5-2020

Blockchain Interoperability with Cross-chain Stablecoin Payments

Ravi Balvantrai Pandhi
Florida Institute of Technology

Blockchain Interoperability with Cross-chain Stablecoin Payments

by

Ravi Balvantrai Pandhi

A thesis submitted to the Department of Computer Engineering and Sciences
of Florida Institute of Technology
in partial fulfillment of the requirements
for the degree of

Masters of Science
in
Computer Science

Melbourne, Florida
May 2020

We the undersigned committee hereby approve the attached thesis,
"Blockchain Interoperability with Cross-chain Stablecoin Payments"
by
Ravi Balvantrai Pandhi

_____

Bernard Parenteau, Ph.D.
Assistant Professor
Computer Information Systems
Major Advisor

_____

Marius C. Silaghi, Ph.D.
Associate Professor
Computer Science
Committee Member

_____

Chul-Ho Lee, Ph.D.
Assistant Professor
Electrical and Computer Engineering
Outside Committee Member

_____

Philip Bernhard, Ph.D.
Associate Professor and Department Head
Computer Engineering and Sciences

Abstract

Title: Blockchain Interoperability with Cross-chain Stablecoin Payments

Author: Ravi Balvantrai Pandhi

Advisor: Bernard Parenteau, Ph.D.

A Peer-to-peer payment system was one of the first proposed applications of blockchain technology. Cryptocurrencies have instead been used as a speculative investment. Stablecoins worth approximately 7 billion USD circulate the cryptocurrency market today, presenting a good case for their use in cryptocurrency payments [2]. Stablecoins have also been issued on a variety of blockchains that operate balkanized from each other. Cross-chain transfer between stablecoins is currently enabled by centralized middlemen. The actions of putting stablecoin transfer in the hands of intermediaries is a path towards centralization of control opposite to the decentralization ideology of blockchains. The inter blockchain transfer between blockchains should try to be as trustless as the intra-blockchain transfer. In this thesis, we propose an alternative system for stablecoin transfer, specifically focused on cross-chain stablecoin transfer between multiple blockchains using blockchain interoperability. We then go on to implement a stablecoin transfer between tokens that are based on two different blockchains by creating a representation of the sender token on the receiver chain.

Table of Contents

List of Figures

Acknowledgement

I would like to thank my advisor and mentor Dr. Bernard Parenteau whose Blockchain expertise was a gift throughout these two years.

I express my profound gratitude to my parents and my beloved sisters for providing me with unfailing support and encouragement throughout these two years. I would like to extend my thanks to Nidhi Ruparelia for all her love and support. This achievement would not have been possible without them.

I would also like to thank my internship mentor Tamer Abuelsaad who helped me navigate the Blockchain field while also suggesting potential research topics.

Finally, I would like to thank my friends Tapas Joshi and Adolf Dcosta who helped me evaluate and correct my thesis progress as well as the thesis document.

Chapter 1
Introduction

1.1 Problem Statement

Satoshi Nakamoto released the Bitcoin Blockchain with the goal of facilitating peer-to-peer online payments [8]. The beginning of the blockchain era thus started with the launch of a proposed decentralized payment system. The blockchain space has had a lot of research interest since then with the application of blockchain to many areas including but not limited to Supply Chain, IoT, Smart Contract Platforms, Decentralized Apps, Medicine, and Digital Identification. There have also been releases of production-grade enterprise platforms facilitating these applications [49]. Bitcoin and other blockchains have also been challenged and questioned about its decentralized nature. Communities have been formed and broken, and blockchains have been spawned and forked. A lot of different cryptocurrencies have been minted and have claimed to be the real alternative to Bitcoin, a P2P system. However, even after eleven years since the launch of Bitcoin, it can be argued that the dream of a decentralized P2P payment system has not yet been realized [50]. Although various factors contribute to cryptocurrency not being used heavily as a P2P payment system, their price volatility is one of the major ones [9]. Cryptocurrencies, from time and time again, have presented themselves as tools of speculation. Coming back to P2P payments, ideally, we would want a currency that has a stable value or has a close to stable purchasing power. The primary use of Tether and other stablecoins launched thus far has been by traders for combating against the volatility swings of the

market [18]. Nevertheless, the scenario is changing now with the use of stablecoins in a variety of applications. Stablecoins, compared to the volatile cryptocurrencies, present a better case for their use in the decentralized payment application. The reason is that they have close to zero price volatility. Stablecoins, just like other cryptocurrencies are implemented on blockchains and are generally collateralized by asset reserves. A majority of the stablecoins that are transacting in the market right now are implemented on the Ethereum blockchain [4]. However, with the launch and rise of crypto kitties and other decentralized applications, we have seen that Ethereum is not yet ready for the blockchain scalability requirements of massive-scale applications [51]. As Ethereum has shown us that it is tough for a single blockchain to handle a massive amount of transactions, it can then be argued that it is a good practice to have multiple blockchains with stablecoins implemented on top of it. Several other stablecoins have also emerged, which are based on blockchains like EOS, Bitcoin, Binance chain, and others [4]. A particular case for this type of implementation could be a scenario when both the stablecoin transacting parties belong to different blockchains. As most of the blockchains are balkanized from each other, there is little to no interoperability between them [52]. To facilitate payment between tokens belonging to different blockchains, we have to then go through a centralized token changer. For example, if we want to convert our token from BTC to XRP, we would have to use centralized services that have accounts on both the chains. Centralized services do work like a charm here, but like every solution, some tradeoffs have to be made. When using centralized services for such a conversion, there is a small commission fee that is deducted by the provider. The problem with centralized services is that it can be more collusion-prone and attack-prone compared to

decentralized services [36]. Now, the fundamental reason Bitcoin, a peer-to-peer payment was launched, was to move away from the centralization nature of payment systems. If we keep on relying on centralized services and keep on outsourcing custody of our funds to institutions, the application of blockchain to payment applications will make little sense. We see here that there is a need for a P2P stablecoin payment system that encourages the participation of multiple tokens belonging to different blockchains and also facilitates conversion between them without centralized entities.

1.2 Proposed Solution

Our proposed approach would be a system that uses blockchain interoperability services to convert from one stablecoin to another. The conversion is needed because both the sending and receiving parties can have accounts on different blockchains. Interoperability between blockchains is needed to ensure that we have a trustless and a decentralized conversion between the stablecoins. To implement a part of our proposed system, we set up instances of ethereum and cosmos blockchains and conduct a transfer between an ethereum stablecoin to a cosmos stablecoin.

1.3 Research Questions

1. How effective is it to have a cross-chain stablecoin payment system?
2. How effectively can we transfer stablecoin from one blockchain to another without using third party services?
3. How can we return stable coins that have been transferred back to the sending chain?

4. How can we ensure that the proposed P2P stablecoin transfer system is decentralized?

1.4 Organization of the Thesis

The rest of the thesis is organized as follows.

Chapter 2 states some of the terms and the concepts that are useful for navigating the field of Stablecoins and Blockchain Interoperability.

Chapter 3 contains the literature review of the past work done in the area of cryptocurrency payment facilitation and blockchain interoperability.

Chapter 4 describes our proposed approach, along with detailed flow diagrams.

Chapter 5 contains the implementation of a prototype token transfer.

Chapter 6 describes the potential future work, revisits the research questions, and also concludes the thesis.

Chapter 2
Background

In this chapter, we will define some of the terms and the concepts that can better enable us to understand the ideas presented in the following chapters as well as gain an understanding of Stablecoins and Inter-Blockchain communication.

Stablecoin

With reference from Hassani et al. [5] and [6], we can define stablecoin as a crypto token that has close to zero price volatility, is used as a unit of accounting in digital payments and can be collateralized by an underlying asset or non-collateralized and operate on the basis of algorithms.

Stablecoin swap

Stablecoin swap can be referred to as a trade of one stablecoin for the other with no change in its monetary value.

Decentralization

As quoted by MIT Media Labs, “Decentralization is the process of dispersing functions and power away from a central location or authority”.[7]

Inter-Blockchain Communication

Inter-blockchain communication can be defined as a set of protocols/technologies that aim to make blockchains interoperable in a decentralized way.

Smart Contracts

As quoted by Wikipedia, “A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract” [59]

Blockchain Consensus

The convention by which nodes on a blockchain agree to accept transactions as validators commit those transactions.

Chapter 3
Literature Review

3.1 Thesis Focus

The focus of the thesis is to research the area of stablecoins as a payment mechanism, and propose an approach for enabling cross-chain conversion of stablecoins using blockchain interoperability principles.

The literature review that follows has three main goals. The first goal is to inform the reader of the research already conducted in the field of cryptocurrency payments and blockchain interoperability. The next goal is to gain and present a better understanding of the thesis topic and the background associated with the same. The third and the last goal is to highlight the gap observed in the field of cross-chain cryptocurrency payments in order to keep the research focused.

3.2 Background

As per cryptocurrency rankings, the total cryptocurrency market volume reported on January 27th, 2020 was wavering around 106 billion dollars [1]. Out of that, as per stablecoin volume rankings, the total volume of the stablecoin sector was approximately 38 billion dollars [2]. The volume of stablecoins has been hovering around one-third of the total cryptocurrency volume for almost a year now [3]. It can be inferred from the above statistics that almost one-third of the cryptocurrencies exchanging hands are stablecoins. From the stablecoin report [4], we can see that there are in total 72 stablecoins that are currently transacting and implemented on different

platforms (blockchain). These statistics convey to us that stablecoins have been gaining adoption for a while now. The other takeaway is that given that stablecoins have been implemented on different blockchains, it is worthwhile to research in the area of cross-chain stablecoin conversion.

3.3 Main Body

Bitcoin and Stablecoins

As the title of the famous Bitcoin whitepaper, 'Bitcoin: A Peer-to-Peer Electronic Cash System' [8], it is implied that the primary goal of Bitcoin launched on January 3, 2009 was to implement a peer to peer electronic payment system. However, even a decade later, Bitcoin has not been able to achieve that goal in its complete sense. Consider a scenario where a merchant sells an item, priced at $500 to a customer in exchange for Bitcoins. At today's rate, which is close to $9200 per bitcoin, the customer has to pay approximately 0.054 bitcoins. Considering the historical price chart of bitcoin to usd, it could be argued that Bitcoin can go as low as $6500 per bitcoin. If that is the case in some near future and the merchant then goes to exchange the received bitcoin for USD, he would get approximately $360 for the item that he sold. Now that is a loss of approximately $140 to the merchant compared to his intended selling price. This scenario presents a significant loss on the side of the merchants. Also, the customers might be reluctant to spend Bitcoin because holding them and then selling them for dollars in the future can instead provide more return. For example, today, 0.05 of a Bitcoin could be used to purchase an item worth $500. In the future, if the price of Bitcoin reaches $13k per bitcoin, the same amount of Bitcoin could be used to purchase an item worth approximately $700.

The primary reason for Bitcoin not being used as a peer to peer payment mechanism could thus be attributed to its price volatility. It has indeed become a financial instrument, as well as a speculative investment [9]. We can infer from coinmarketcap.com that not only bitcoin but all the cryptocurrencies except stablecoins have undergone substantial price swings. To circumvent the volatility issues of Bitcoin and other cryptocurrencies and also to provide a stable cryptocurrency alternative, Tether was launched in July 2014. Tether is a method to maintain a one-to-one reserve ratio between a cryptocurrency token and a fiat currency. Tether is also a cryptocurrency token which belongs to the category of collateralized (fiat-backed) stablecoins meaning 1 tether token (1 USDT) is equal to a United States dollar. [10] Traders heavily transacted Tether during the crypto price boom of 2017 to hedge their positions and also add a crypto-fiat component to their cryptocurrency holdings [18]. Tether was initially launched on the Bitcoin blockchain using the Omni Layer protocol. As the demand for Tether skyrocketed in recent years, as of Jan 27, 2020, we have tether implementations on Ethereum, Tron, EOS, and Liquid blockchains [11].

With the lure of the success that Tether had in 2017, it led to multiple stablecoins coming into existence, including but not limited to USDC, TUSD, GUSD, DAI, and PAX. Also, from the stablecoin report [4], we see that approximately 25 coins have been implemented on the Ethereum blockchain. Another reason for the launch of these multiple competitions to Tether was the conflicts surrounding Tether. Tether has been questioned many times on the backing of the number of USD dollars representing the total tether tokens (USDT) in circulation [33]. A lawyer of Tether, in April of 2019, admitted that the stablecoin was only 74% backed by cash and equivalents. In November of

2019, Tether then admitted that it was fully backed. These incidents have led the community to believe that Tether lacks transparency on the aspect of collaterals backing the crypto tokens.

Let us take a look at a detailed analysis chart of stablecoin volume to date.

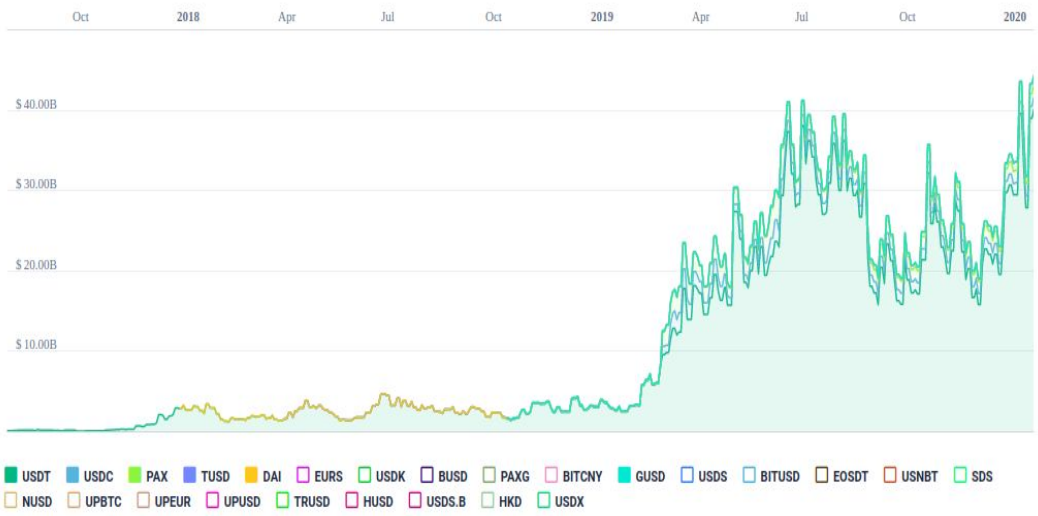

Figure 3.1 — Changes in Stablecoin Volume with time.

The chart in Figure 2.1 represents the total stablecoin volume as it changed with time [19]. On the X-axis, we have chronological periods, and on the Y-axis, we have total stablecoin volume in USD. For simplistic representation, the top six stablecoins as per the gross volume have been selected. From the above chart, one can infer that the total stablecoin volume has changed significantly since the year of 2018. The change, for the most part, has been in an upward trend, meaning the total volume has kept on increasing with time. Also, as mentioned before, the total volume of stablecoins (38 billion USD) represents

almost one-third of the total cryptocurrency volume (106 billion USD). Stablecoins have thus proved itself to be a heavily transacted cryptocurrency.

Stablecoins can be broadly categorized into collateralized and non-collateralized. Collateralized stablecoins represent that there is an asset backing it or it is collateralized by an asset. The collateral could be fiat currency (USD, EUR, etc.), a basket of fiat currencies, a valuable asset such as gold, cryptocurrency (BTC, ETH, etc.), or a combination of any of the asset collaterals. Tether (USDT), Paxos Standard (PAX) are examples of fiat collateralized stablecoins. By pegging stablecoins to cryptocurrency, reliance on centralized systems preserving cash reserves is nullified. Crypto collateralized stablecoins exist because the crypto community strives to push itself towards a system of increasing decentralization. DAI and nUSD can be categorized as crypto collateralized stablecoins. Non collateralized stablecoins are the ones that achieve price stability using a combination of algorithmic tools and simple and deterministic coin supply rules [20]. Stablecoins like USDX aims to be a network similar to an 'algorithmic central bank' where supply and demand of currency are governed by elastic monetary policy and data analysis rather than being governed by centralized institutions [30].

These different stablecoins exist because there is no perfect stablecoin design or "Holy Grail of crypto" [21]. Stablecoins are designed to remain stable, but there have been still minor levels of volatility in their prices [22]. Trading was one of the primary use cases of stablecoins, but it is being challenged now, and people can do a lot more with stablecoins. Some of the potential, as well as implemented use cases of stablecoins, are presented below.

Stablecoin Potential

Stablecoins present a strong case for being used as a payment mechanism for peer-to-peer payments. There has also been a consideration for two different types of settlement units. One is the retail stablecoin, which is an asset that is available to a wide range of users. The other one is the wholesale stablecoin, which is only available to participating organizations.

JPM coin, a digital fiat coin launched by J.P. Morgan, for now, is categorized as a wholesale stablecoin which is only available to their institutional clients [27]. IBM has also launched a framework named IBM World Wire, which connects large financial institutions and facilitates cross border payment instantly. The framework is built using Stellar blockchain and extensively uses stablecoins that are native to the stellar chain [23].

Taking the case of retail stablecoins, perhaps the most prominent crypto news of 2019 was the launch of Libra, a stable cryptocurrency by Facebook and The Libra Association. Libra aims to be the payment network connecting now popular social media applications, namely WhatsApp, Facebook & Instagram. It is by design, a stable currency backed by a basket of bank deposits and government securities [29]. There are even wallets like Trust Wallet, Everex, and Bitpay, which allow users to spend their bitcoin with supported merchants.

Some papers have also proposed an algorithmic price manipulation design integrating financial services like loans and lending along with and on top of the stablecoin framework [24]. There are even tons of services which use ethereum to facilitate financial application in a decentralized manner. Some widely used examples of DeFi applications include Maker, Compound,

Synthetix, and others[25]. These services accommodate the native currency of Ethereum blockchain, ether as well as DAI, an algorithmic stablecoin.

People's Bank of China has also recently announced that they are ready with a prototype version of their Central Bank Digital Currency (CBDC). There have been speculations on whether the currency uses distributed ledger technology or a blockchain [26][34][35]. The IMF has also proposed the concept of synthetic CBDC, which allows e-money providers like private banks and other firms to hold CBDC reserves [28]. If a country decides to go down that path, it then becomes a very significant policy consideration. If implemented, it presents a huge financial opportunity for compliant stablecoin issuers.

Centralized applications or services are the ones in which a service is provided by a central server(s), which is controlled by an institution or a small group of institutions. Decentralized application (DApp) or services are the opposites of centralized applications in which the service is provided by replication of data on a large group of servers, and the servers are not controlled by any centralized authority. Stablecoins have been touted to aid in the wider adoption of DApps [32]. Financial interactions/transactions in the Ethereum DApp ecosystem can be facilitated using on-chain stablecoin, DAI. This provision opens up a host of opportunities for providing services without intermediaries.

These were some of the potential as well as implemented use cases for stablecoins. There is a considerable amount of untapped benefit yet to be derived from the stablecoin ecosystem. For the entire stablecoin community to

thrive and get adopted, the apps or services that facilitate stablecoin payments need to interoperate with each other for the transfer of value.

Just like there is no single currency to facilitate every trade on the planet, there is no single stablecoin to support all digital trades. Also, in the absence of merchants, people might still want to exchange one stablecoin for the other.

Stablecoin Payment Scenarios

We will now be listing out various P2P stablecoin payment scenarios. Let us consider a scenario in which a merchant accepts USDC stablecoin for the sale of goods. USDC can be kept in an Ethereum blockchain supported cryptocurrency wallet because USDC is an ethereum token. Let us also assume that the buyer has required USDC balance to purchase an item of his choice. If this is the case, we do need any token swap here because the sending and the receiving tokens are the same. The purchase can be facilitated here, with the buyer sending required USDC balance from his ethereum account address to the merchant's ethereum account address. Figure 2.2 below represents the same scenario with a diagram.

Figure 3.2 — A scenario demonstrating transfer between the same stablecoin.

Let us now consider a scenario in which a merchant accepts TUSD stablecoin for the sale of goods. TUSD can also be kept in an Ethereum blockchain

supported cryptocurrency wallet because TUSD is an ethereum token. In this case, the buyer has the required balance to purchase an item, but it is in USDC. In this case, we need a token swap from USDC to TUSD because the sending and the receiving tokens are different. The purchase can be facilitated by using a decentralized swapping service.

Decentralized swapping services like AirSwap and Uniswap are available, and they are specifically targeted towards swapping ethereum blockchain-based tokens using smart contracts[15][16]. These decentralized swapping services facilitate the execution of a stablecoin swap between tokens that are native to a single blockchain using smart contracts and without an intermediary. The same scenario can be represented with a diagram as follows.

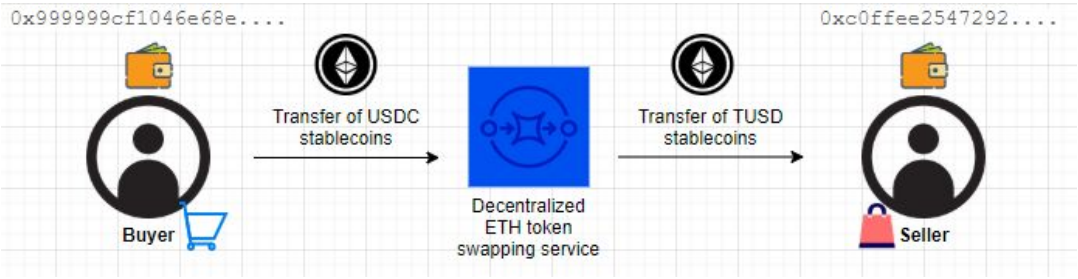

Figure 3.3 — A scenario demonstrating transfer between different stablecoins but implemented on the same blockchain.

Now let us consider a scenario in which a merchant accepts stablecoin EOSDT for purchases. EOSDT is implemented on the EOS blockchain. Now it is certainly possible that customers that come to the shop would have a different 'USD stablecoin', let's say, for example, TUSD. Now, TUSD is implemented on the ethereum blockchain. Because the source and the destination chains are different, this is one such scenario wherein a cross-chain stablecoin swap is required. Here, TUSD needs to be converted to EOSDT to enable the merchant

to sell the requested items to the customer. The swap, in this case, could be facilitated by a centralized token swap service. These service providers usually have liquid accounts on both the source and the destination chains and, in exchange for a small commission, facilitate the transfer. The scenario discussed is represented below with a diagram.

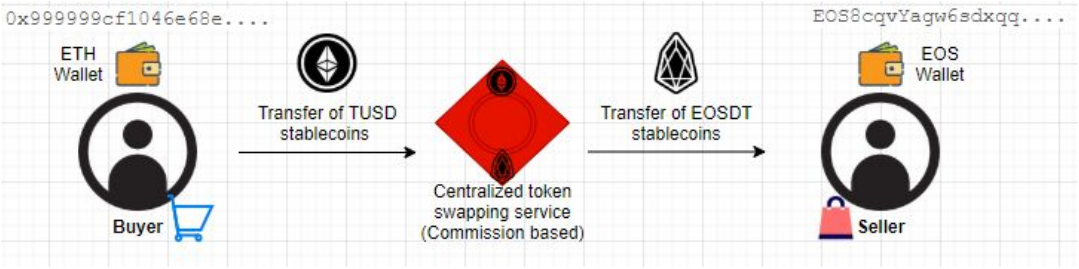

Figure 3.4 — A scenario demonstrating transfer between different stablecoins implemented on different blockchains.

Some of the examples of the centralized swapping services mentioned above are Changenow, Changelly, Shapeshift, Swapy, and others. These providers facilitate swapping between the same and different blockchain tokens [14]. The problem with these services is that they are centralized and commission-based. With the centralization aspect, they cannot be regarded as censorship-resistant. The goal of the very first blockchain release was to promote a discussion on the flaws that are brought about by centralized systems. The idea was to move away from the control of financial institutions because they can be exposed to the risks, including but not limited to the lack of transparency, corruption, and misuse of power. They can also potentially act as a single point of failure [36].

Also, as presented before, there are potential business use cases for stablecoins as well. It can undoubtedly be stated that two businesses might

want to transfer tokens of value with each other. The scenarios presented thus represent a case wherein we would require the conversion of one stablecoin to another. As presented before, there do exist multiple stablecoins implemented on different blockchains. The list of a majority of all the stablecoins in existence can be viewed at many of the curation websites, one of them is stable.report [4]. We see that there are stablecoins implemented in a variety of different blockchains, namely Ethereum, Stellar, EOS, Tron, and others.

A blockchain, in the technical sense, is a set of software protocols followed by all the nodes in the network. Different blockchains may have similar protocols, but it is evident that they differ in some set of protocols. For example, Bitcoin and Ethereum follow the same consensus mechanism of Proof of Work (PoW). Now, Bitcoin is a blockchain for a specific purpose, which is the currency application, and Ethereum strives to be 'The World Computer', a blockchain catering to multiple applications. Bitcoin uses SHA-256 as the mining algorithm, while Ethereum uses Ethhash as the mining algorithm.

Due to the technical implementation differences between blockchains, these different blockchains were not designed to be interoperable from the start. Consequently, the world of blockchains has grown to be balkanized from each other, neglecting the interoperability needs between them.

Now to facilitate swapping between different blockchains without an intermediary, the blockchains in question need to interoperate with each other. These swaps are also known as cross-chain atomic swaps [31]. There also exist cross-chain decentralized atomic swap services. Liquality is one of the services which lets the users exchange between ether and bitcoin. The problem with existing cross-chain atomic swap services is that they do not

support exchanges between stablecoins belonging to more than two blockchains.

As we have seen, there are multiple successful implementations of stablecoins. Also, there is a massive potential in the number of applications emerging out of stablecoin interoperability.

We will now be reviewing the work done in the field of blockchain interoperability to gauge if we can apply blockchain interoperability principles to the problem of swapping tokens between multiple blockchains.

Blockchain Interoperability

Blockchain interoperability has been labeled to be the Blockchain 3.0 after Bitcoin (Blockchain 1.0) and Ethereum (Blockchain 2.0) [37]. With the launch of many blockchain and blockchain startups, there is a need for collaboration between them [40]. The collaboration could be achieved in a trustful way by the agreement between blockchain committee members, or it could be achieved in a trustless way by supporting blockchain interoperability. The interoperability problem with blockchains has also been attempted to be solved by comparing blockchain with the early days of the Internet. By doing so, the problems that the Internet faced in its early days can be modeled, and the solution that solved the problems can be applied to the problems currently faced by blockchain [41]. The research towards a blockchain-interoperable system has also accelerated because there is a need for solving problems like asset portability [38], cross-chain oracles [39], and atomic swap [38].

It is this problem of interconnecting blockchains that many projects are aiming to solve. Several notable startups like Cosmos, Polkadot, and others are racing

in to provide their solutions to facilitate interoperability between blockchains. We will be listing out the details about some of the projects that have or claim to have work done in the areas of blockchain interoperability, specifically to support token transfer.

Rootstock

This project aims to build a smart contract platform for the bitcoin blockchain so that it could support multiple applications on the blockchain rather than just the currency application. The project also has achieved interoperability between its RSK blockchain and the existing Bitcoin blockchain. Recently, it also released a bridge module that can communicate between RSK blockchain and the ethereum blockchain [42]. Notably, a bitcoin-backed stablecoin, Money on Chain (MOC) was also released on the RSK blockchain.

Liquality

Liquality launched a cross-chain application that lets users transact between ethereum and bitcoin in a trustless and decentralized manner. They have enabled a bridge application using atomic swaps and hash time-locked contracts [48] that can enable the conversion between Bitcoin and Ethereum.

Syscoin

This project alike Rootstock has also released a bridge known as Sysethereum bridge that facilitates transfer between SPT (a token on Syscoin blockchain) and ERC20 (a token standard on the ethereum blockchain) [43].

Cosmos

Cosmos Network and Interchain Foundation have been working on blockchain interoperability since 2014. In their whitepaper, they have proposed Inter Blockchain Protocol (IBC), which aims to establish interoperability between all the chains that follow Tendermint consensus protocol [37]. Cosmos also provides libraries and tools to create application-specific blockchains that are based on Tendermint consensus protocols. For blockchains that do not follow Tendermint consensus protocol, for example, bitcoin and ethereum blockchains, they have also developed bridge chains that can achieve the interoperability between the same.

The bridge chain that can handle interoperability between a Tendermint based chain and the ethereum chain is termed as Peggy. It consists of a set of tools and libraries for swapping ethereum based tokens to Cosmos based tokens and vice versa. [44]

The bridge chain that can handle interoperability between a Tendermint based chain and the bitcoin chain is termed as bitcoin-peg. It consists of libraries that can be used in a cosmos application to bitcoin to Cosmos based tokens and vice versa. [45]

Polkadot

Another noteworthy project working on blockchain interoperability protocols, Polkadot has one of its founders as Gavin Wood, who notably also co-founded Ethereum.

Polkadot, a multi-chain protocol, encourages the idea of parachains, chains created using libraries provided by Parity technologies. Similar to Cosmos, Parity technologies also encourage the idea of having specialized chains for each blockchain application and establishing interoperability between them using Polkadot protocol.

Polkadot has also released a bridge chain to connect parachains to the ethereum blockchain [46]. It has recently been awarded a grant to connect parachains with bitcoin blockchain [47].

We can argue from the presented blockchain token bridge applications that these services have integrated two-way bridges between two specific blockchains. For example, RSK has created a bridge module between bitcoin and the RSK chain. Syscoin has created a bridge module between the syscoin blockchain and the ethereum blockchain. Cosmos has created bridges for interoperation between Cosmos to bitcoin and Cosmos to ethereum. Moreover, Cosmos has also provided protocols for interconnection between chains developed using their consensus protocol. The Polkadot framework can be explained with the same reasoning as Cosmos. A notable similarity between some of these bridge applications is that they have not been standardized, i.e. they have not been thoroughly researched upon nor highlighted extensively in their whitepaper. Most of them just have a Github repository that presents the interoperability idea and a reference implementation. Although it is not specifically mentioned in the bridge applications, we assume that these bridge applications can also be utilized to facilitate stablecoin transfer, given that they can be utilized to facilitate token transfers.

As per the best of our knowledge, we see that there is a lack of a P2P stablecoin payment system that is facilitated by one or a combination of the mentioned interoperability services.

Chapter 4
Proposed Approach

4.1 Black Box View of the System

As highlighted in the literature review, there is a lack of a P2P payment system that can facilitate cross-chain stablecoin transfers. We will first be detailing out the input and the output of our proposed system and then detailing out all the components that govern the working of our system.

The input to the system will be stablecoin tokens sent by the sender, and the output of the system will be the stablecoins that the receiver wants to receive. Our system should provide paths or directions to handle the conversion. Broadly classifying, we can list out four probable scenarios that could highlight the token transfer variants.

1. The first scenario would be when we have a similar sender and receiver stablecoin type.
2. The second scenario would be when the type of sender and the receiver stablecoin are different, but both the stablecoins are implemented on the same blockchain.
3. The third scenario would be when the sender and receiver blockchains are different and we need to represent sender stablecoin on the receiver blockchain.
4. The fourth scenario would be when the type of sender and the receiver stablecoins are different and they belong to different blockchains.

The component that forms a critical part of our system would be a collection of interoperability services. Some of the services that we highlighted in the literature review chapter were Cosmos, RSK, Polkadot, and others. We need a collection of interoperability services because the services that we reviewed integrate only two specific blockchains at a time. The next important component would be the algorithm that governs the further processing on the basis of the four scenarios presented. The other components are covered later in this chapter when we present the detailed design of our proposed P2P system.

The placement of our system in an abstract view is represented in the below figure.

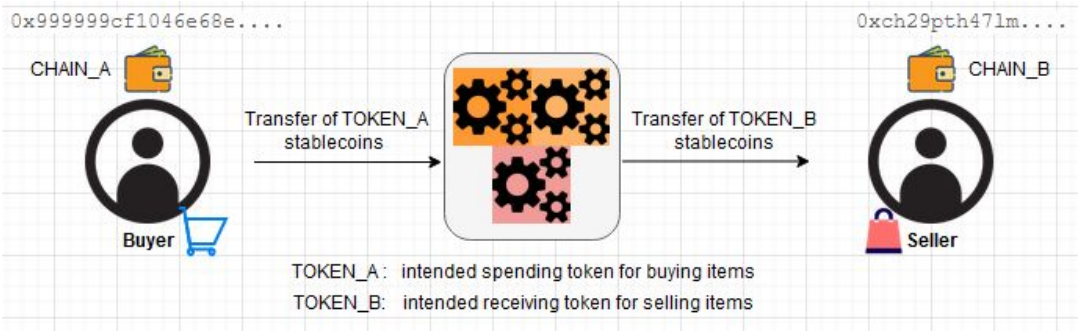

Figure 4.1 — Representing proposed system in a blackbox view.

We want to specify here that it is essential that the system does not have tight boundaries. Boundaries surround the system in the diagram just for the ease of representation. If it has boundaries, it can become a service that can reside on a server, a centralized entity, and taking that trail leads us towards the path of increasing centralization.

4.2 Stablecoin Transfer Scenarios

Let us now dive deep into the scenarios highlighted in the previous section and the processing instructions that may suffice for each of them.

Same Stablecoin, Same Blockchain

As highlighted in the literature review, when the sender and receiver want to transact with a similar stablecoin, the sender needs to use the address of the receiver, and the underlying blockchain protocol would facilitate the transfer. In this scenario, our system would thus be checking if the sender and receiver chains are equal. If they are, the system will connect to the nodes of the blockchain in question, and the transaction would then be ready to be validated by the other nodes of the blockchain.

Different Stablecoin, Same Blockchain

This is a scenario wherein the sender is connected to a similar blockchain as the receiver, but the sender wants to pay in a different stablecoin than the intended stablecoin that the recipient wants to receive. In such a case, our goal is to keep the system from navigating towards centralized token changers. As mentioned in the literature review, we can make use of decentralized atomic swap services. For example, for ethereum, we have Uniswap and Airswap as the two major atomic swap services. Our system, in this case, would direct the control towards the available services to handle the transaction.

Same Stablecoin Representation on Different Blockchains

We have seen scenarios wherein both the sender and the receiver chain are similar. This particular case represents that the sender and the receiver want

to transact in different stablecoins, and hence we need to represent the sender stablecoin on the receiver's blockchain. Our system would deduce that we need to use interoperability services to represent the sender token on the receiver chain, thus facilitating the transfer.

Different Stablecoin, Different Blockchains

This scenario, wherein the sender and the receiver wants to transact in the different stablecoin type and they belong to different blockchains. For example, you could need USDC to TUSD stablecoin transfer and assume that USDC is implemented on Ethereum and TUSD is implemented on Cosmos. In this case, our system first needs to use the processing instructions mentioned in the second scenario and then apply third scenario instructions to enable cross-chain transfer. The second scenario is applied to convert from USDC on Ethereum to TUSD on Ethereum. The TUSD on Ethereum is then sent to TUSD on Cosmos. We have labelled this scenario as out of scope for the purpose of this thesis as it includes further research depending on the integration of both inter blockchain transfer and intra blockchain transfer.

4.3 System Workflow for Cross-chain Stablecoin Transfer

For our thesis, we are more interested in the same stablecoin transfer cross-chain between different blockchains, which is represented by the third scenario presented above. We will now be covering the architecture and the design of our system that we believe takes care of the third scenario.

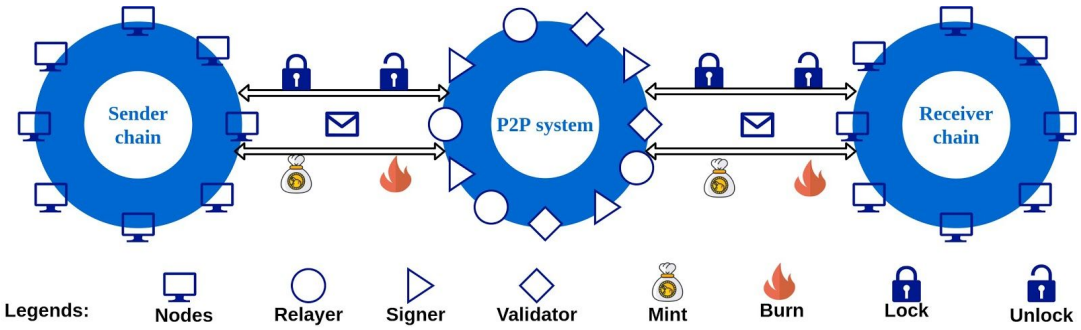

Figure 4.2 — Design for P2P cross-chain transfer.

The leftmost part of Figure 3.2 denotes an instance of the sender blockchain, and the rightmost part of Figure 3.2 denotes an instance of the receiver blockchain. The nodes on each of these blockchains represent the full nodes that act as the validators of blockchain transactions. P2P system is the blockchain that acts as the intermediary between the two blockchains and facilitates interactions between them. The components of our proposed P2P system are represented below.

Relayer: This is a node type in the P2P system which relays event information from the sender chain to the receiver chain and vice versa.

Signer: This is also a node type with the function of creating receiver chain transactions out of sending chain transactions and subsequently signing those transactions.

Validator: A node that validates transactions taking place on the P2P system.

Lock: Stablecoins, may it be the sender's assets or receiver's assets are locked within their blockchain and are enforced to be stagnant using smart contracts on the sender chain.

Mint: When stablecoins are locked on the sender chain, an equivalent number of stablecoins on the receiver chain is minted.

Burn: Stablecoins can be burned on the receiver chain in order to reverse the cross-chain transaction.

Unlock: Stablecoins can be unlocked on the sender chain, resulting in the freeing of the asset. However, for the stablecoins to be unlocked, an equivalent number of tokens should be burned on the receiver's chain.

The four events presented above are executed using interoperability services between the sender and the receiver chain. Relayers that are a part of the bridge blockchain relay these events along with their info messages.

Looking at the proposed system from a security standpoint, the security aspects of the events can be understood with the following description and analogy. Cosmos uses Byzantine fault-tolerance consensus algorithm and its security is ensured via super-majority (greater than ⅔) voting and a locking mechanism. Together, they ensure that greater than 2⁄3 voting power must be Byzantine in order to execute a security breach in which more than two values are committed [37]. We follow the same security practice for ensuring the correct happenings of all the four events. For example when a lock notification is noted by the system, it should be noted by greater than two-third of the validators to deem it as an actual locking event. The same approach is applied to the other three events.

Figure 3.3 presented below is a flowchart that demonstrates the transfer of stablecoins from one blockchain to the other. The flowchart also highlights the process flow of our system.

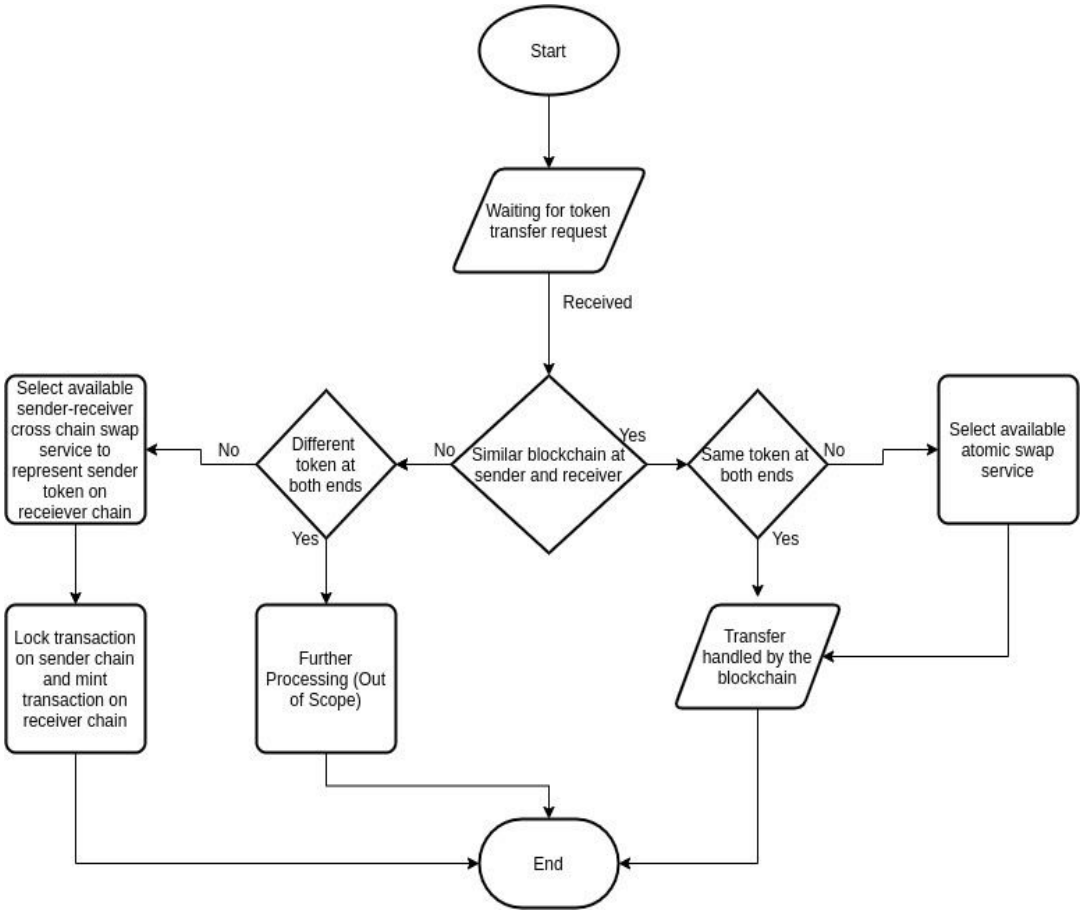

Figure 4.3 — Flowchart representing P2P stablecoin transfer.

For transferring stablecoins that originate at the sender blockchain to the receiver blockchain, we will be locking the tokens on the sender blockchain. The information about the locking would be transmitted to the receiver blockchain, and an equivalent amount of tokens would be generated on the same. We accomplish the locking of the tokens using interoperability service

between the sender and the receiver chain. Now the tokens on the sender blockchain are forced to be stagnant. This process is accomplished using escrow smart contracts. When tokens are locked, they cannot be moved from one sender chain address to another. That is necessary in order to prevent double-spending of the tokens. Now we will be covering the process associated with each step of the flow chart in detail.

The start of the flowchart indicates that the transfer from the sender chain to the receiver chain can now be facilitated. The necessary condition is that both the blockchains should be up and running along with the deployment of the smart contracts governing the conversion.

The witness node, in our case, would be listening to the events on the sender blockchain. Specifically, it would be listening to the lock event that indicates that the tokens are locked on sender blockchain. Once the sender blockchain validates the lock transaction, the witness waits for a preset number of blocks before it sends the lock message ahead to our P2P system. The lock message is then forwarded to the signer, which then creates a lock message that can be understood by the receiver blockchain, signs the same, and then relays it to the receiver chain. The bridge module that is essentially a bridge between the sender and the receiver blockchain takes the message and converts it to a generic oracle claim. The oracle module receives the oracle claim and then waits for the consensus on the claim. The consensus means that it waits until 2/3rd of the validators agree to it. Once that is achieved, the claim is given finality, and is registered on the receiver blockchain. With the registration of the claim on the receiver blockchain, the bridge module mints new stablecoins and sends them to the address of the receiver chain recipient.

Thus the originating tokens are locked on the sender blockchain, and new tokens are added to the receiver's address. The newly minted tokens are free to move in the receiver blockchain, and they can be sent to any other recipient address in the receiver chain.

In the scenario mentioned above, a token, for example, TOKEN_A on the sender chain, was converted to a token, for example, TOKEN_B on the receiver chain. Now, the minting app should not be able to mint TOKEN_B for any other random token transfer. It implies that we need to use the mechanisms of whitelisting or blacklisting tokens for the authentication of token swap pairs. If we use the mechanism of whitelisting, only the token pairs that are whitelisted will be facilitated by the swap feature.

Now there can be a scenario in which the transaction might need to be reversed. The tokens can be burned on the receiver blockchain and the stablecoins that were locked in the sender blockchain can now be unlocked.

This process would work in a reverse manner in which the burning token transaction would have to be validated on the receiver blockchain, and the information about the burning should be relayed to the smart contracts on the sender chain. The smart contracts would, in turn, unlock the stablecoins that had been locked before and sent to the recipient specified. Again, the transaction of unlocking stablecoins would have to be validated by the sender blockchain, and then the stablecoins would be sent back to the sender.

The process described here denotes the cross-chain transfer of stablecoins between the sender chain and the receiver chain. Now, it is certainly possible that at a different time, the sender chain could become the new receiver chain,

and the receiver chain could be the new sender chain. We propose that the process would work in a similar manner except for the selection of interoperability service. Using the blockchain interoperability services, we thus presented a way of representing stablecoins originating on the sender chain on to the receiver chain.

Chapter 5
Implementation

5.1 Choosing the Chains

The design chapter presented and described the system model that could be used to make two blockchains transfer stablecoins with one another using blockchain interoperability.

We highlight in the design chapter that for the sending chain and the receiving chain to achieve cross-chain transfer of stablecoins, there needs to be an interoperable service facilitating the inter blockchain communication.

Now, as highlighted in literature review, these interoperability services, tools and libraries are developed by emerging blockchain startups. A Bloomberg study concluded that close to 80% of the ICOs launched until 2018 were identified to be scams [53]. A github data study group presented their analysis stating that although blockchain startups secured a lot of crowdfunding, there are only a handful projects out of those which made significant github commits [54]. These revelations are shocking and it builds a perception of looking at blockchain projects with a questionable mindset. We inferred that before believing the fact that the available interoperability services can enable cross chain token transfer in a trustless manner, there is a necessary need to test these services.

Our implementation chapter thus encompasses setting up of instances of two blockchains Ethereum, as the sender chain and Cosmos, as the receiver chain. It also covers a stablecoin transfer from the sender to the receiver chains and a

reverse transfer from the receiver to the sender chain. We have chosen Ethereum as one of the chains because, as highlighted in the literature review, it is the blockchain with the most number of stablecoins issued on top of it [4]. We have presented a few interoperability projects in the literature review that have built bridges with Ethereum. We decided to test and use interoperability services and tools provided by Cosmos. The reasons we were inclined to use Cosmos are presented below.

1. The Cosmos project is in the top five positions for the most number of github code commits among other blockchain projects [55] and not only that but they have an active youtube channel explaining how to setup and configure services enabled by their products [56].
2. They have built bridge tools and libraries that enable interoperability between Cosmos and Ethereum and also Cosmos and Bitcoin.
3. Enabling the bridge between Cosmos and a blockchain means that the blockchain in question can potentially interoperate with any of the other Tendermint powered chains. The protocol that can enable the communication between Tendermint based chains is termed as IBC. IBC has been released but it is only in the test phase right now.

We will be utilizing the tools and libraries listed under Cosmos' Inter-blockchain connection (IBC) protocol and also Peggy, a side chain based on Cosmos [44]. The approach here is to utilize the mechanism of locking and minting in conjunction with unlocking and burning. Events emitted by the contracts on both the blockchains are utilized to get information about the transactions. This method could thus be used to swap any stablecoins between two different blockchains. We also present an implementation so that it could

present itself as a reference point for further implementing cross-chain transfers.

We would be considering a scenario of a stablecoin transfer between the blockchains. The reason for choosing stablecoins could be attributed to the following major reasons.

1. As mentioned in the literature review, stablecoins have been the highest volume grossing tokens in the cryptocurrency space.
2. As stablecoins are the tokens with a near-constant stable value, it would be helpful for the purpose of this thesis, to hide some of the concerns that token price volatility brings along with it.
3. Again, as highlighted in the literature review, stablecoins present an excellent case for their use in peer to peer payments. It can also be argued that two stablecoin exchangers (payment exchangers) can belong to two separate blockchains.

Now before we implement and follow the design model presented in the design chapter, we would have to complete some prerequisites to enable cross-chain stablecoin transfer.

5.2 Prerequisites for Cross-chain Transfer

Starting below, we have made sections for each of the prerequisites. Each section would also talk in detail about the need for the prerequisite and the procedure used to complete the same.

Setting up Blockchains

The first step is to set up blockchains for which we want to transfer tokens from one chain to the other. As mentioned above, for our implementation purpose, we have chosen the Ethereum blockchain and the Cosmos blockchain.

The instances of both the chains have been chosen to be local. Swish Labs provides us a utility called Ethereum Bridge (ebd) that could be used to spin up a local cosmos blockchain and, along with it, a client for ethereum bridge [57]. Ethereum bridge provides useful methods that could be used to facilitate the interaction between cosmos and ethereum chains. Figure 4.1 presented below denotes a local instance of cosmos chain.

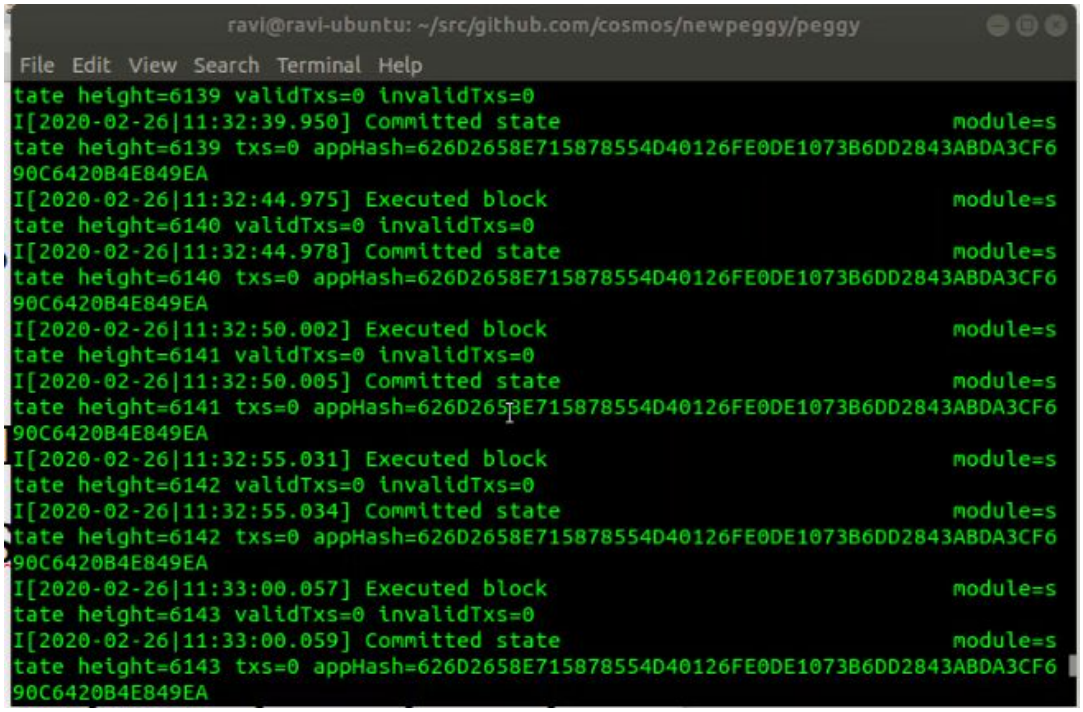

Figure 5.1 — Local instance of Cosmos blockchain.

Truffle provides us with a utility called Ganache that could spin up a local ethereum chain and allow us to interact with and control the same [58].

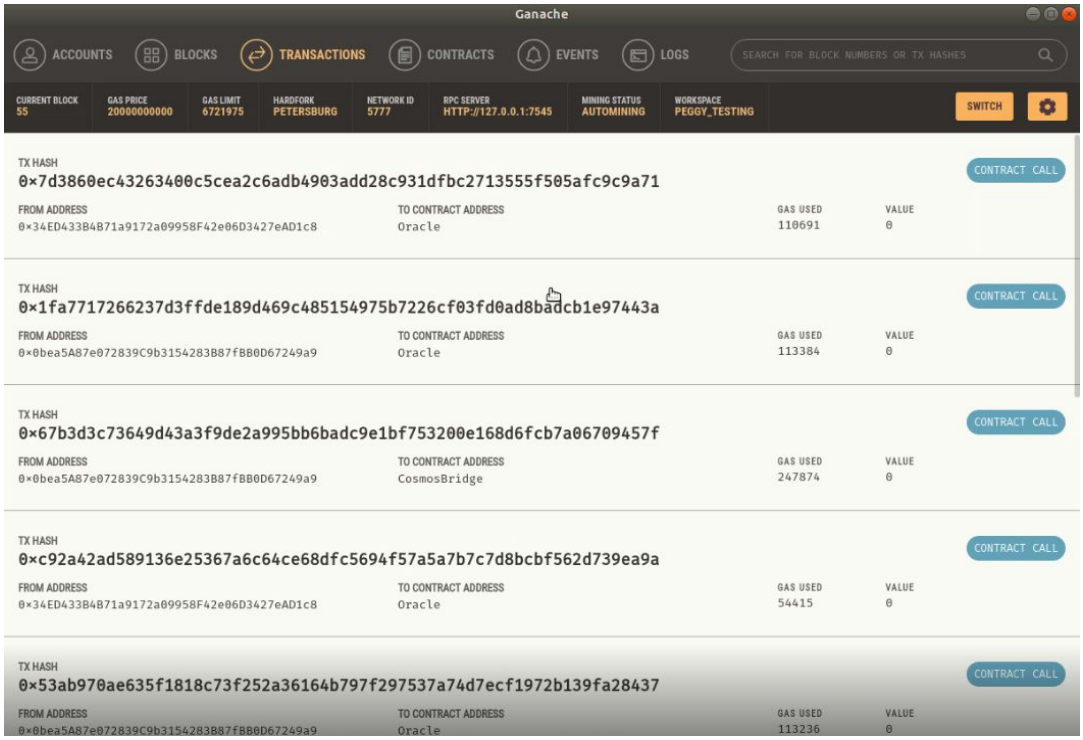

Figure 5.2 — Local instance of Ethereum blockchain using Ganache.

Setting up Self-executing Smart Contracts

In our case, we need smart contracts for most of the steps that accomplish the conversion of tokens. We will first be listing out the smart contracts deployed on the ethereum chain used in the current implementation and stating the need for each of them. Then, we will be covering the smart contract deployments on Cosmos.

Now, the lock transaction could take place on the ethereum chain to initiate minting on Cosmos. The unlock transaction on ethereum could be initiated by a burn transaction on the cosmos chain. This shapes itself as a one-way communication in which the sender is ethereum, and the receiver is Cosmos. It

could be argued that there is also a need for Cosmos to be the sender and ethereum as the receiver. Hence, we would also need to lock and unlock transactions on the cosmos chain. The smart contracts and the modules that we will be setting up would facilitate Duplex communication. Duplex communication would thus involve transactions originating from both the blockchains.

Originator Bank: A smart contract that locks and unlocks ERC20 stablecoins on the Ethereum chain.

Receiver Bank: A smart contract that would facilitate minting and burning of cosmos representative stablecoins on Ethereum.

Registry: A smart contract that acts as an escrow for the token conversion.

Bridge: As the name suggests, this smart contract is a bridge or a line of communication between the two blockchains. It creates burn or lock predictions on the ethereum chain when it hears events happening on the cosmos chain.

Oracle: This contract enables validators to make oracle claims on a prediction claim signaling their agreement to the prediction.

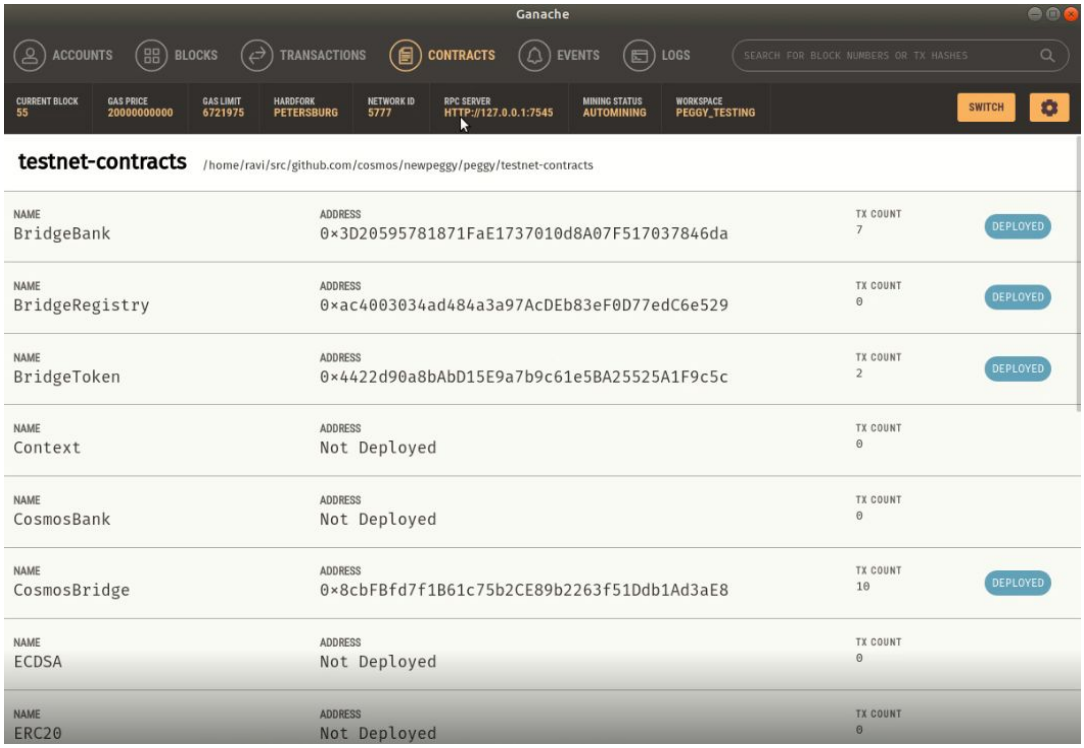

Figure 5.3 — Smart Contracts on the local ethereum chain.

Cosmos allows developers to build application-specific blockchains. Cosmos also provides a rich set of tools within cosmos SDK that could be used to build functionalities on top of the blockchain. On the cosmos side, for our implementation, we use a chain built for our specific purposes. This chain can also be named as a stablecoin transfer specific blockchain. The functionality of this blockchain is decided by how different modules interact with one another.

For our scenario, we need the following modules.

Originator Bank: This module manages locking and unlocking of cosmos stablecoins on the cosmos chain.

Receiver Bank: This module manages the minting and burning of ethereum representative stablecoins on cosmos.

Registry: A module that acts as an escrow for the token conversion.

Auth: This module authenticates the users based on their cosmos address and private key. It also authenticates validators in order to be sure that they are the ones validating the transactions. It also provides features to add new accounts to the cosmos chain.

Setting up Nodes of the P2P Cross-Chain Transfer System

These two blockchains are now set up individually with the modules and the smart contracts deployed. They can now function independently, but we need communication between both to enable a token swap.

A P2P cross-chain transfer system consisting of signers, relayers, and witnesses would facilitate the communication. The validators can have any number of roles from the mentioned three roles. The communication about the activities happening on one chain has to be relayed to the other chain in order to inspire activity on the other chain.These communication messages need to be created, signed, and sent in a way that is understood by the other chain. This is where the three validator roles mentioned in the design chapter come into the picture. Setting up of the nodes with these roles was carried out using the *ebrelayer* utility provided by the cosmos chain [60]. These nodes interface with both the blockchains, subscribing to the events happening, and also interacting with the smart contracts to generate transactions. The

blockchain formed by these nodes is also a type of cosmos blockchain, and thus, it would use utilities from the Cosmos SDK.

The nodes in the P2P system can now listen to the events on one chain and act accordingly with the other chain. For example, nodes would listen to a lock transaction on the ethereum chain and consequently mint new tokens on the cosmos chain.

Why do we need a Stablecoin Bridge Chain?

As mentioned above, we can achieve and execute lock, burn, mint, unlock events and relayer services using open-source libraries provided by Cosmos. Now Blockchain Interoperability Services cater to a large number of Cross-chain applications. For example Cosmos provides tools to the community to create Blockchains, but specifically Cosmos is a network of independent blockchains. They encourage the community to create application specific blockchains [37]. In the implementation chapter, we have presented a stablecoin-conversion specific blockchain and it was developed using Cosmos tools. Ofcourse, in our proposed approach, we have just created the blockchain locally. For the blockchain to be adopted by a large number of nodes, there is a need to create network effects.

Creating Stablecoin Tokens

As mentioned in the design chapter, we can facilitate the transfer of tokens for pairs that are whitelisted. To reiterate, for example, if we wish to swap TOKEN_A on Ethereum for TOKEN_B on Cosmos, we need to whitelist the pair

of TOKEN_A->TOKEN_B at the side of Cosmos. If this is whitelisted, it will validate the cosmos bank module to mint new TOKEN_B tokens.

We have created a token contract named ESC on the ethereum local chain, which is a representation of a stablecoin on ethereum. For our implementation, we would be enabling the transfer of ESC to the Cosmos chain. The resulting token on the Cosmos chain is essentially a proxy of ESC, denoted by ESCP.

If the transfer can be achieved, it can be argued that enabling transfer of multiple tokens on both the chains to and fro is then just a matter of implementing mapping data structures on both the chains which keep track of whitelisted pairs.

Setting up Test users on Both Chains

We will now realize the swap of tokens between the two separate addresses in which the sender is on the local ethereum chain, and the receiver is on the local cosmos chain.

Ganache, along with spinning up a local ethereum chain, also gives us ten wallet addresses. We will be using the address[0], the first address on Ganache, which would be the sender. For simplicity, let us call this address ETH_USER. As described before, the auth module in the cosmos SDK provides a utility to generate new cosmos wallets. We will be adding a new user using the same. For simplicity, let us call this address COS_USER.

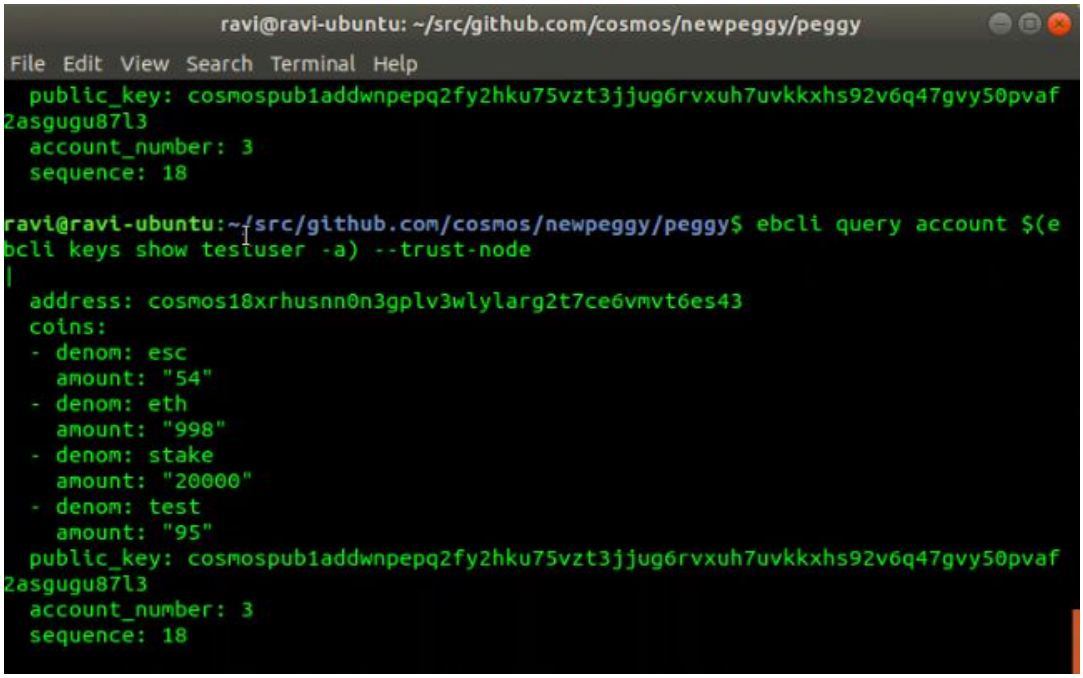

Figure 5.4 — Testuser on the cosmos chain.

Now that we have blockchains, smart contracts, and test users set up, we have all the prerequisites complete, and we will now be describing the process of token swap in detail.

In our case, let us say ETH_USER, a user on the local ethereum chain wants to swap ESC to ESCP(a proxy of ESC on Cosmos) so that COS_USER can use ESCP. ETH_USER is then the sender here, and COS_USER is the receiver. The first step would be to lock ESC from the ETH_USER account, and the next step would be to mint equivalent amounts of ESCP to the COS_USER account.

There could also be a scenario in which the COS_USER wants to swap ESCP to ESC, to send it back to ETH_USER or any other ethereum chain account. For achieving that swap, the first step would be to burn ESCP tokens on Cosmos,

and then the next step would be to unlock equivalent amounts of ESC to send it to an ethereum user.

5.3 Transfer from Ethereum to Cosmos

Lock ESC, Mint ESCP

To facilitate the transfer of ESC from ETH_USER to COS_USER, the smart contracts deployed on ethereum would be locking up ESC. Subsequently, the cosmos modules on the pegged blockchain would trigger minting of equivalent ESC tokens on the cosmos chain. The process has been described below figuratively in Figure 4.5.

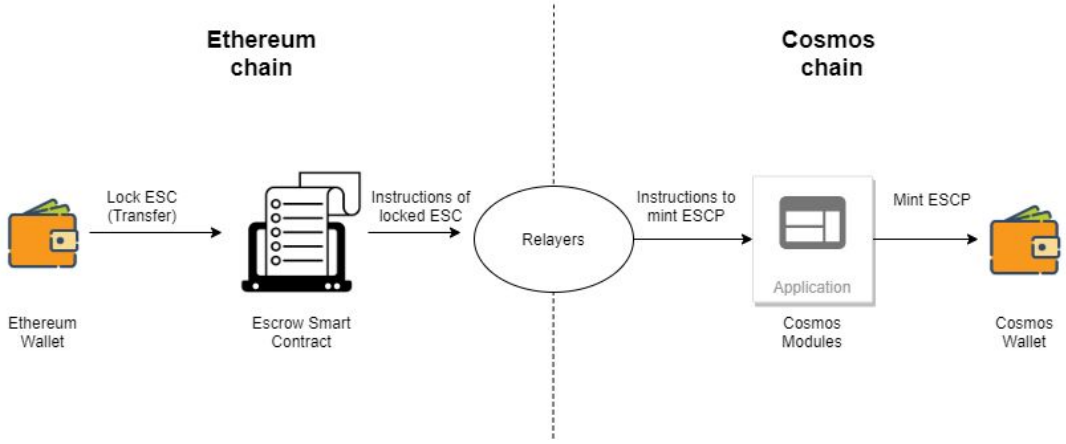

Figure 5.5 — Transfer from ESC to ESCP.

The Registry Smart Contract, deployed on the ethereum chain, acts as an escrow, meaning ESC tokens are sent to this contract address. Once the transfer is complete, the ESC tokens are deemed to be locked. An event containing all the information about the locked ESC is broadcasted to the ethereum chain. The information is a collection of values such as the address

of the ethereum sender, the address of the cosmos recipient, the amount of token with its denomination and the token contract address.

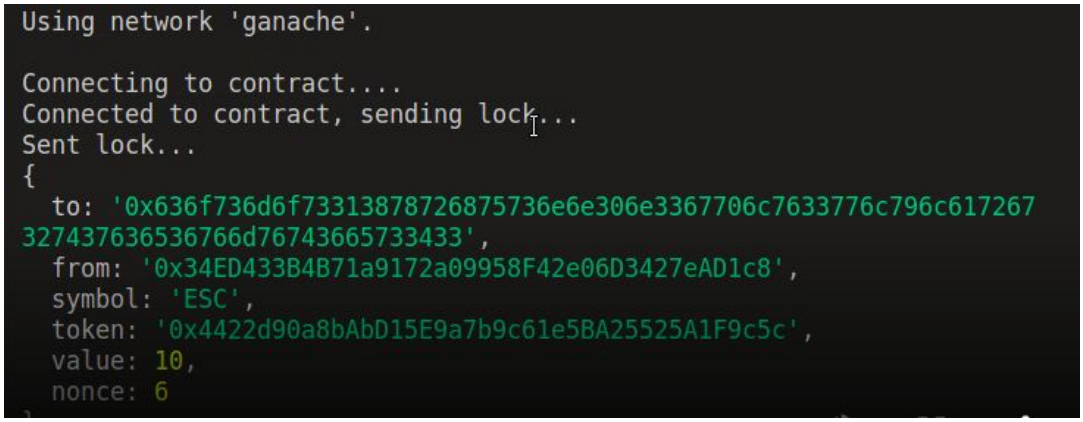

Figure 5.6 — Lock transaction at the ethereum chain.

As described in the flowchart (Fig:2), once the transaction is validated and a witness on the pegged chain witnesses the event, a signed message, representing the ethereum prediction is created. The ethbridge module takes the message and converts it to an oracle claim that could be signed by validators. Once the consensus is achieved on the pegged blockchain, the ethbridge module sends instructions to the cosmos modules. The supply module gets the instruction to increase the supply by the number of tokens to be transferred. The auth module then authenticates the recipient, and on successful authentication, the supply module mints the new tokens, ESCP, and transfers it to the cosmos recipient.

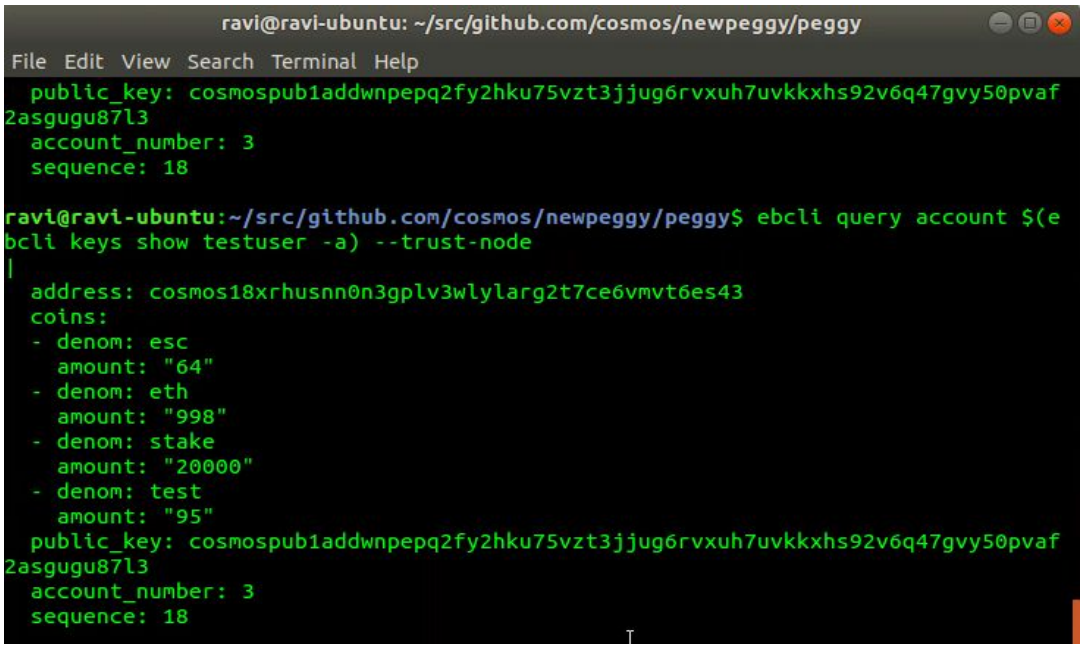

Figure 5.7 — Mint at the cosmos chain.

Thus, the ESC tokens on the ethereum chain have now been made stagnant, and an equivalent amount of ESCP has been minted on the cosmos chain. This concludes ESC to ESCP transfer.

5.4 Reverse Transfer from Cosmos to Ethereum

Burn ESCP, Unlock ESC

The process of transfer from COS_USER TO ETH_USER of ESCP has been described below figuratively in Figure Y.

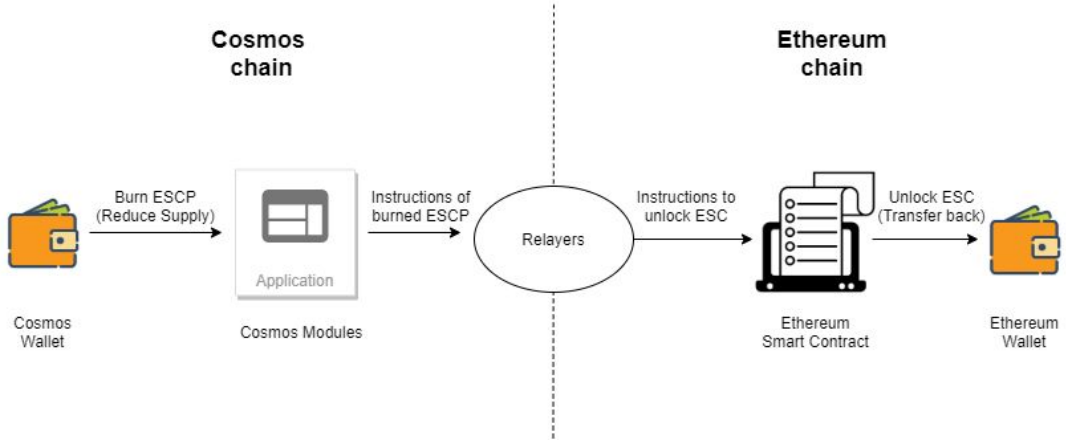

Figure 5.8 — Transfer from ESCP to ESC.

When a token burn is initiated from the cosmos chain, the supply module deflates the supply by the number of tokens to be burned and then consequently broadcasts a burn event. The information about the burn event includes token denomination, amount to be burned, the ethereum recipient, the ethereum token contract address, and all the other information that could be used to identify the transaction uniquely.

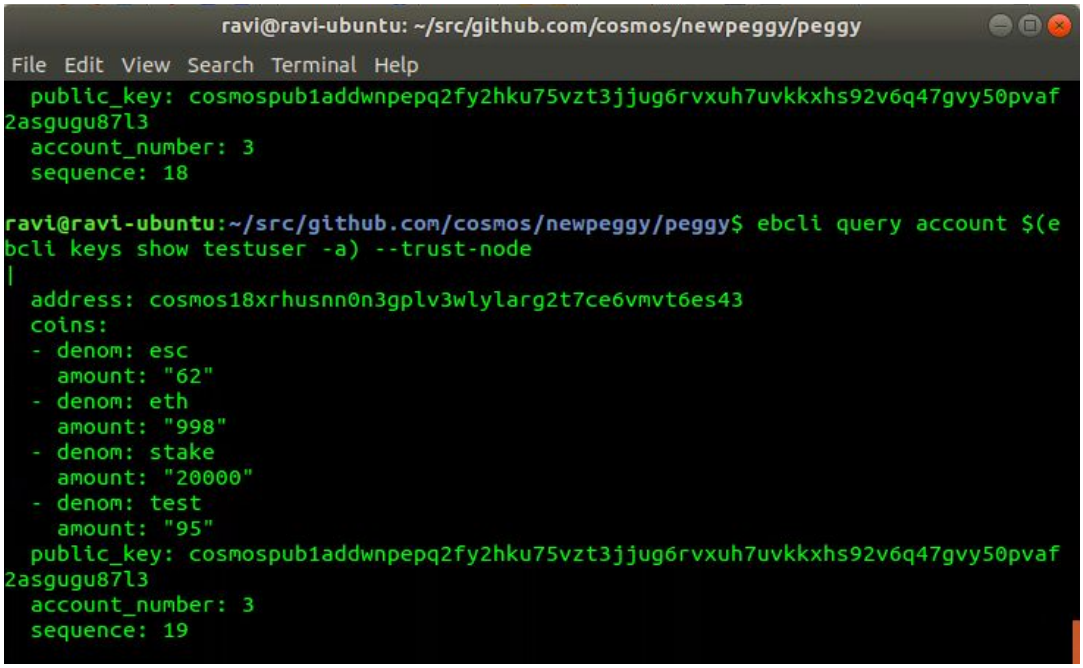

Figure 5.9 — Burn from testuser cosmos account.

Once the transaction is validated and witnessed by the validators on the bridge blockchain, the validator on the bridge blockchain invokes the bridge smart contract on ethereum to create a prediction. This prediction represents a burn event on the cosmos chain. The oracle contract on the ethereum chain then creates a generic oracle claim that ethereum validators can sign. Once the consensus is achieved on the oracle claim, the locked ESC tokens are unlocked by the registry contract and then sent to the intended recipient. Before unlocking the tokens, the locked balance is validated to check if the contract holds enough ESC tokens. This could be understood as a reverse transaction to the escrow transaction that we saw in the first case of locking ESC.

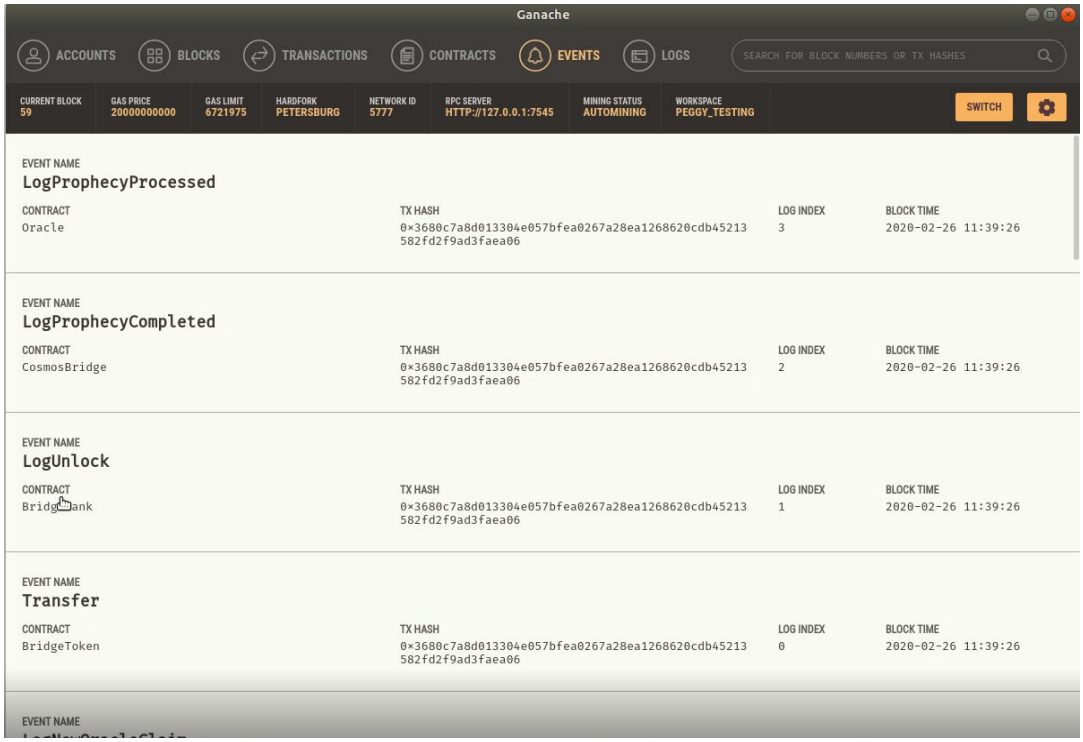

Figure 5.10 — Unlock event at the ethereum chain.

Thus, the ESCP tokens have now been burned on the cosmos chain, and an equivalent number of ESC tokens have been unlocked. This also represents a transfer from the cosmos chain to the ethereum chain, essentially from ESCP to ESC.

The above two processes facilitated the swap of stablecoins that originated at the ethereum chain. Similarly, we can carry out the swap of stablecoins that originate at the cosmos chain. For achieving the same, the assets (tokens) on the cosmos chain would have to be locked to generate cosmos proxy ERC20 tokens on ethereum. Similarly, the proxy tokens on the ethereum chain could be burned to unlock the assets on the cosmos chain.

Chapter 6
Conclusion and Future Work

In the literature review, we highlighted that the problem with the current state of cryptocurrency payments is that volatile cryptocurrencies and centralized intermediaries drive the field. With further analysis and statistics, we inferred that the best solution for enabling cryptocurrency payments is via stablecoins. We also believe that there would be many chains facilitating stablecoins on a global level. This belief pushed us in the direction of designing a system that makes use of the available blockchain interoperability services to enable cross-chain stablecoin transfer.

6.2 Revisit

Let us revisit the research questions that we set about to explore the answers to at the beginning of the thesis.

1. *How effective is it to have a cross-chain stablecoin swap system?*

   Based on the literature review, we infer that there has been considerable interest in the field of stablecoins. Stablecoins have found many use cases in Permissioned as well as Permissionless blockchains. Major organizations and even the governments have been exploring the field for a while now. It can be argued that everyone would not agree on using a single blockchain. Hence the need for a cross-chain stablecoin swap system is justified.

2. *How effectively can we transfer stablecoin from one blockchain to another without using a trusted third party?*

   To answer this question, we explored the interoperability services proposed by various blockchain startups. We were able to transfer stablecoin from the ethereum blockchain to cosmos blockchain without relying on any trusted third party. We achieved the cross-chain transfer utilizing the tools and the utilities provided by Cosmos. We were able to lock stablecoin on the ethereum blockchain and consequently mint stablecoin on the cosmos blockchain.

3. *How can we return stablecoins that have been transferred back to the sending chain?*

   We were able to reverse a stablecoin transfer from the cosmos blockchain to the ethereum blockchain. Utilizing cosmos interoperability services, we can burn stablecoins that are minted on the cosmos chain and consequently unlock on the ethereum blockchain.

4. *How can we ensure that the proposed P2P stablecoin transfer system is decentralized?*

   We can put the nodes of interoperability services on a blockchain to ensure that a small group of validators does not exploit it. Only after our P2P system has received consensus, it triggers the sender and the receiver chain to take action.

We found that because the blockchain technology and the concepts of blockchain interoperability being relatively new, there is a lack of stability in

their implementation. We also inferred that they are rapidly changing and hard to deploy. We believe that the research shows that there is a possibility of designing and implementing a system of cross-chain stablecoin transfer across multiple blockchains without an intermediary.

6.3 Future Work

The system presented here could be expanded to enable the scenario of transfer of different stablecoins on different blockchains. It could then also be utilized to enable cross-chain smart contract calls that can potentially enable cross-chain decentralized finance as well as other blockchain applications like supply chain, digital identification, and others.

The system has not analyzed blockchain miner and validator fees for stablecoin transfer. There can be potential research that analyzes the gas requirements of both the sender as well as receiver chains when performing a cross-chain stablecoin transfer.

The system presented here assumes that for the stablecoin transfer, the underlying represented currency would be the same (in our case USD). It is certainly possible that in the future, there might be a need to enable cross-chain stablecoin transfer between different underlying currencies. For example, we may need a cross-chain transfer between a stablecoin representing USD to a stablecoin representing EUR. The transfer could then be facilitated using trusted, independent sources for the exchange rate and potentially also require counterparties.

References

[1] Cryptocurrency Rankings. (n.d.). Retrieved from https://cryptoslate.com/coins/

[2] Stablecoin Cryptocurrencies. (n.d.). Retrieved from https://cryptoslate.com/cryptos/stablecoin/

[3] CryptoCurrencyChart - Chart top 100. (n.d.). Retrieved from https://www.cryptocurrencychart.com/top/100

[4] Stablecoins. (n.d.). Retrieved from https://www.stable.report/

[5] Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. Journal of Management Analytics, 5(4), 256-275.

[6] What Are Stablecoins? (n.d.). Retrieved from https://www.cbinsights.com/research/report/what-are-stablecoins/

[7] Anderson, M. (2019, February 7). Exploring Decentralization: Blockchain Technology and Complex Coordination · Journal of Design and Science. Retrieved from https://jods.mitpress.mit.edu/pub/7vxemtm3

[8] Nakamoto, S. (2019). Bitcoin: A peer-to-peer electronic cash system. Manubot.

[9] Wolla, S. A. (n.d.). Bitcoin: Money or Financial Investment? Retrieved from https://research.stlouisfed.org/publications/page1-econ/2018/03/01/bitcoin-money-or-financial-investment

[10] Tether: Fiat currencies on the Bitcoin blockchain. (n.d.). Retrieved from https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf

[11] Transparency. (n.d.). Retrieved from https://wallet.tether.to/transparency

[12](n.d.). Retrieved from https://www.bloomberg.com/news/articles/2019-04-30/tether-says-stablecoin-is-only-backed-74-by-cash-securities

[13] Floyd, D. (2018, October 30). The Race to Replace Tether (In 3 Charts). Retrieved from https://www.coindesk.com/race-replace-tether-crypto-stablecoin-charts

[14] Mizrahi, A., Tassev, L., Cryptophyl, Sedgwick, K., Kai, Sedgwick, K., … Btc. (2019, October 13). 5 of the Best Crypto Swapping Services. Retrieved from https://news.bitcoin.com/5-of-the-best-crypto-swapping-services/

[15] Trade Tokens Easily, Securely, & Without Trading Fees. (n.d.). Retrieved from https://www.airswap.io/tokens

[16] Uniswap is a protocol for automated token exchange on Ethereum. (n.d.). Retrieved from https://uniswap.io/

[17] Cosmos. (2020, February 4). cosmos/ics. Retrieved from https://github.com/cosmos/ics

[18] Griffin, J. M., & Shams, A. (2019). Is bitcoin really un-tethered?. Available at SSRN 3195066.

[19] Stablecoins - List, Information, and Overview. (n.d.). Retrieved from https://coincodex.com/stablecoins/

[20] Dell'Erba, M. (2019). STABLECOINS IN CRYPTOECONOMICS: FROM INITIAL COIN OFFERINGS TO CENTRAL BANK DIGITAL CURRENCIES. New York University Journal of Legislation & Public Policy, 22(1).

[21] Blockchain Luxembourg, S. A. (2018). The State of Stablecoins.

[22] Jan. (2018, December 19). How Stable Are Stablecoins? Retrieved from https://santiment.net/blog/stablecoin-volatility/

[23] IBM World Wire. (n.d.). Retrieved from https://beta.stellar.org/case-studies/ibm-world-wire

[24] Orlicki, J. I. (2017). A Stable Coin with Pro-rated Rebasement and Price Manipulation Protection. arXiv preprint arXiv:1708.00157.

[25] DeFi Pulse: The DeFi Leaderboard: Stats, Charts and Guides. (n.d.). Retrieved from https://defipulse.com/

[26] Yao, Q. (2018). A systematic framework to understand central bank digital currency. Science China Information Sciences, 61(3), 033101.

[27] J.P. Morgan Creates Digital Coin for Payments: J.P. Morgan. (n.d.). Retrieved from https://www.jpmorgan.com/global/news/digital-coin-payments

[28] Adrian, M. T., & Griffoli, M. T. M. (2019). The rise of digital money. International Monetary Fund.

[29] The Libra Association, "An Introduction to Libra." https://libra.org/en-us/whitepaper.

[30] Tiutiun, R., Porco, L., Gord, M., & Lee, D. S. USDX: A Decentralized Monetary Policy System.

[31] Herlihy, M. (2018, July). Atomic cross-chain swaps. In Proceedings of the 2018 ACM symposium on principles of distributed computing (pp. 245-254).

[32] Bullmann, D., Klemm, J., & Pinna, A. (2019). In search for stability in crypto-assets: Are stablecoins the solution?. ECB Occasional Paper, (230).

[33] Ehrlich, S. (2019, May 3). After An $850 Million Controversy, What Everyone Should Know About Bitfinex, Tether And Stablecoins. Retrieved from https://www.forbes.com/sites/stevenehrlich/2019/05/02/after-an-850-million-controversy-what-everyone-should-know-about-bitfinex-tether-and-stablecoins/#25ab6032492f

[34] Zhao, W. (2019, August 16). China's Digital Fiat Wants to Compete With Bitcoin – But It's Not a Crypto. Retrieved from https://www.coindesk.com/is-chinas-digital-fiat-a-cryptocurrency-heres-what-we-know

[35] Sinclair, S. (2020, February 18). China's DCEP Unlikely to Impact Crypto Markets in the Long Term, eToro Analyst Says. Retrieved from https://www.coindesk.com/chinas-dcep-unlikely-to-impact-crypto-markets-in-the-long-term-etoro-analyst-says

[36] Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?. Available at SSRN 2709713.

[37] Kwon, J., & Buchman, E. (2016). Cosmos: A network of distributed ledgers. URL https://cosmos. network/whitepaper.

[38] Vitalik Buterin.Chain Interoperability. 2016. URL:https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf

[39] BlockchainHub.Blockchain Oracles.2018.URL:https://blockchainhub.net/blockchain-oracles/

[40] Johnson, S., Robinson, P., & Brainard, J. (2019). Sidechains and interoperability. arXiv preprint arXiv:1903.04077.

[41] Hardjono, T., Lipton, A., & Pentland, A. (2019). Toward an interoperability architecture for blockchain autonomous systems. IEEE Transactions on Engineering Management.

[42] Lerner, S. D. (2019, January 29). RSK Bitcoin Powered Smart Contracts. Retrieved from https://www.rsk.co/Whitepapers/RSK-White-Paper-Updated.pdf

[43] Sysethereum. (n.d.). Retrieved from https://bridge.syscoin.org/

[44] Cosmos. (2020, March 27). cosmos/peggy. Retrieved from https://github.com/cosmos/peggy

[45] Nomic-Io. (n.d.). nomic-io/bitcoin-peg. Retrieved from https://github.com/nomic-io/bitcoin-peg

[46] Hicommonwealth. (n.d.). hicommonwealth/edgeth-bridge. Retrieved from https://github.com/hicommonwealth/edgeth-bridge

[47] Baker, P. (2020, March 5). Web3 Foundation Funds Technical Bridge Connecting Polkadot to Bitcoin. Retrieved from https://www.coindesk.com/web3-foundation-funds-technical-bridge-connecting-polkadot-to-bitcoin

[48] Cross-chain Atomic Swaps for Bitcoin and Ethereum. (n.d.). Retrieved from https://liquality.io/

[49] Blockchain Technology Projects. (n.d.). Retrieved from https://www.hyperledger.org/projects

[50] Nace, S. (n.d.). Topic: Bitcoin. Retrieved from https://www.statista.com/topics/2308/bitcoin/

[51] Wong, J. I. (2017, December 5). CryptoKitties is jamming up the ethereum network. Retrieved from https://qz.com/1145833/cryptokitties-is-causing-ethereum-network-congestion/

[52] Avoiding Blockchain Balkanization. (n.d.). Retrieved from https://consensys.net/research/avoiding-blockchain-balkanization/

[53] Crypto Asset Market Coverage Initiation: Network Creation. (n.d.). Retrieved from https://research.bloomberg.com/

[54] Gaurav. (2020, March 3). Analyzing Cryptocurrencies Github activity. Retrieved from https://blog.coincodecap.com/analyzing-cryptocurrencies-github-activity/

[55] (n.d.). Retrieved from https://coincodecap.com/coins

[56] Cosmos. (n.d.). Retrieved from https://www.youtube.com/channel/UC8HFOUdnMnpoWmQMgeKoB3A/video

[57] Swishlabsco. (2019, June 5). swishlabsco/cosmos-ethereum-bridge. Retrieved from https://github.com/swishlabsco/cosmos-ethereum-bridge

[58] Truffle Suite. (n.d.). Ganache. Retrieved from https://www.trufflesuite.com/ganache

[59] Smart contract. (2020, February 2). Retrieved from https://en.wikipedia.org/wiki/Smart_contract

[60] Cosmos. (n.d.). cosmos/peggy. Retrieved from https://github.com/cosmos/peggy/tree/master/cmd/ebrelayer

[61] Binance Academy. (2020, January 19). What Is a Blockchain Consensus Algorithm? Retrieved from https://www.binance.vision/blockchain/what-is-a-blockchain-consensus-algorithm