TU WIEN Informatics

Tracing Cryptoassets Across Chains: An Empirical Analysis of the Terra Network

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Data Science

eingereicht von

Dipl. -Ing. Nikolas Haimerl, BSc (WU) BSc
Matrikelnummer 01452766

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Univ.Prof. Matteo Maffei
Mitwirkung: Dr. Bernhard Haslhofer

Wien, 30. August 2022

Nikolas Haimerl

Matteo Maffei

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

TU WIEN Informatics

Tracing Cryptoassets Across Chains: An Empirical Analysis of the Terra Network

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Data Science

by

Dipl. -Ing. Nikolas Haimerl, BSc (WU) BSc
Registration Number 01452766

to the Faculty of Informatics

at the TU Wien

Advisor: Univ.Prof. Matteo Maffei
Assistance: Dr. Bernhard Haslhofer

Vienna, 30th August, 2022

Nikolas Haimerl

Matteo Maffei

Technische Universität Wien
A-1040 Wien • Karlsplatz 13 • Tel. +43-1-58801-0 • www.tuwien.at

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Erklärung zur Verfassung der Arbeit

Dipl. -Ing. Nikolas Haimerl, BSc (WU) BSc

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 30. August 2022

Nikolas Haimerl

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Danksagung

Ich möchte diese Gelegenheit nutzen, um meinem Co-Betreuer Bernhard Haslhofer und seinem Team von der CryptoFinance-Forschungsgruppe am Complexity Science Hub für ihre konsequente Unterstützung, sowie ihre prompten und detaillierten Beiträge und für die Möglichkeit zur Zusammenarbeit mit ihrer Forschungsgruppe zu danken. Während der Recherche über die verfügbare Literatur und der Durchführung von Analysen führten wir mehrere Gespräche über die Blockchain-Technologie, die Rückverfolgbarkeit von Kryptowährungen, dezentralisierte Finanzen und Designentscheidungen. Diese Gespräche haben mir sehr geholfen, die Gesamtqualität meiner Diplomarbeit auf eine neue Ebene zu heben. Darüber hinaus möchte ich mich bei Matteo Maffei für seinen Einsatz als Betreuer bedanken.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Acknowledgements

I would like to take this opportunity to thank my co-supervisor Bernhard Haslhofer and his Team from the CryptoFinance research group at the Complexity Science Hub for their consistent assistance, as well as their prompt and detailed input, and for the opportunity to collaborate with their research group. Throughout the process of searching through the available literature and conducting analysis, we had several conversations about blockchain technology, the traceability of cryptocurrencies, decentralized finance, and design decisions. These conversations were of tremendous assistance to me in elevating the overall quality of my thesis to an entirely new level. In addition, I would want to express my gratitude to Matteo Maffei for all of his hard work as my supervisor.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Kurzfassung

Dem Internet der Blockchains werden stetig neue Blockchains hinzugefügt, was die Relevanz von Blockchain Interoperabilität erhöht. Coins und Tokens sind nicht mehr an eine bestimmte Blockchain gebunden, sondern fließen über verschiedene Blockchains, indem dezentrale Börsen genutzt werden. Die Interoperabilität von Blockchains stellt jedoch auch ein Systemrisiko dar, da Ausfälle oder Probleme in einer Blockchain auch Auswirkungen auf andere Blockchains haben können.

In Bezug auf dezentralisierte Finanzen und Anwendungen, mit dem Ziel der Interoperabilität zwischen Blockchains, ist das Terra-Netzwerk eine Blockchain, die sowohl von institutionellen als auch von einzelnen Investoren große Aufmerksamkeit erhalten hat. Die Fähigkeit des Terra-Netzwerks, über eine Reihe von Protokollen und Blockchain-übergreifende dezentrale Börsen mit anderen Blockchains zu kommunizieren, war ein wichtiges Argument für Terra.

Diese Arbeit untersucht das Terra-Netzwerk, sowohl vor als auch während des Zusammenbruchs, und betrachtet seine On-Chain-Aktivität zwischen Smart Contracts und Benutzerkonten, sowie dessen Cross-Chain-Transaktionen. Die erste Forschungsfrage fokussiert sich darauf, welche Assets bei Cross-Chain-Asset-Transfers zwischen Terra und anderen Blockchains, durch die dezentrale Börse Thorchain, verwendet wurden. Das wichtigste Asset war BUSD auf der Binance-Blockchain, gefolgt von BTC und ETH. Die zweite Forschungsfrage betraf den Assetfluss zwischen Konten und Smart Contracts innerhalb von Terra vor und während des Zusammenbruchs. Die Analyse zeigt, dass Nexus und Anchor Protocol die dominierenden Smart Contracts mit einem starken Abfluss während des Zusammenbruchs waren. Die Analyse der letzten Forschungsfrage, dass Zentralisierungsprobleme insbesondere bei Cloud-Computing-Diensten, Validator Standorten und IBC-Relayern existieren.

Die Implikationen der Arbeit sind, dass Asset-Flows durch die analysierten Cross-Chain-Technologien sichtbar und nachvollziehbar sind, wie man es auch von On-Chain-Daten erwarten würde. Zentralisierung ist ein Thema auf verschiedenen Analyseebenen bei den meisten analysierten Blockchains und Technologien. Validatoren sind stark zentralisiert durch Standort- und Cloud-Computing-Diensten, die verwendet werden.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Abstract

Cross-chain interoperability is becoming more critical as additional blockchains are added to the Internet of Blockchains. Assets are no longer bound to a specific blockchain but flow across different blockchains, often by making use of decentralized exchange services. However, the interoperability of blockchains also poses a system risk, as failures or issues in one blockchain can have ripple effects on other blockchains as well.

In decentralized finance and cross-chain interoperability, the Terra Network is a blockchain that has received significant attention from both institutional and individual investors. The Terra Network's ability to communicate with other blockchains via a number of protocols and cross-chain bridges was a key selling point.

This thesis investigates the Terra network in depth, both before and during its collapse, looking at its on-chain activity between smart contracts and user accounts and its cross-chain transactions using some of the most popular cross-chain technologies. The first research question was about which assets were used in cross-chain asset transfers between Terra and other blockchains connected through the decentralized exchange Thorchain. The main asset was BUSD on the Binance blockchain, followed by BTC and ETH. The second research question was about the flow of assets between accounts and smart contracts within Terra before and during the collapse. The analysis shows that Nexus and Anchor Protocol were the dominant smart contracts with a severe outflow during the collapse. The last research question was about analysing how decentralized Terra, Thorchain and the inter-blockchain communication between Terra and the Cosmos Ecosystem are. It was shown that several centralization issues are present, especially amongst computation services, validator locations and IBC relayers.

The implications of the thesis are, that asset flow through the analysed cross-chain technologies is visible and can be tracked, as one would expect from on-chain data as well. Centralization is an issue on various levels of analysis with most analysed blockchains and technologies. Validators are heavily centralized by location and computation services used.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Contents

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 1

Introduction

Ever since Bitcoin introduced blockchain technology and the use of digital assets to conduct transactions, the blockchain industry has seen a massive inflow of human and monetary capital. With the goal of revolutionizing our conventional monetary system from an economic as well as technological point of few, different sectors in the modern economy have been looking into the adoption of this technology in their respective markets. One of the first widely adopted sectors is the financial sector and its blockchain-based adoption which is now known as decentralized finance (Defi). From exchanges to insurances, banking, lending and borrowing, custody and other markets from the traditional world of finance have started to show adoption of blockchain technologies [8].

The development of blockchain technology has been pushed forward by many research and development groups that often differ in which aspect of the use of the distributed system is more relevant, be it privacy, security, speed, or scalability [12]. Therefore, various projects have endorsed their own blockchain in recent years. With many blockchains to choose from, it is often hard for individuals or institutions that want to move over to a decentralized alternative to know which blockchain is best suited for their needs and where adoption will continue to flourish in their field of interest. This sparked the need for blockchain interoperability, meaning the seamless transition of funds from one blockchain to another and the existence of projects that utilize multiple different blockchains instead of being tied to only one [11].

The further adoption of blockchain technology on an institutional as well as the governmental level requires blockchain technologies to fall in line with modern regulations and conduct of business [8]. It is therefore crucial for the use of many of the applications in decentralization to have some way of tracing the activities of individuals and entities across multiple blockchains [17]. Governments rely on

traceability to identify tax payments and taxable activities. Also, companies need transparent transactions for auditory and money laundering compliance to do due diligence or prospective merger and acquisitions. For decentralized finance to move to further adoption in the financial industry, traceability and thus verifiability of the origins of funds is a necessity [6].

Decentralized exchanges are a key instrument in decentralized finance, and cross-chain interoperability is only becoming more important with more blockchains entering the internet of blockchains. Especially the link between these blockchains, represented by cross-chain decentralized exchanges, is a very new and unregulated part of decentralized finance and may raise concerns among regulators as existing regulations have yet to address the issues that come with operating such services. It is expected that further knowledge of how blockchain technology may be used to circumvent entities from having insight into another's activity on existing blockchains lets regulators rule out these possible threats through regulatory instruments and therefore set regulations which serve as guidance for institutions and individuals, so they are assured that they are operating within the boundaries of the lawmaker. As a result, decentralized finance adoption among institutional investors is expected to advance as the cryptocurrency space becomes more regulated and threats from regulators or environmental, social and governmental (ESG[1])compliance can be mitigated.

One blockchain that has sparked particularly great interest amongst institutions, as well as retail users, is the Terra Network. One particularly interesting aspect of the Terra Network was its connectivity to other blockchains through various protocols and cross-chain bridges. It was also well known for its decentralized finance industry and has attracted billions of dollars in investments and speculative money. Its collapse in May 2022 was detrimental to decentralized finance and the cryptocurrency space. Due to the nature of blockchains, transactions before and during the collapse should be visible to any blockchain participant.

Therefore, this thesis analyses the Terra Network on its on-chain activities between smart contracts and regular accounts as well as cross-chain transactions with some of the most frequently used cross-chain technologies before and after the collapse of the network.

1.1 Aim of this Work

The aim of this work is to analyse how far the interoperability of blockchains in the domain of decentralized exchanges has progressed and what technologies were used to provide their cross-chain functionality with the Terra Network. This is necessary,

[1] https://www.investopedia.com/terms/e/environmental-social-and-governance-esg-criteria.asp

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

as understanding how cross-chain transactions are performed is a prerequisite to analysing their chain of transactions and smart contract calls on different blockchains as assets move in and out of the Terra Network. The goal of the thesis is to be able to identify, for specific types of cross-chain technologies linked to the Terra Network, how the cross-chain transactions are performed, what assets are used in conjunction with the Terra network, how the collapse of the Terra network unfolded from an on-chain and cross-chain perspective and whether there are any aspects of centralization with the cross-chain technologies.

This particular case is of great interest to the public, as investigations on the collapse of the network are still ongoing as of writing this thesis. Showing how and what assets were used in cross-chain communication with the Terra Network exemplifies the necessity of building an understanding of cross-chain technologies and the ability to trace and visualizing events such as the collapse of Terra.

There are different types of technologies offering cross-chain interoperability. It is therefore not part of this thesis to explore all of them, but select a few highly relevant implementations that show high transaction throughput. Furthermore, only decentralized technologies which feature cross-chain transactions will be discussed, as technologies that only offer swaps between assets in their respective blockchain ecosystem are not relevant for cross-chain traceability.

The main novelty of the Master Thesis lies in the investigation of the flow of digital assets from existing blockchains into the Terra Network and vice versa, as well as analysing the behaviour of entities once they have entered the Terra Network.

The proposed solutions should give stakeholders insight inflow of assets into the Terra Network and an answer to why entities seek to move their assets in and out of the Terra Network, as well as give an on-chain perspective of events before and after the collapse of the network. The clarity and understanding provided in the solution about the current situation aim at contributing to higher institutional adoption of and regulator integration to the blockchain industry.

1.2 Research Questions

The following paragraphs summarize the different aspects of the thesis. They are motivated by the related research questions.

- *RQ1: What assets were used in cross-chain asset transfers between Terra and legacy chains before and during the collapse of the network?*

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

RQ2: What is the flow of assets between accounts and smart contracts on Terra before and during the collapse of the network ?

- *RQ:3 How decentralized are cross-chain technologies that are connected to Terra ?*

1.3 Overview

The first section 2 provides the background knowledge that is necessary to understand blockchains, decentralized finance and decentralized exchanges, in particular, the Cosmos Ecosystem and the collapse of the Terra Network. Ethereum is a good example of a blockchain that supports the use of smart contracts and is therefore discussed in more detail. A lot of the other blockchains that are relevant in this thesis have a similar mechanism as Ethereum, including the Terra Network.

In the second section 3 of this thesis an overview of the state-of-the-art in research on blockchain analysis, traceability on centralised and decentralized exchanges, as well as traceability of privacy-preserving cryptocurrencies.

Section 4 will give an insight into how cross-chain transactions work, which entities are involved, how information about the on-chain and cross-chain activities are generated, as well as what are the limits to the technologies and methods used to extract information. This section is especially relevant for *RQ1* and *RQ2* as an understanding of the technologies used is essential for analysing the extracted information. However, also the understanding of how Thorchain and IBC work is necessary to understand aspects of centralization, which is the topic of *RQ3*.

In Section 5 the information extraction is described and how data about on-chain and cross-chain activities can be generated. Also, the data gathered on the mechanism of decentralization of the technologies used are described in this section. Therefore, it is relevant to all three research questions.

In Section 6 the information gathered is presented graphically, so that insight from the data can be visualized and interpreted. It gives an answer to each research question illustrated by the corresponding data visualization.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 2

Background

This section gives background information about blockchain-based systems with a focus on smart contracts, decentralized finance, decentralized exchanges, cross-chain interoperability and Ethereum as a representative for Ethereum Virtual Machine (EVM) compatible blockchains. The core approaches and underlying consensus primitives utilized in smart contracts and blockchain technology are described in Section 2.1. The overall use case of blockchain technology in decentralized exchanges is discussed in Section 2.3. At last, since most blockchains that offer smart contract compatibility utilize the EVM, Ethereum is discussed and the transaction mechanism is described as well in Section 2.2. The latter will be important when analyzing cross-chain transactions later on.

2.1 Blockchain

A blockchain is a revolutionary kind of digital technology that combines encryption, data management, networking, and incentive mechanisms to enable parties to verify, carry out, and record transactions. Blockchains are also known as distributed ledgers. A list or chain of transaction groups, which are collectively referred to as blocks, constitutes a blockchain ledger. The parties who are proposing a transaction have the ability to include it in a group of transactions, called a block, that will be recorded on the ledger at a later time. The processing nodes in the blockchain system take some of these transactions, verify their authenticity, and then record them in new blocks on the distributed ledger. The contents of the blockchain ledger are replicated among a number of processing nodes that are spread out in different locations. The consensus process determines which transactions are included in the next block and in what order they are included. [2].

The first use of blockchain technology was for the Bitcoin digital currency. However, the technology is currently being deployed on many other platforms and utilized for a range of additional reasons far beyond the initial goal of a digital currency. In the same way that a conventional database may be used to record transactions or information in a centralized location, a blockchain can store these transactions decentralized, using an account or UTXO model. Blockchains provide a number of important advantages over conventional databases. These discrepancies have an effect on the architecture of systems that are enabled by blockchain technology [28].

Emerging blockchain systems like Ethereum make it possible to store and run computer programs as part of the transactions that are recorded on the distributed ledger. Even though the programs are often not particularly smart and are usually unconnected to legal contracts, they are commonly referred to as smart contracts.

The writing of computer programs in a Turing complete language is made possible by blockchains such as Ethereum, which permits the usage of smart contracts. This kind of language is theoretically capable of the same level of expressiveness as any other general-purpose programming language. As a consequence of this, blockchains have the potential to be more than simply a straightforward distributed database. They also have the potential to be universal computing platforms, but with significant constraints on the computational complexity, they can support at the time. This capability provides a significant increase to the power of blockchain systems as well as to the variety of applications they support and the innovation opportunities they provide. [2].

In reaction to certain triggers, decentralized blockchains execute computer programs known as smart contracts. To account for the immutability of the blockchain, smart contracts are developed using a methodology that is distinct from that of traditional computer software. Once a smart contract has been published on a blockchain, it cannot be modified or updated to add security updates. As a result, developers need to include robust security measures prior to deployment in order to reduce the likelihood that it will be exploited in the future. In addition to this, given that a smart contract is stored on a blockchain, the bytecode of the underlying code for the contract is viewable by anybody who uses the blockchain. [21].

2.2 Ethereum

From the beginning, Ethereum allows developers to construct and deploy their own smart contracts on the Ethereum network. It had a significant impact on other blockchains, which enabled smart contracts on their primary networks as a result of its development. Because of this, Ethereum's programming language, *Solidity*, is now the most popular language for designing and coding smart contracts. This is because *Solidity* was developed by Ethereum itself. As a result, a more in-depth description

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

of the primary components that make up the Ethereum blockchain is provided in the following paragraphs. They are made of different states and transitions between states, accounts, messages, and transactions [26].

Accounts

The state of the system in Ethereum is composed of objects that are referred to as accounts. Each account has a 20-byte address, and state transitions are direct transfers of currency and information between accounts. Within an Ethereum account, the following four fields may be found [4]:

- **Nonce:** The nonce is a counter that ensures that each transaction is only performed once.
- **Balance:** The current ether balance in the account.
- **Code:** If applicable, that is if the account in question is a smart contract, the contract code for the account.
- **Storage:** The account's storage, which is usually updated as functions in the smart contract of that account are called.

Ethereum's internal virtual currency is called *Ether*, and it is used to pay the transaction costs associated with using Ethereum. There are two types of accounts that may exist: contract code accounts, which are controlled by the contract code, and externally owned accounts, which are maintained by private keys. Both types of accounts are feasible. However, when a contract account receives a message, its code is activated, allowing it to read and write to internal storage and, in turn, send other messages or build contracts. An externally owned account does not have any code, and as a result, the only way it can send messages is by generating and signing a transaction. A contract account, on the other hand, can only send messages by generating and signing a transaction.

Transactions

The phrase *transaction* is used in Ethereum to describe a data block that has been signed and includes a message that is going to be sent from an account. The following elements may be discovered in various transactions: [4]:

- A receipt of the message to be transmitted.
- A signature that confirms the sender's identity.
- The quantity of ether that should be sent from the sender to the receiver.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- A data field that can be left blank.
- A startgas value that represents the transaction execution's maximum number of computing steps.
- A gasprice value indicating the charge paid by the sender for each computing step.

The startgas and gasprice variables need to have data entered into them in order for Ethereum's anti-denial of service paradigm to function properly. Each transaction is required to declare a restriction on the maximum number of computing steps of code execution that it may make use of. This is done as a protection against unintended or malicious endless loops as well as other forms of computational waste in the code. Gas is the fundamental unit of computing; typically, a computational step costs one gas. However, certain actions cost more gas than others if they are either more computationally demanding than other actions or increase the quantity of data that must be stored as part of the state. Gas is the fundamental unit of computing. In addition to that, there is an extra cost of 5 gas for every single byte of data that is included in the transaction data. A user is obligated to pay a proportional amount for each resource that they use, which includes computing, bandwidth, and storage space. As a consequence, each transaction that results in the network using a higher quantity of any of these resources must be subject to a gas tax that is approximately equal to the increase in resource consumption. This price must be paid by the user before the transaction can be completed [4].

Messages

One of the fundamental aspects of contracts is that they may transfer messages to other contracts. A message is a kind of virtual object that is incapable of being serialized and only lives inside the context of the Ethereum execution environment. A message may be described as [4]:

- That entity who sent the message.
- The sender of the message's intended receiver.
- The quantity of ether to be sent in conjunction with the message.
- A data field that is optional.
- A startgas value.

A message, in its most fundamental form, may be compared to a transaction; however, unlike a transaction, a message is generated by a contract rather than by an external

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

actor. When a piece of contract code that is now being run performs an operation using the CALL opcode, messages are generated. The CALL operation code is responsible for both the creation and the execution of the message. The receiver account will execute the code associated with a message just as it would with a transaction when the message is received [4].

State and State Transitions

The global state is an identification of a mapping that exists between addresses (160-bit IDs) and account states (state). This mapping will not be retained on the blockchain, however, it is envisaged that the implementation will preserve it in a modified Merkle Patricia tree[1]. The usage of a plain database backend that maintains a mapping of byte arrays to byte arrays is required by the tree. This kind of database is referred to as the state database. Consequently, there are a variety of benefits to be gained. The root node of this structure is cryptographically dependent on all internal data, and therefore, its hash may be utilized as a safe identity for the full system state. Second, since it is an immutable data structure, it enables any past state (whose root hash is known) to be remembered by simply updating the root hash in the proper manner to restore the previous state. All such root hashes are preserved on the blockchain, so earlier states may be simply recovered [26].

A state transition is considered valid if it takes place as a direct consequence of the successful completion of a transaction. Validating the transition from one state to another is the responsibility of the function known as the state transition. It guarantees the following [26]:

- Validate the transaction's structure by making sure that a signature is authentic and that a nonce, which is a unique number used once in a transaction, matches the nonce that is stored in the sender's account. A nonce is a number that is used once in a transaction. Any issue that arises must produce an error.
- Multiplying the price of the gas that was consumed together with the price of the gas overall results in the transaction charge being calculated. The sender's signature serves as the basis for deriving the sender's address. After this step, the nonce will be incremented, and the sender's account balance will be checked for accuracy. In the event that there are not sufficient coins in the account, an error will be shown.
- When money is moved from one account to another, the transaction goes from the account of the sender to the account of the recipient. In the event that the receiving account does not already exist, a new one is created. Additionally, the

[1] https://eth.wiki/fundamentals/patricia-tree

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

code of the contract to which contract accounts are associated will be executed by those contract accounts. The whole of the contract's code is run, up to the point when there is no more gas available.

- In the case of a transaction failure due to insufficient balance or gas contained in the transaction, all state changes, saved for the payment of fees, are reversed, and the transaction fees are transferred to the miners.

- After the appropriate payments have been made to the miners, the remainder of the ether is changed back to the original sender. At this point in the process, the state of the function may be determined.

When compared to the Bitcoin blockchain, Ethereum's blockchain has more processing capability. The most significant distinction between these two cryptocurrencies is that Ethereum blocks keep not just a copy of the transaction list, but also the most current state. Bitcoin blocks include a copy of the transaction list, the block number and the difficulty [4].

2.3 Decentralized Exchanges

General applications in the field of decentralized finance imitate preexisting financial services or businesses that are transaction-based such as insurance, exchanges and lending services. They provide a decentralized alternative to these well-established businesses. In most cases, the goal is to turn a service that is very centralized into one that is decentralized. As a direct consequence of this, a large variety of applications for decentralized finance exist. For the purposes of this thesis, a selection of two applications that are highly significant are made.

An exchange that provides the ability to trade one good or service for another is a vital component of any financial system that provides a variety of financial services in addition to the currencies or commodities that are used in the transactional process of compensation. For decentralized exchanges, the ledgers documenting the parties' offers and bids are also decentralized. This is accomplished in a variety of ways, each of which is described by the protocols governing the exchange in question. A key advantage of this technology is that it encourages fewer trusting relationships than is typical in many other applications of blockchain technology. In addition, one of the perks of using such exchanges is the opportunity to possibly pay cheaper transaction costs and to have access to less liquid cryptocurrencies. Decentralized exchanges are rarely bound by the regulations of a single government. As a result, decentralized exchanges can offer higher levels of privacy than centralized exchanges, which further attracts users who do not see their needs met in the traditional financial market [13].

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

In general, decentralized exchanges have experienced considerable growth [3]. This rise, particularly in 2020, may be linked to the surge in decentralized finance (DeFi), which accounted for 1,178 % more transaction volume when compared to the number of transactions in the previous year [14].

In the year 2020, a significant number of brand-new apps for decentralized finance that are built on smart contracts emerged or acquired significant popularity. Decentralized exchanges found that they needed to offer a more diverse portfolio of tokens and also handle a larger number of transactions as a result of the introduction of different use cases of DeFi. This meant that the number of different tokens that run these services dramatically increased.

Architecture and Protocols

A distributed exchange protocol (DEX protocol) is a software program that, in general, facilitates peer-to-peer transactions which are automatically settled on a distributed ledger. This software program may be hosted on or incorporated into one or more distributed ledgers (for example, Ethereum). A decentralized exchange (DEX) application is built on top of a decentralized exchange protocol and includes an on-chain or off-chain order book database in addition to a graphic user interface (GUI) and/or application programming interfaces (APIs) to make the information simple to access. It is possible that various decentralized exchanges will use different implementation methodologies for the same functionality of the exchange. This also implies that the degree to which each exchange is decentralized may differ between them.

In the case of decentralized exchanges, the exchanges often take the form of websites, with the backends of those websites being linked to one or more distributed ledgers, depending on the currencies and tokens that are being traded on the exchange. Users have the ability to engage in trades and exchange assets with one another on a peer-to-peer basis via the front end of the platform, and these transactions are automatically resolved on the distributed ledger. The way in which transactions are settled might differ from one exchange to another, but it is common practice to make use of on-chain or off-chain order books, which are databases that keep the counterparties' offers and compare them to one another. The assets that are traded on exchanges have become even more decentralized thanks to the implementation of technologies such as UniSwap and Thorchain, which enable the usage of so-called liquidity pools. When opposed to those that employ order books, decentralized exchanges that use these decentralized liquidity pools are able to provide a greater degree of decentralization to their users [13].

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Platform & Technical Compatibility

The majority of DEXs provide users with the opportunity to trade tokens that are stored on the same distributed ledger platform. This is done with the rationale that transactions that take place on the same blockchain are less likely to have difficulties with latency, stability, or technology. The most significant participant in this market is Ethereum, which has a stake of almost 90 percent[1]. Some decentralized exchanges have begun to implement atomic swaps, which allow users to trade cryptocurrencies that are stored on various blockchain networks in an atomic fashion. However, in order to participate in atomic exchanges, the currencies involved need to adhere to the same technical specifications. The high latencies associated with cross-chain swaps continue to be a problem and, unless they are overcome, they will continue to be a barrier to the vertical integration of cryptocurrencies based on a variety of blockchain technologies on a single DEX [13].

Counter Party Discovery Mechanism

Exchanges need to have some system in place to match buyers to sellers at the correct prices. Order types such as market and limit orders have always been the most popular choices on CEXs. An order book would be used to compile all submitted orders, after which counterparties would be matched up with those orders depending on their respective parameters. This, of course, is synonymous with centralization, and the degree to which DEXs are decentralized is mainly dependent on the operation of this essential component. DEXs that contain order books may either host them in distributed ledgers (on-chain) or have third parties handle the order book management for them (off-chain). There are certain DEXs that do not employ order books because they instead rely on reserves to fulfil customer orders. These are generated by smart contracts that run on the blockchain and come with a settlement procedure.

If one uses on-chain order books, one should be aware that they are constrained by the same performance, cost, and security features as the underlying blockchain. This is the primary disadvantage of using on-chain order books. Due to the fact that the speed of blockchain transactions as well as their scalability have proven to be significant obstacles, activities such as high-frequency trading will not be simply substituted by on-chain protocols. In addition, if a person places an order for a token and the price of that token drops significantly in the time between blockchain updates of the order book, the order may go through with significant losses since the latencies of the underlying blockchain network are unable to accurately represent the current market valuation of an asset that is the subject of a trade [13].

Off-chain order books, which are centralized entities that aid matching parties are used by certain DEXs. This method also allows for avoiding the transaction fees that

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

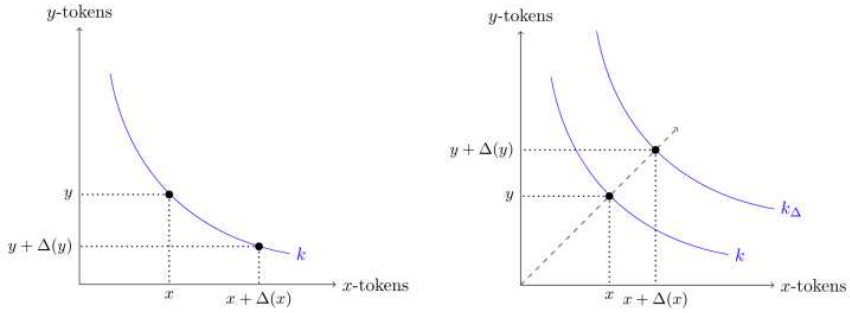

Figure 2.1: Token Reserves of a Liquidity Pool [22]

are often associated with on-chain financial dealings. This, of course, comes at the expense of confidence and the normal inaccurate order books associated with CEXs. One example of a DEX that uses off-chain order books is 0x. On this exchange, third parties known as Relayers host, operate and publish the order books. Orders are pooled once relayers have purchased them from prospective sellers and have added them to their respective order books. After that, buyers are able to query these order books in search of a suitable order, which they can subsequently purchase from the Relayers. Shared order books across Relayers contribute to increased liquidity and price stability in the market [13].

The use of liquidity pools is another alternative that DEXs make use of. A liquidity pool is a smart contract that stores at least two crypto assets in a reserve and makes it possible for anyone to deposit tokens of one type on the smart contract and then withdraw tokens of the other type. The liquidity pool can be modelled as the following. There is a constant k that always is equal to reserves $r_x * r_y$ of two coins x and y.

$$x * y = k. \tag{2.1}$$

When a trade is being made, the equation changes to

$$(x + \Delta x) * (y + \Delta y) = k \tag{2.2}$$

which results in the shift depicted in Figure 2.1. As the reserve of one coin approaches zero the price for it stipulated by the smart contract price mechanism will approach infinity and the reserve can therefore not be depleted [22]. Arbitrageurs exploiting the price difference between the market price of the two coins and the price stipulated by the smart contract in the reserve keep the price at the market level. A popular implementation of a liquidity reserve is the KyberNetwork. [22].

Some DEXs use smart contract aggregation where they scrape prices over multiple liquidity pools and then offer the best option out of those to the buyer or seller. This strategy works as long as the number of pools selected is not too narrow, otherwise, it could lead to monopolistic price setting [22].

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

In summary, some DEXs have turned to peer-to-peer protocols, in which participants may query the network for counterparties who are interested in trading a certain pair of cryptocurrencies and then negotiate the exchange rate directly with those counterparties. In most cases, the process of inquiring and connecting the two parties is carried out by an automated system, but the actual negotiation is still carried out face-to-face between individual users.

2.4 Cosmos Ecosystem

The Terra Network is embedded in the Cosmos Ecosystem which is designed for cross-chain communication. In the following section, the technology used in the Cosmos Ecosystem is presented and subsequently, its relevance is discussed.

In general, a blockchain can be divided into three conceptional layers.

- **Application:** In this layer of the architecture, transactions are processed and the state of the system is updated in response to the transactions that have been processed.
- **Networking:** Transactions and consensus-related communications are propagated via this layer of the system.
- **Consensus:** Nodes can agree on the present state of the system because of the layer of networking that exists between them.

At the time of bitcoin's introduction, there were two alternatives for developing decentralized applications, either fork the bitcoin source or build on top of it. The bitcoin codebase was quite monolithic, with the conceptual layers of networking, consensus, and application being mixed up into one technology. Furthermore, the Bitcoin programming language was both restrictive and unintuitive for people not familiar with the language. There was a pressing need for more effective instruments. With the introduction of Ethereum in 2014, a new approach to the development of decentralized apps was introduced. The developers of Ethereum anticipated that there would be a single blockchain on which individuals would be able to install any kind of application. Ethereum was able to do this by converting the application layer into the EVM. Thousands of developers were able to start constructing decentralized apps based on this new technique. However, the limits of this practice quickly became evident, and they continue to be so to this day. The EVM is a sandbox for any type of application and it optimizes for the most common use case. This implies that developers will have to make trade-offs when it comes to their application's design and efficiency. Additionally, they are restricted to a small number of programming languages and are unable to do code executions automatically. All blockchains

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

seeking to establish a universal platform have these restrictions, not only Ethereum. This is what Cosmos is trying to solve [10].

Cosmos forms the Blockchains' three conceptual layers into separate pieces of the overall architecture. A collection of open-source tools, including Tendermint, the Cosmos SDK, ABCI, and the Interoperable Blockchain Consortium (IBC), is helping to realize this goal. The Tendermint SDK was developed to provide a byzantine fault-tolerant consensus mechanism out of the box that is also able to provide networking capabilities. The application layer that is built on top of the Tendermint SDK can be optimized to achieve a certain goal, be it speed, security, privacy or something else entirely. The results, therefore, are specific use-case blockchains that are built for a specific industry or application area. To be able to seamlessly move assets from one application to another a mechanism which provides fast, cheap and reliable cross-chain communication is necessary. That is what the IBC was designed to do. While the Tendermint SDK provides a fast and reliable framework for the consensus and networking layer, programmers are not restricted to using it. The bridge called ABCI is responsible for converting the semantic logic of the Tendermint SDK to the application layer. Therefore, it is possible to create a unique consensus and networking layer that is different to the Tendermint SDK and still be able to connect to an existing application layer by implementing the link between ABCI and the networking layer. Furthermore, the Cosmos SDK provides a framework, similar to what the Tendermint SDK does for the networking and consensus layer, for building an application layer. It is built to be able to communicate with the ABCI and has a number of modules built into it including the IBC module. Developers are thus free to choose what part of the three conceptual layers of blockchains they wish to build themselves or make use of an already existing standard and simply adapt the application layer to better fit the purpose of the blockchain [10].

2.5 Terra Network Collapse

The Luna crypto collapse that occurred at the beginning of May 2022 caused the Terra Luna cryptocurrency to fall to an all-time low, crashing severely in terms of price, and resulting in the loss of its peg to the TerraUSD (UST) stablecoin.

The UST cryptocurrency is a kind of algorithmic stablecoin; it is run by computer programs, which contribute to the coin's continued price stability. In order to keep the value of these tokens stable, the procedure entails minting new LUNA or UST or burning existing ones.

When a UST is minted, $1 of Luna is burnt, whereas the process also works in the other direction when it comes to the minting of Luna and the burning of UST. The holders of UST will sell their UST for $1 of Luna (or burn it) when the price of UST

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

approaches falling below its peg. This will result in a little profit. This will continue until UST gets beyond $1, at which point it will promote the opposite behaviour.

The value of the stablecoin began to fluctuate when a significant quantity of UST was dumped. During the widespread panic, more UST were sold, which resulted in more Luna being minted and an increased amount of Luna in circulation. This resulted in the price of Luna plummeting as a direct consequence of the domino effect.

Since the market crisis, there has been a significant acceleration in this circulating supply inflation. In the past, there was around 345 million Luna in circulation across the economy. According to the data gathered through analytics, on May 12, 2022, it was 3.47 billion Luna. As of July 26, 2022, it had reached 6,568.79 billion Luna, and it has stayed at that level ever since.

At its peak, Luna and UST had a market cap of around $37 billion and $17.5 billion respectively [2] [3]. At the time of writing their market caps stand at $618 million $278 million, a drop of 98.33% and 98.36%.

[2] https://coinmarketcap.com/de/currencies/terra-luna/
[3] https://coinmarketcap.com/de/currencies/terrausd/

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 3

Related Work

Related work to this thesis evolves around the research topic of crypto asset analytics. There have been a number of papers discussing either traceability on blockchains in general or looking at decentralized exchanges such as Uniswap [1] to extract information on user behaviour. In the following, the research that has been done in this field is discussed. They are separated in research that has been done on the topic of traceability on the Bitcoin network, see Section 3.1, on centralized and decentralized exchanges, see Section 3.2, and on privacy-preserving blockchains, see Section 3.3.

3.1 Traceability on the Bitcoin Blockchain

By being the first and largest cryptocurrency to date, Bitcoin has received a lot of attention regarding its traceability. Research has focused on answering how anonymous is Bitcoin, how traceable the origins of funds are and how well real-world events can be visualized from on-chain data. Thus, it is important for this thesis to look at existing research on the traceability of Bitcoin, as it in large builds the foundation for traceability derived from on-chain data, a method that is crucial for the content of this thesis.

Bitcoin is a wholly online virtual currency that is not backed by physical commodities or state obligations. Instead, it depends on a mix of cryptographic security and a peer-to-peer protocol for witnessing settlements in order to function properly. As a result, Bitcoin has the counterintuitive characteristic that, although the ownership of money is implicitly anonymous, the movement of money is visible to everyone on the planet. Using heuristic clustering to combine Bitcoin wallets based on evidence of

[1] https://uniswap.org/

shared authority, and then using re-identification attacks (i.e., empirical purchase of goods and services) to categorize the operators of those clusters, Meiklejohn et al. [15] investigate this one-of-a-kind trait in further depth. Based on their analysis, they are able to define longitudinal changes in the Bitcoin market, the strains that these changes are putting on the system, and the challenges that anyone attempting to utilize Bitcoin for illegal or fraudulent reasons on a large scale would face. Meiklejohn et al. [15] focus on traceability solely on activity on the bitcoin network, whereas this thesis aims, foremost, at showing how traceable the Terra collapse is from an on-chain and cross-chain perspective, as well as discuss unavailing traceability threats when utilizing existing cross-chain decentralized exchanges.

In a paper from 2013, Ron et al. [20] downloaded the whole history of the Bitcoin blockchain and examined numerous statistical aspects of the transaction graph that were linked with it. They analysed how users of the network acquire and spend their Bitcoin, the amount of Bitcoin they keep in their accounts, and how they move bitcoins between their various accounts in order to better protect their personal information and disguise the traceability of their activities. Clearly, their work was performed before the introduction of Smart Contract enabling blockchains and therefore no traceability in the context of applications based on Smart Contracts was taken into account in their work.

Spagnuolo et al. [23] developed BitIodine, a modular framework that parses the Bitcoin blockchain, clusters addresses that are likely to belong to the same person or group of users, classifies and labels such individuals, and ultimately visualizes the complex information retrieved from the Bitcoin network. Using information about a user's identity and behaviours that are automatically gathered from publicly accessible information sources, BitIodine labels them semi-automatically. As an additional feature, BitIodine facilitates manual research by discovering routes and reversing pathways between addresses or users.

In a forum post [5] in 2013 the method of Coinjoin was introduced to increase privacy on the Bitcoin network in order to make it more difficult for outside parties to establish which spender paid which receiver or recipients. CoinJoin is a trustless way for joining numerous Bitcoin payments from various spenders into a single transaction. Because Coinjoin transactions do not need any changes to the bitcoin system, they are more secure than many existing privacy solutions.

A systematic approach to known traceability diminishing techniques was done in the work of Moser et al. [18]. The review and compare four well-known approaches to diminish traceability. In the choice of users' protection measures against traceability of their on-chain activity, there is a trade-off between the chance that corresponding transactions will be singled out and the loss of privacy as a result of smaller anonymity sets until a significant mass of users accepts the technique. They investigate the technologies of CoinSwaps, CoinJoin and Stealth Addresses. While these

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

technologies aim at eroding traceability and providing technologies, they utilize a different mechanism than a decentralized exchange, which is the topic of this thesis.

3.2 Traceability across Centralized and Decentralized Exchanges

Decentralized exchanges can be quite complex in the functionality and interplay of various smart contracts. In this thesis, decentralized exchanges play a critical role in extracting and interpreting data upon which the collapse of the Terra network is analysed. Centralized exchanges existed before decentralized exchanges, and methodologies to derive traceability from centralized exchanges can help in doing the same for decentralized exchanges. That is why it is important to look at the relevant literature that has looked into the traceability of centralized and decentralized exchanges.

Centralized exchanges such as ShapeShift, make it simple to conduct cross-currency deals without the need for human intervention. In the work of Yousaf et al. [29] they looked at the traceability of crypto assets across multiple blockchains on a centralized exchange. They investigate this subject using data gathered from ShapeShift over a thirteen-month period, as well as data from eight other blockchains. As part of their research, Yousaf et al. [29] are identifying numerous patterns of cross-currency exchanges as well as general use of cryptocurrency platforms, with the ultimate objective of determining whether they are being used to further criminal or profit-driven agendas. While Yousaf et al. [29] do place an emphasis on cross-chain traceability, they do so via a centralized exchange, whereas this thesis aims at covering traceability in a decentralized environment using decentralized exchanges.

Examining decentralized exchanges, the study from Xia et al. [27] looks into the identification of scam projects traded on Uniswap. Fraudulent coins continue to stream into the cryptocurrency ecosystem as Uniswap maintains its position as the most important bitcoin decentralized exchange. In their work, they make an attempt in identifying and characterizing fraudulent tokens on the Uniswap cryptocurrency exchange. A guilt-by-association heuristic combined with a machine-learning-powered strategy is used to develop an accurate approach for spotting scam tokens on Uniswap. The findings in their study indicate that there is a pressing need to detect and combat fraud in the decentralized financial ecosystem and that the proposed technique may serve as a whistleblower by identifying scam tokens in their early phases of development. While the work of Xia et al. [27] does not focus specifically on traceability, it does show the possibilities when analysing data generated from decentralized exchanges, which are important for the purpose of this thesis.

Decentralized exchanges are meant to be used by anyone in the blockchain network and transactions on these DEXs are thus not controlled by a single entity. With

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

centralized exchanges, all transactions necessary for the exchange of two assets, are done by a single entity. This is not the case with DEXs transactions, where all transactions can usually be traced. These transactions, on the other hand, are prone to manipulation and deception. The paper of Victor et al. [24] describes how wash trading behaviour may be detected on two of the first prominent limit order book-based decentralized exchanges on the Ethereum blockchain, IDEX and EtherDelta, as well as on other decentralized exchanges. A lower limit of accounts and trading structures that match the legal standards of wash trading is identified, and it is discovered that they are responsible for a wash trading volume in the equivalent of 159 million United States Dollars, according to the authors. While self-trades and two-account setups are the most common, there are other, more sophisticated arrangements. The address traceability when analysing whether wash trading has been performed on a particular asset. This thesis covers a different aspect of traceability as it tries to identify assets as they move within Terra and across blockchains via cross-chain technologies.

3.3 Traceability on Privacy Preserving Blockchains

Cross-chain decentralized exchanges provide the service of exchanging assets between blockchains. Therefore, the traceability of assets and therefore the extraction of the corresponding data is also limited to the traceability of assets on any blockchain that these cross-chain decentralized exchanges connect to. Thus, the literature of how traceable certain privacy-preserving blockchains are is important for the interpretation of trading activities from cross-chain decentralized exchanges.

In a paper by Miller et al. [16] from 2017, the authors focused on Monero. It lets users conceal their transactions by inserting chaff coins, referred to as "mixins," among the real coins they spend. Two shortcomings in Monero's mixing sampling mechanism are examined in their study, which is based on empirical evidence. First and foremost, about 62% of transaction inputs including one or more mixins are susceptible to "chain-reaction" analysis, which means that the true input may be inferred by elimination. Secondly, the age distribution of Monero mixins is sampled in such a manner that they can be clearly separated from the genuine coins; in other words, the real input is almost always the "newest" input. On all transactions involving one or more mixins, the authors believe that this heuristic can be used to accurately predict the genuine input with an accuracy of 80 %, on average. Their work shows that traceability may also not be guaranteed with modern privacy-preserving cryptocurrencies such as Monero.

Building on the results of Miller et al. [16] a paper from Hinteregger et al. [7] in 2018 further looks into traceability matters on the Monero blockchain. Up until the point of their study there had been a number of protocol adjustments implemented, however,

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

the efficacy of these improvements had not yet been evaluated. Furthermore, there is limited information available concerning the traceability of Monero transactions between hard fork chains. On the basis of currency hard forks, Hinteregger et al. [7] defined a novel approach for tracking Monero transactions that may be applied to other cryptocurrencies. It is using this technique that they conduct a traceability study, on data from Monero and original blockchains, and the authors discovered that only a tiny percentage of the inputs are traceable to their source. Afterwards, they utilized the data to assess the efficiency of known heuristics for recent transactions, and they discovered that they do not exceed random guessing by a substantial margin. The authors believe that Monero is now generally immune to known passive attack vectors and resistant to monitoring and tracing techniques deployed to other cryptocurrencies, based on their research results. While this thesis focuses on a different area of traceability, the studies of Miller et al. [16] and Hinteregger et al. [7] are important when it comes to native cross-chain swaps to a privacy-preserving chain, as the data analysed in this thesis originates from on-chain data and the flow of assets that involve a privacy-preserving blockchain has the potential to obscure the results.

A well-regarded privacy-preserving cryptocurrency is Zcash, one of the many alternative cryptocurrencies that have sprung out since Bitcoin's inception. Because of this, Zcash is sometimes referred to as the cryptocurrency with the strongest anonymity guarantees. In the work of Kappos et al. [9] the authors investigate the degree to which anonymity may be accomplished in the Zcash version that has been implemented. Zcash transactions are investigated in detail, from their transparency to their interactions with and inside its major privacy feature, a shielded pool that serves as an anonymity set for users who prefer to spend their coins discreetly. The authors conclude that, although it is feasible to utilize Zcash privately, it is also possible to significantly reduce the anonymity set available to users by establishing simple heuristics based on recognizable patterns of use and implementing them.

Another study by Quesnelle [19] looking into traceability on Zcash demonstrates that the vast majority of coins supplied to shielded addresses are eventually returned to transparent addresses. Afterwards, he looks for round-trip transactions in which the same, or nearly the same, amount of coins is transmitted from a transparent address to a shielded address, followed by a return transfer to the original transparent address. Quesnelle contends that such conduct is highly linkable, particularly when it occurs in proximity to one another in time. Using this technique, Quesnelle [19] was able to match 31.5 % of all bitcoin transmitted to protected addresses in his investigation. The works of Kappos et al. [9] and [19] is important for this thesis in the same way as the papers on Monero were, which is to provide an understanding of how well privacy-preserving cryptocurrencies, which a cross-chain decentralized exchange may offer trading pairs for, are in diminishing traceability.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

In a survey from 2020 Wang et al. [25] explore privacy-preserving technologies in the blockchain space that include coin mixing mechanisms, zero-knowledge proof, ring signature, and other technologies. A full comparison and study of blockchain privacy protection from the perspectives of technical features and anonymity has been carried out by them among the eight primary privacy protection solutions described in their research. The results are that the centralized coin mixing system and hidden addresses provide the least amount of privacy protection for users. However, the decentralized coin mixing process and ring signature provide the most privacy protection. The work of Wang et al. [25] shows how traceability can be disguised by utilizing various technologies, which are can be dependent on the different underlying blockchains. Swapping from one blockchain to another with different degrees of traceability can thus provide methods to erode traceability for trading pairs on these decentralized exchanges.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 4

Cross-Chain Interoperability

In this section, the different technologies that are used for cross-chain interactions are discussed.

First, the analysed routes that assets take across blockchains are discussed and technologies that are used to realize the transfer of assets are described. An especial emphasis is put on the cross-chain technologies, namely the cross-chain decentralized exchange Thorchain which connects Terra to other blockchains that are outside the Cosmos Ecosystem, such as Bitcoin and Ethereum. Furthermore, the main cross-chain technology within the Cosmos Ecosystem, IBC, is discussed. At last, traceability erosion is discussed which is possible with the technologies discussed, as they may distort the insight that is generated by data extracted from blockchain technologies.

4.1 Cross-Chain Route

Research question *RQ1* focuses on the asset flow between legacy chains and Terra before and during the collapse of the network. Thus, an entry point for legacy chains to the Terra network is needed. In this thesis, legacy chains refer to blockchains that have existed for a prolonged time. They include the blockchains Bitcoin, Ethereum, Binance Chain and Litecoin. For this purpose, a cross-chain decentralized exchange is necessary, as centralized exchanges are not investigated in this thesis. One of the largest cross-chain decentralized exchanges that let entities swap assets between Terra and legacy chains is Thorchain. Therefore, the access point into Terra for legacy chains will be through the Thorchain blockchain.

From Figure 4.1 one can see how the different decentralized exchange technologies are connected and how communication is established. On the left end of Figure 4.1 one can see the legacy chains such as Ethereum and Bitcoin. Thorchain consists

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

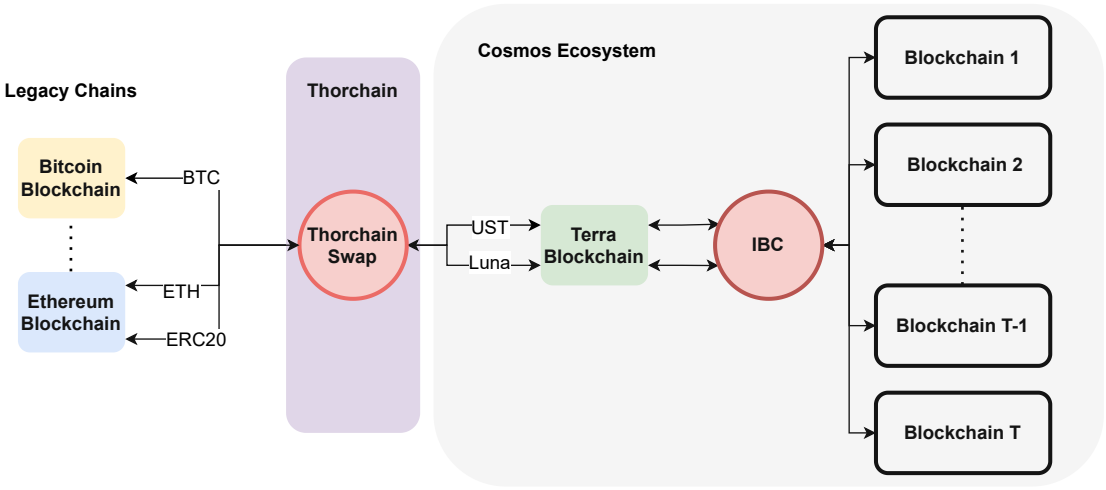

Figure 4.1: Transaction routes from legacy chains into the Cosmos Ecosystem

of certain adapter technologies called Bifrost 4.1.1 which plug into legacy chains and Thorchain simultaneously, thus establishing a connection between the two. On Thorchain one of the most important services is the Thorchain Swap. It allows entities to swap between blockchains natively. In Figure 4.1 the swap between legacy chains and the Terra blockchain is shown. The two assets that can be used on Terra that are supported by Thorchain are its native coins, UST and Luna. Terra is part of the Cosmos Ecosystem, and it utilizes IBC 4.1.2 to connect to other blockchains in the Cosmos Ecosystem. Entities can use the route shown in Figure 4.1 to go back and forth between legacy chains, Terra, and other blockchains in the Cosmos Ecosystem.

The following will explain the mechanism of Thorchain as its functionality is important for the acquiring and analysis of data from the Thorchain swap service.

4.1.1 Thorchain

Thorchain is responsible for monitoring incoming user deposits to vaults, executing business logic (such as swapping assets or adding and removing liquidity), and processing outbound transactions. Thorchain's primary function is that of a leaderless vault manager. It ensures that each and every step of the process of swapping assets is Byzantine fault-tolerant.

Bifrost

As can be seen from Figure 4.2 the Bifrost service is responsible for processing recorded transactions that are happening on the blockchains that Thorchain is connected to. It thus serves as an adapter that is plugged into Thorchain as well as legacy chains to establish a connection between them. Every node on Thorchain is

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

equipped with a Bifrost service that manages the complexities of connecting to the various chains. When nodes in the Thorchain have been synchronized, they begin monitoring vault addresses located on the blockchains that Thorchain is connected to. If at any point they come across an incoming transaction to one of these vaults, they will read it and turn it into a witness transaction for the Thorchain. The Bifrost service accepts witness transactions with a specific set of parameters, see Listing 4.1.1, regardless of the kind of chain they belong to since they are almost the same across all chains. Thorchain will process each transaction that has been seen while it waits for consensus. When there is consensus among a sufficient number of nodes about a given transaction on Thorchain, the status of that transaction changes from *pending* to *finalized*. Therefore, there are two types of node services that are part of the Thorchain logic which runs the Bifrost protocol, Observers and Signers. A single physical Thorchain node can and often does run Observer and Signer logically at the same time. The Observer is responsible for detecting and converting incoming transactions into a logic that is understood by the Thorchain protocol. The signers do the opposite part, signing transactions once the transaction has been formed and broadcasting them to the destination blockchain.

Listing 4.1: Examplatory witness transaction parameters for the Bifrost service, for a swap between ETH to LTC

```
type Tx struct {
        ID          TxID    "7AA99C01A628EA9DCDD4079EED1BE3/
F6EB900C813B4C1EEBB54C721F54BFCF74"
        Chain       Chain   json:"ETH"
        FromAddress Address json:"0xf293f9e575aec02d3da5952b5fd95353c53a134e"
        ToAddress   Address json:"ms26azuzu5ick6r2zhns1dnfkoztz4infh"
        Coins       Coins   json:"ETH.ETH"
        Gas         Gas     json:"0.00691847"
        Memo        string  "SWAP:LTC.LTC:/
MS26AZuzU5iCK6r2zhns1dnFkoZtZ4iNfh:10940083"
}
```

Observers

An observer is a node running on the Thorchain network. It is also listening to a specific vault address on blockchains connected to Thorchain and records incoming transactions to that vault address. They run the Bifrost service and broadcast the witness transaction once the data conversion described in Listing 4.1.1 is finished. The connectivity of a Thorchain node is visualized in Figure 4.3. Inside the Observer node, the Bifrost service consists of a node of the outside blockchain, a corresponding client for connectivity and the Observer logic which converts the logic from outside blockchains into Thorchain logic by converting it into witness transactions.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

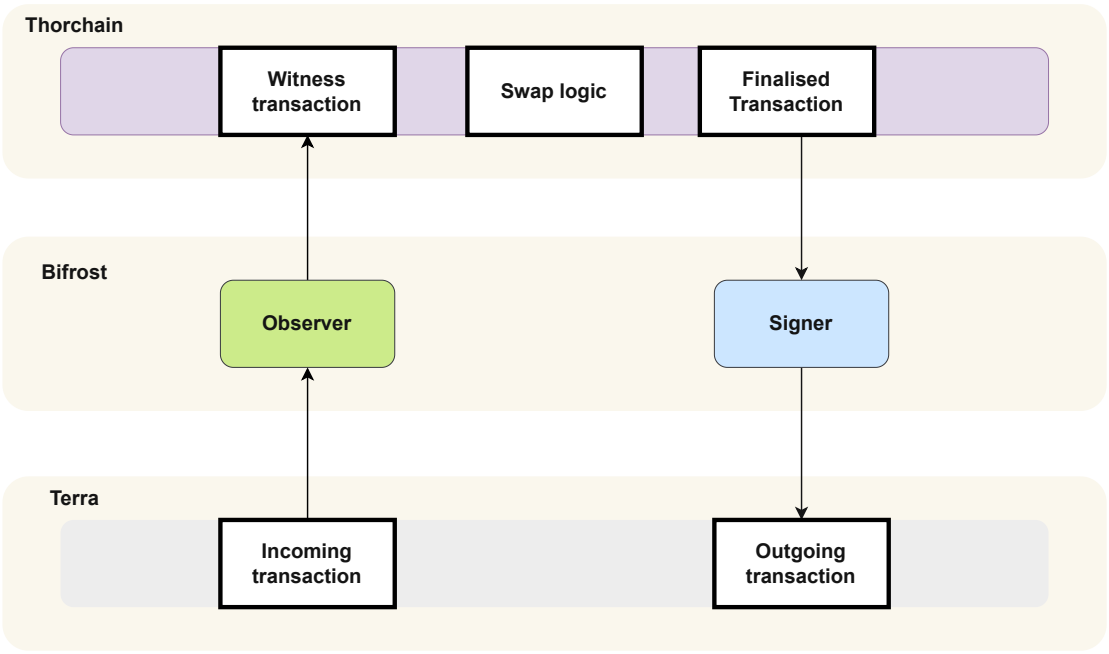

Figure 4.2: Architecture of Bifrost Protocol

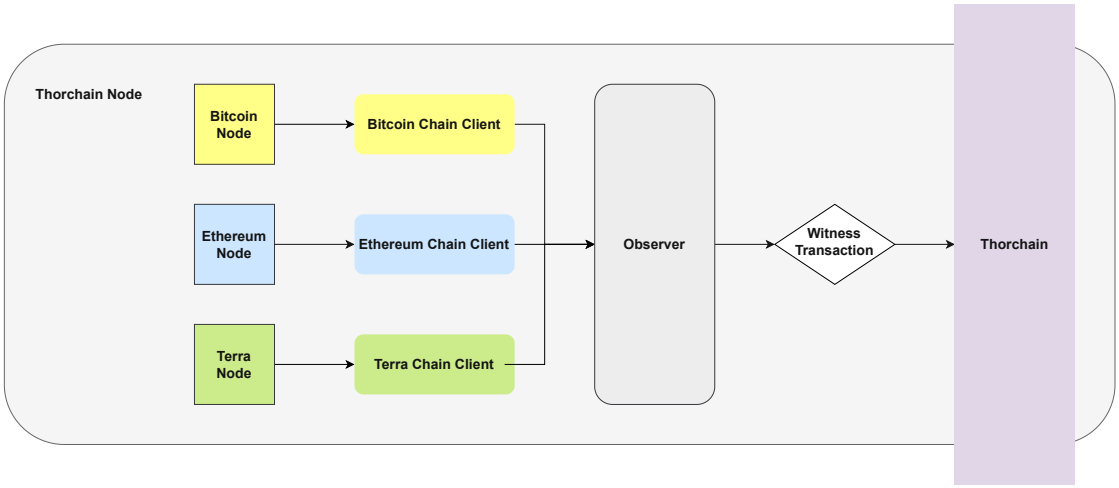

Figure 4.3: Observer node connectivity

Signer

The Thorchain node running the Signer logic of the Bifrost protocol has a connection to the Thorchain blockchain to know when finalized transactions have been formed, the logic for signing transactions on the connected blockchains, a client for the outside blockchain to form valid transactions, the TSS module which is responsible

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

for the threshold signature procedure used by Thorchain to sign any outgoing transaction and nodes to the outside blockchains which are used for broadcasting the validly signed outbound transaction, see Figure 4.4.

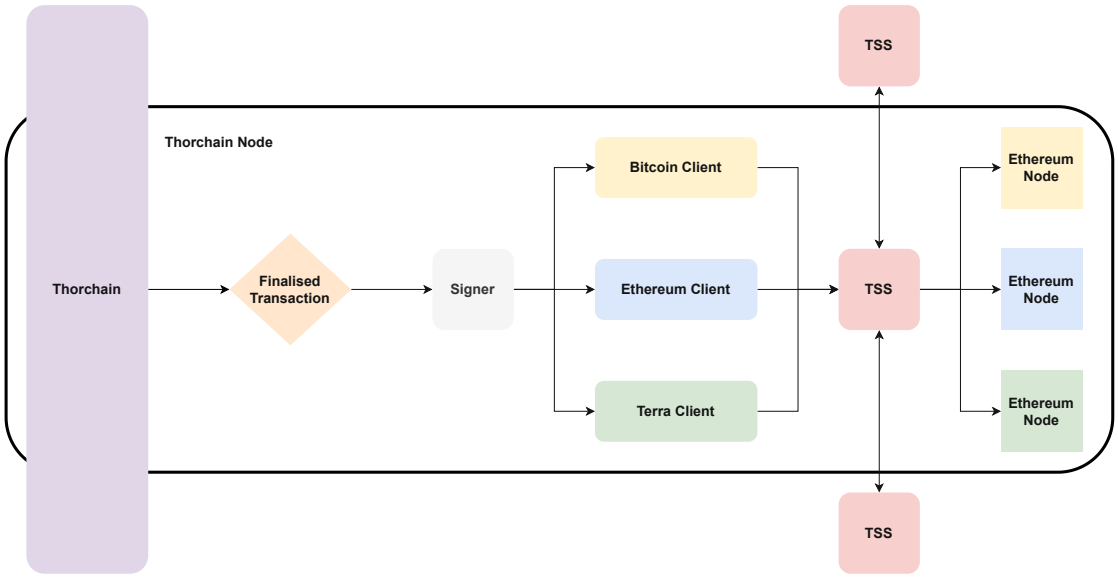

Figure 4.4: Signer node connectivity

State Machine

As depicted in Figure 4.5 the state machine is responsible for processing the completed transaction and carrying out logic operations. These operations include the sequencing of transactions, the computation of state modifications, and the delegation of transactions to a specific outbound vault. When a transaction is delegated to a specific outbound vault, the swap process is complete, and a *txOut* item is produced and placed in a key-value store to be picked up by an Observer.

Vaults

In the Thorchain system, there are two different kinds of vaults known as inbound vaults and outbound vaults. The inbound vaults are called Asgard vaults and are protected by threshold signatures (TSS) meaning that transactions that are signed by Asgard vaults have to include 27 out of 40 participating nodes in the system. To

Figure 4.5: Thorchain state machine process flow

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

increase the number of nodes running on Thorchain an Asgard vault is split into two anytime the number of vaults multiplied by 40 is lower than the total number of nodes running Thorchain. With 100 nodes operating on the Thorchain blockchain, there are thus three Asgard vaults at any time per blockchain connected to Thorchain. The limitation of TSS is the bottleneck for inbound transaction throughput. On the other side, the outbound transactions are handled by Yggdrasil vaults, which only require one signature from a node for them to be accepted by the network. This limits throughput issues, as one inbound transaction may correspond to multiple outbound transactions.

A Yggdrasil vault has a certain value and in order for a node to not exploit assets inside the Yggdrasil vault, the node has to bond more assets to the Yggdrasil vault than there are inside the vault. Each Yggdrasil outbound vault thus has a maximum capacity equal to 25 % of the value of its bond in assets, which is regularly monitored and augmented by the state machine. If a node were to bond $10 million, for example, then up to $2.5 million in assets may appear on its vault. Yggdrasil+ memos are used to keep track of these top-up transactions.

Transactions

Communicating with Thorchain is done through the operating nodes of Thorchain. They listen to inbound transactions that interact with vault addresses assigned to Thorchain. The purpose and content of the communication is derived from memos, a piece of data that is sent alongside the transaction. Most blockchains feature this kind of data transfer to derive content from a transaction. Additionally, to the type of transactions that an entity wishes to perform, all the information necessary to go through with the transactions is submitted through the memo. The specific data elements are discussed in the methodology section 5. The different memo types relevant to this thesis are the following.

- SWAP: An entity wishes to perform a swap.
- ADD: Adding liquidity to a certain pool.
- Withdraw: Withdraw liquidity of a certain pool.

4.1.2 IBC

The second research question *RQ2* aims at analysing the behaviour of users that have assets on the Terra network before and during the collapse. At large, these interactions are dominated by inter-blockchain communication (IBC) or interactions between account addresses (users) and smart contracts. The following will explain the mechanism of IBC, as its functionality is important for the acquisition and analysis of data.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

To showcase how IBC works in general, the Cosmos Hub is discussed. It is the first blockchain to be deployed on the Cosmos Ecosystem. It serves as a multi-asset distributed ledger, which makes it possible for blockchains leveraging the Cosmos SDK and subsequently the IBC module to communicate with the Cosmos Hub and make cross-chain transfers. Each blockchain that uses the Cosmos SDK, the ABCI and some consensus and networking protocol like Tendermint is called a Zone. The Terra network would thus be considered a Zone. In Figure 4.6 it is shown how this mechanism works. The Cosmos Hub exists so that every blockchain in the

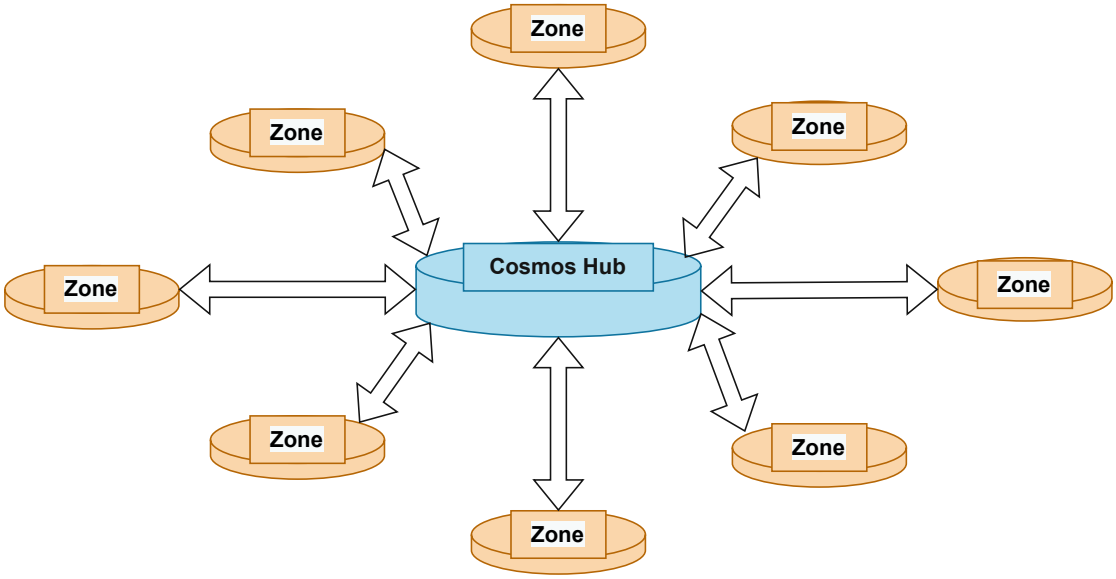

Figure 4.6: Cosmos Hub and its interaction with other Zones

Cosmos Ecosystem does not have to be connected to every other blockchain via IBC, but it is sufficient for each blockchain to be connected to a few Cosmos Hubs in order to reach full connectivity to all others blockchains. Without the Cosmos Hub, the number of connections would have to be n^2 with n blockchains existing in the Cosmos Ecosystem to reach full connectivity. To ensure the scalability of the Cosmos Ecosystem, Cosmos Hubs serve as connectivity centres to bring down the overall number of IBC connections. The protocol of the Cosmos Hub interacting with different zones is described in the following. The interaction of messages is shown in Figure 4.7. Let's suppose there are three blockchains, Zone A, Zone B, and the Cosmos Hub. Let's further assume that for example, Zone A wants to create a packet, i.e. some asset to be transferred, that is intended for Zone B which will travel via the Cosmos Hub. First, Zone A delivers proof of transfer to the receiving chain in order to move a packet from one blockchain to another. The evidence asserts that a packet for the purported destination was published by the transmitting chain, in this example Zone A. This evidence must be checked by the receiving chain, which must

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

be able to keep up with the sender's block headers at all times. This approach needs two interacting chains to be aware of one another through a bidirectional stream of proof-of-existence datagrams, which is similar to the process used by asymmetric cryptography [10]. The IBC protocol, therefore, runs through four different stages in

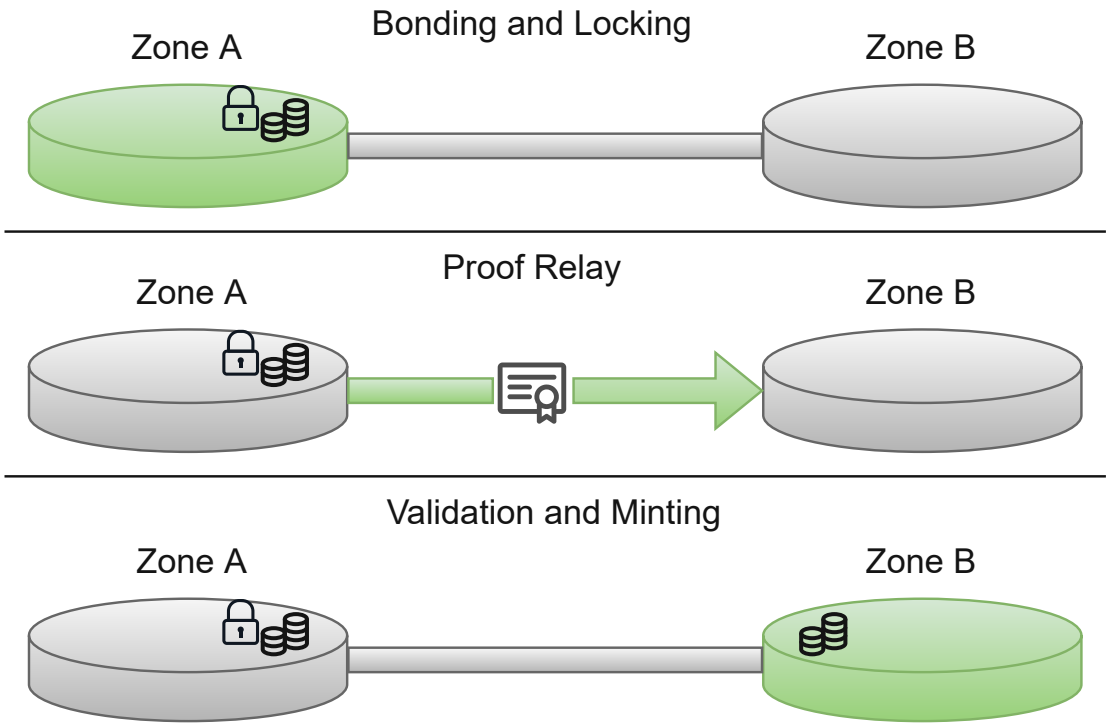

Figure 4.7: IBC interaction protocol

a cross-chain transaction.

- **Tracking:** Zone B gets headers from Zone A in a continuous loop, and the reverse is true. In this way, the validator sets of both chains may be tracked. In essence, each link is a continuation of the previous one. This step is a prerequisite for any IBC transfer, as Zone A and Zone B need to be aware of the latest state of each others' ledger.
- **Bonding:** In order for the IBC transfer to go through, the asset to be transferred on Zone A must be locked up, i.e it is bonded.
- **Proof Relay:** Then a proof is sent from Zone A to Zone B, which states that the asset has been bonded.
- **Validation:** The asset's corresponding proof is generated on Zone B if the proof from Zone A can be confirmed against the header on Zone A.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

It is important to note that the asset that has been generated in Zone B is not genuine in its kind since the actual asset can only be found in Zone A. In addition to being a representation of the asset from Zone A, they also serve as evidence that the asset is frozen in Zone A. When the asset returns to its original chain, the process is reversed in a similar way [10].

In the case of the Terra blockchain, to use IBC an entity that wants to send assets from Terra to another blockchain, they have to query the correct port on the Terra blockchain that corresponds to a relayer that connects Terra to the blockchain the entity wants to send assets to via IBC. Similarly to Thorchain, the relayer picks up transactions addressed to the port they service and forwards the transfer using the IBC protocol.

The Terra network makes use of the IBC protocol to connect to the Cosmos Hub, Osmosis, and other IBC-enabled blockchains in the Cosmos Ecosystem.

4.2 Preventing Traceability

In this section, the possible technologies and methodologies to circumvent traceability are discussed. It is important to point these out, as the later analysis of the asset flow can only account for routes and transactions which are traceable. Also, knowing the possible methods to erode the traceability of transactions helps in facilitating trust in the cross-chain technologies as it is visible to observers of the networks if an entity engages in these privacy-preserving technologies, although it is not possible to see what happens with the assets.

The easiest and most straightforward way of losing traceability for entities using cross-chain decentralized exchanges is for them to swap from non-privacy-preserving blockchains to privacy-preserving blockchains. This way the cross-chain transaction of Thorchain is visible, however, the destination address may not reveal any information about the actual address under control by the entity using the swapping service. Furthermore, even if the destination address is connected to the swapping entity in some way, simply forwarding the swapped asset to another address that is also controlled by the same entity will result in a loss of traceability. This of course requires the underlying blockchain technology to provide proven privacy-preserving transactions. The most well-known blockchains which are privacy-preserving are Monero and Zcash. Both of them have seen thorough investigations into how robust the privacy-preserving mechanism are in multiple studies [16] [7] [9].

The cross-chain decentralized exchange Thorchain has not yet integrated either Zcash or Monero as a swapping partner to legacy chains. However, in recent developer updates from Thorchain, it is stated that both of the privacy-preserving blockchains are currently under development to be integrated with the Thorchain

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

swapping protocol [1]. It is not clear, at the time of writing, whether the integration will be successful, nor which swapping pairs will be available.

There is however an existing swapping pair that provides an opt-in privacy-preserving feature. Litecoin has recently introduced its privacy-preserving protocol MimbleWimble [2] which uses technologies called Transaction Cut-Through [3] and Confidential Transactions [4] which leverage zero-knowledge proofs to preserve privacy. It is thus possible to swap to Litecoin via Thorchain, conduct an opt-in privacy-preserving transaction on Litecoin and then move the assets back to the original chain with a different address without revealing the entire route of transactions to an observer.

When looking at the possible privacy-preserving technologies blockchains that are reachable through IBC, the most prominent blockchain is Secret Network [5]. It uses trusted execution environments (TEEs) that node operators have to run in order to participate as a validator in the network. The TEEs used are usually very specific, and in the case of Secret Network, the Intel SGX is used [6]. Similar to the other privacy-preserving blockchains, traceability can be diminished by moving assets to Secret Network through Thorchain and IBC and then making transactions on the Secret Network.

4.3 Liquidity

Another critical aspect of cross-chain decentralized exchanges is the amount of liquidity they hold in a specific trading pair. Liquidity is essential for the exchange to service swap transactions of a certain size. The swap volume has to be a lot lower than the maximum pool depth, otherwise, the liquidity pool is in danger of being destabilized. After a swap transaction goes through, the pool has to stabilize itself again to keep the desired ratio between the swapped coins in balance. Therefore, slippage is important for these pools. Slippage is used to re-balance the pools, it is usually only a small percentage of the trading volume but can be a costly factor when trading volume is large relative to the depth of the liquidity pool. A graphical representation of the liquidity pool *BTC-ETC* on Thorchain is shown. As of writing this thesis, the pool depth is about $100.000.000, and the corresponding loss of funds due to slippage depending on the relative percentage of the trading volume to the pool depth can be seen in Figure 4.8.

It is clear to see that only a certain amount of volume can be routed through the pool at once. Splitting up the volume into smaller transactions can alleviate this cost of

[1] https://medium.com/thorchain/dev-update-144-146-23f03df603d6
[2] https://litecoin.com/en/news/litecoin-mimblewimble-december-recap-update
[3] https://bitcointalk.org/index.php?topic=281848.0
[4] https://academy.bit2me.com/en/what-are-confidential-transactions/
[5] https://scrt.network/
[6] https://docs.scrt.network/protocol/sgx.html

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

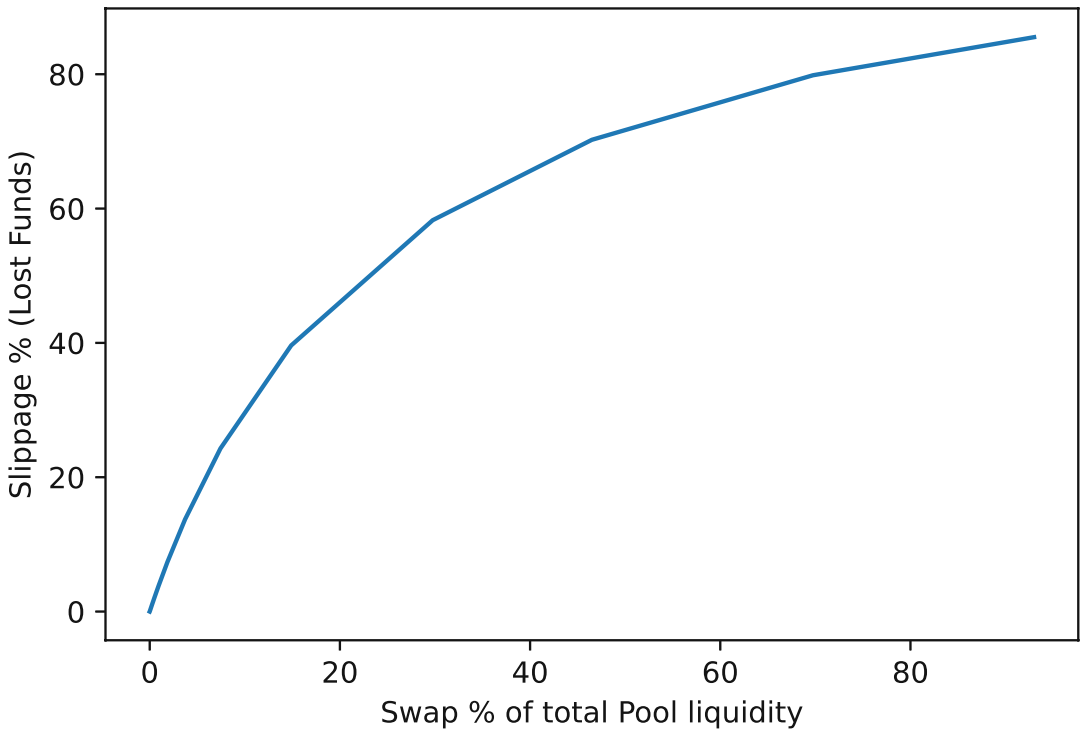

Figure 4.8: Slippage of BTC-ETH trading pair on Thorchain in dependence of the relative trading volume to the pool depth

slippage, however, one has to pay a multiple of the transaction fees due to a higher number of transactions. Thus, cross-chain decentralized exchanges are limited in how much liquidity they can route through their protocol and might not be an option for entities with large funds seeking to swap their assets for another.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 5

Data & Methods

In this section, the methodology used for data extraction, data preprocessing and data analysis will be discussed. First, the required data sources, how data was and can be acquired and what limitations were dealt with will be described. After that, the preprocessing of the data, especially the extraction of information from on-chain data is presented and how these data points can be interpreted, linked and collected into a meaningful final dataset. In the final part, the different methods for analysing and visualizing the acquired data are presented.

5.1 Data Acquisition

To understand how data from the blockchains Thorchain and Terra were acquired, it is necessary to have an understanding of how data transmission in the different distributed databases takes place. In principle, there are different types of network participants in a blockchain. Most of the participating clients, also called nodes, are light nodes, which means they don't store data from the blockchain but only participate in communication with other nodes for the purpose of conducting transactions. These nodes typically do not run any consensus mechanism nor participate in validating and mining blocks. This task is usually performed by validators in a proof of stake blockchain or miners in a proof of work blockchain. Validator nodes participate in the proof of stake consensus mechanism, receive broadcasted transactions, validate and propose new blocks and store past information of the blockchain if they also act as full nodes.

5.1.1 Full Nodes

Full nodes are participants in the network that store the entire past blockchain on their local device and thus keep a record of past transactions and new transactions that accumulate with every new block proposed in the system. They are therefore quite resource intensive, as they have to have a decent amount of fast storage and good connectivity to the internet. Consequently, a full node is the best option to keep track of transactions. For this thesis, there were essentially two blockchains that needed to be kept track of in order to extract the data necessary. The blockchains that data was acquired from are Thorchain for tracking swaps between legacy chains and the Terra network to see network activity with relayers and smart contract interactions. Thorchain and Terra are the main sources of data for tracking assets across blockchains.

Public Full Nodes

A full node can usually either be accessed through a public full node or by running a full node locally. The former option does not require one to acquire the necessary hardware to run a full node but usually means less data throughput as bandwidth and access time is shared amongst all users of the public full node.

These public full nodes are usually run by the development teams of the corresponding blockchain. In other cases, there are private options for gaining access to the data of full nodes through some data service that provides blockchain data through an API against payment per request.

In this thesis both options, acquiring data from a public full node and running a full node, were explored. However, due to hardware limitations, data that was acquired for the analysis came from public full nodes.

The data that was necessary for the analysis of the Thorchain network was acquired from a public full node providing data under the domain of thornode.ninerealms.com [1]. It generally provides data about network activity, network status, pool information and of course transactions. Since the connection between Thorchain and the Terra network was only made public with the release of the Thorchains mainnet in March 2022 the analysis timeframe was restricted to the months of March, April and May. The block range for Terra was 6600000 to 7007751 and for Thorchain the block range was from 4971758 to 5236345.

[1] https://thornode.ninerealms.com/thorchain/doc/#/

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Private Full Node

The data from the public Thorchain node was acquired with a query including the block height [2]. At first, the data for the Terra blockchain was acquired through the public full node[3], however, due to the Terra collapse in early May the public endpoint stopped servicing requests and therefore the service of a private endpoint was used [4].

5.1.2 Data on Decentralization

To evaluate the degree of decentralization of Thorchain, IBC and the blockchains running on the Cosmos Ecosystem posed in research question *RQ3* several data sources were used. The information on Thorchain node operators was gathered from a public endpoint run by the developers of Thorchain [5]. By using the nodes' IP addresses, the information regarding their location and ISP provider was extracted. The information about Asgard vault addresses was embedded in the information gathered by the public Thorchain node. For the information on relayers, the popular Cosmos Ecosystem blockchain explorer was used. Since Osmosis and Cosmos Hub are the two largest blockchains by IBC traffic, their connection was chosen to showcase the level of decentralization. Their connection can be found under the relayer section on mint scan [6,7]. The information on the node operators from the Cosmos Ecosystem can be found through the Kepler wallet [8].

The data acquisition was done by running a python script that acquired data from the mentioned APIs at regular intervals. To speed up the process of data acquisition and since the program was CPU bound and not I/O bound, a multiprocessor parallelization was used with 32 virtual cores running at the same time. The data was stored in persistent storage and for the given time frame the data from Thorchain and Terra amounted to 1.0 GB and 4.5 GB respectively.

It was also attempted to run a full node for the Terra blockchain, since the amount of data required for the analysis was quite large and thus took a long time to get through the use of an API. However, due to hardware limitations, running a full node was not pursued any further. To be able to provide further analysis over a longer time period, it would make sense to set up a full node for each of the networks that one wishes to analyse. Especially networks such as the Secret Network would be

[2] https://thornode.ninerealms.com/txs?limit=10000&tx.height={BLOCKHEIGHT}
[3] https://lcd.terra.dev/swagger/
[4] https://luna.getblock.io
[5] https://ops.ninerealms.com/nodes
[6] https://www.mintscan.io/cosmos/relayers/channel-141
[7] https://hub.mintscan.io/ibc-network
[8] https://wallet.keplr.app/

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

of interest as one could track an entity until traceability was lost. For this thesis, however, only public nodes or private nodes exposing an API for the data were used.

5.2 Data Processing

In this section, the processing of the data is discussed. First, a description of the data, what it is composed of and an interpretation of the different parts of the acquired data are presented. Afterwards, different methods were used to arrive at a dataset which contains the exact information necessary for tracking the asset flow over different blockchains. For the tracking of assets, there were two main sources of data used which has different compositions of data. These were the blockchain data from Thorchain and Terra.

5.2.1 Data Composition and Interpretation

In this part, the structure and composition of the data extracted from the two blockchains will be discussed.

Thorchain Data

For research question *RQ1* data which links incoming assets into Asgard vault addresses with the respective swap partner have to be acquired. The following goes through the different steps in processing the raw return data into semantically correct datasets used in the analysis. The structure of the raw data JSON object returned by the public Thorchain node can be seen in Table 5.1. The **txs** column contains all transactions that occurred during a single block. The further sub-structures of the relevant **txs** JSON object can be seen in table 5.2. The **tx** object was then searched for any valuable information for asset tracking. The relevant contents of the **tx** JSON object used for tracking Thorchain data had the format described in Listing 5.1. The **id** for the transaction serves as a unique identifier of the transaction, and the **from** and **to** addresses show where the assets came from and where they are supposed to go. The **type** of the transaction signals whether it is an inbound or outbound transaction, meaning whether funds are moved into an Asgard vault or out of a Yggdrasil vault. The memo is important as it gives information about what type of service from Thorchain was used. At last, the columns **asset** and **amount** stand for the type of asset and the amount of that asset that was used for the Thorchain service.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Column	Datatype
total_count	Integer
count	Integer
page_number	Integer
page_total	Integer
limit	Integer
txs	JSON Object

Table 5.1: Raw data public Thorchain node

Column	Datatype
height	Integer
txhash	String
data	String
raw_log	String
logs	JSON Object
gas_wanted	Integer
gas_used	Integer
tx	JSON Object
timestamp	DateTime
events	JSON Object

Table 5.2: Txs-JSON of Thorchain raw data

Listing 5.1: Relevant data of **tx** JsonObject

```
{
"type":String,
"value":{
    "msg":[{
        "type":String,
        "value":{
            "txs":[{
                "tx":{
                    "id":String,
                    "chain":String,
                    "from_address":String,
                    "to_address":String,
                    "coins":[{
                        "asset":String,
                        "amount":Integer}],
                    "block_height":Integer,
                    "memo":String,
                    ...}}]}}]}
```


Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Terra Data

Similarly to the Thorchain raw data, the data acquired from the private Terra node was filtered for the **tx** column and relevant information for the tracking of assets where extracted. The data extracted from Terra is used for research question *RQ2* as IBC transfers and smart contract interactions are visible from them.

5.2.2 Data Combination

The data received from the public and private full nodes on Thorchain and Terra do not yet reveal the necessary information to be able to track assets across blockchains.

Linking Thorchain Data

The only types of transactions that are of relevance to the likeability of Thorchain transactions are *ObservedTxIn* and *ObservedTxOut* which correspond to incoming and outgoing transactions to the Asgard vaults and from Yggdrasil vaults. For incoming transactions, the columns in Table 5.3 are extracted for further processing. Especially the memo reveals important information which will be important when trying to link incoming with outgoing transactions. The general pattern of the memo for the Thorchain services is

$$FUNCTION : PARAM1 : PARAM2 : PARAM3 : PARAM4$$

and for the swap service this boils down to the following patterns in the memo of an incoming transaction

$$SWAP : ASSET : DESTADDR$$
$$=: ASSET : DESTADDR : LIM$$
$$s : ASSET : DESTADDR : LIM : AFFILIATE : FEE$$

, where *ASSET* stands for the asset that the user wants to swap into, *DESTADDR* is the destination address of the swap, *LIM* is the minimum of coins received after the swap. The fields *AFFILIATE* and *FEE* are used to define an affiliate of the transaction and allocate transaction fees to that affiliate if desired. These latter two are not of importance for traceability.

The pattern of outgoing transactions links the outgoing transaction to the incoming transaction and thus closes the information gap between incoming and outgoing transactions to ensure traceability.

$$OUT : TX\_IN$$

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Column	Description
Service	Type of service (swap, add liquidity,...)
Asset_Out	Outgoing asset (BTC,ETH,Luna,...)
Destaddr	Address of the destination after swap is completed
Limit	Minimum of assets received
Asset_In	Incoming asset (BTC,ETH,Luna,...)
Tx_Id	Unique identifier of the transaction
User_Address	Address of the entity who initiated the service
Vault_Address	Address of Asgard vault that served as incoming asset pool
Amount_Payed	Amount of coins paid denominated in Asset_In
Memo	Memo of the transaction
timestamp	Timestamp of the transaction

Table 5.3: Incoming transactions dataset after filtering and memo information extraction

Column	Description
Asset_Out	Outgoing asset (BTC,ETH,Luna,...)
To_Address	Address of the destination after swap is completed
Tx_Id_In	Unique identifier of the corresponding incoming transaction
Tx_Id	Unique identifier of the outgoing transaction
From_Address	Address of the entity who initiated the service
Amount_Out	Amount of coins received denominated in Asset_In

Table 5.4: Outgoing transactions dataset after filtering and memo information extraction

Column	Datatype
timestamp	DateTime
tx.value.msg.type	String
tx.value.msg.value.txs.tx.id	String
tx.value.msg.value.txs.tx.from_address	String
tx.value.msg.value.txs.tx.to_address	String
tx.value.msg.value.txs.tx.memo	String
tx.value.msg.value.txs.tx.coins.asset	String
tx.value.msg.value.txs.tx.coins.amount	Integer

Table 5.5: Final dataset for the preprocessed Thorchain data

With this, all information that is necessary for traceability has been gathered for the Thorchain data and the final dataset for Thorchain is given in Table 5.5. Since it is possible that incoming transactions are reverted due to errors such as invalid memos, incorrect limits being set or simple network failures, only those incoming transactions that have a matching outgoing transaction were considered.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Column	Description
txhash	Unique identifier of the transactions
tx.body.messages.source_channel	Channel of the IBC endpoint
tx.body.messages.sender	Address of the sender of assets
tx.body.messages.receiver	Address of the receiver of the sent assets
tx.body.messages.token.denom	Token which is being sent
tx.body.messages.token.amount	Amount of the sent token
timestamp	Timestamp of the transaction

Table 5.6: Final dataset for the preprocessed Thorchain *transfer* data

Column	Description
txhash	Unique identifier of the transactions
tx.body.messages.sender	Address of the sender of assets
tx.body.messages.contract	Address of the contract of the sent assets
tx.body.messages.token.value.denom	Token which is being sent
tx.body.messages.token.value.amount	Amount of the sent token
timestamp	Timestamp of the transaction

Table 5.7: Final dataset for the preprocessed Thorchain *smart contract execution data*

Linking Terra Data

With the data acquired by the private Terra full node, there is no need to link two different types of transactions together in order to achieve traceability. However, the raw data from Terra can be split into three different kinds of transactions, which decreases dataset sizes due to non-overlapping columns and separates areas of concern. The **type** column has three different values which are of interest for this thesis, and they are *MsgSend*, *MsgTransfer* and *MsgExecuteContract* which signal transactions where assets are either sent within the Terra blockchain, transferred via IBC to other blockchains in the Cosmos Ecosystem or are sent to a contract by interacting with the contract.

By separating the raw dataset into these three categories, a leaner and thus faster processing speed of every dataset is achieved. For IBC and smart contract interaction tracking, however, only the *MsgTransfer* and *MsgExecuteContract* transactions are relevant. The final columns of the resulting datasets are shown in Tables 5.6 and 5.7.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 6

Analysis & Results

This chapter presents the evaluation of tracing asset flow across Terra and its cross-chain connections. The evaluation can be divided into three main parts, i.e., the asset flow through Thorchain, the interaction with smart contracts or IBC-enabled blockchains of users on the Terra network. The evaluation sections will highlight the paragraphs in which answers to the three research questions stipulated in Section 1 are given.

6.1 Asset Flow between Legacy Chains and Terra

The first research question *RQ1* was about what assets were used for cross-chain transfers before and during the collapse. Therefore, the first part of the evaluation is the flow of assets through Thorchain into Terra before and during the collapse of the network. cryptocurrencies usually do not hold a consistent price ratio between each other. To show the flow of assets between multiple different cryptocurrencies, one, therefore, needs to denominate the trading pairs constantly.

Terra has two main coins on its network, Luna and UST, with the former being a fluctuating asset like ETH and the latter being an algorithmic stablecoin that depegged during the collapse of the network. Therefore, asset flows were divided up into trading pairs with Terra Luna and UST to separate the denomination of these two assets. Furthermore, to show cross-chain asset flows, trading between UST and Luna was omitted as they do not represent true cross-chain swaps as they are both native on the same blockchain.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

6.1.1 Absolute and Relative Flow of Assets

While looking at the total amount of trading volume between legacy chains and Terra, an accumulative approach grants a good overview of which trading pairs are overall sought after. However, it does not reveal any events or changes in users' trading behaviour. Therefore, the swapping between legacy chains and the Terra network was evaluated over time. This gives insight into which assets are used for exchanges between legacy chains and Terra, and also how the collapse of the network unfolds from on-chain data over time.

The figures used to interpret the data either show the absolute or relative trading volume between two assets denominated in either Luna or UST. For visibility for every asset pair, the five biggest trading pairs are visualized, with all other trading pairs being summed up in one category. The legend of each plot shows the cryptocurrency that either Luna or UST was traded against, and they show the blockchain they are run on too. For example, *BNB.BUSD* would correspond to the token BUSD that is stored on the Binance Chain. The volumes are either traded against Luna or UST and are therefore also dominated in either one of them, meaning that if BNB.BUSD was traded against UST the trading volume shown is denominated in UST.

From Figures, 6.1,6.2,6.4 and 6.3 one can see the absolute and relative volumes of different trading pairs from legacy chains to Terra and back, denominated in UST.

It is visible from 6.2 and 6.3 that overall asset flows remained consistent with BUSD being the dominating traded asset for UST across time. There was an unusually large amount of BTC bought with UST in the middle of April, see Figure 6.1 and overall BUSD is less dominant with assets flowing out of Terra than it is the other way around, see Figure 6.4, suggesting that the demand for UST bought with BUSD is higher than the demand of BUSD bought with UST.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

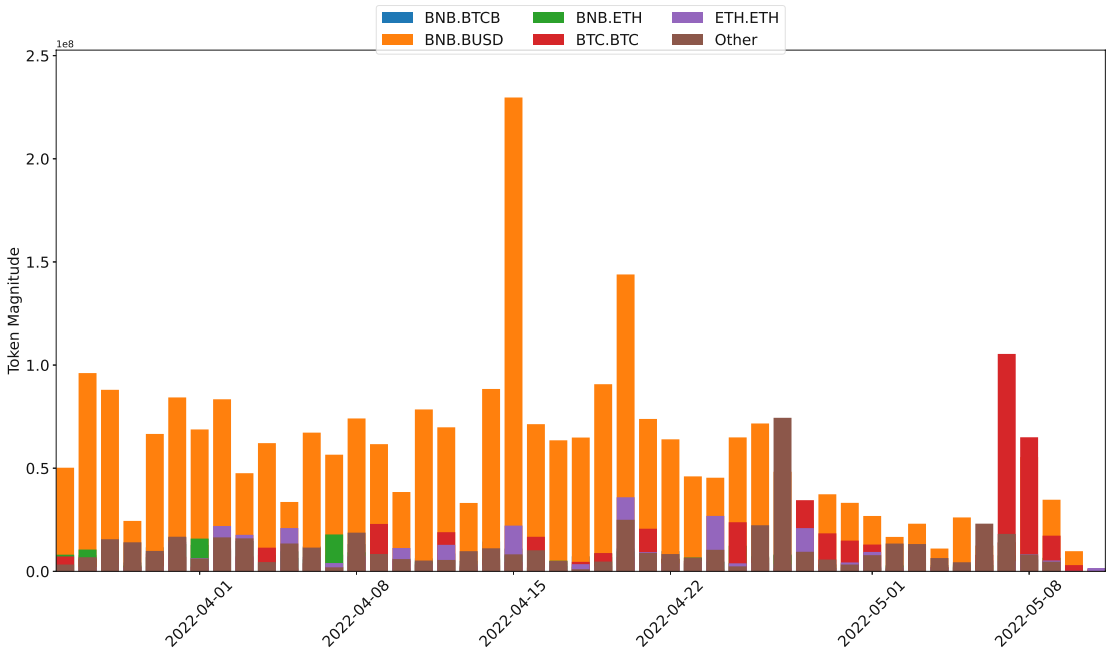

Figure 6.1: Asset flow from legacy chains to Terra over time denominated in UST

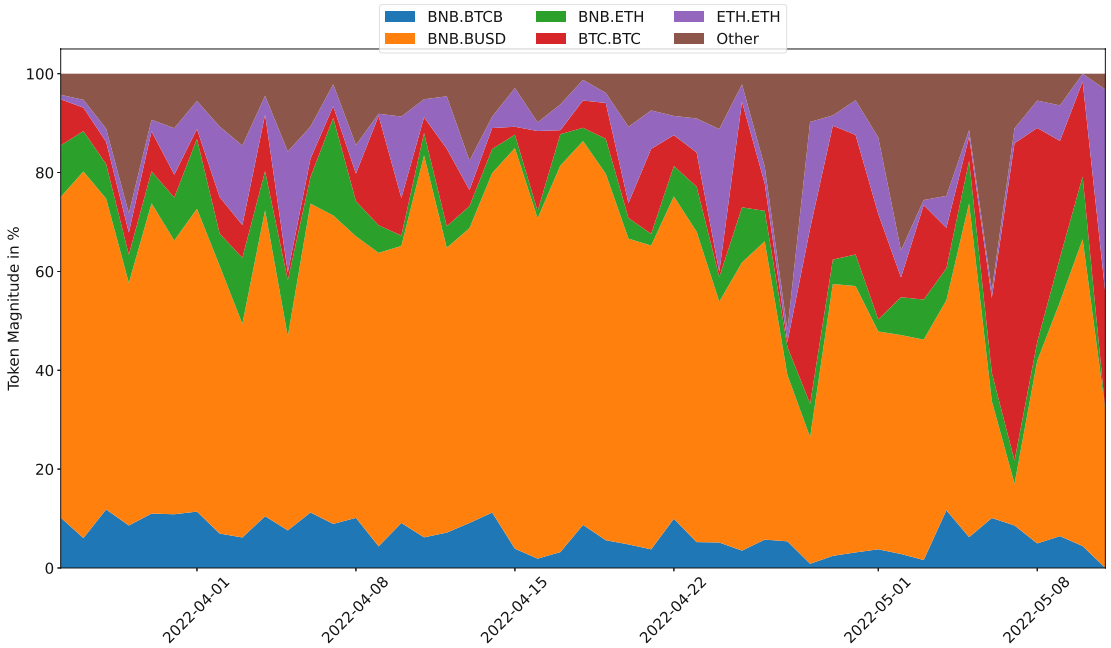

Figure 6.2: Relative asset flow from legacy chains to Terra over time denominated in UST

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

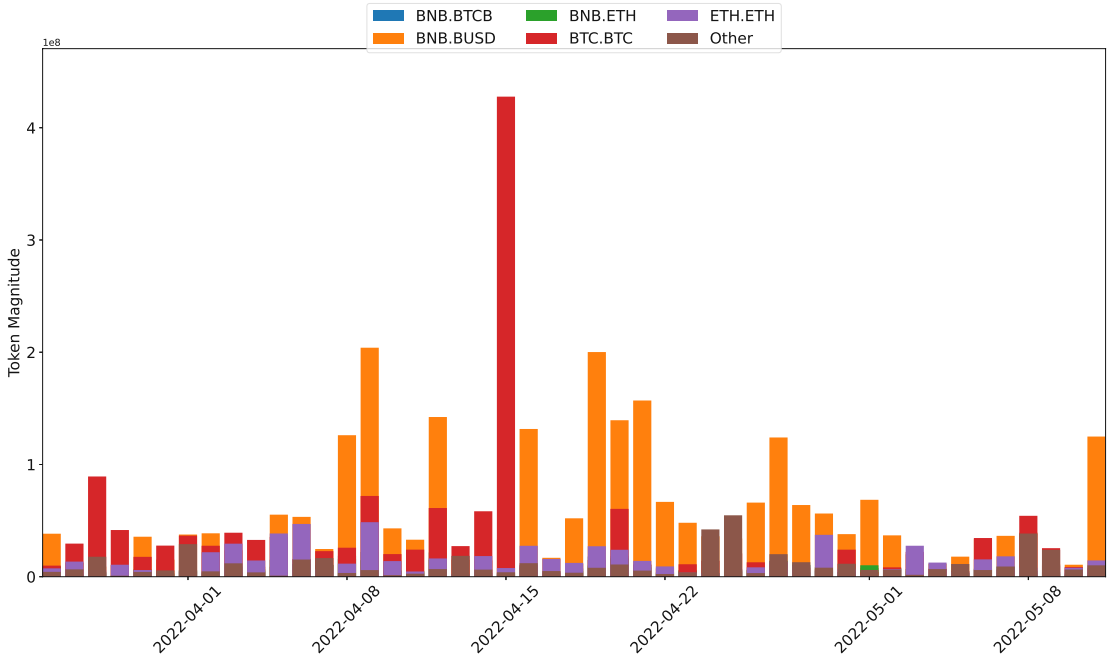

Figure 6.3: Asset flow from Terra to legacy chains over time denominated in UST

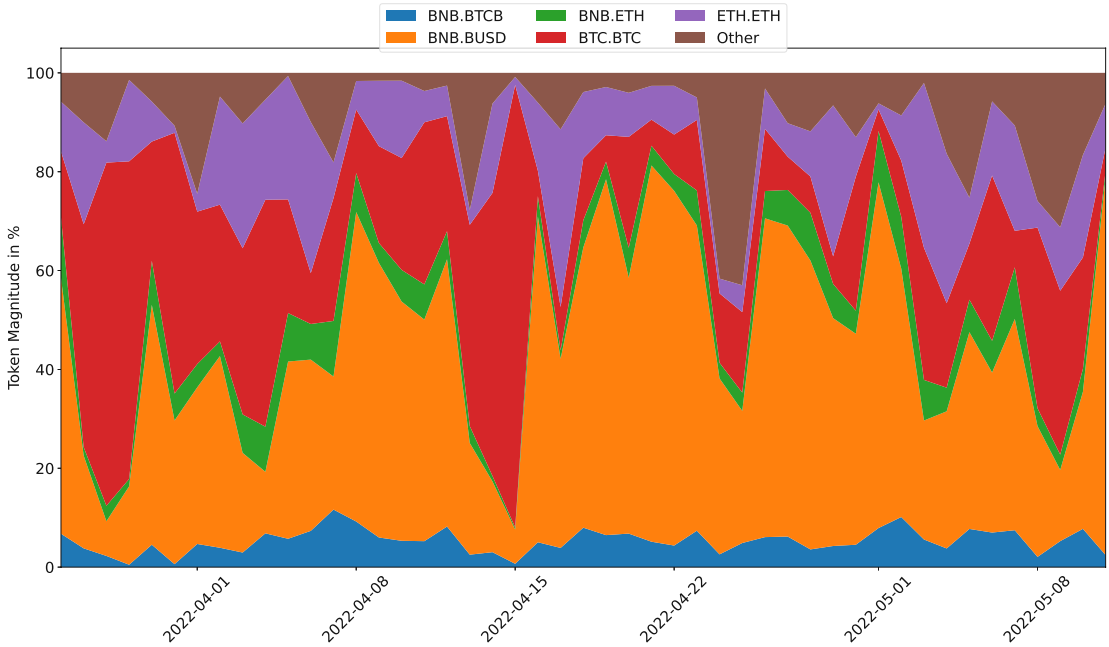

Figure 6.4: Relative asset flow from Terra to legacy chains over time denominated in UST

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

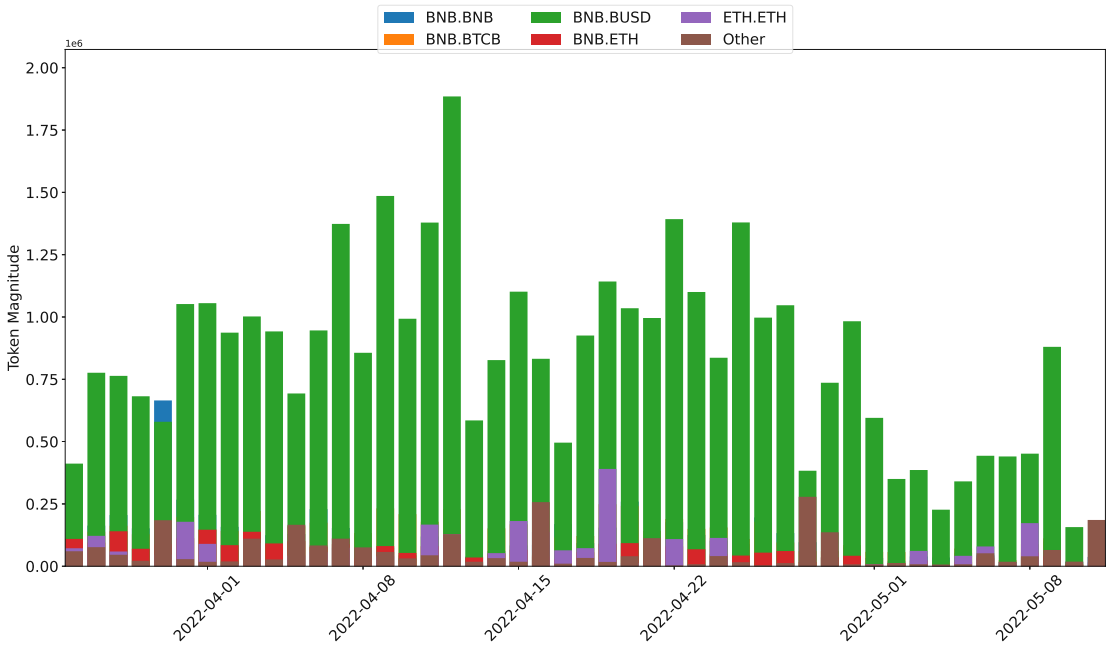

Figure 6.5: Asset flow from legacy chains to Terra over time denominated in Luna

The same statistics are shown for the absolute and relative flow of assets from and to Terra denominated in Luna in Figures 6.5,6.6,6.8 and 6.7.

When looking at the flow of Luna from Terra to the legacy chain, the Terra network collapse towards the beginning of May is clearly visible. A spike in the outflow of Luna especially into BUSD, signalling users trying to lose exposure to the collapsing cryptocurrency, can be seen in Figures 6.8 and 6.7. The inflow from legacy chains to the Terra Luna shows that not only were users transferring little amounts of funds to Terra Luna but also that the previously dominating trading pairs were hardly used to make the trade, see Figures 6.5,6.6. A better explanation of these phenomena is given in Section 6.1.2.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

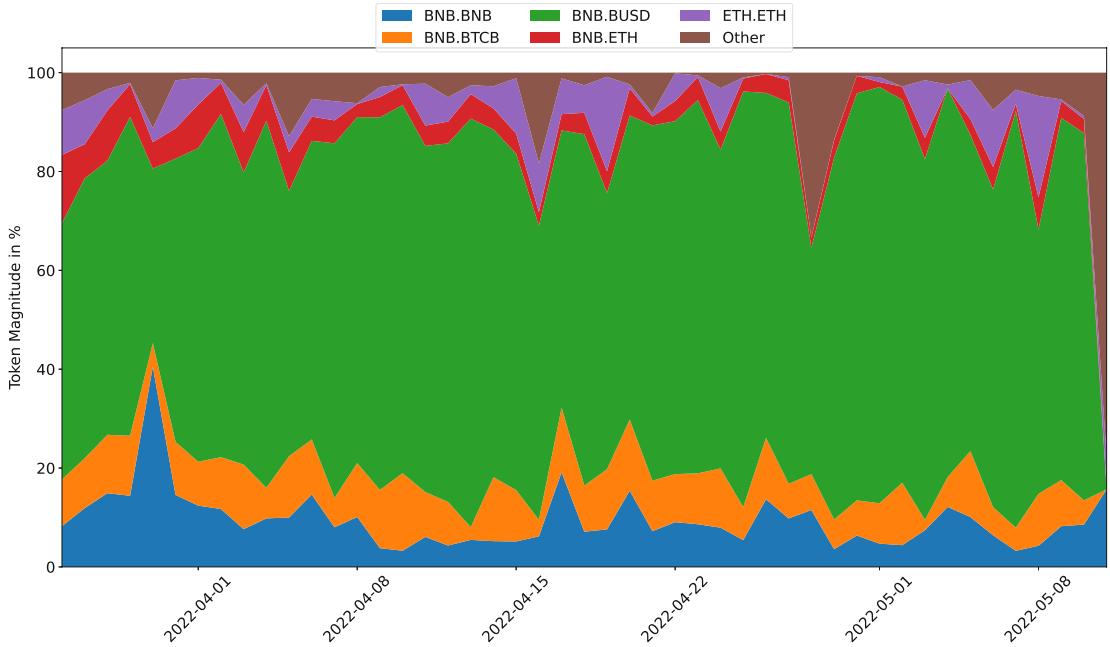

Figure 6.6: Relative asset flow from legacy chains to Terra over time denominated in Luna

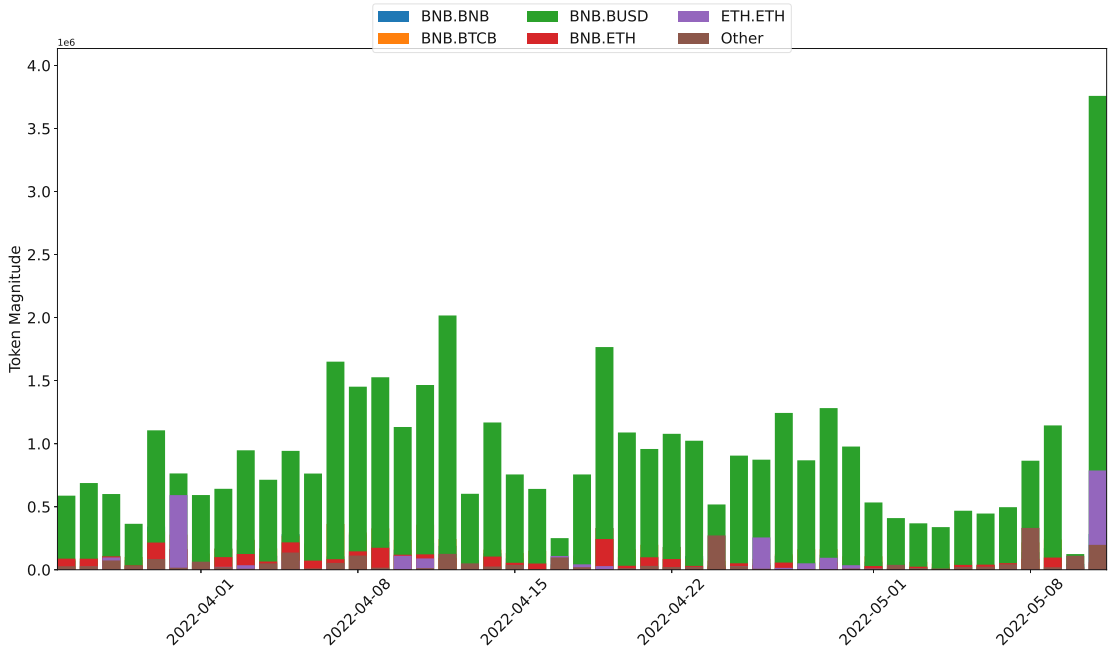

Figure 6.7: Asset flow from Terra to legacy chains over time denominated in Luna

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

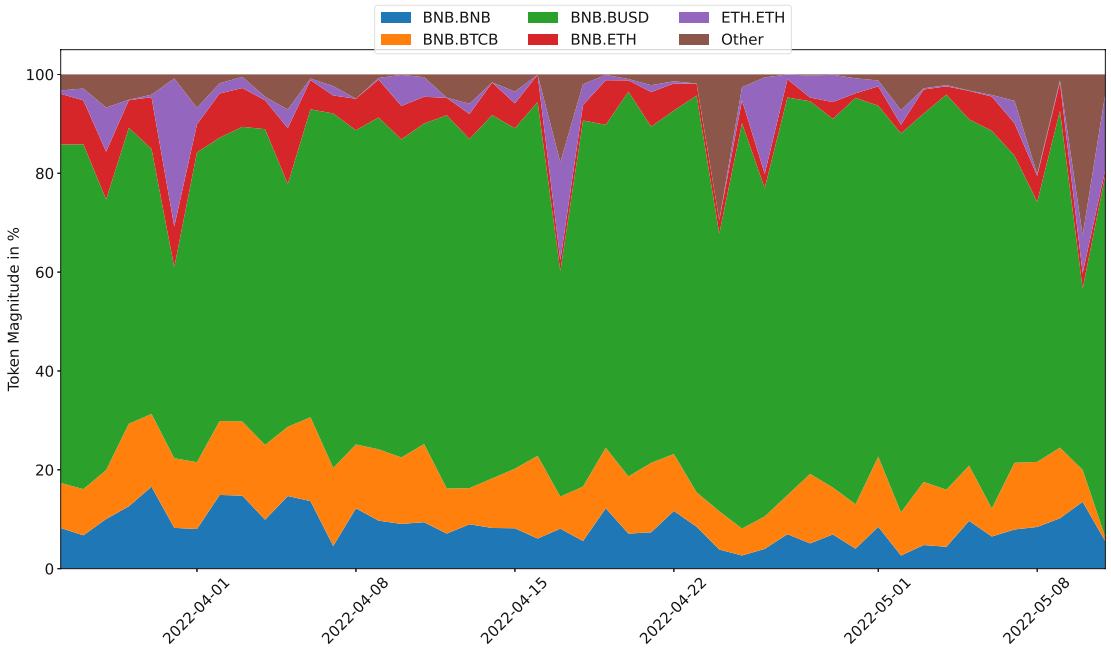

Figure 6.8: Relative asset flow from Terra to legacy chains over time denominated in Luna

6.1.2 Failed Transactions

The rise of the trading volume of Luna and to some degree to UST can also be explained by the rapid decrease of the value of these assets against other cryptocurrencies such as BTC and ETH. Therefore, an additional analysis of user behaviour to derive an understanding of how to interpret the rise in trading volume is necessary.

Thus, transactions on the Thorchain swap service that failed over the same time span were analysed. Transactions on the Thorchain network can fail if the memos that were sent in the transactions contained errors, or simply if there is an overload of the Thorchain network. The former is expected to be consistent and represent some version of background noise, while the latter is an indicator of how many transactions were broadcast by users. These failed transactions from assets flowing from Terra to legacy chains can be seen in Figure 6.9.

One can clearly see the sharp rise in failed transactions towards the beginning of May and the middle of May, which was around the time when Terra block validators resumed block production. The most dominant asset used in transactions that failed was Rune, Thorchain's native currency. The graph visualizes the panic selling of users as Luna's price crashed by over 95% in a few days. Also, noteworthy is that in addition to the spike in Rune trading pairs, BTC also experienced a sudden uptrend. It is important to note here, that trading pairs between UST and LUNA and legacy

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

chains were paused by Thorchain during the days of the collapse, so the number of failed transactions also gives a hint into what asset pairs might have been up for longer than other trading pairs as users tried to get as little exposure as possible in Luna.

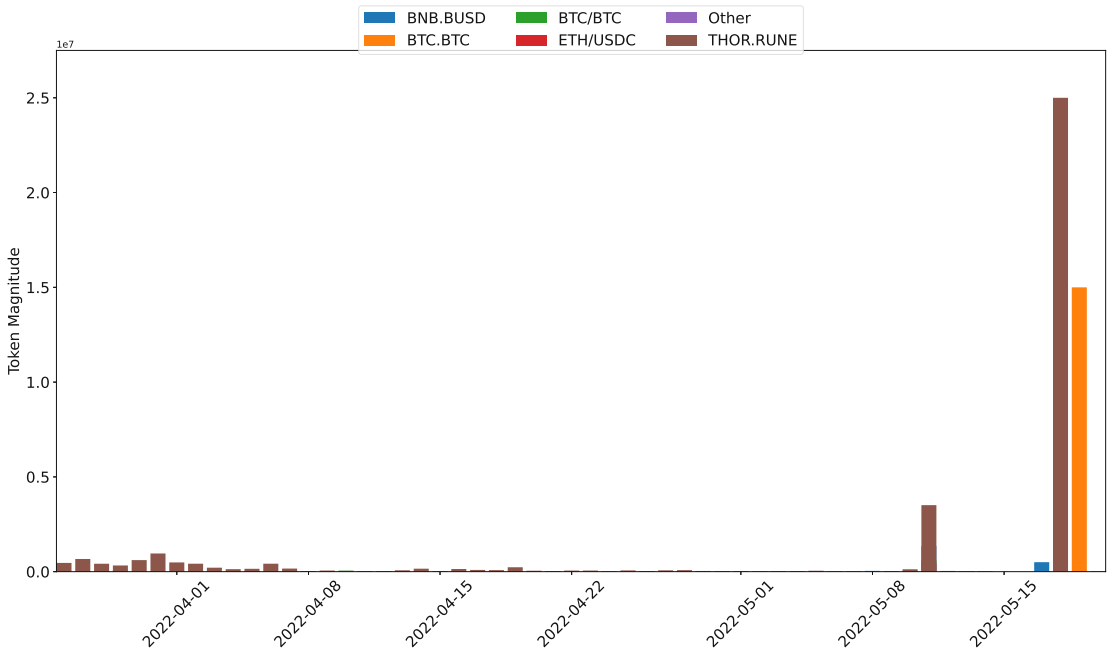

Figure 6.9: Failed transactions from asset flow from Terra to legacy chains over time denominated in Luna

6.1.3 Summary

The dominant assets used for cross-chain swaps between blockchains like BTC, ETH, BNB and LTC were the stablecoin BUSD on the Binance blockchain. This was consistent over time, even throughout the collapse of the Terra network. Overall the dominant swap partner for Luna and UST for the Thorchain Swap service was Binance including its derivatives of BTC and ETH.

Failed transactions from the Terra network to Thorchain show that the panic caused by the Terra collapse can be clearly seen from on-chain data as well. The dominant assets in failed transactions were Rune and BTC, with a sharp increase in volume during the collapse. The data shows little to no failed transactions before the collapse, while during the breakdown, volumes of failed transactions spiked to a higher order of magnitude than overall transaction volumes that succeeded during the same time period.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

6.2 Terra User IBC and Smart Contract Interaction

In this section, the interaction of users of the Terra network with smart contracts on Terra or with other IBC-enabled blockchains will be discussed. The flow of assets to other parts of the Cosmos Ecosystem paints a good picture of how Terra users are engaging with other blockchains. Users can also be filtered out for those who also interacted with Thorchain. The interaction with smart contract gives an insight into why users used Terra in the first place and the exclusion of non-Thorchain users aims at finding differences in user behaviour between users who already have cross-chain experience and those who do not.

6.2.1 IBC Transactions

The second cross-chain technology that was analysed to show the asset flow of users is IBC. For this analysis, the only assets used in IBC that were analysed were Luna and UST. Other assets that were transferred to other blockchains through IBC were insignificant in transfer volume compared to that of UST and Luna.

When looking at users of the Terra network in general, Figures 6.10 and 6.11 show the asset flow from Terra to other IBC-enabled blockchains. Figure 6.10 shows that shortly before the collapse, there was a strong rise in IBC transfers. Osmosis is by far the most frequent destination with the most volume, followed by Axelar, Crescent Network and Secret Network, see Figure 6.11. Osmosis is the largest decentralized exchange on the Cosmos Ecosystem as of writing this thesis. Its main utility for users is the exchange of tokens and coins and providing liquidity. The exchange is vital as some coins from blockchains in the Cosmos Ecosystem are not available on centralized exchanges but only on decentralized exchanges in the Cosmos Ecosystem itself. Users who want to use one of these blockchains first have to acquire some of their native tokens in order to pay transaction fees on the network. Osmosis provides this service by offering swap pairs and IBC relay functionality to send the coins off to their native chain.

The asset flow of Luna to other IBC-enabled blockchains is similar to that of UST transfers, as can be seen from Figure 6.13, which shows the relative asset flow of Luna through IBC. The most obvious difference is that Secret Network is not as dominant with Luna transfers as it was with UST transfers.

The collapse of the cryptocurrency Luna can be seen from the absolute asset transfer over time visualized in Figure 6.12. In early May, the IBC transfers shot up to unprecedented levels. This has two reasons, with the first being the collapse of the currency itself and users trying to exit their exposure to Luna, the second is that since the graph is denominated in Luna and Luna itself was crashing meaning the price was going down dramatically, a lot more Luna was available quickly which could potentially inflate the numbers in Figure 6.12. The relative asset flow over

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

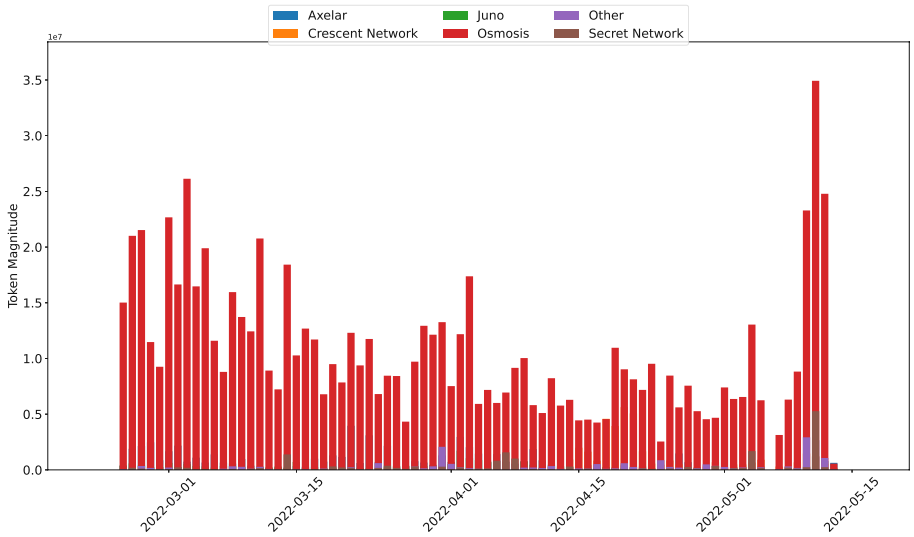

Figure 6.10: Asset flow over time denominated in UST of Terra users using IBC

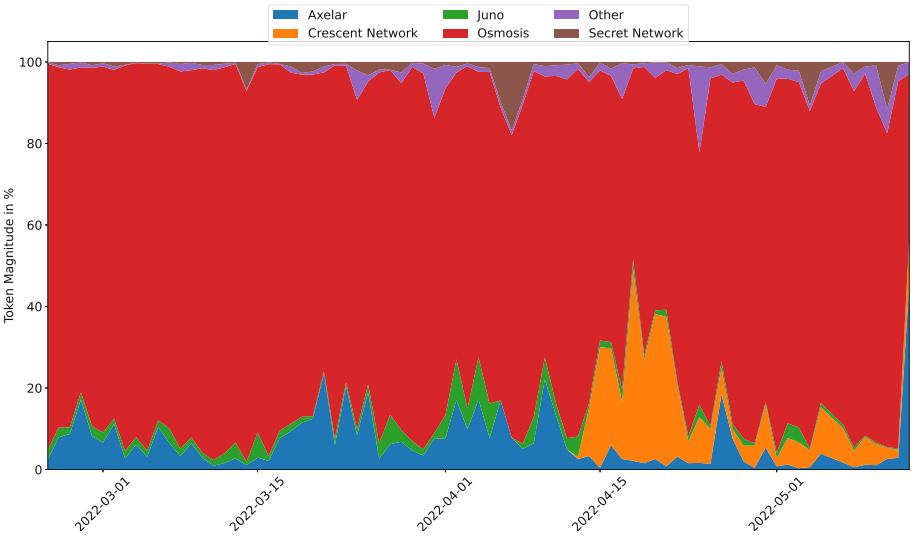

Figure 6.11: Relative asset flow over time denominated in UST of Terra users using IBC

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

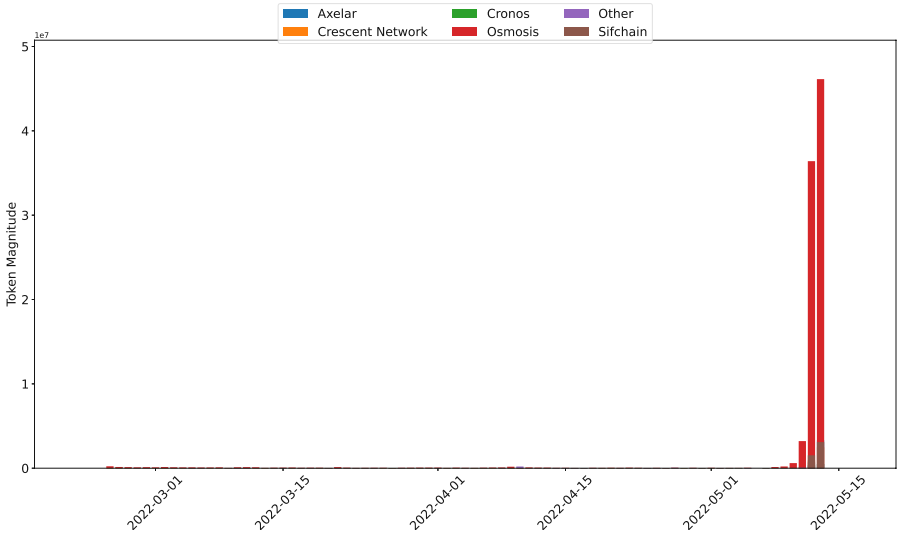

Figure 6.12: Asset flow over time denominated in Luna of Terra users using IBC

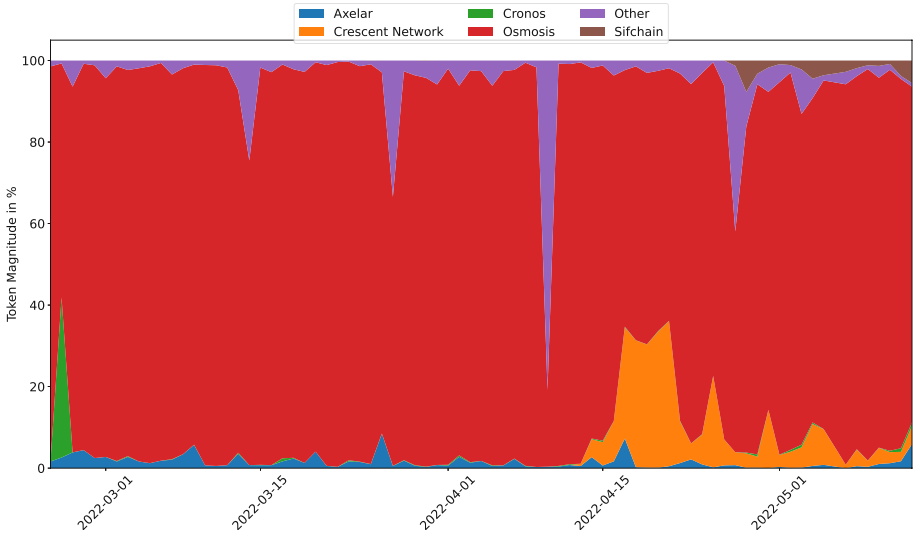

Figure 6.13: Relative asset flow over time denominated in Luna of Terra users using IBC

time denominated in Luna can be seen from Figure 6.13. As with UST, it shows that Osmosis stayed dominant throughout the observed time period.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

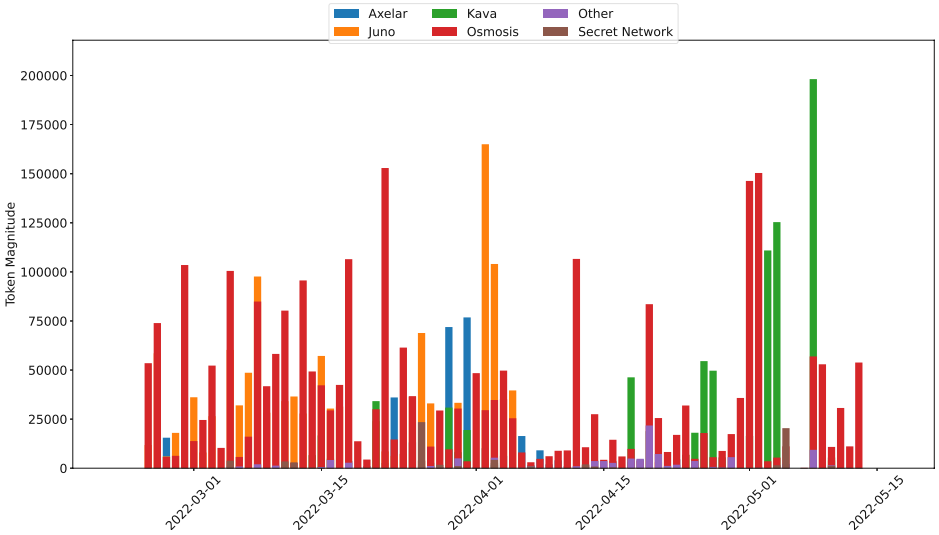

Figure 6.14: Asset flow over time denominated in UST of Terra and Thorchain users using IBC

Figures 6.14,6.16 and 6.16 show absolute and relative asset flow of UST and Luna of Terra accounts that have also made use of the Thorchain swap service.

Users of the Terra network who are using IBC and have also made use of the Thorchain swap service show slightly different behaviour in their IBC transfers. The transfers of UST show a strong dominance of Osmosis and Juno, see Figure 6.14, until the beginning of May when the Kava network gained dominance, which suggests that users wanted to transfer their UST to an Ethereum bridge since the Kava network is mainly used for transferring funds between the Cosmos Ecosystem and Ethereum. A similarly dramatic picture is visible from Thorchain users who transferred Luna, towards the end of the Terra network, as can be seen from Figures 6.15 and 6.16. The major difference to UST transfers is that Crescent Network was the predominant exit point in the last days of the Terra network, while it was barely used prior to the crash, as it is visualized in 6.16. Prior to the crash, Axelar and Secret Network had much larger shares of the overall volume of Luna being sent.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

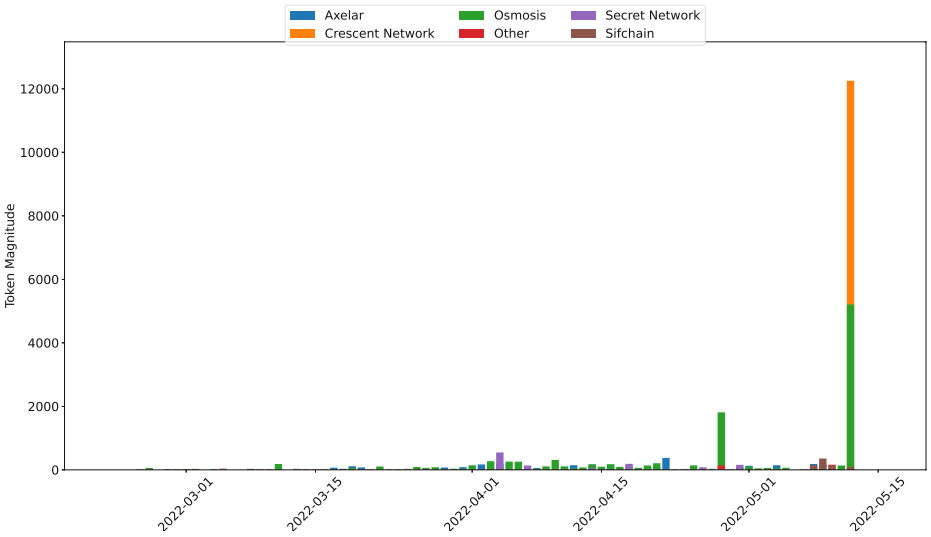

Figure 6.15: Asset flow over time denominated in Luna of Terra and Thorchain users using IBC

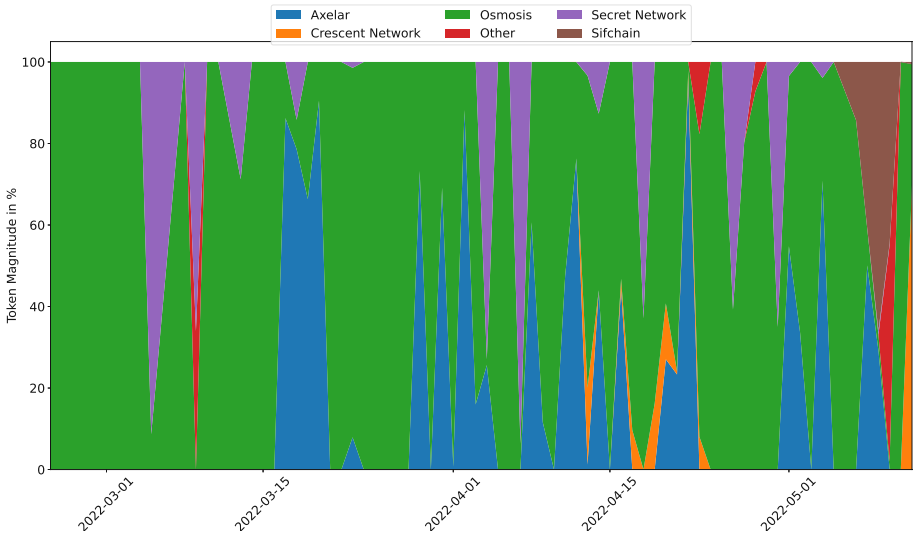

Figure 6.16: Relative asset flow over time denominated in Luna of Terra and Thorchain users using IBC

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

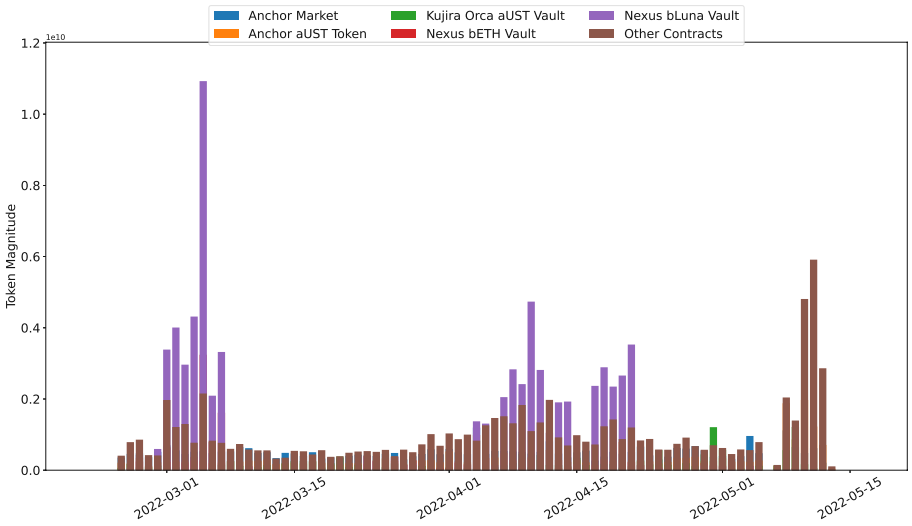

Figure 6.17: Inflow of contract interaction of UST over time on the Terra network

6.2.2 Contract Interaction

To answer the research question *RQ2* regarding the flow of assets between accounts and smart contracts on Terra before and during the collapse of the network, contract interactions were analysed. By looking at the smart contract interaction, it becomes more clear why users transfer assets to the Terra network and therefore the Cosmos Ecosystem from legacy chains. The analysis took the five largest smart contracts by accumulative inflow or outflow volume and looked at their respective in and outflows over time.

The contract interaction of assets denominated in UST is shown in Figures 6.17 and 6.18. Four different smart contracts dominate smart contract interaction. They are associated with Anchor Protocol, Nexus, Kujira Orca and Terra swap. The analysis also shows that in and outflows to and from smart contracts on the Terra network seem to be similar in terms of addresses where assets are transferred between.

As can be seen from Figure 6.17 addresses interaction with the *Nexus bLuna Vault* show three different spikes along the analysed time period with the largest being in early March. A similar pattern is visible in outgoing transactions, see Figure 6.18.

Whereas the five largest smart contracts that were involved in UST transactions were identifiable by looking at the block-explorer of Terra [1], two of the 5 largest smart contracts where Luna transfers were used could not be identified.

[1] https://finder.terra.money/

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

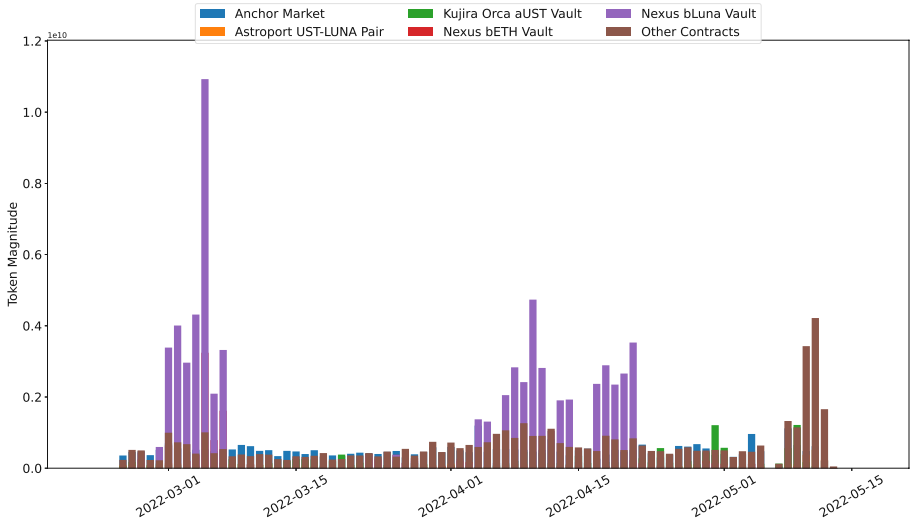

Figure 6.18: Outflow of contract interaction of UST over time on the Terra network

When looking at the asset flow of smart contract interaction denominated in Luna, it is clear that there is a difference in smart contracts that are being used with UST and Luna.

Figures 6.19, 6.20 show the absolute and relative inflow of Luna to smart contracts on the Terra network. Transfers to smart contracts inside the Terra network using Luna were strongly dominated by Astroport, a decentralized exchange on Terra, suggesting that Luna was more so used for trading activities than UST, see Figures 6.19 and 6.20. In the days of the collapse of the network the largest swap on Terra, Terra Swap, saw the most numbers of tokens being transferred to it, suggesting users wanted to lose exposure to the asset.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

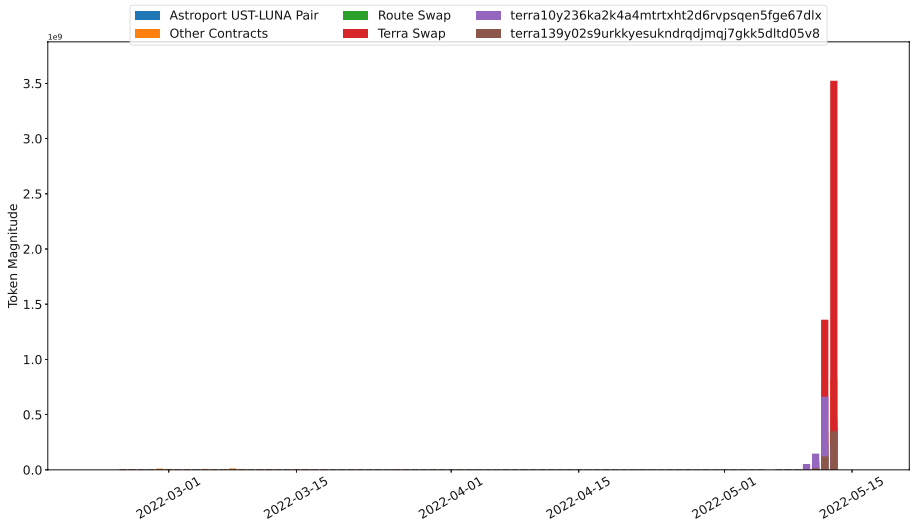

Figure 6.19: Inflow over time of contract interaction of Luna over time on the Terra network

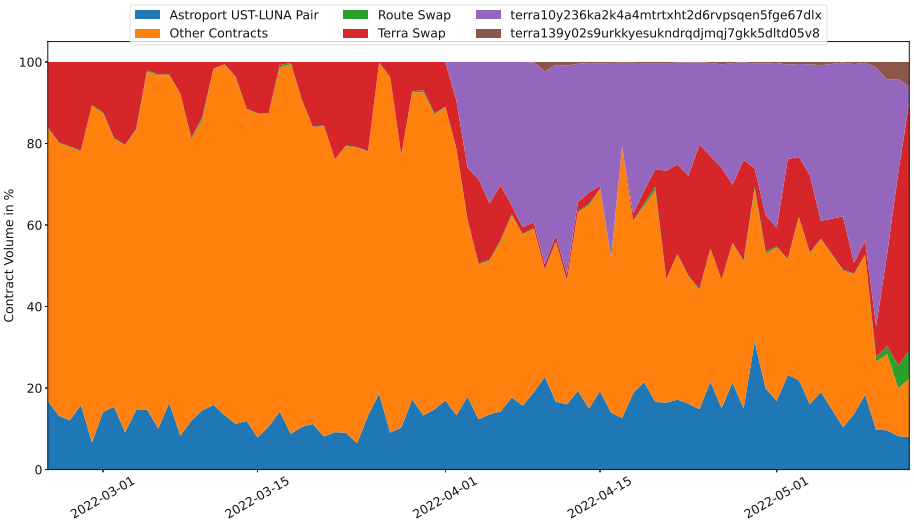

Figure 6.20: Relative inflow over time of contract interaction of Luna on the Terra network

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

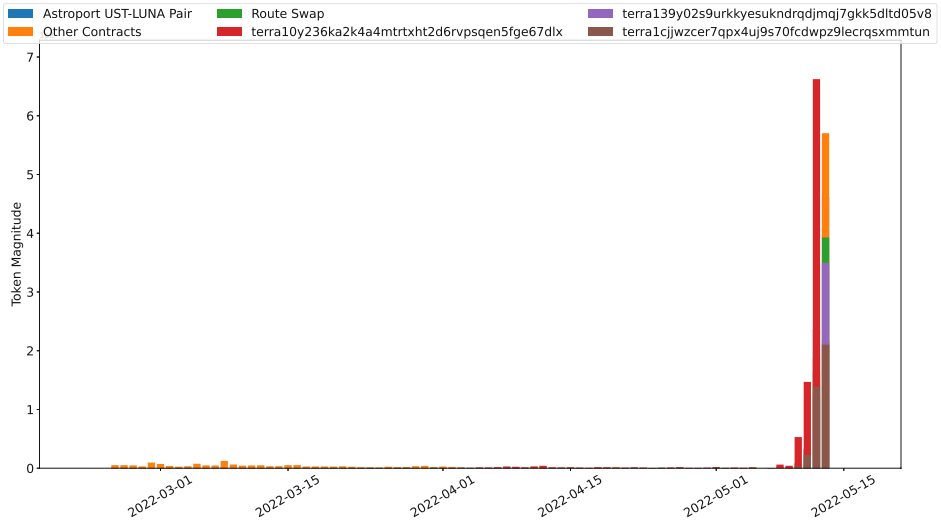

Figure 6.21: Outflow over time of contract interaction of Luna over time on the Terra network

Figures 6.21, 6.22 show the absolute and relative outflow of Luna to smart contracts on the Terra network. What is notable with Luna asset flow is that outflows from smart contracts are much more heavily dominated by the Terra Swap than the inflows as depicted in Figures 6.21 and 6.22. The outflow of smart contract funds by Luna transfers shows again the dramatic scenario towards the crash of the Terra network. In absolute volumes, see Figure 6.21 one can see that the dominant outflow from smart contracts was from UST-Luna pairs and swapping smart contracts. The exchange between UST and Luna has a number of implications. For one, arbitrage trading could have been the motivator while UST was off its pegg for users who still believed in the recovery of the network or users might also want to take the opportunity of a low price of the Luna token and buy it with UST reserves.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

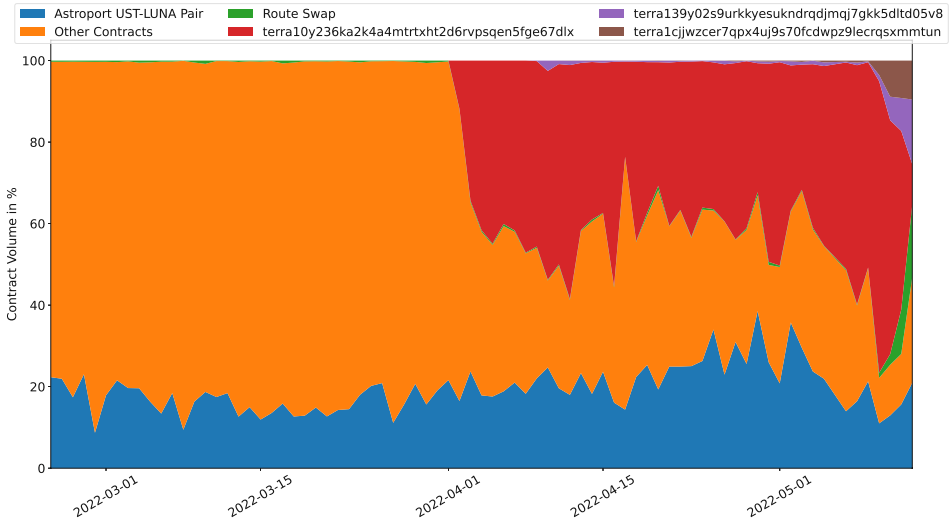

Figure 6.22: Relative outflow over time of contract interaction of Luna on the Terra network

A notable difference in the interaction between addresses and smart contracts can be seen for addresses that were also involved in Thorchain transactions. Figures 6.23, 6.24,6.25 and 6.26 show absolute and relative in and outflow of UST to and from smart contracts for Thorchain users.

They were particularly interested in transferring their funds to the Anchor Protocol as depicted in Figure 6.23 and 6.24, suggesting that users were primarily swapping BUSD for UST to then receive the high yield of $\tilde{2}0\%$ offered by Anchor Protocol. Also, outgoing transactions were heavily dominated by the Anchor Protocol as shown by Figure 6.25 and 6.26, although the addresses used for outgoing transactions are different to the incoming transactions.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

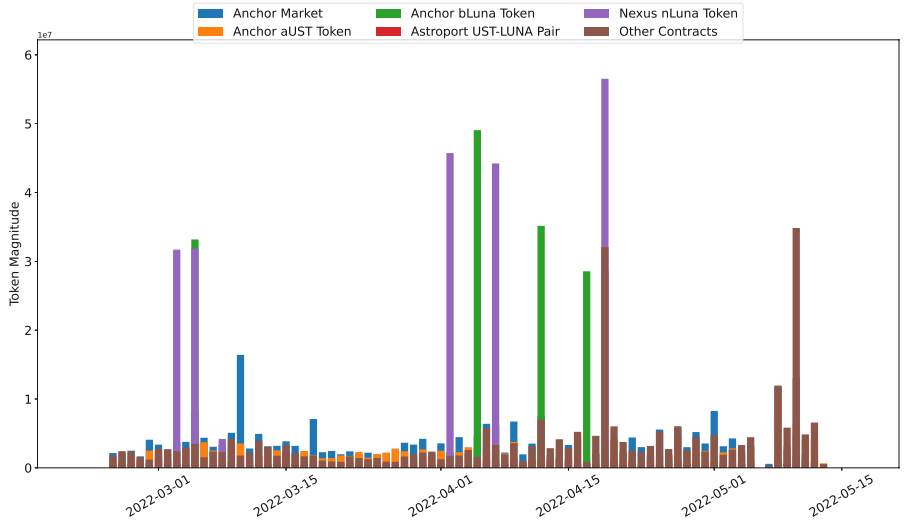

Figure 6.23: Inflow over time of contract interaction of Thorchain and Terra users denominated in UST on the Terra network

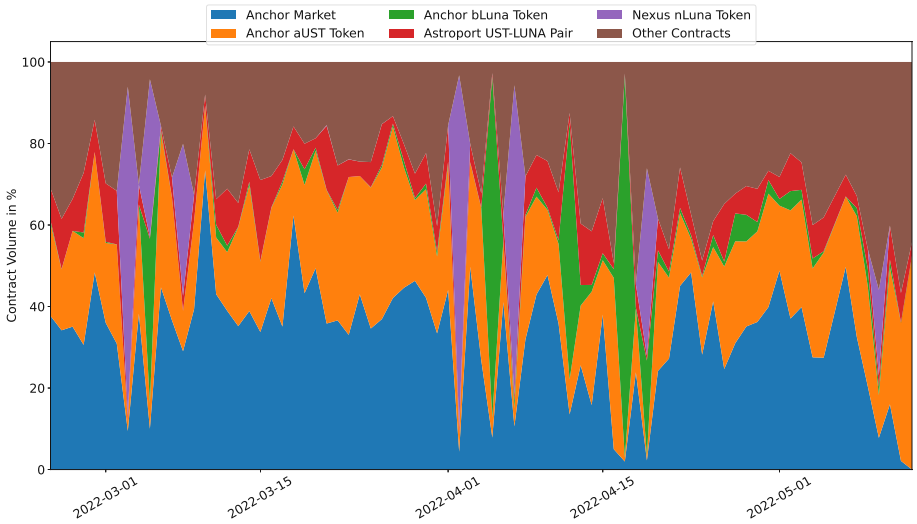

Figure 6.24: Relative inflow over time of contract interaction of Thorchain and Terra users denominated in UST on the Terra network

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

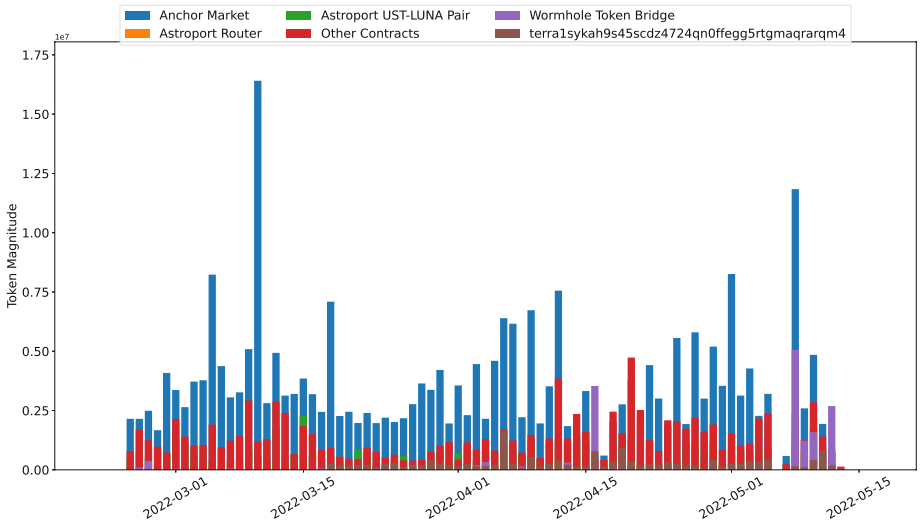

Figure 6.25: Outflow over time of contract interaction of Thorchain and Terra users denominated in UST on the Terra network

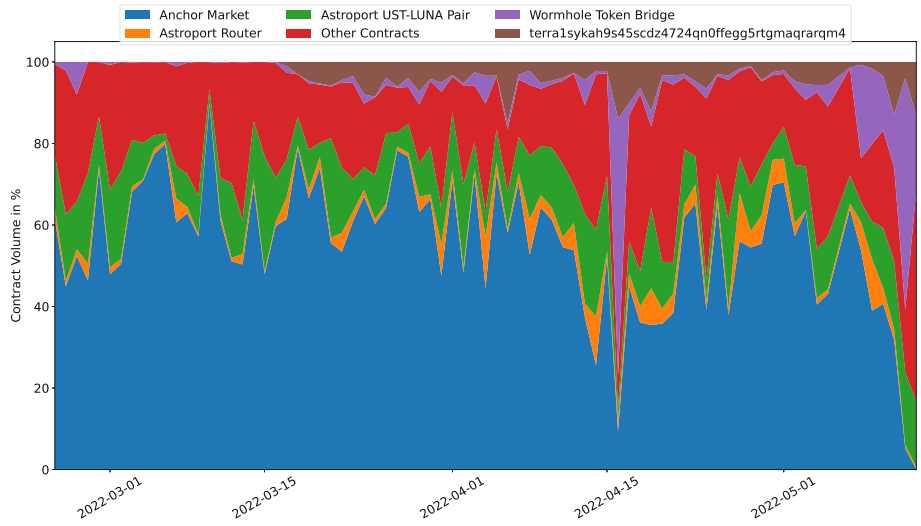

Figure 6.26: Relative outflow over time of contract interaction of Thorchain and Terra users denominated in UST on the Terra network

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

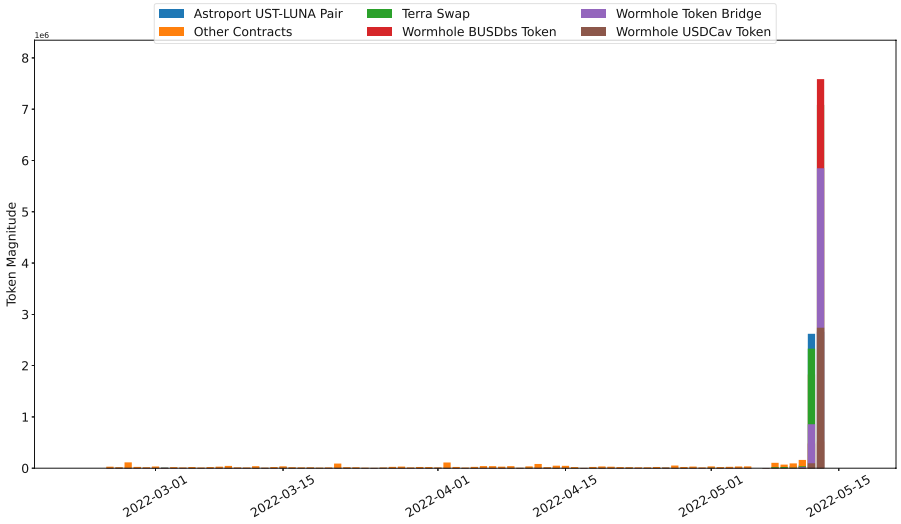

Figure 6.27: Inflow over time of contract interaction of Thorchain and Terra users denominated in Luna on the Terra network

Figures 6.27, 6.28,6.29 and 6.30 show absolute and relative in and outflow of Luna to and from smart contracts for Thorchain users.

Thorchain users who were using their Luna assets in smart contract interactions are particularly interested in bridging their tokens to other blockchains with the Wormhole bridge, as can be seen from Figures 6.27 and 6.28. Also, outflow from smart contracts using Luna, see Figures 6.29 and 6.30, was heavily skewed towards the bridging service Wormhole, but only towards the collapse of the network. Until May 2022 most inflow was actually dominated by other contracts than the five largest ones by inflow volume. This shows how drastic the volumes in the days and hours of the crash were so that they skew the accumulative volume of almost three months towards a few smart contracts associated with swapping and cross-chain functionality.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

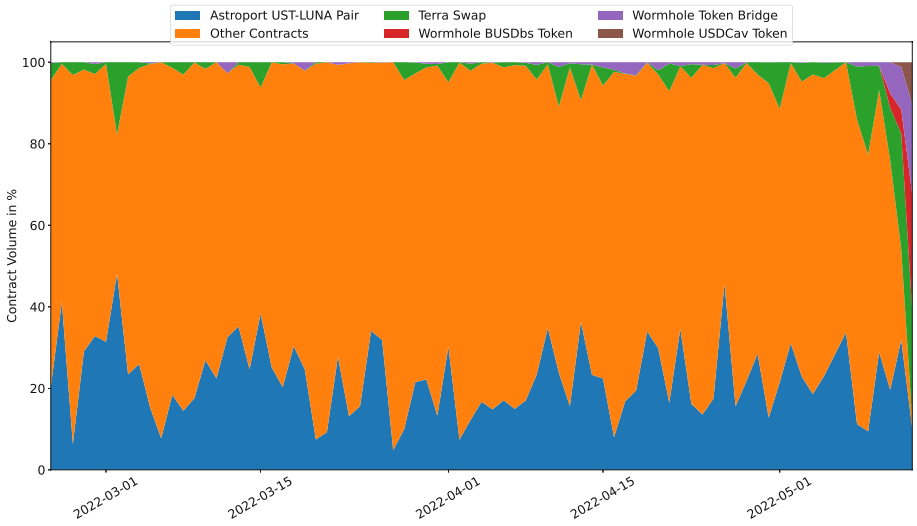

Figure 6.28: Relative inflow over time of contract interaction of Thorchain and Terra users denominated in Luna on the Terra network

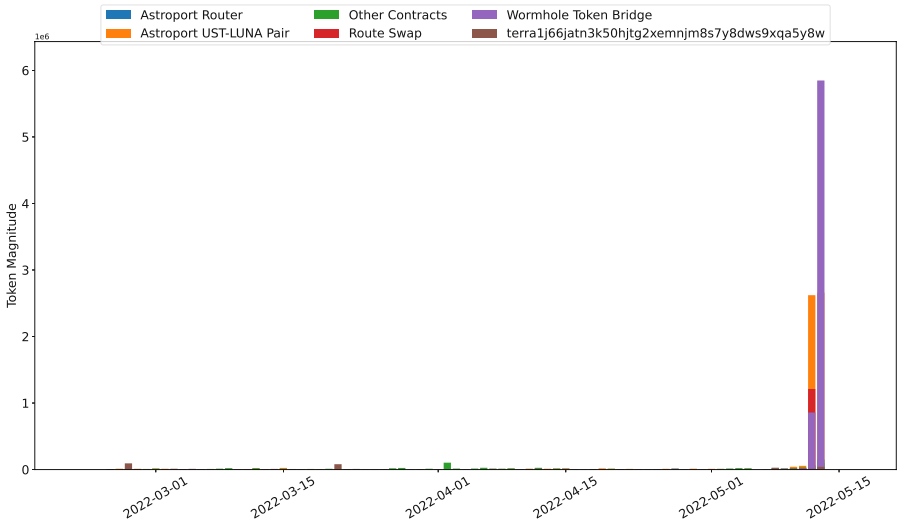

Figure 6.29: Outflow over time of contract interaction of Thorchain and Terra users denominated in Luna on the Terra network

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

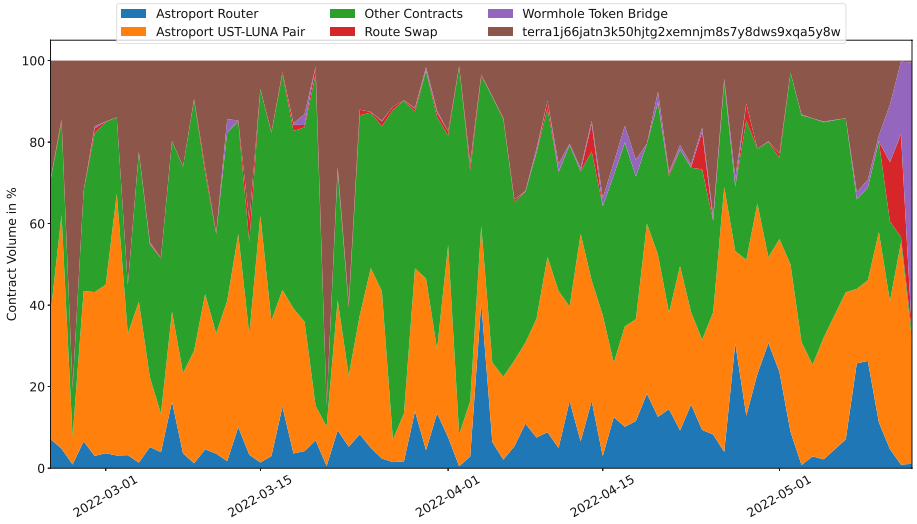

Figure 6.30: Relative outflow over time of contract interaction of Thorchain and Terra users denominated in Luna on the Terra network

6.2.3 Summary

In terms of cross-chain transactions, Terra users were predominantly using IBC to connect to the decentralized exchange Osmosis, which was especially dominant during the collapse of the network as users were trying to exchange their declining assets into more stable cryptocurrencies. Users who have already had experience with cross-chain technologies like Thorchain were more inclined to use cross-chain technologies offered in the Cosmos Ecosystem.

The smart contract interaction of Terra users on the network itself was heavily dominated by Nexus and the Anchor Protocol, which are both applications of decentralized finance. Especially the latter recorded massive outflows of UST and Luna during the collapse of the network as UST started to depegg. From the data, it is visible that Thorchain users were especially interested in the Anchor Protocol, which is in line with the assumption made in the previous section as to why the stable swap between BUSD and UST was the most prevalent swap pair on Thorchain across time.

6.3 Decentralization of Cross-Chain Technologies

To answer research question *RQ3* in this section, the route described in Section 4.1 will be analysed on potential centralization issues.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

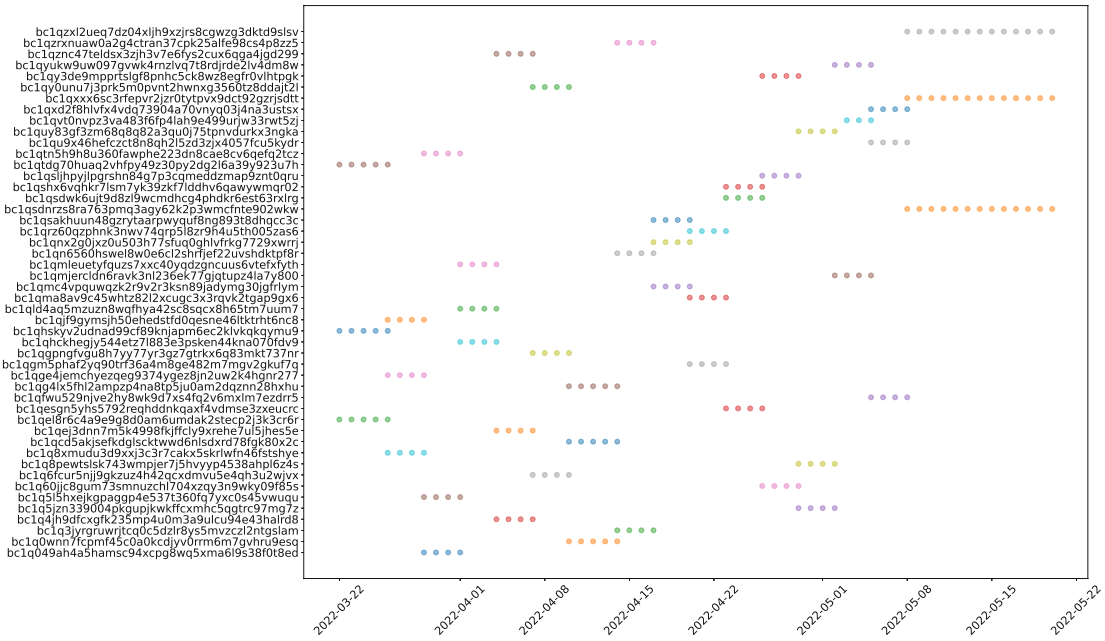

Figure 6.31: Asgard vault addresses for BTC over time

6.3.1 Thorchain

Thorchain is a blockchain that uses independent nodes to transform and broadcast incoming transactions from chains that they are connected to, and Thorchain supports it. Due to the use of memos to derive context from transactions, they are easily traceable. Incoming transactions are identifiable by the address the Asgard vault has on the respectively connected blockchain. The same is true for outgoing transactions with Yggrdasil vaults. Outgoing transactions are furthermore associated with their corresponding incoming transactions, which makes it possible to track asset flows from one blockchain to another through Thorchain.

As described in Section 4 at the current number of nodes there are three different Asgard vaults active at the same time. For security reasons, these vaults are changed in periodic intervals. To validate this behaviour and show the traceability of Asgard vault addresses over time, on-chain data directly from Thorchain was used to visualize the rotation of Asgard vault addresses over time. In Figure 6.31 one can see the Asgard vault addresses for the Bitcoin network over time. It is clearly visible that there are always three addresses active at the same time, and that they change addresses periodically. By changing the Asgard vault addresses and having more than a single vault, centralization and thus single point of failure is less of an issue should a vault be compromised.

In terms of decentralization of the Thorchain blockchain itself, the most important

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

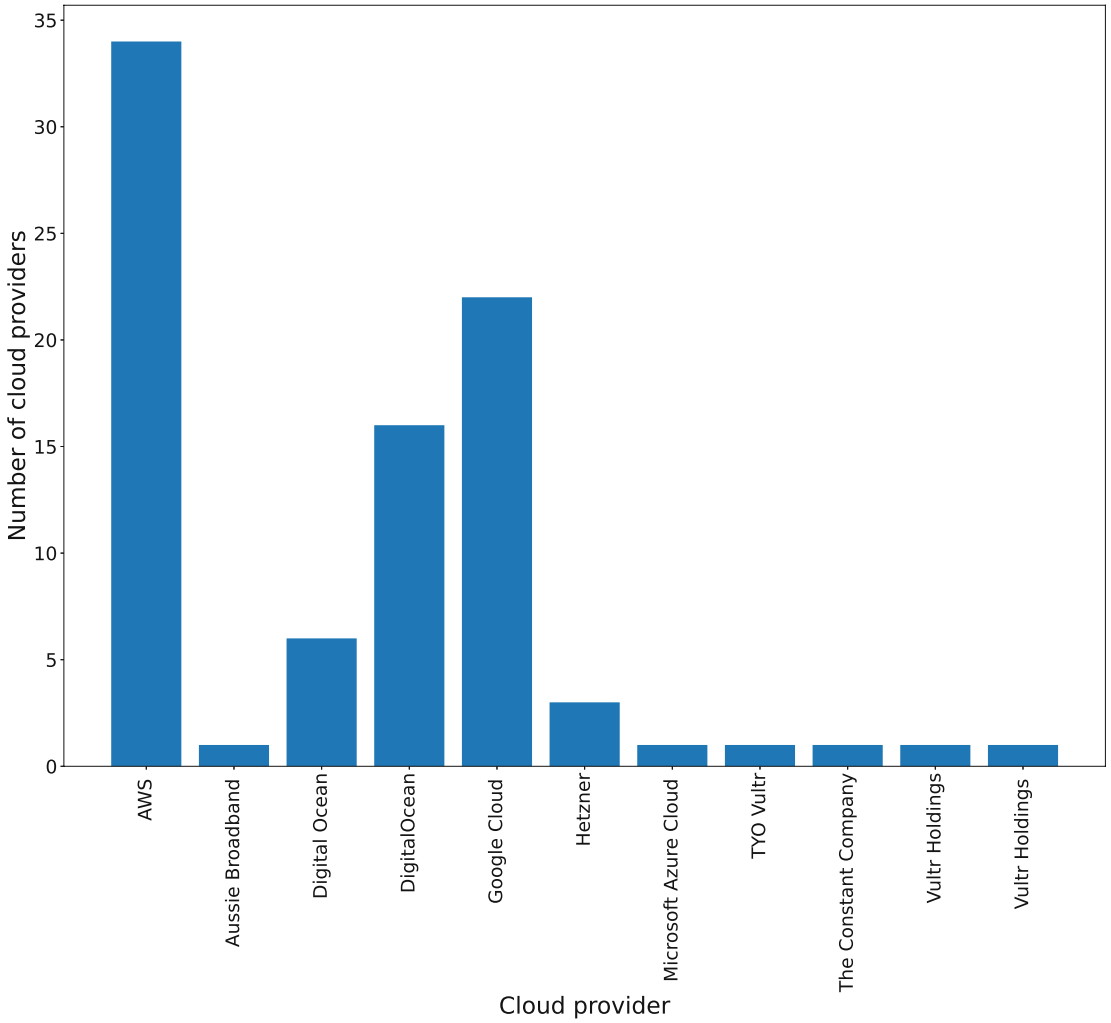

Figure 6.32: Cloud providers used for Thorchain nodes

factor to look at are node operators. The node operators are anonymous and do not know each other based on data from Thorchain. It is therefore not possible to tell whether the same entity runs some nodes. What can be gathered from Thorchain however, is what cloud provider is used to running the nodes and subsequently in which geographical region the nodes are run from. This is visible in Figures 6.32 and 6.33. From Figure 6.32 one can see that centralization is an issue when it comes to cloud providers used as only a handful of relayers are responsible for most IBC transactions in the connection between Osmosis and Cosmos Hub.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

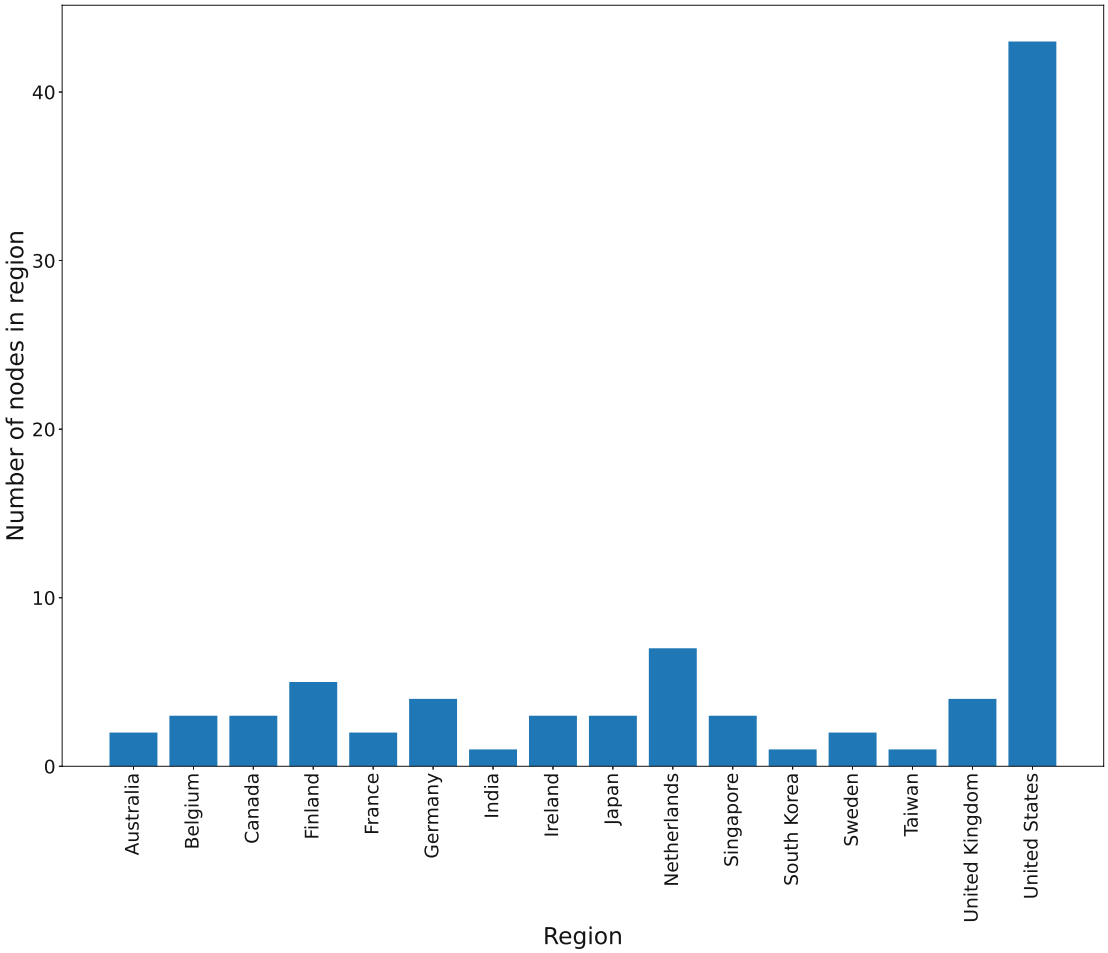

Figure 6.33: Geographical location of node

6.3.2 Relayers

According to the largest blockchain scanner of the Cosmos Ecosystem, Mint Scan, at the time of writing this thesis, there are 616 relayers over 39 chains. When looking at the largest entity in terms of IBC volume, Osmosis, the number of relayers amounts to 67 relayers out of which 27 are active. The distribution of the volume processed by relayers between Osmosis and Cosmos Hub, the largest of the connections that Osmosis has, can be seen in Figure 6.34. It is clear that most transactions are handled by only a few relayers which raises concerns about the decentralization of the relayer system.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

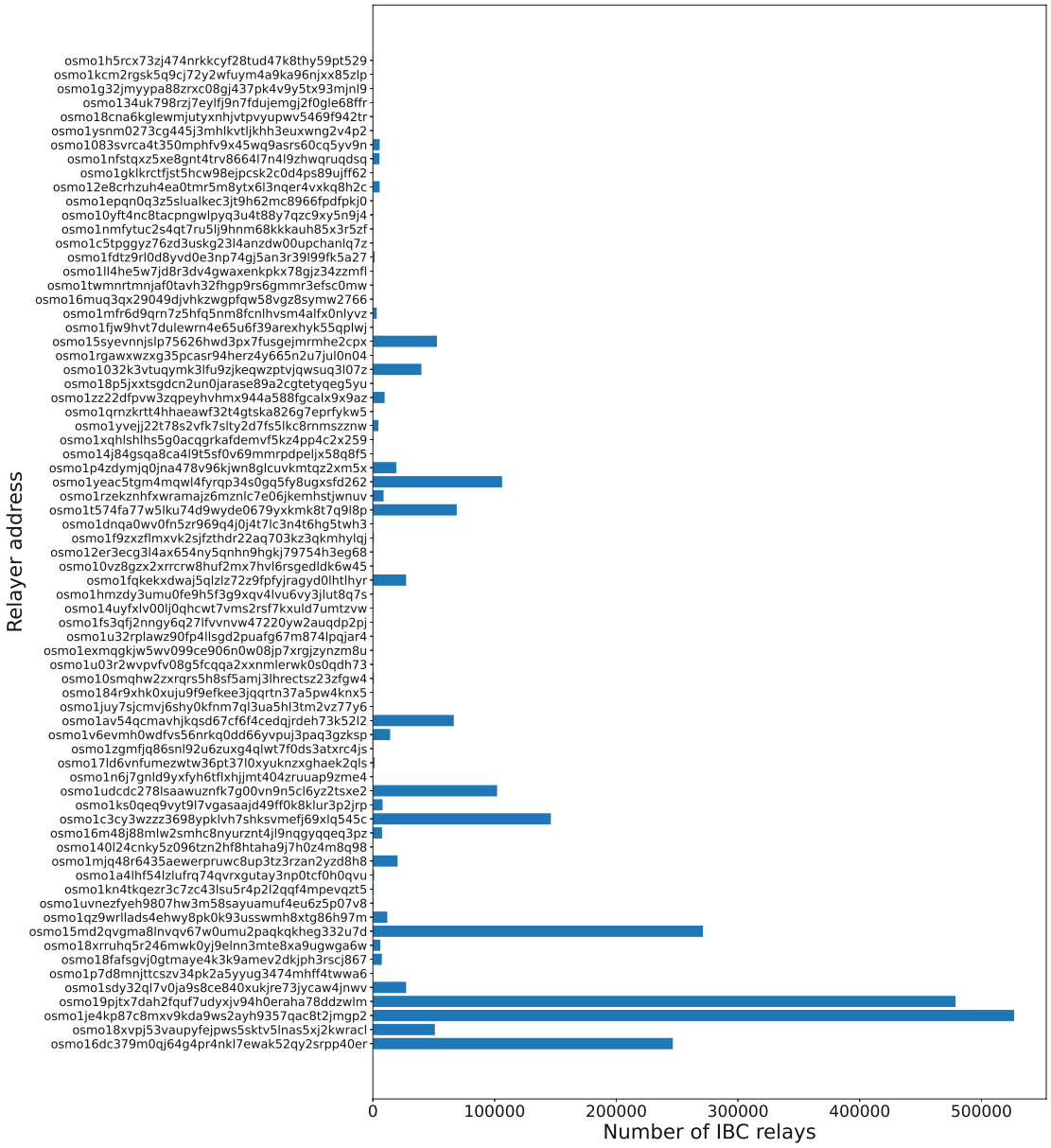

Figure 6.34: Distribution of relayers by number of successful relays on the Osmosis blockchain to the Cosmos Hub

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

6.3.3 Blockchain Decentralization

The cosmos ecosystem evolves around the idea of having a sovereign blockchain built for specific use cases and dApps and then connecting them to the other blockchains via IBC. The interconnecting component is the decentralized exchanges utilizing the IBC to connect the different blockchains of the cosmos ecosystem together. The largest decentralized exchanges using IBC are the Cosmos Hub and Osmosis. So, when evaluating the degree of decentralization of the cosmos ecosystem, one has to look at the level of decentralization of each chain and the decentralized exchanges connecting them together. Due to the fact that multiple chains are run in parallel, they are so far decentralized as the number of validators of each chain is large enough and validators vary from chain to chain. Osmosis and Cosmos Hub currently have 118[2] and 150[3] validators respectively. One has to point out that several validators found on one chain can also be found on another, and there is no direct way to check whether validators run nodes on several blockchains in the ecosystem using a different identification.

In comparison, popular proof of stake-based blockchains like Polkadot, Cardano, Terra, and Solana have 297[4], 1893[5], 130 [6] and 1651 [7] validators at the time of writing this thesis.

6.3.4 Summary

The analysis shows that along the described route of transactions there are issues of centralization. At the consensus mechanism layer, Thorchain and Terra have fewer validators than other blockchains like Solana or Cardano and those validators are prone to be centralized in terms of who owns the hardware necessary to offer the validator services. Most of them are run by a few cloud computing providers, which is a concern for potential centralization. Furthermore, the Thorchain blockchain is centralized geographically, with the overwhelming majority being based in the USA. The Asgard vault addresses are changed in regular intervals that are traceable across time, with three vaults being active at the same time to reduce the risk of taking down the entire service by compromising a single Asgard vault. While the number of IBC relayers is greater than the number of validators in most Cosmos Ecosystem based blockchains, the distribution of the number of transactions which they serve is highly centralized, with only three relayers servicing almost all cross-chain transactions in the case of the Cosmos Hub to Osmosis connection.

[2] https://wallet.keplr.app/#/osmosis/stake
[3] https://wallet.keplr.app/#/cosmoshub/stake
[4] https://polkadot.js.org/apps/#/staking
[5] https://adapools.org/
[6] https://docs.terra.money/docs/full-node/manage-a-terra-validator/faq.html#: :text=The%20active%20validator%20se
[7] https://solana.com/validators

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 7

Discussion & Conclusion

Since Bitcoin launched blockchain technology and digital asset transactions, the blockchain sector has experienced tremendous human and monetary capital influx. Different sectors of the contemporary economy are looking at using this technology to revolutionize our current monetary system. Decentralized finance is one of the first areas to utilize blockchain technology. From exchanges to insurance, banking, lending and borrowing, custody, and other financial sectors, blockchain is being used to cut out the middleman, increase inclusion and participation and decentralize control over the industry.

Many research and development organizations have worked to further blockchain technology. They often disagree on which component of the distributed system is more important: privacy, security, speed, or scalability. Therefore, in recent years, several initiatives have endorsed their own blockchains. With so many blockchains to select from, it's challenging for people or institutions to decide which is ideal for them and whether acceptance will grow in their area. This created the demand for blockchain interoperability, connecting different blockchains to one another and benefiting from their respective focus on technology.

One blockchain that was particularly successful in attracting users and capital was Terra, which had a catastrophic meltdown in early May 2022. It was well known for its ecosystem of decentralized finance and was embedded in the Cosmos Ecosystem, the largest internet of blockchains focusing on cross-chain functionality. The fact that Terra was connected to many other blockchains, older and more recent ones, provides a unique opportunity to investigate a collapse of a major blockchain from the perspective of cross-chain exchange technologies to see where assets were flowing before and at the time of the collapse, what technologies were used and how the event unfolded on-chain.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

This thesis thus aims at providing a view of the cross-chain and on-chain activities of the Terra network in terms of where assets were flowing, what applications users interact with and where assets were moving during the collapse. Furthermore, an investigation on the state of decentralization of these technologies is performed.

7.1 Discussion of research questions

Three research questions in the field of asset flow and traceability were introduced in Section 1. Here, concrete answers to these questions are summarized.

RQ1 **What assets were used in cross-chain asset transfers between Terra and legacy chains before and during the collapse of the network?**
The stablecoin BUSD on the Binance blockchain became the most important asset for doing cross-chain swaps across blockchains such as Bitcoin, Ethereum, Binance Coin, and Litecoin. This remained the case even during the dismantling of the Terra network. Binance, with its derivatives of Bitcoin and Ethereum, was the most important swap partner for both Luna and UST when it came to the Thorchain Swap service. The fear that was induced by the collapse of the Terra network can be readily visible from on-chain data as well, as seen by failed transactions that were sent from the Terra network to Thorchain. Rune and Bitcoin were the most common assets involved in unsuccessful transactions, and there was a significant rise in volume during the crash. According to the data, there were virtually no unsuccessful transactions prior to the breakdown; however, during the breakdown, the number of unsuccessful transactions skyrocketed to a greater order of magnitude than the overall volume of transactions that were successful during the same time period.

RQ2 **What is the flow of assets between accounts and smart contracts on Terra before and during the collapse of the network ?**
In terms of cross-chain transactions, Terra users primarily utilized IBC to connect to the decentralized exchange Osmosis. This particular exchange was especially dominant during the collapse of the network when users were attempting to exchange their depreciating assets into more stable cryptocurrencies. Users who already have some familiarity with cross-chain technology, such as Thorchain, are more likely to make advantage of the cross-chain options provided by the Cosmos Ecosystem.

Nexus and the Anchor Protocol, which are both applications of decentralized finance, substantially dominated the smart contract interaction of Terra users on the network itself. Smart contracts highly dominated this interaction. Especially the latter reported significant outflows of UST and Luna as the network was collapsing and UST was beginning to depegg. Based on the data, it is clear that

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

users of Thorchain were particularly interested in the Anchor Protocol. This finding is consistent with the assumption that was made in the previous section regarding the reason the stable swap between BUSD and UST was the most common swap pair used on Thorchain over the course of time.

RQ3 **How decentralized are cross-chain technologies that are connected to Terra?**

According to the findings of the investigation, there are centralization problems all along the path of transactions that was detailed. At the consensus mechanism layer, Thorchain and Terra have fewer validators than other blockchains like Solana or Cardano. Additionally, those validators have a higher propensity to be centralized in terms of who controls the hardware required to give the validator services. The fact that just a few companies control the majority of them is cause for alarm over the possibility of further centralization. Additionally, the geographical distribution of nodes on the Thorchain blockchain is highly concentrated, with the United States constituting the vast majority of these locations. The addresses of the Asgard vaults are rotated at regular intervals in such a way that their history can be followed, and there are three vaults operational at the same time. This is done to limit the likelihood that a single compromised Asgard vault would bring the whole service to a halt. Even though the number of IBC relayers is higher than the number of validators in the majority of Cosmos Ecosystem-based blockchains, the distribution of the number of transactions that they service is highly centralized. For example, in the case of the Cosmos Hub to Osmosis connection, only three relayers service almost all cross-chain transactions. This is because the Cosmos Hub connects to Osmosis.

7.2 Limitations

This work has several limitations that are pointed out in this section. Data were retrieved from the public blockchains Terra and Thorchain. The collapse of the Terra network is only interpreted from the perspective of the cross-chain technologies IBC and Thorchain. No analysis of on-chain decentralized exchanges like Terra Swap or centralized exchanges was done, which may show different results to those gathered from the insight from cross-chain decentralized exchanges.

The Terra network stopped block production at various points during the collapse and once it resumed a lot of liquidity and funds were already removed from the blockchain. The data extracted from the Terra network thus does not show the entirety of the situation around the collapse of the network.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

The analysis of the smart contract interaction does not show the mechanisms of each smart contract. It is possible that larger systems such as lending protocols or exchanges use multiple smart contracts. Therefore, the interpretation of funds flowing in and out of certain smart contracts that belong to a larger suite of smart contracts that form one of these systems is limited.

While most large smart contract addresses by transaction volume on the Terra network could be identified, it is less clear what entities are controlling the addresses that are not smart contracts. The interpretation of the actions of these addresses in relationship to the collapse of the network is therefore limited to what can be seen from their transactions on Terra.

7.3 Future work

In this section, possible extensions and improvements to the analysis of asset flow and traceability are outlined.

While Thorchain is at the date of writing the largest cross-chain decentralized exchange which enables native swaps between legacy chains and the Cosmos Ecosystem, it is not the only technology which aims at solving the challenge of cross-chain functionality. There have been a number of other promising cross-chain projects such as Axelar, Wormhole or Multichain. Analysing the collapse of the Terra network from these other exchanges and bridges may reveal a different behaviour of users or insight into events and activities that occurred during the crash that were not visible on the Thorchain swap or IBC transfers.

This thesis focused predominantly on the flow of assets, the interaction of users with cross-chain and on-chain applications, and how they changed during the crash of the Terra network. A potential future work may conduct a deeper investigation on specific user addresses which were involved in large and frequent transactions with some smart contracts on Terra, especially during its collapse, or amounted to large sums of cross-chain transfers in the same time period.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

List of Figures

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

List of Tables

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Bibliography

[1] AminCad. *Market share of Ethereum-based tokens grows to 91%*. May 2018. url: https://medium.com/@amincad/market-share-of-ethereum-based-tokens-grows-to-91-fdefadfd9f6e.

[2] Luke Anderson et al. "New kids on the block: an analysis of modern blockchains". In: *CoRR* abs/1606.06530 (2016). arXiv: 1606.06530. url: http://arxiv.org/abs/1606.06530.

[3] Angelo Aspris et al. "Decentralized Exchanges: The 'Wild West' of Cryptocurrency". In: *SSRN Electronic Journal* (Oct. 2020). doi: 10.2139/ssrn.3717330.

[4] *Ethereum Whitepaper*. url: https://ethereum.org/en/whitepaper/.

[5] Gmaxwell. "CoinJoin: Bitcoin privacy for the real world". In: 2013. url: https://bitcointalk.org/index.php?topic=279249.0.

[6] Geoff Goodell and Tomaso Aste. "Can cryptocurrencies preserve privacy and comply with regulations?" In: *Frontiers* (Jan. 1AD). url: https://www.frontiersin.org/articles/10.3389/fbloc.2019.00004/full.

[7] Abraham Hinteregger and Bernhard Haslhofer. "An Empirical Analysis of Monero Cross-Chain Traceability". In: (Dec. 2018).

[8] Lysanne Jurjens, Jeroen van der Kroft, and Daphne Sweers. "Unleashing cryptocurrency potential – four ways to increase institutional adoption". In: *EY* (Dec. 2021). url: https://www.ey.com/en_nl/banking-capital-markets/unleashing-cryptocurrency-potential-4-ways-to-increase-institutional-adoption.

[9] George Kappos et al. "An Empirical Analysis of Anonymity in Zcash". In: *Proceedings of the 27th USENIX Conference on Security Symposium*. SEC'18. Baltimore, MD, USA: USENIX Association, 2018, pp. 463–477. isbn: 9781931971461.

[10] Jae Kwon and Ethan Buchman. "Internet of blockchains". In: *Cosmos Network* (). url: https://v1.cosmos.network/resources/whitepaper.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

[11] Pascal Lafourcade and Marius Lombard-Platet. “About blockchain interoperability”. In: *Information Processing Letters* 161 (2020), p. 105976. issn: 0020-0190. doi: https://doi.org/10.1016/j.ipl.2020.105976. url: https://www.sciencedirect.com/science/article/pii/S0020019020300636.

[12] “Layer 1 solutions”. In: *RugDoc Wiki* (). url: https://wiki.rugdoc.io/docs/layer-1-solutions/.

[13] Legal Counsel at Interstellar Lindsay X. Lin and Stellar Development. “Deconstructing Decentralized Exchanges”. In: *Stanford Journal of Blockchain Law Policy* (Jan. 5, 2019). https://stanford-jblp.pubpub.org/pub/deconstructing-dex.

[14] Cyrus McNally. *DeFi boom drives 1,200% increase in DApp volume in 2020: Report*. Dec. 2020. url: https://cointelegraph.com/news/defi-boom-drives-1200-increase-in-dapp-volume-in-2020-report.

[15] Sarah Meiklejohn et al. “A Fistful of Bitcoins: Characterizing Payments among Men with No Names”. In: *Commun. ACM* 59.4 (Mar. 2016), pp. 86–93. issn: 0001-0782. doi: 10.1145/2896384. url: https://doi.org/10.1145/2896384.

[16] Andrew Miller et al. “An Empirical Analysis of Linkability in the Monero Blockchain”. In: (Apr. 2017).

[17] David Z. Morris. “Consensus 2021: Can Privacy Coins, exchanges and regulators coexist?” In: *CoinDesk Latest Headlines RSS* (May 2021). url: https://www.coindesk.com/policy/2021/05/27/consensus-2021-can-privacy-coins-exchanges-and-regulators-coexist/.

[18] Malte Moser and Rainer Bohme. “Anonymous Alone? Measuring Bitcoin’s Second-Generation Anonymization Techniques”. In: Apr. 2017, pp. 32–41. doi: 10.1109/EuroSPW.2017.48.

[19] Jeffrey Quesnelle. “On the linkability of Zcash transactions”. In: *ArXiv* abs/1712.01210 (2017).

[20] Dorit Ron and Adi Shamir. “Quantitative Analysis of the Full Bitcoin Transaction Graph”. In: *Financial Cryptography and Data Security*. Ed. by Ahmad-Reza Sadeghi. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 6–24. isbn: 978-3-642-39884-1.

[21] Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. “Smart Contract: Attacks and Protections”. In: *IEEE Access* 8 (2020), pp. 24416–24427. url: https://doi.org/10.1109/ACCESS.2020.2970495.

[22] Fabian Schär. “Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets”. In: *SSRN Electronic Journal* (2020). doi: 10.2139/ssrn.3571335.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

[23] Michele Spagnuolo, Federico Maggi, and Stefano Zanero. “BitIodine: Extracting Intelligence from the Bitcoin Network”. In: *Financial Cryptography and Data Security*. Ed. by Nicolas Christin and Reihaneh Safavi-Naini. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 457–468. isbn: 978-3-662-45472-5.

[24] Friedhelm Victor and Andrea Marie Weintraud. “Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges”. In: *CoRR* abs/2102.07001 (2021). arXiv: 2102.07001. url: https://arxiv.org/abs/2102.07001.

[25] Dan Wang, Jindong Zhao, and Yingjie Wang. “A Survey on Privacy Protection of Blockchain: The Technology and Application”. In: *IEEE Access* 8 (2020), pp. 108766–108781. doi: 10.1109/ACCESS.2020.2994294.

[26] Gavin Wood et al. “Ethereum: A secure decentralised generalised transaction ledger”. In: *Ethereum project yellow paper* 151.2014 (2014), pp. 1–32.

[27] Pengcheng Xia et al. “Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange”. In: *Proc. ACM Meas. Anal. Comput. Syst.* 5.3 (Dec. 2021). doi: 10.1145/3491051. url: https://doi.org/10.1145/3491051.

[28] Xiwei Xu, Ingo Weber, and Mark Staples. *Software Architecture for Blockchain Applications*. Springer, 2019.

[29] Haaroon Yousaf, George Kappos, and Sarah Meiklejohn. “Tracing Transactions Across Cryptocurrency Ledgers”. In: *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 837–850. isbn: 978-1-939133-06-9. url: https://www.usenix.org/conference/usenixsecurity19/presentation/yousaf.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.