockchains is defined as a transaction that transfers assets from an address to the same address on another blockchain through a cross-chain bridge[2]. By nature, a cross-chain transaction is not an atomic transaction since it involves at least two blockchains. Actually, it consists of two transactions: one on the source chain that transfers assets to a bridge smart contract, and another on the target chain that transfers assets from a bridge smart contract to the receiver address.

2.3 Mechanism of Stargate

Stargate is a combination of a cross-chain bridge and liquidity pools that enables the transfer of native assets instead of wrapped tokens, while also providing unified liquidity. This unified liquidity refers to the sharing of liquidity across different chains for the same cryptocurrency, thereby enhancing capital efficiency. The underlying mechanism of Stargate relies on the LayerZero protocol, which is a decentralized cross-chain communication protocol enabling direct asset and data transfer among different blockchains. According to the whitepaper of LayerZero[30], we summarize two primary mechanisms employed by Stargate to achieve cross-chain asset transfer.

[2]https://docs.polygon.technology/pos/how-to/bridging/

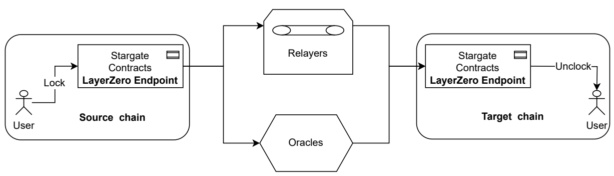

Figure 1: The process of cross-chain transactions via Stargate.

- *Cross-Chain Message Transmission:* Stargate achieves cross-chain asset transfers primarily through three main components: Endpoints, Oracles, and Relayers. Endpoints are a series of smart contracts deployed on each chain, with each chain having a single endpoint responsible for sending information to external chains. These can be utilized by apps on the same chain to initiate cross-chain communication. Oracles, provided by third-party services like Chainlink, help in reading and authenticating block header information and transmitting it to the target chain. Relayers are off-chain data storage services, their main function is to read and feed the transaction proof from the original chain to the target chain.
- *Decentralized Liquidity Pools:* Stargate employs decentralized liquidity pools to facilitate instantaneous asset transfers. Whenever a user intends to perform a cross-chain asset transfer, they effectively send the assets to a liquidity pool on the source chain and withdraw an equivalent amount of assets from the corresponding liquidity pool on the target chain. These liquidity pools are provided by the community, and the funds within the pools are contributed by liquidity providers (LPs). The LPs offer cross-chain transfer services to users implicitly in this manner and earn rewards in return.

The general process of cross-chain transactions via the Stargate bridge is elucidated in Figure 1. When a user initiates a cross-chain transaction, they shall call the Endpoints contract and send the assets to Stargate's contract on the source chain. Then the Oracle verifies the block header, while the Relayer stores the transaction proofs off-chain. After that, the Oracle and Relayer transmit this information to the target chain. The Stargate bridge contract on the target chain allows unlocking assets and transferring them to the user's address upon receiving the notification from Oracle and Relayer. It is notable to highlight that the sender address and receiver address of cross-chain transactions are the same on EVM-based blockchains.

Stargate utilizes a liquidity balancing mechanism to optimize capital efficiency. This mechanism is illustrated in Figure 2. The hexagon represents the six investigated blockchains, and each large triangle represents one of the chains. The orange area represents the liquidity pool of the token which the user transfers, while the purple area represents the liquidity pools of other tokens. After users transfer tokens to the Stargate contract, the Stargate contract will then lock the assets and integrate them into the liquidity pool of the source chain. Stargate's Delta (Δ) algorithm, as detailed in its whitepaper [29], will check if the liquidity pools of the same token on other chains have an adequate amount of balance. If there

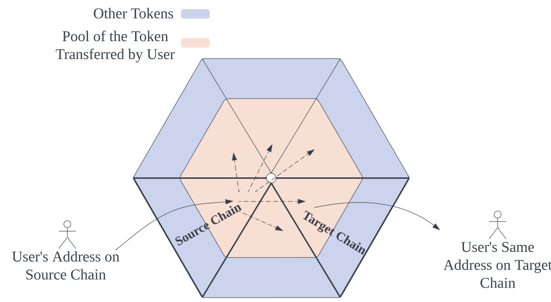

Figure 2: The liquidity balancing mechanism of Stargate.

exists a shallow liquidity pool, the Delta algorithm will redistribute liquidity on the source chain to lower liquidity pools on other chains, as illustrated by the dotted lines.

2.4 Related Work

With years of development, blockchain is still suffering from the trilemma[3] that none of the existing blockchains can achieve security, decentralization and scalability simultaneously. Ethereum, the most comprehensive blockchain at the moment, can only process around 15 transactions per second. Layer-2 and Layer-0 solutions are currently the prevalent solutions[14]. Current Layer-2 protocols can be classified into channels and sidechains[9, 24]. Channels allow users to conduct numerous transactions off-chain, settling the final state on the main chain. Sidechains are independent blockchains running alongside a main chain, reducing the computational burden from the main chain[1]. Examples of Layer-2 solutions include Polygon[13] and Arbitrum[12]. Layer-0 solutions focus more on optimizing the way data transfer among different Layer-1 blockchains[28]. The leading Layer-0 solutions are Cosmos[16] and Polkadot[25].

Current literature on cross-chain bridges mainly focuses on identifying bridge vulnerabilities and implementing safer protocols. Lee et al.[19] provide a comprehensive review of cross-chain attacks, categorized by the bridge component which the attack exploits: Custodian attacks exploit the bridge contract on the source chain; Debt Issuer attacks focus on exploiting the smart contract that sends assets to users on the target chain; Communicator attacks breach into the data transition process between the source and target chain; Token Interface attacks scam users' funds directly. Zhang et al.[31] identify three attacks of cross-chain transactions, namely Unrestricted Deposit Emitting, Inconsistent Event Parsing and Unauthorized Unlocking. They also develop a tool to monitor potential scamming transactions. Duan et al.[8] classify attacks from multiple perspectives, such as being on-chain or not and the vulnerability of different blockchain structures. They also review major successful exploits that result in substantial economic loss. Xie et al.[26], Dai et al.[7], and Lan et al.[17] propose novel and more secure protocols to facilitate cross-chain transactions. Although there is an increasing number of studies on cross-chain bridges, few studies focus on the analysis of the actual transactions that travel across bridges.

Table 1: Blockchains and Their Layers.

Blockchain	Layer
Ethereum	L1
Avalanche	L1[4]
Polygon	L2
Binance Smart Chain	L2
Arbitrum	L2
Optimism	L2

Table 2: An overview of the important data fields.

Data Field	Description
timeStamp	Timestamp of the transaction.
chainId	Target chain.
dstPoolId	Transferred assets.
from	The sender and receiver address.
amountUSD	The value of assets transferred.
eqFee, protocolFee and lpFee	Different types of incurred fees.
sourcechainId	Source chain.
eqReward	Reward granted to users.

3 DATA COLLECTION

Stargate supports the transfer of a collection of tokens across multiple blockchains. We choose the assets with the highest transaction volumes [3], which are BUSD, USDT, USDC, DAI, FRAX and Ether. To collect the data, we first identify the corresponding events and contracts. Stargate uses the same event *Swap()* on all supported blockchains to perform cross-chain transactions, which is deployed on bridge endpoint contracts on respective chains. Subsequently, we retrieve the log data related to the *Swap()* event using the API of each blockchain explorer. Finally, we parse the acquired raw data using the Application Binary Interface (ABI) of the relevant token contracts. The pipeline is illustrated in Figure 3. In total, we collect 13,925,567 transactions across Ethereum, Binance Smart Chain, Polygon, Arbitrum, Optimism and Avalanche, spanning from March 17^{th}, 2022 to October 26^{th}, 2023. Table 1 presents the corresponding blockchain layers, and Table 2 summarizes the important data fields.

As per the definition of a cross-chain transaction in the previous subsection, a cross-chain transaction should consist of two transactions. We have only collected transactions on the source chain, but it is still sufficient for our analysis. The reasons are as follows: (1) we have the necessary data fields to identify which assets are moved between different blockchains; (2) we are confident that our data is the "source part" of a cross-chain transaction, as we collect event data from bridge contracts, which indicates that users indeed transfer their assets to these contracts.

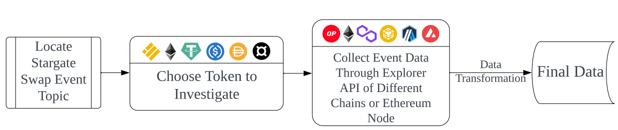

Figure 3: Pipeline for Stargate data collection.

4 RESULTS

4.1 Transaction Dynamics

Figure 4 illustrates Stargate's fees, transaction volumes and the number of transactions, categorized by assets. It shows an overall increasing trend in cross-chain transaction numbers, volumes and associated fees. Notably, USDT emerges as the dominant asset in terms of both transaction quantities and volumes. Additionally, there is an upward trend with an increase in the number of transactions and the transaction volumes around April 2023, as illustrated in Figures 5 and 6. Figures 5, 6 and 7 visualize the same metrics, but categorized by blockchain. We could see that most cross-chain transactions and the majority of trading volumes originate from layer-2 blockchains, especially Arbitrum. The blockchains analyzed and their corresponding layers are detailed in Table 1. It is interesting to see that in Figure 5, although there are only a few transactions sending assets from Ethereum, the trading volume of these transactions in Figure 6 is comparable to transactions initiated from other chains, implying that transactions starting from Ethereum are of high value.

In Figure 6 and 7 and the first two plots of Figure 4, a notable spike is observed on October 7^{th}, 2022, but not in Figure 5 or the third plot of Figure 4. These figures collectively indicate a significant increase in trading volume on the aforementioned date, while the number of transactions remains relatively consistent. Furthermore, this suggests that the increase in trading volume is likely driven by a few high-volume transactions on that day. Upon conducting a detailed analysis of the data for October 7^{th}, 2022, we identify a significant rise in transaction volume attributed to a single address transferring stablecoins out from Binance Smart Chain, as depicted in Table 5 in the appendix. This anomaly is later verified as an exploitation on Binance Smart Chain (BSC) by Nansen[20]. According to Nansen's report, the perpetrator borrows stablecoins using BNB as collateral on Binance Smart Chain, then transfers the funds to other chains using Stargate and Multichain[5] in smaller batches ranging from 400 thousand to 5 million USD. This case highlights that Stargate sometimes can be exploited by the malicious to quickly transfer assets as it provides an efficient means for seamlessly transferring assets across different blockchains.

On April 26^{th}, 2023, another notable surge is observed in three subplots depicted in Figure 4. The surge is attributed to the news of the LayerZero airdrop[15], leading to a 30% increase in the volume on the Stargate cross-chain bridge as investors seek to qualify for the airdrop. This event significantly boosts trading activities on Stargate, resulting in a tenfold increase in its total volume in USD, as depicted in both Figure 4 and Figure 6. Additionally, analysis from Figure 5 indicates that transactions originating from Arbitrum and Optimism drive this surge, with both the number of transactions and transaction volumes exhibiting substantial increases on these two blockchains during this period.

4.2 Fees and Rewards

In Section 2.3, we briefly mention Stargate's Delta algorithm with its effort to balance liquidity pools on different chains. While it

[3]https://defillama.com/bridge/stargate
[4]https://www.techopedia.com/cryptocurrency/best-layer-1-crypto-%20projects
[5]https://multichain.xyz/

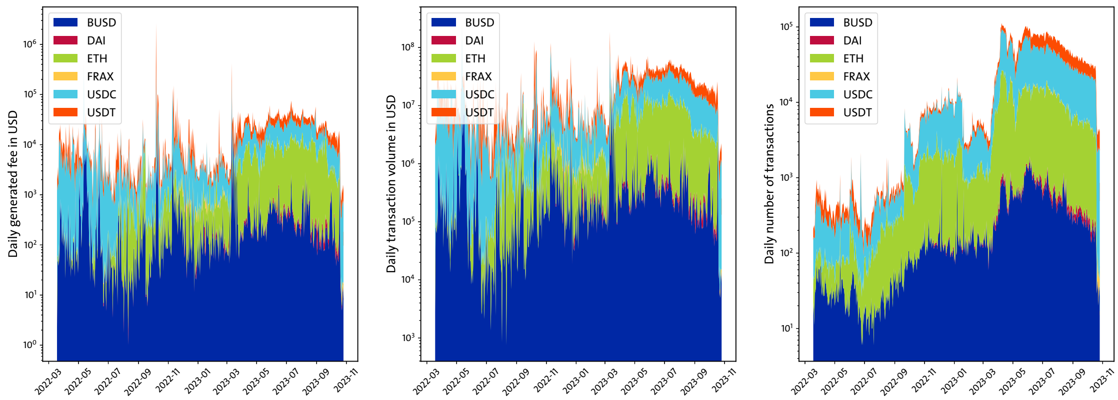

Figure 4: Stack plot of total fees, trading volumes and transaction numbers on Stargate over time, categorized by asset.

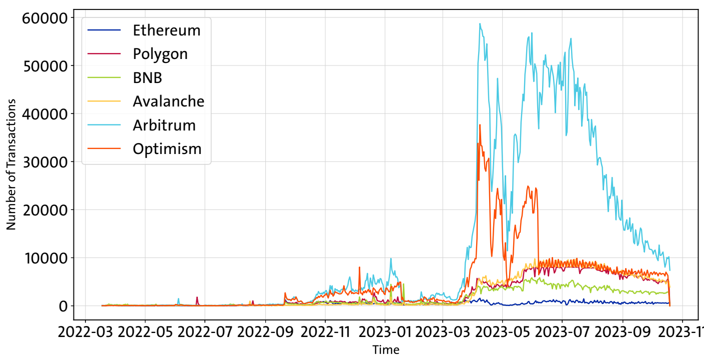

Figure 5: Number of cross-chain transactions via Stargate over time.

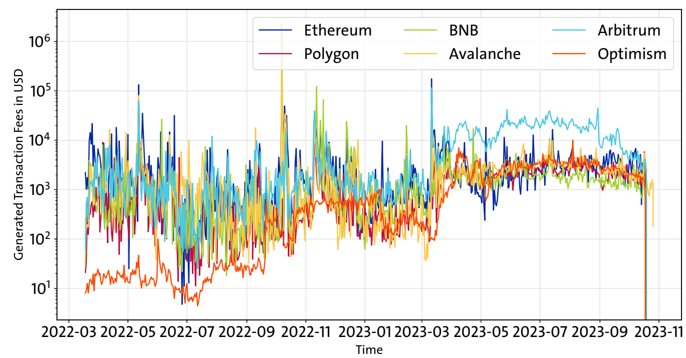

Figure 7: Generated fees in USD over time, categorized by blockchain.

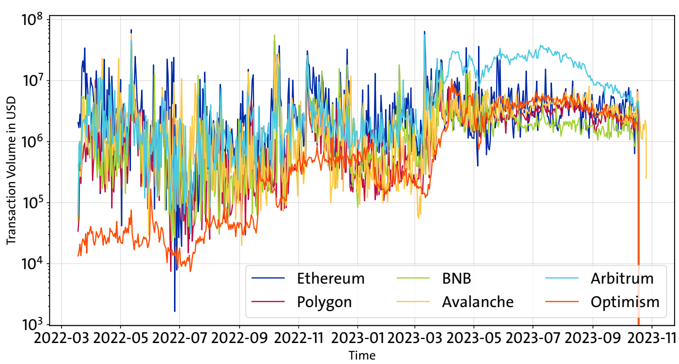

Figure 6: Trading volumes of cross-chain transactions via Stargate over time.

generally works well, this algorithm still suffers from the problem of potentially drained liquidity pools on certain chains as stated in Section 3.4 of Stargate's white paper[29]. To address this, Stargate implements a reward system which encourages users to send transactions that "balance" liquidity pools on different chains by financially rewarding them with an "equilibrium reward". The reward system will monitor every transaction and the balance of liquidity pools when a cross-chain transaction has been issued. If a transaction drains a liquidity pool with relatively low funds, it will be penalized with an additional transaction fee called "eqFee". All collected "eqFee" will be stored in a reward pool, which is backed by both "eqFee" collected from transactions and the Stargate Treasury[6]. Conversely, if a transaction adds liquidity to a token pool with liquidity lower than a certain threshold, this transaction will be infused with a reward during the Swap event, which is proportional to the difference between the post-transaction balance and the target balance[7]. The user who initiates this transaction will be reimbursed with an "equilibrium reward" when the assets arrive at the destination chain[29]. While every transaction has the possibility to be rewarded, we find that in reality only a small number of transactions satisfy the condition and receive a reward. Among the 13,925,567 transactions collected, only 1,112,751 transactions are eligible for an "equilibrium reward", accounting for 7.99% of the whole dataset.

[6]https://stargateprotocol.gitbook.io/stargate/v/user-docs/tokenomics/protocol-fees
[7]Section "Stargate Rebalancing Fees" in https://stargateprotocol.gitbook.io/stargate/v/user-docs/tokenomics/protocol-fees.

The design of "equilibrium reward" seems well-suited to solve the balancing problem. However, we are wary of the potential risks it poses as users might be able to exploit this design to gain revenue if the "equilibrium reward" within a single transaction is greater than the sum of all incurred fees. To be more specific, in such cases, users initiate cross-chain transactions via Stargate, pay the transaction fees, then obtain the same amount of assets on the target chain, plus a reward that is greater than the previously paid fees. Since the "equilibrium reward" is partially backed by the Stargate Treasury, if users can earn excessive transaction rewards, the Stargate Treasury may potentially need to allocate additional funds to sustain the reward scheme.

In order to validate the potential presence of such exploitations, we filter the transactions where the "equilibrium reward" exceeds the sum of all three types of fees shown in Table 2. In total, we have 64,029 such transactions, which is comprised of 0.46% of all the transactions and 5.75% of the transactions with an "equilibrium reward". The initiators of these transactions obtain an excessive amount of rewards, defined as the difference between "equilibrium reward" and the sum of transaction fees. Our findings reveal that these 64,029 transactions yield an excessive reward totaling 3.4 million USD. The highest excessive reward gained from a single transaction is 149,458 USD, generated from a transaction where 8,000,000 USDT was moved from Ethereum to Binance Smart Chain[8].

Given that we have validated the existence of reward exploitations, we proceed to analyze the characteristics of the transactions with excessive rewards. Figure 8 and Table 3 provide insights from the perspective of assets and addresses. From Figure 8, we can see that USDT transactions are the most common asset with excessive rewards, accounting for more than 70% of total excessive rewards. Addresses with the highest gain from excessive rewards are shown in Table 3. The top address earns around 600,000 USD in total, making up 17% of the total excessive rewards. Figure 9 illustrates the evolution of excessive rewards chronologically. From the plot, we can see that excessive rewards are unevenly distributed over time, either close to zero or with a large value. However, after June 2023, excessive rewards become sparse as the number of such transactions significantly decreases.

Table 3: The top 5 addresses which gain the highest amount of excessive rewards on Stargate.

Address	Total Gained Excessive Rewards (USD)
0x89***5eaf	592552.13
0x66***1de1	456707.51
0xee***63a7	409556.25
0xa3***9c37	254720.31
0x1d***bbf1	221640.78

[8]The depositing transaction on Ethereum: https://etherscan.io/tx/0x7169713f1a5ef1eabaf67529f1994fd1d90ed16aa8008cbeda18b8975cbb9947 and the receiving transaction on the Binance Smart Chain: https://bscscan.com/tx/0xb7e188b7da185f3de8d4f1ea0c7a6835cc062c27c54629a047afa5229b123e08

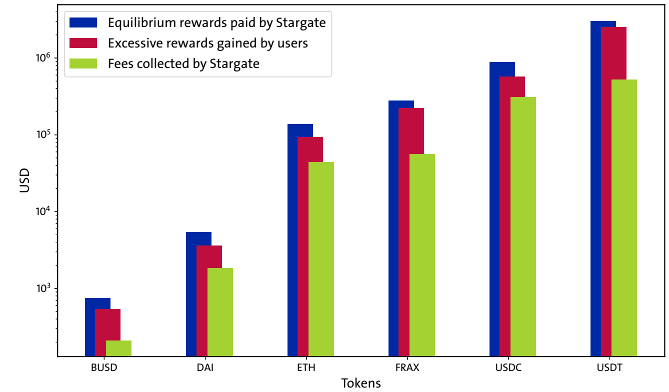

Figure 8: An overview of the transactions with a larger "equilibrium reward" than the sum of respective fees. The "Excessive rewards" are calculated by deducting the sum of all fees from the "equilibrium reward". All values are in USD.

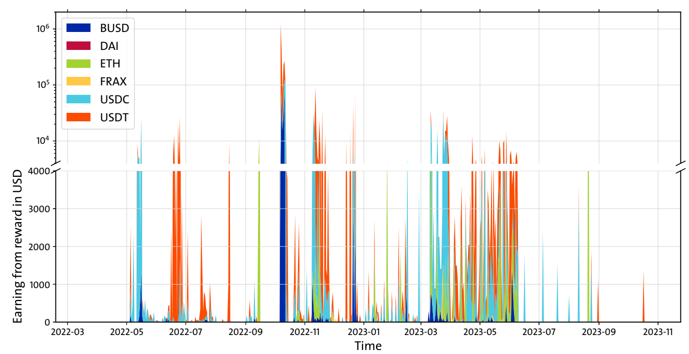

Figure 9: Excessive rewards in USD over time, categorized by assets.

4.3 Token Net Flow Cross Chains

Figure 10 depicts the net flow of multiple tokens across six blockchains via Stargate. Net flow refers to the net transfer of a specific token from one chain to another. For example, when 100 USDC is transferred from Chain A to Chain B and 200 USDC is sent from Chain B to Chain A, the net flow of USDC between Chain A and Chain B is that Chain B transfers 100 USDC to Chain A. Each node in the graph represents a token presented on one blockchain, and each edge indicates the net flow of a token between two chains, with the arrow direction representing the flow direction. Additionally, the width of the edge illustrates the logged amount of net flow, thicker lines suggest larger net flows.

Firstly, we aim to investigate whether there is a significant flow of tokens from Ethereum, which has long been criticized for slow transaction speeds and high fees, to other blockchains through Stargate, and to identify the primary destination blockchain. Following our analysis, it is observed that the majority of assets from Ethereum flow towards the Optimism blockchain compared to the other four blockchains. Regarding tokens, the six types of tokens on Ethereum listed in Figure 10 are found to flow towards other

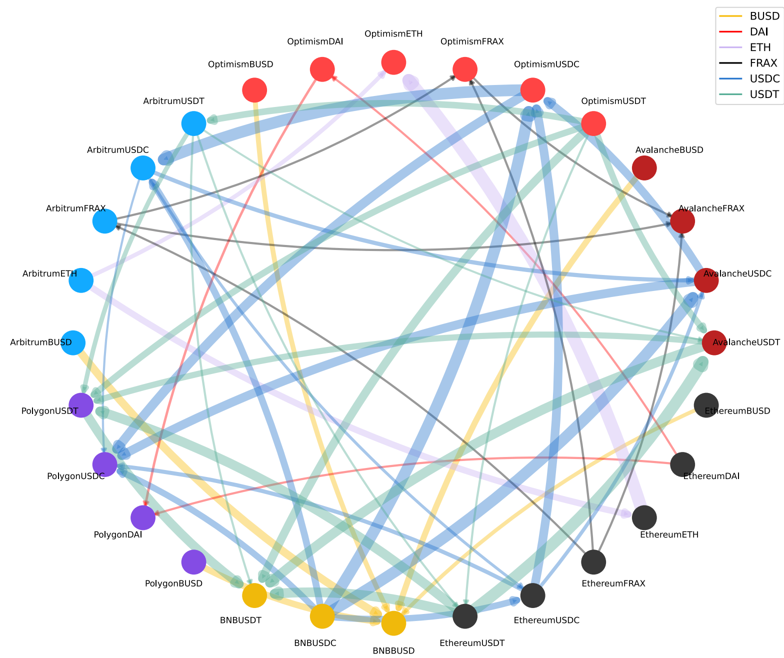

Figure 10: Net token flows across chains through the Stargate bridge.

blockchains, with USDT experiencing the highest outflow, totaling approximately 360 million USD.

Subsequently, we examine the flow of assets between blockchains, with Table 4 that outlines the total historical transaction volumes for each pair of blockchains. The results reveal that the transaction volume between Arbitrum and Optimism is the highest among all blockchain pairs. Moreover, it is noted that there are higher transaction volumes between Layer-2 blockchains rather than between Layer-1 and Layer-2 blockchains. The blockchains analyzed and their corresponding layers are detailed in Table 1. Furthermore, the majority of token inflows are directed towards Layer-2 blockchains, indicating that Layer-2 blockchains, which serve as a potential scalability solution for Layer-1, exhibit more active cross-chain activities, likely attributed to their higher transaction speeds and lower fees.

5 CONCLUSION

In this study, we present a comprehensive analysis of Stargate, a cross-chain bridge utilizing a Lock-and-Unlock mechanism to facilitate multi-chain asset transfers. We first introduce Stargate's unique cross-chain mechanism, then collect data from various EVM-based chains using their blockchain explorers. Utilizing this dataset, we analyze the trends and dynamics of cross-chain transactions over time and across six blockchains. Our analysis reveals distinct transaction patterns and potential vulnerabilities in cross-chain transactions. For instance, the cross-chain transaction number, volumes and associated fees show an overall increasing trend, with USDT comprising the largest proportion of cross-chain transactions. Notably, we also identify two potential exploitations related to cross-chain securities. Furthermore, we investigate the potential for exploitation of Stargate's reward system by examining fee trends and trading volumes over time. Lastly, we visualize the net flow of assets across six blockchains and observe a higher number of cross-chain transactions and transaction volumes between Layer-2 blockchains compared to interactions between Layer-1 and Layer-2 blockchains. Our work enriches the existing body of research by offering a detailed examination of the dynamics of Layer-0 cross-chain

Table 4: Total transaction volumes between chains. All values are in USD.

Blockchain pair	Transaction volume(USD)
Arbitrum/Optimism	$2.51x10^{9}$
Arbitrum/Ethereum	$1.87x10^{9}$
BSC/Ethereum	$1.15x10^{9}$
Avalanche/Ethereum	$1.09x10^{9}$
Arbitrum/Avalanche	$1.08x10^{9}$
Arbitrum/Polygon	$8.45x10^{8}$
Arbitrum/BSC	$7.88x10^{8}$
Avalanche/BSC	$6.84x10^{8}$
Avalanche/Polygon	$5.50x10^{8}$
BSC/Polygon	$4.04x10^{8}$
Ethereum/Polygon	$3.34x10^{8}$
Ethereum/Optimism	$2.98x10^{8}$
Polygon/Optimism	$2.59x10^{8}$
Avalanche/Optimism	$2.02x10^{8}$
BSC/Optimism	$1.29x10^{8}$

bridges and highlighting potential vulnerabilities within Stargate's reward system.

In future research, it is pertinent to broaden the scope beyond Layer-0 cross-chain bridges to conduct a comparative analysis of multi-chain bridges across various blockchain layers, enhancing our understanding of their operational efficiencies and security features. Additionally, given that we have found potential user misbehavior exploiting the reward system of Stargate and malicious actors have utilized Stargate as a means of quickly transferring funds to other blockchains, we suggest investigating abnormal transactions and user misbehavior using statistic methods and machine learning methods to improve the security and reliability of cross-chain bridges.

ACKNOWLEDGMENTS

This research was supported by the China Scholarship Council (No. 202006980012) and the DLT Science Foundation (No. RES01923).

REFERENCES

[1] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew K. Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille. 2014. Enabling Blockchain Innovations with Pegged Sidechains. https://api.semanticscholar.org/CorpusID:61340590

[2] Rafael Belchior, Peter Somogyvari, Jonas Pfannschmidt, André Vasconcelos, and Miguel Correia. 2023. Hephaestus: Modeling, Analysis, and Performance Evaluation of Cross-Chain Transactions. *IEEE Transactions on Reliability* (2023). https://api.semanticscholar.org/CorpusID:266421379

[3] Vitalik Buterin. 2015. A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM. https://api.semanticscholar.org/CorpusID:19568665

[4] Chainlink. 2024. What is a Cross Chain Bridge?: Chainlink. https://chain.link/education-hub/cross-chain-bridge. (Accessed on 02/10/2024).

[5] Joao Otavio Chervinski, Diego Kreutz, Xiwei Xu, and Jiangshan Yu. 2023. Analyzing the performance of the inter-blockchain communication protocol. In *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 151–164.

[6] CoinShares. 2023. Cosmos Guide. https://etp.coinshares.com/knowledge/crypto-guides/cosmos-guide. (Accessed on 02/10/2024).

[7] Bingrong Dai, Shengming Jiang, Menglu Zhu, Ming Lu, Dunwei Li, and Chao Li. 2020. Research and Implementation of Cross-Chain Transaction Model Based on Improved Hash-Locking. In *Blockchain and Trustworthy Systems*, Zibin Zheng, Hong-Ning Dai, Xiaodong Fu, and Benhui Chen (Eds.). Springer Singapore, Singapore, 218–230.

[8] Li Duan, Yangyang Sun, Wei Ni, Weiping Ding, Jiqiang Liu, and Wei Wang. 2023. Attacks Against Cross-Chain Systems and Defense Approaches: A Contemporary Survey. *IEEE/CAA Journal of Automatica Sinica* 10 (2023), 1647–1667. https://api.semanticscholar.org/CorpusID:260171455

[9] Ankit Gangwal, Haripriya Ravali Gangavalli, and Apoorva Thirupathi. 2022. A Survey of Layer-Two Blockchain Protocols. *J. Netw. Comput. Appl.* 209 (2022), 103539. https://api.semanticscholar.org/CorpusID:248227300

[10] Christopher G. Harris. 2023. Cross-Chain Technologies: Challenges and Opportunties for Blockchain Interoperability. *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS)* (2023), 1–6. https://api.semanticscholar.org/CorpusID:260254307

[11] Maurice Herlihy. 2018. Atomic Cross-Chain Swaps. *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing* (2018). https://api.semanticscholar.org/CorpusID:4853066

[12] Harry A. Kalodner, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten. 2018. Arbitrum: Scalable, private smart contracts. In *USENIX Security Symposium*. https://api.semanticscholar.org/CorpusID:52046120

[13] Jaynti Kanani, Sandeep Nailwal, and Anurag Arjun. 2021. Matic whitepaper. *Polygon, Bengaluru, India, Tech. Rep., Sep* (2021).

[14] Inwon Kang, Aparna Gupta, and Oshani Wasana Seneviratne. 2022. Blockchain Interoperability Landscape. *2022 IEEE International Conference on Big Data (Big Data)* (2022), 3191–3200. https://api.semanticscholar.org/CorpusID:254854003

[15] Oliver Knight. 2023. Airdrop Hunters Push Volume on Cross-Chain Bridge Stargate (STG) With Sights on LayerZero (ZRO) Token. https://www.coindesk.com/business/2023/04/27/cross-chain-bridge-stargates-volume-soars-as-airdrop-hunters-set-sights-on-layerzero-token/. (Accessed on 03/7/2024).

[16] Jae Kwon and Ethan Buchman. 2019. Cosmos whitepaper. *A Netw. Distrib. Ledgers* 27 (2019), 1–32.

[17] Rongjian Lan, Ganesha Upadhyaya, Stephen Tse, and Mahdi Zamani. 2021. Horizon: A Gas-Efficient, Trustless Bridge for Cross-Chain Transactions. *ArXiv* abs/2101.06000 (2021). https://api.semanticscholar.org/CorpusID:231627891

[18] LCX. 2023. Cross-chain Bridges explained. https://www.lcx.com/cross-chain-bridges-explained/. (Accessed on 02/10/2024).

[19] Sung-Shine Lee, Alexandr Murashkin, Martin Derka, and Jan Gorzny. 2022. SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks. *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2022), 1–14. https://api.semanticscholar.org/CorpusID:253223945

[20] Nansen. 2022. BNB Chain's Cross-Chain Bridge Exploit Explained | Nansen. https://www.nansen.ai/research/bnb-chains-cross-chain-bridge-exploit-explained. (Accessed on 03/8/2024).

[21] Babu Pillai, Kamanashis Biswas, Zhé Hóu, and Vallipuram Muthukkumarasamy. 2022. Cross-blockchain technology: integration framework and security assumptions. *IEEE Access* PP (2022), 1–1. https://api.semanticscholar.org/CorpusID:248162871

[22] Cosimo Sguanci, Roberto Spatafora, and Andrea Vergani. 2021. Layer 2 Blockchain Scaling: a Survey. *ArXiv* abs/2107.10881 (2021). https://api.semanticscholar.org/CorpusID:236318111

[23] Narges Shadab, Farzin Houshmand, and Mohsen Lesani. 2020. Cross-chain Transactions. *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2020), 1–9. https://api.semanticscholar.org/CorpusID:219872484

[24] Gang Wang. 2021. SoK: Exploring Blockchains Interoperability. *IACR Cryptol. ePrint Arch.* 2021 (2021), 537. https://api.semanticscholar.org/CorpusID:233733288

[25] Gavin Wood. 2016. Polkadot: Vision for a heterogeneous multi-chain framework. *White paper* 21, 2327 (2016), 4662.

[26] Tiancheng Xie, Jiaheng Zhang, Zerui Cheng, Fan Zhang, Yupeng Zhang, Yongzheng Jia, Dan Boneh, and Dawn Song. 2022. ZkBridge: Trustless Cross-Chain Bridges Made Practical. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (Los Angeles, CA, USA) *(CCS '22)*. Association for Computing Machinery, New York, NY, USA, 3003–3017. https://doi.org/10.1145/3548606.3560652

[27] Min Xu, Xingtong Chen, and Gang Kou. 2019. A systematic review of blockchain. *Financial Innovation* 5, 1 (2019), 1–14.

[28] Jyoti Yadav and Ranjana Shevkar. 2021. Performance-Based Analysis of Blockchain Scalability Metric. *Tehniki glasnik* (2021). https://api.semanticscholar.org/CorpusID:233803132

[29] Ryan Zarick, Bryan Pellegrino, and Caleb Banister. 2021. : Solving the Bridging Trilemma. (2021). https://stargateprotocol.gitbook.io/stargate/

[30] Ryan Zarick, Bryan Pellegrino, and Caleb Banister. 2022. LayerZero Whitepaper. https://layerzero.network/publications/LayerZero_Whitepaper_V1.1.0.pdf. (Accessed on 02/10/2024).

[31] Jiashuo Zhang, Jianbo Gao, Yue Li, Ziming Chen, Zhi Guan, and Zhong Chen. 2023. Xscope: Hunting for Cross-Chain Bridge Attacks. In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering* (Rochester, MI, USA) *(ASE '22)*. Association for Computing Machinery, New York, NY, USA, Article 171, 4 pages. https://doi.org/10.1145/3551349.3559520

A LIST OF TRANSACTIONS OF BSC EXPLOITER ON OCTOBER 7TH, 2022

Table 5: List of transactions of BNB exploiter address 0x489a8756c18c0b8b24ec2a2b9ff3d4d447f79bec

Transaction Hash	Source Chain	Target Chain	Asset	Amount
0x36493f33ad36714b744ef75090d6bf7e1b9d97fb9545325c64110a07ab633cc1	BSC	Avalanche	USDT	4,993,396
0xeea253e5fb3380120f6d16a520b861fc40632cb9a31c9fb30d562e1a92e2de42	BSC	Avalanche	USDT	4,992,835
0x79067c22ab23cc142a59f82641a6d634474780fc54c985286317b2626499eec5	BSC	Ethereum	USDT	4,991,563
0x01f6a192600c9ed5587a333832cfa63a414f8fc1d127b16101d7b28313355d60	BSC	Avalanche	USDC	4,340,470
0xf84deb6346f1460f48a69cb5df339c63dbc0497e9c235e895d5fa1f436d31f88	BSC	Avalanche	USDT	3,507,105
0x1e2e4228cd556381baa3050bf164446db34bc86afe8f0126263242e9ffaa7997	BSC	Avalanche	USDT	3,229,161
0xda65a00eb43428a8880e3d9dd8d19cd25fe9428b652234fc7a4c84ac7034f375	BSC	Ethereum	USDT	3,121,602
0x0a5e8c673904897c47b4e6c7b53b9c280803722a665945b40c331b05cb885694	BSC	Ethereum	USDT	2,482,147
0xce73b80a561a08f468d688089f373475ccab3fd38ef2dfb75e411269981d8bb2	Avalanche	Ethereum	USDT	2,429,111
0x89f9f280be67c093b61a3f4a69ec662bccbcd98274c16b7d4e66ed98290c42ab	BSC	Ethereum	USDC	2,352,505
0x13528238586a817251f78fc8ba8c98d70c077b60158df90d0ec41de844eaf856	BSC	Ethereum	USDT	2,279,694
0x9089fc9bb91632f8c850a99c278d1cb8fc618b43b5e4c36b42d311905d0fe2b0	BSC	Arbitrum	USDT	2,127,466
0x4c42acc95ce7bf95efda38ae1512f0346065913c186eee250afa2db1a15ace1b	BSC	Polygon	USDT	1,875,590
0x06a695ce06aee345091e42e61e1ae9d51deb1aa3fedf3ced48133a97a4f4cac1	BSC	Polygon	USDT	1,756,386
0xb8b0214b0c12e767befcd3c504ca093cf50c69a89306a6571a8850f995339087	BSC	Ethereum	USDT	1,702,409
0x967dd1d3ec76c32afe202f7a3753ae3484219c73571c4f335ece7ecb3a9e8ae3	BSC	Ethereum	USDT	1,668,002
0xdba51303d16ff14514ba2a3a912fca03adaf8adada1a3124976311b9ecc1e774	BSC	Ethereum	USDC	1,645,588
0xa06c7409911558e0af20a82756d6c2ccae79c1bda7eb9e6c50c7971146baf2c8	BSC	Ethereum	USDT	1,312,946
0xa4c82300379970ceeac9b3a7c7e4d01b385218f41323e22ecf884fb4ed312bc0	BSC	Ethereum	USDT	1,147,773
0x890c71d4cb1f9fc3d41ad1191c0489068f8ab93132f75838db60669432227d10	BSC	Optimism	USDC	1,102,163
0x5f0afa467d2a8704678a0af2641fc02d57d1326d6c74f95d5e0826a29d58dc81	BSC	Arbitrum	USDC	1,061,240
0xa7c4c5b3a907708dcb56dc84e5318c1e627503ce550a56e736bf408c38ab7315	BSC	Avalanche	USDC	999,400
0x2301b41b897b121146e7b7a16f285a9864ed478e7771631de5b1af8562264174	BSC	Avalanche	USDT	976,338
0xa5a1e7b2c83af8ad89fe03a47bb797b4fa2a40405b57dcb657d0f9edda140f00	BSC	Arbitrum	USDC	839,238
0xaf05972263c01ea78eddb86ac0661b0edf51f500bd60f7c2d14168fdea1c7781	BSC	Polygon	USDC	399,895