UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Cross Chain Transactions in Blockchain Technology

Diploma Thesis

Andreas Mavris

Supervisor: Tousidou Eleni

September 2022

UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Cross Chain Transactions in Blockchain Technology

Diploma Thesis

Andreas Mavris

Supervisor: Tousidou Eleni

September 2022

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Διασταυρωμένες Συναλλαγές στις τεχνολογίες Blockchain

Διπλωματική Εργασία

Ανδρέας Μαυρής

Επιβλέπουσα: Τουσίδου Ελένη

Σεπτέμβριος 2022

Approved by the Examination Committee:

Supervisor **Tousidou Eleni**
Laboratory Teaching Staff, Department of Electrical and Computer Engineering, University of Thessaly

Member **John Moodanos**
Associate professor, Department of Electrical and Computer Engineering, University of Thessaly

Member **George Thanos**
Laboratory Teaching Staff, Department of Electrical and Computer Engineering, University of Thessaly

Acknowledgements

This dissertation would not have been possible without the support of many people. Many thanks to my adviser, Professor Eleni Tousidou, who read my numerous revisions and helped make some sense of the confusion. Also thanks to the committee members, George Thanos and John Moodanos, who offered guidance and accepted being a part of this thesis. I would like to thank Professor Emmanuel Vavalis for introducing me to the path of blockchain technologies.

Finally I would like to thank my family and friends for the guidance and moral support they have given me over the years.

DISCLAIMER ON ACADEMIC ETHICS AND INTELLECTUAL PROPERTY RIGHTS

«Being fully aware of the implications of copyright laws, I expressly state that this diploma thesis, as well as the electronic files and source codes developed or modified in the course of this thesis, are solely the product of my personal work and do not infringe any rights of intellectual property, personality and personal data of third parties, do not contain work / contributions of third parties for which the permission of the authors / beneficiaries is required and are not a product of partial or complete plagiarism, while the sources used are limited to the bibliographic references only and meet the rules of scientific citing. The points where I have used ideas, text, files and / or sources of other authors are clearly mentioned in the text with the appropriate citation and the relevant complete reference is included in the bibliographic references section. I also declare that the results of the work have not been used to obtain another degree. I fully, individually and personally undertake all legal and administrative consequences that may arise in the event that it is proven, in the course of time, that this thesis or part of it does not belong to me because it is a product of plagiarism».

The declarant

Andreas Mavris

Diploma Thesis

Cross Chain Transactions in Blockchain Technology

Andreas Mavris

Abstract

The implementation of cross-chain transactions in blockchain technology is the focus of this research. The goal of this essay is to investigate the issue in depth and to identify the potential and problems presented by this new technological sector of blockchain technology. The essay takes a closer look at the innovation of those cross chain actors and the way transactions are implemented on these protocols. These bridges use a variety of approaches, which operate across blockchains to improve communication and remove trust obstacles. Throughout this dissertation, bridges are classed as natively, externally, or locally certified systems, based on what they connect, asset movement, functionality, and trust.

The descriptive and inductive studies highlighted the adoption of this solution as influential and necessary for the blockchain area, with future growth potential.

Keywords:

cryptocurrency, blockchain, cross chain

Διπλωματική Εργασία

Διασταυρωμένες Συναλλαγές στις τεχνολογίες Blockchain

Ανδρέας Μαυρής

Περίληψη

Η υλοποίηση συναλλαγών μεταξύ των αλυσίδων στην τεχνολογία blockchain είναι το επίκεντρο αυτής της έρευνας. Στόχος αυτού του δοκιμίου είναι να διερευνήσει το θέμα σε βάθος και να εντοπίσει τις δυνατότητες και τα προβλήματα που παρουσιάζει αυτός ο νέος τεχνολογικός τομέας. Σε αυτό το δοκίμιο εξετάζεται πιο προσεκτικά η καινοτομία αυτών των παραγόντων πολλαπλής αλυσίδας και ο τρόπος με τον οποίο υλοποιούνται οι συναλλαγές σε αυτά τα πρωτόκολλα. Αυτές οι γέφυρες χρησιμοποιούν μια ποικιλία προσεγγίσεων, οι οποίες λειτουργούν σε όλες τις αλυσίδες blockchain για τη βελτίωση της επικοινωνίας και την άρση των εμποδίων εμπιστοσύνης. Σε όλη αυτή τη διατριβή, οι γέφυρες ταξινομούνται ως εγγενώς, εξωτερικά ή τοπικά πιστοποιημένα συστήματα, με βάση το τι συνδέουν, την κίνηση των περιουσιακών στοιχείων, τη λειτουργικότητα και την εμπιστοσύνη.

Οι διάφοροι προβληματισμοί και αναλύσεις μέσα από μελέτες τόνισαν την υιοθέτηση αυτής της λύσης ως σημαντικής και απαραίτητης για την περιοχή του blockchain, με μελλοντικές δυνατότητες ανάπτυξης.

Λέξεις-κλειδιά:

κρυπτονόμισματα, διασταυρωμένες συναλλαγές, αποκεντρωμένη οικονομία

Table of contents

Abbreviations

dApps	Decentralize Applications
DeFi	Decentralized Finance
BTC	Bitcoin
ETH	Ethereum
WBTC	Wrapped Bitcoin
DAO	Decentralized Autonomous Organisation

Chapter 1

Introduction

Blockchain is one of the main technologies that has revolutionized many aspects in Finance and Internet of Things. It had an immediate impact on several industries. It was initially used from drug traffickers via the dark web. Over the course of the economy in the last decade, the growth of blockchain has demonstrated that it can be used not only to capture cryptocurrency capabilities, but also to avoid financial disasters. Mismanagement of the economy, such as growing inflation and the cut off balances in Cyprus in 2012 and sanctions against Russia in 2022, demonstrated that decentralized systems are a place where everyone is equal and users are the only ones managing their funds.

Blockchain technology enables decentralized, transparent, and secure networks. It is a distributed ledger system that keeps track of transactions and secures them via encryption. Transactions are recorded in blocks, and these blocks are linked together using hashes. Satoshi Nakamoto first utilized it in 2008 for public bitcoin transactions [1].

This dissertation focuses on the present and dynamic transfer of assets in cryptocurrencies via cross-chain transactions between blockchains. A cryptocurrency (or virtual currency) is a means of exchange that functions similarly to money (it may be used to purchase and sell goods and services), but unlike traditional currencies, it is not bound by national boundaries, central banks, sovereignty, or decrees [2]. The advancement of technology in the twenty-first century has resulted in this new financial breakthrough.

DeFi, short for “Decentralized Finance”, is an umbrella name for a number of financial applications developed on a blockchain with the goal of disrupting financial intermediaries. Most decentralized finance applications are built using Ethereum, the second-largest cryptocurrency network, which differs from the Bitcoin network in that it is simpler to use and to

construct decentralized applications other than standard transactions. Even these more complex financial use cases were highlighted by Ethereum developer Vitalik Buterin in the initial Ethereum white paper back in 2013 [3].

Blockchains have varied operating environments, and different blockchains enable different protocols, dApps(decentralized Applications), and encrypted assets. If someone wishes to keep Bitcoin but also participate in the DeFi protocol on Ethereum, or just trade Bitcoin for Ether (Ethereum's native token), cross-chain infrastructure will be essential. Different blockchains cannot access the data on each other's chains directly since they cannot interact directly, and direct transfers across chains are not possible. To devise a strategy for connecting the disparate assets, cross-chain solutions became essential to the crypto world.

The purpose of this dissertation is to identify the reasoning behind the expansion of dApps beyond the Ethereum blockchain, how the blockchain scalability problem pushed solutions with innovative networks into creation and how a cross chain transaction works. We will analyze the various categories of cross chain applications and how to measure the trust of those implementations. Furthermore, we will examine how cross chain aggregators are designed to meet the demands of everyday users in order to provide results that will be added to the pre-existing literature on the issue and are useful for any source of interest in this manner. For instance, users must be informed of the differences between centralized cross chain platforms and decentralized ones as well as be informed of the risks of lost funds regarding some of those applications. While the DeFi adoption grew in an incredible rhythm during the last years, the need to be cautious still remains intact.

Therefore, the contribution of this dissertation is to try to answer the following questions that justifiably arise:

1. How a cross chain transaction works?
2. What are cross chain bridges?
3. Is cross chain Defi a real sector of growth in the blockchain space?
4. Are cross chain bridges trusted?
5. How important are cross chain aggregators?
6. What is the experience transacting on cross chain aggregators platforms?
7. How are cross chain aggregators compared?

1.1 Methodology

This is a bibliographic study that involved a lengthy investigation into the availability of data from the scientific as well as the cryptocurrency community. In practise, cross chain transaction protocols were build in the last two years therefore data points are sourced from this time frame. Data is initially gathered from scientific sources such as journals, books, and conferences on the subject. These are available in print and online, and may include data, graphs, and tables. Google Scholar is a valuable resource for collecting articles and scientific publications, but so are Science Direct, Research Gate, foreign library websites, and so on. Publications of well-known crypto periodicals such as Coindesk, The Block, Decrypt, and Messari are also noteworthy sources. The information was chosen based on the most current posting date and the prominence of the writers and the validity of facts.

In the next chapters the blockchain conceptual definition will be provided through the Bitcoin blockchain along with the explanation of how blockchain transactions work in Chapter 2. Ethereum Network and the creation of DeFi space will be described in Chapter 3 followed by the description of the blockchain scalability problem, factors affecting scalability of the Ethereum network. The Scalability Trilemma Problem will be addressed in Chapter 4. Which ecosystems were created to tackle these problems and how will be explained in 5, while cross chain transactions referring to the life cycle of a cross chain transaction, Bridges as a spectrum of trust and cross chain aggregators will be presented in Chapter 6. Results from the thesis are found in 7 and lastly, conclusion will be revealed in Chapter 8.

Chapter 2

Bitcoin

Bitcoin is an opt-in currency governed by the "consensus" or will of its users. It is formed of a growing network of people who willingly adhere to the Bitcoin protocol's regulations. They employ decentralized infrastructure to conduct peer-to-peer transactions and hold currency independently of any government, corporation, or financial institution. There is no need to seek authorization to use Bitcoin, and there is no danger of being disconnected from the system. This chapter will provide a comprehensive overview of the Bitcoin network, namely how Bitcoin transactions function and the utility of this currency.

2.1 Overview

Bitcoin emerged as a digital currency in 2009 by an anonymous person using the pseudonym Satoshi Nakamoto [1]. Bitcoin was founded in order to solve the middle men problem which is observed in the real world with the banking system. Satoshi built Bitcoin to run on decentralized trust with no central entities authorizing the transactions of the network. Cryptography is used by network nodes to validate transactions, which are ultimately deposited in a public distributed ledger known as a blockchain.

As stated by Antonopoulos [2], users have the ability to use Bitcoin to accomplish almost anything that can be done with traditional currencies, such as purchase and sell items, send money to people or organizations, and provide credit. At central exchanges, Bitcoin may be bought, traded, and swapped for other currencies. Bitcoin is, in some ways, the ideal form of online money since it is quick, safe, and borderless.

From a technological standpoint, bitcoin is a new sort of database that allows "everyone"

(i.e., anybody who is a part of the bitcoin network) to read it. It is distinct from a regular database system in that no one may change or remove a transaction. Bitcoin is not connected to the Internet, but it does require a means of communication, such as radio waves or Bluetooth. Bitcoin is a unique unit on the blockchain, not a money per se. The bitcoin's owner has the option of transferring ownership to another individual. Figure 2.1 shows how Nakamoto solves the problem of privacy. The privacy is usually provided by the bank in the traditional transfer mechanism. For bitcoin, when the anonymity is built into the protocol, there is no alternative.

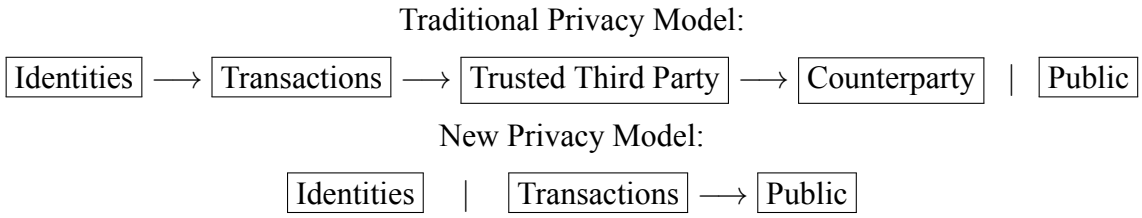

Figure 2.1: Privacy Model suggested by Satoshi Nakamoto

2.1.1 Proof of Work (PoW)

A proof of work is a piece of data that was difficult (expensive, time-consuming) to create in order to meet particular standards. Generating a proof of work can be an arbitrary and low-probability procedure, requiring a lot of trial and error on average before a suitable proof of work is achieved. Bitcoin employs hashcash proof of work, whereby all bitcoin miners, whether CPU, GPU, FPGA, or ASICs, commit effort to generate hashcash proofs-of-work (counts as compute power), which function as a vote in the blockchain development and validate the blockchain ledger of transactions [1].

The proof-of-work consensus algorithm involves looking for a hashed value that begins with an amount of zero bits, such as the algorithm SHA-256. The median amount of effort required is related to the number of required zero bits and may be confirmed with only a single hash. In their timestamp network, Nakamoto developed proof of work by significantly improving a "nonce" in the block before a number is discovered that yields the block's hash with the required zero bits [4]. Nonce is an abbreviation for "number used once". It is a random number which can only be used once. Nonces are created for a specific purpose, most commonly to alter the outcome of a function in a cryptographic transaction. A nonce is often a number that changes over time to ensure that some values cannot be repeated. It

might be a timestamp or a specific marking used to prevent illegal file replication.

The purpose of Bitcoin's PoW mining method is to solve a mathematical puzzle in order to get the next block hash and earn Bitcoin rewards. Figure 2.2 shows the Bitcoin block hash. The header of each block on the Blockchain contains the Merkle Root (A Merkle root is the hash of all the hashes of all the transactions in a blockchain network that comprise a block), timestamp, preceding block hash, and a nonce. The nonce is the sole non-predetermined field in the header.

Miners must obtain a nonce value that, when fed into the hashing process, produces a hash value less than the goal difficulty. The nonce may be thought of as the final piece of the puzzle required to identify the next block, and miners earn the block reward.

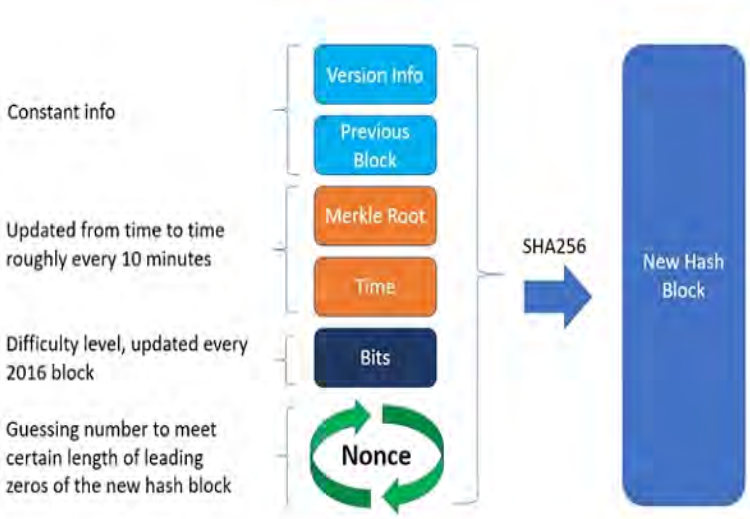

Figure 2.2: Bitcoin Block Hashing (source: B.2)

Proofs of work linked to each block's data are necessary for the blocks to be approved. The difficulty of this work is changed to limit the network's ability to produce new blocks to one every 10 minutes. Because of the extremely low likelihood of successful generation, it is impossible to anticipate whichever worker node in the network will be able to create the next block.

To be legitimate, a block must hash to a number smaller than the current goal; this implies that each block demonstrates that effort was done to generate it. Each block contains the hash of the previous block, resulting in a chain of blocks containing a tremendous amount of work. Replacing a block (which can only be accomplished by creating a new block with the same predecessor) necessitates regenerating all successors and performing the work they contain. This prevents tampering with the block chain.

The proof-of-work also solves the problem of determining representation in majority decision-making. Everyone with access to a vast number of IP addresses could undercut a one-IP-address-one-vote consensus. In proof-of-work, one CPU represents one vote.The longest chain with the highest proof-of-work effort indicates the majority preference. If honest nodes control the overwhelming bulk of CPU power, the truthful chain will grow the fastest and exceed all others.To modify a prior block, an attacker would have to reconstruct the proof of work for that block, as well as all following blocks, and afterwards make up ground with and outperform the honest nodes' effort. To address these difficulties, massive processing power and cutting-edge technology are necessary. Miners are compensated in Bitcoin, which is then issued into circulation, thus the phrase Bitcoin mining.

2.2 Bitcoin Transactions

Transactions are similar to lines in a double-entry ledger. Each transaction has one or more "inputs", which function similarly to debits on a bitcoin account. There are one or more "outputs" on the other side of the transaction, which are similar to credits deposited to a bitcoin account. The debits and credits (inputs and outputs) do not always add up to the same amount. Instead, outputs are slightly less than inputs, and the difference is an inferred transaction fee, which is a slight charge received by the miner who records the transaction [1]. For each amount of bitcoin (inputs) whose value is being spent, the transaction additionally contains evidence of ownership in the form of a digital confirmation from the owner, which can be independently confirmed by anybody. Signing a transaction that transfers value from a prior transaction to a new owner indicated by a bitcoin address is known as "spending" in bitcoin. To understand how Bitcoin transactions operate, have a look at the instance below.

Bob is broadcasting his planned transaction to the Bitcoin network using his wallet software. Before they can be validated by a specialized group of network users known as "miners", Bob's keys have to be able to obtain the inputs (i.e., the address(s) out of which he acquired over time the bitcoin he seems to represent). Miners can also generate a block by merging a list of other transactions which were broadcasted to the network simultaneously as of Bob's. Any miner who has completed the "Proof of Work" is permitted to recommend a new block to be placed to the blockchain or "connected" to it by citing the previous block.The new block is then broadcast to the network. Other network members (nodes) will forward it

if they agree it is a valid block (i.e., its transactions satisfy all protocol requirements and correctly reference the prior block). Another miner will ultimately build on top of it by alluding to it as the preceding block when proposing the next block. Any transactions in the previous block will have been "verified" by the following miner. As blocks are added to the chain, the count of approvals for Bob's transaction climbs.

2.2.1 Constructing the Transaction

This section will define each component and illustrate how to utilize them in conjunction to create entire transactions.

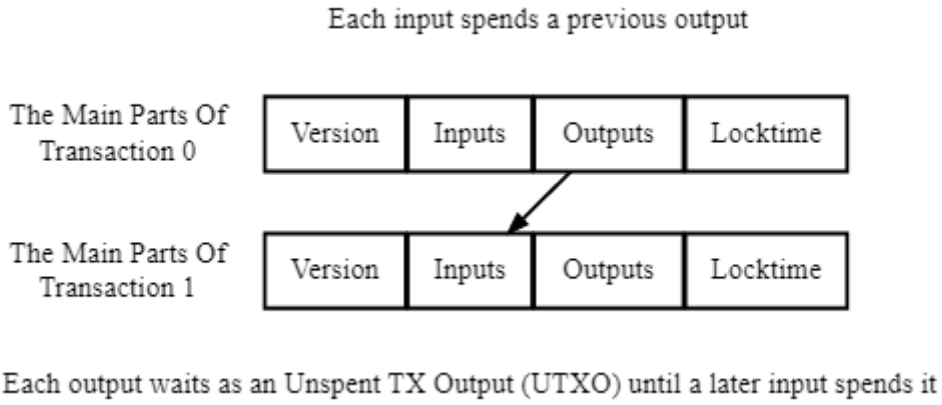

Figure 2.3: Components of a Bitcoin transaction (source B.2)

The diagram in Figure 2.3 depicts the essential components of a Bitcoin transaction. Each transaction contains one or more inputs and outputs. The satoshis (base unit of bitcoin, more about definition in B.1) paid to a prior output are spent on each input. Each output then acts as an Unspent Transaction Output (UTXO) until it is spent by a subsequent input. When your Bitcoin wallet displays a 10,000 satoshi balance, it actually implies that you own 10,000 satoshis in one or more UTXOs.

A four-byte transaction version number precedes each transaction, informing Bitcoin peers and miners about the body of norms to be applied to validate it. This allows developers to create new transaction criteria without invalidating current ones.

Based on its position in the transaction as shown in Figure 2.4 , each output has an implied index number— first output's index is zero. A satoshi payout to a conditional pubkey script is also included in the output. Anyone who can fulfill the pubkey script's conditions may spend up to the number of satoshis contributed to it.

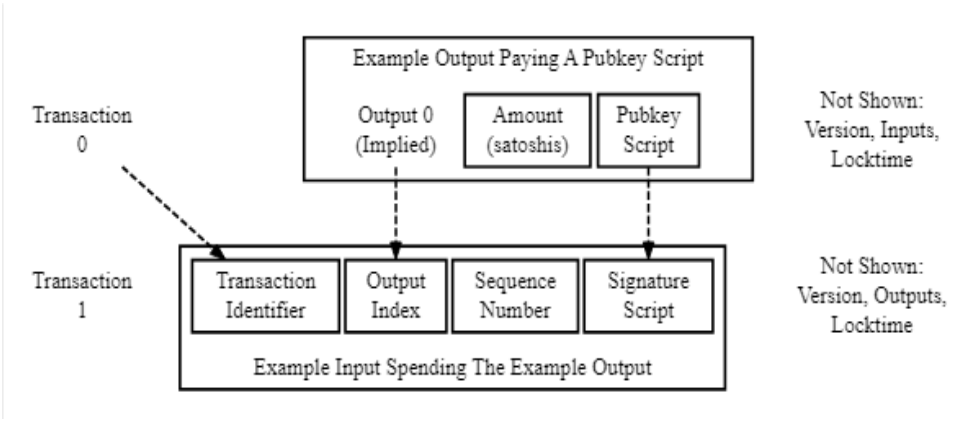

Figure 2.4: Overview of Transaction Spending (source B.2)

An input identifies a specific output to be spent by using a transaction identifier (txid) and an output index number (commonly termed "vout" for output vector). It also has a declaration script that permits it to provide data parameters that satisfy the conditionals of the pubkey script. (The sequence number and the locktime are linked and will be described together in the following paragraph.)

The graphics in Figure 2.5 represent the process Alice uses to send Bob a transaction and which Bob subsequently uses to spend that transaction, which helps to clarify how these capabilities are employed. Both Alice and Bob will utilize the most popular Transaction type Pay-To-Public-Key-Hash (P2PKH). This type enables Alice to spend satoshis to a regular Bitcoin address, and thereafter Bob to spend those same satoshis using a simple cryptographic key pair.

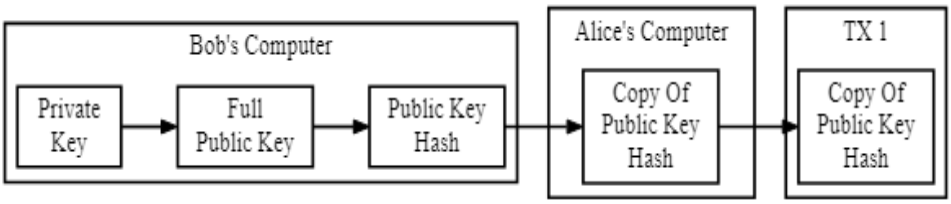

Figure 2.5: Creating a P2PKH Public Key Hash To Receive Payment (source B.2)

Bob must first create a private/public key pair so Alice can make the first transaction. Bitcoin employs the Elliptic Curve Digital Signature Algorithm (ECDSA) with the secp256k1 curve; secp256k1 private keys are 256 bits of arbitrary data. A copy of the data is deterministically converted into a secp256k1 public key. The public key is not required to be saved because the transformation may be securely performed later.

The public key (pubkey) is then hashed cryptographically. This pubkey hash may also be successfully replicated afterwards so it isn't necessary to preserve it. The hash shortens and obfuscates the public key, making manual transcription easier and protecting against unanticipated mistakes that could make private key rebuilding using public key data at a later date.

Bob gives the pubkey hash to Alice. Pubkey hashes are almost often transmitted as Bitcoin addresses, that are base58-encoded strings including an address version number, the hash, and an error-detection checksum to identify typos. The address can be communicated through any medium, including one-way channels that prevent the sender from communicating with the receiver, and it can also be encoded into some other shape, including a QR code with only a "bitcoin" URI (Unique Resource Identifier, more about definition B.1).

After knowing the address and decoding it back into a regular hash, Alice may initiate the first transaction. She prepares a standard P2PKH transaction output with directions that enable anybody to spend the output provided they can demonstrate ownership of the private key that matches to Bob's hashed public key. These instructions are referred to by the pubkey script or scriptPubKey.

The transaction is broadcasted by Alice and added to the block chain. It is classified as an Unspent Transaction Output (UTXO) by the network, and it is shown as a spendable balance by Bob's wallet software. When Bob intends to spend the UTXO later as shown in Figure 2.6, he must establish an input that identifies the transaction Alice generated by its hash, known as a Transaction Identifier (txid), and the exact output she used by its index number (output index).

He must next construct a signature script, which is a collection of data attributes that fulfill the conditions Alice stated in the pubkey script for the preceding output. Signature scripts are sometimes known as ScriptSigs. Pubkey and signature scripts provide a customizable authorisation system by combining secp256k1 pubkeys and signatures with conditional logic.

Bob's signature script will comprise the following two bits of data for a P2PKH-style output:

- His entire (unhashed) public key, so that the pubkey script may confirm that it conforms to the exact same number as Alice's pubkey hash.
- The ECDSA cryptographic procedure was used to construct a secp256k1 signature by mixing certain transaction data (described below) with Bob's private key. This enables

the pubkey script to validate Bob's ownership of the private key that created the public key. Bob's secp256k1 signature not only demonstrates that he has authority over his private key; it also makes the non-signature-script elements of his transaction tamper-proof, enabling Bob to send them securely through the peer-to-peer network.

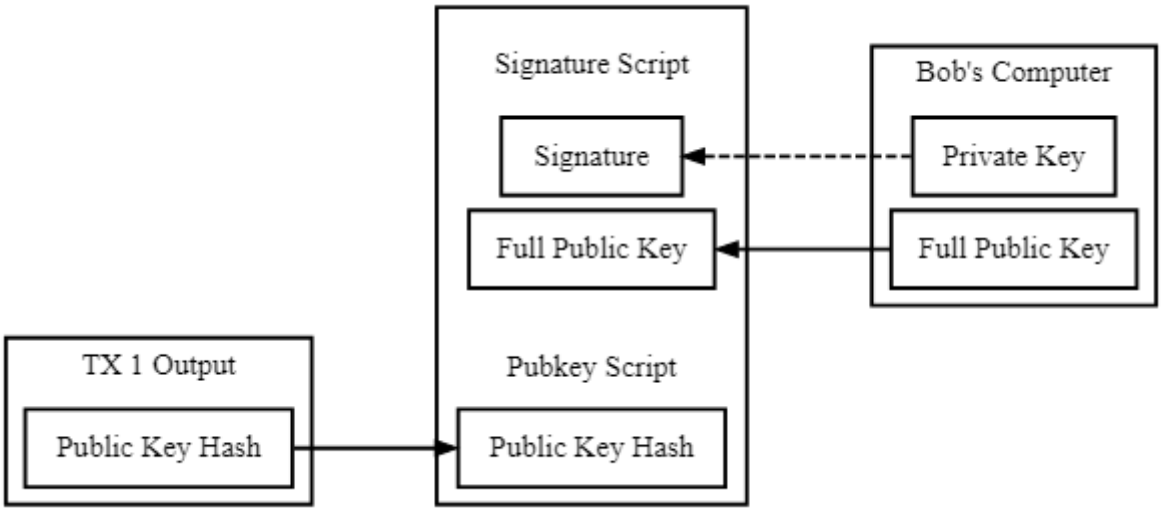

Figure 2.6: Spending A P2PKH Output (source B.2)

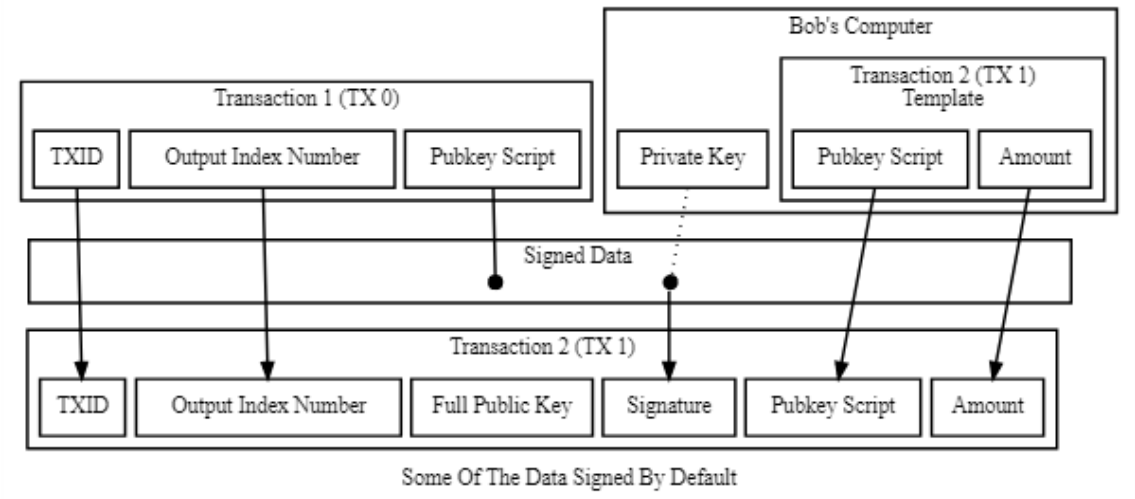

Figure 2.7: Collective data of a transaction (source B.2)

As shown in Figure 2.7, the information Bob signposts confirms the full transaction's txid and output index, the previous output's pubkey script, the pubkey script Bob produces that will enable the very next recipient to splurge this transaction's output, and the amount of satoshis to spend to the next recipient. In effect, the entire transaction is verified, with

the exception of any signature scripts including the full public keys and secp256k1 signings. Bob transmits the transaction to Bitcoin miners via the peer-to-peer network after putting his signing and public key into the verification script. Each peer and miner validates the transaction individually before broadcasting it further or attempting to incorporate it in a fresh block of transactions.

2.2.2 Use of Bitcoin

Bitcoin has been referred to as a money, a commodity, and an investment. On both sides, there are supporters and opponents. The increase of futures trading as a percentage of Bitcoin's trading volume implies that most people consider it as a commodity rather than a currency. Bitcoin has been labeled as digital money, digital gold, a hoax, an asset, a commodity, and the end of modern capitalism as we recognize it over the years. With the price of the largest cryptocurrency continuously climbing, it's worth revisiting where Bitcoin sits in the eyes of those seeking to define it.

Bitcoin as a form of currency, may be used to purchase a wide range of goods. From vacations to artwork, cuisine, vehicles, and real estate, there is something for everyone. Laszlo Hanyecc agreed to pay 10,000 Bitcoin in exchange for two Papa John's pizzas in May 2010 [5], which was one of the first proofs of concept for Bitcoin. The occasion is now lovingly known as "Bitcoin Pizza Day"

Since then, over 100,000 different websites have begun to accept Bitcoin as a form of payment. Interestingly, it looks that Bitcoin is drifting away from its position as a currency. Since 2018, Bitcoin's trading volume has been falling, with Ethereum taking over as the most traded asset. Furthermore, according to Stevens [6], the number of Bitcoin addresses holding more than 0.1 coins (now approximately $4,700) is at an all-time high metrics as Glassnode (Glassnode is a top tier on chain blockchain data platform) data suggest, while the number of addresses holding more than 100 coins (currently about $4,700 million) has hit a six-month high.

Last but not least, for a cryptocurrency to be viable, its volatility must be low. When a currency fluctuates dramatically, it is difficult to accurately price commodities and services. Particularly once Bitcoin transaction latencies are included. You can decide on a price for an item, but the value may rise or fall throughout the transaction time - which might be days if the network is congested - making money flow management extremely difficult.

The yearly volatility rate of most major currencies is between 0.5 and 1 percent every 30-60 days. Bitcoin's price hovered at 4-5 percent throughout 2018, but has subsequently fallen. At the time of writing and as shown in Figure 2.8, it has dropped to 2.25 percent in the previous 60 days. However, in terms of stability, it is still a long way from the US Dollar. So, while you may certainly use Bitcoin to buy and sell items, it looks that the majority of the crypto community views the project as more useful as something else.

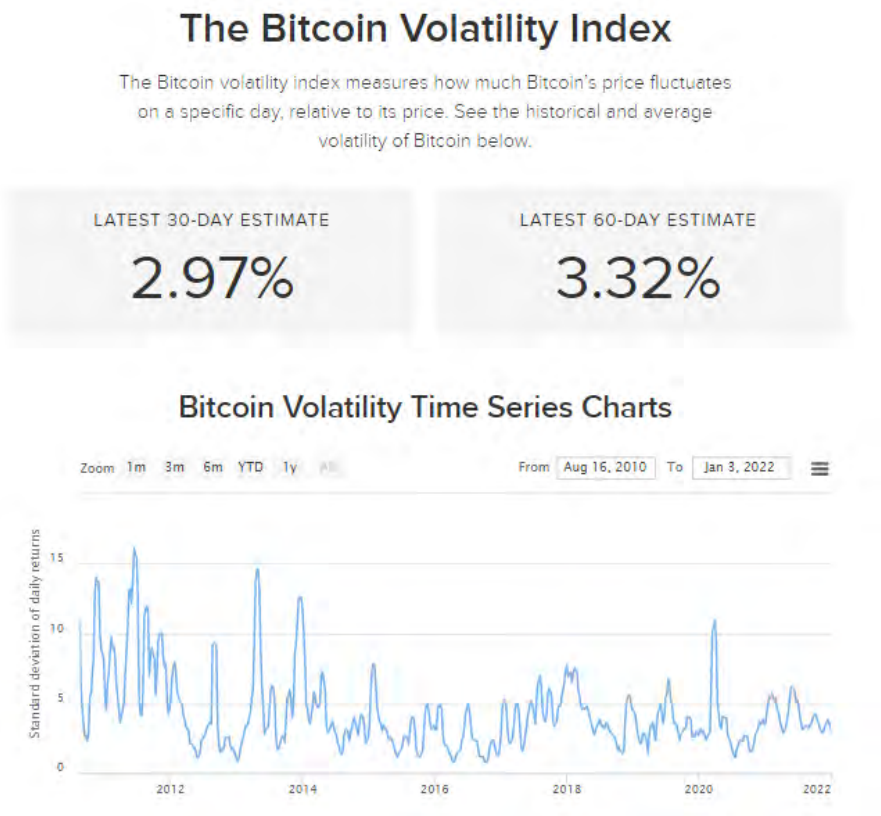

Figure 2.8: Bitcoin Volatility (source B.2

By observing Bitcoin as a holding tool, something you acquire and retain in the belief that the price will rise, there appear to be two factions: Bitcoin enthusiasts and Bitcoin skeptics [7]. According to Pokima [8] companies like MicroStrategy Tesla and Square, have placed large bets on Bitcoin as an investment. These firms are widely recognized as Bitcoin's most prominent institutional investors, having invested approximately $11.8 billion in the cryptocurrency. They have two perspectives on Bitcoin's potential as an asset.

The first is concerning its status as a money supply that goes beyond the quantitative easing that some of the world's greatest nations are now doing. As per MicroStrategy CEO Michael Saylor, when traditional finansial institutions create money, the value of all purchases made with that currency, including stocks and bonds, falls [9]. Nobody or nothing, however,

can reverse that with Bitcoin. It is non-inflationary and has a fixed money base. As a result, believers consider BTC to be an investment. And it's easy to understand why. On a $550 million investment, MicroStrategy had a $133 million profit.

The second is its capacity to serve as an on-ramp for vast swaths of the world that are not currently served by financial services. Chaia et al., found that currently, 2.5 billion individuals worldwide do not utilize banks or microfinance organizations to save or borrow money [10]. Part of this is due to banks' perceptions of this group's profitability versus the expenses to contact them. The other factor is the status of the currencies that many of the world's unbanked must utilize.

While the US dollar, Euro, British Pound, and Japanese Yen are often regarded as the cornerstones of global currency markets, there are many more currencies that are less reliable. The Venezuelan Bolivar Soberano and the Zimbabwe Dollar, for example, have both plummeted by more than 70% versus the US dollar this year. Others, though, are not far behind: the Seychelles Rupee, the Zambian Kwacha, and the Brazilian Real have all lost 20% of their value[11].

When currencies depreciate rapidly, governments tend to restrict citizens' access to foreign money in order to avoid further depreciation. Furthermore, banks regard banking citizens of these fluctuating currencies as too hazardous, keeping them out of such markets. Bitcoin, on the other hand, has not similar concerns. Anyone with an internet connection and a USB stick may invest, making it an ideal investment tool for one-third of the world's population—and thus an excellent investment to make now for when that happens.

However, others see Bitcoin as a terrible investment vehicle especially because it does not comply to the structures and organizations that fiat money does. Mariathasan in IPE, a renowned newspaper for institutional investors in Europe, advised its readers early in 2020 to avoid Bitcoin as an investment due to a lack of clear legislation governing things like credit intermediation and regulation [12]. It said that because there was no established marketplace for institutional-only cryptocurrency trading and no significant banks providing liquidity to traders, it was viewed as an investment that was too far beyond what wealth managers would normally choose.

There is also the argument that investments are not the same as speculative assets such as commodities. As an example, consider the pension sector. The worldwide pool of capital now held in pension funds, estimated at $3.6 trillion, would not invest or speculate on

currency performance. This is happening because it is a zero-yielding asset, which means that keeping it produces no extra earnings beyond the rise and fall of the underlying asset. Property, for example, is a high-yielding asset, making it a popular choice for the world's pension administrators. That isn't to say that there aren't new methods to generate income from cryptocurrencies; for example, AAX's Savings, a feature in AAX cryptocurrency exchange, is a terrific way to earn interest on crypto assets. Those in possession of some of the world's greatest sums of money, on the other hand, are staying away for the time being.

So, if Bitcoin fails to remain stable to really be a currency, and its lack of control makes it unappealing for large investments, how does it do as a commodity? As a review, commodities are a form of fundamental good that may be exchanged for other items of the same type. A commodity produced by one producer is essentially the same as a commodity produced by another producer. Commodities in the real world include gold, grain, oil, beef, natural gas and foreign currency.

More financial items, like Bitcoin, have been added to the commodities list in recent years. In the United States, the Commodities Futures Trading Commission classified Bitcoin as a commodity in 2015. But, in practice, what does this mean? Commodities have historically had more price volatility than assets such as real estate or money sources such as currency, making them a fertile environment for speculators attempting to forecast an asset's rise and fall and betting accordingly. This is where futures trading takes place, a market in which traders try to forecast which direction a commodity will swing.

Since the Chicago Board Options Exchange (CBOE) launched the first Bitcoin futures product in December 2017, they have surged in popularity, accounting for more than 75% of all Bitcoin transaction activity [13]. Bitcoin appears to function on two separate investing horizons as a commodity. Short-term volatility, daily volatility, and long-term speculation.

Additionally, Bitcoin is more tightly managed as a commodity than it is as money or an investment. There is an air handling units that has sussed out non-compliant exchanges as a result of the Chicago Board Options Exchange. The most notable example is BitMEX Exchange, which has been accused of running an unregulated trading platform, according to [14]. Because futures markets enable customers to speculate without owning the underlying asset, corporate interest in Bitcoin has grown, allowing Bitcoin to be regarded as being more of a commodity then anything.

Chapter 3

Ethereum

Ethereum is a community-run platform that underpins the ether (ETH) cryptocurrency as well as numerous of decentralized apps. It uses blockchain software to prevent smart contracts and bitcoin trades without involving a third party. Ethereum supports two types of accounts: externally owned accounts and contractual accounts. Ethereum enables developers to create a diverse range of decentralized applications. This chapter will examine the Ethereum network and the development of Decentralize Finance in the cryptocurrency area, as well as an overview of its multiple applications.

3.1 Overview

In 2013, Vitalik Buterin, who is credited with inventing the initial Ethereum concept, issued a white paper introducing Ethereum. Buterin and Joe Lubin, creator of the blockchain software startup ConsenSys, established the Ethereum platform in 2015 [3]. The Ethereum creators were among the first to evaluate the entire potential of blockchain technology, which goes beyond allowing safe exchange of virtual money. Ethereum is frequently referred to be the second most common cryptocurrency after Bitcoin.Alternatively, Ethereum refers to itself as a decentralized computer network based on blockchain technology. Ethereum native token is called Ether (ETH). Like Bitcoin, Ether can be used to purchase and exchange goods and services. Its value has also surged significantly in recent years, putting it a speculative investment. Regardless, what sets Ethereum apart is that users may construct applications that "run" on the blockchain in a same way that software "runs" on a computer. These applications have the capacity to store and exchange private information as well as execute complex

financial transactions.

The Ethereum network may also be utilized for data storage and the execution of decentralized apps [15]. People may host apps on the Ethereum blockchain rather than on a server owned and controlled by Google or Amazon, where just one business controls the data. This provides consumers autonomy over their data and allows them to freely use the app because there is no centralized authority regulating everything.In the Ethereum universe, there is a single, canonical computer (called the Ethereum Virtual Machine, or EVM) whose state everyone else on the Ethereum network agrees on. Every Ethereum network member (every Ethereum node) stores a copy of this computer's state. In addition, any user can send a request to this computer to do any arbitrary computation. When a demand is published, other network members check, confirm, and carry out the computation ("execute"). This execution results in an EVM state alternates, which is verified and broadcast across the network [16].

Self-executing contracts, also known as smart contracts, are one of the most exciting use cases for Ether and Ethereum. As with any other contract, two parties form an agreement concerning the supply of products or services in the future. Unlike traditional contracts, no attorneys are required: The contract is coded on the Ethereum blockchain by the parties in Solidity program language, and when the requirements of the contract are satisfied, it self-executes and distributes Ether to the relevant party. Furthermore, given the importance and expanding scale of the Ethereum network, Ethereum is the main blockchain for non-fungible tokens (NFTs), which are growing in size and popularity at an astounding rate, with a burgeoning scholarly literature analyzing the nature of these new forms of art [17].

3.2 Ethereum Consensus: PoW to PoS

Similar to Bitcoin, Ethereum now employs a proof-of-work (PoW) consensus process. The network is maintained safe by the fact that defrauding the chain would need 51 percent of the network's computer power. This would necessitate such large investments in equipment and energy that you would most certainly end up spending more often than you would gain [18].

Ethereum intends to transition to a proof-of-stake (PoS) consensus mechanism. Validators who have staked ETH participate in the process of proof-of-stake. To produce new blocks, share them with the network, and collect rewards, a validator is picked at random. Instead

of performing intensive computing labor, you must merely have staked your ETH in the network. This is what motivates good network behavior [19].

Proof-of-stake introduces many enhancements to the proof-of-work system:

1. Improved energy efficiency
2. Lower access barriers, less hardware needed – It is not necessary to have high-end hardware to be able to create new blocks
3. More resistance to centralization — proof-of-stake should result in more nodes in the network
4. Improved shard chain support — a critical step forward in scaling the Ethereum network

Proof-of-stake is the fundamental technique that activates validators when sufficient stake is received. To become a validator on Ethereum, individuals must invest 32 ETH. Validators are picked at random to produce blocks and are in charge of inspecting and validating blocks that they do not generate. A user's stake is also utilized to motivate positive validator behavior. For example, a user may lose a portion of their share if they go offline (fail to validate) or their entire stake if they engage in willful collusion. Validators, unlike proof-of-work, do not require considerable amounts of processing power since they are chosen at random and are not competing. They do not need to mine blocks; instead, they must produce blocks when they are selected and validate suggested blocks when they are not. This is referred to as attesting. Attesting might be thought of as stating, "This block seems okay to me". Validators are rewarded for suggesting new blocks and attesting to those they've seen. You lose your stake if you attest to malicious blocks [18].

3.3 Gas – Block Limit

One significant distinction that investors should be aware of is how the Ethereum and Bitcoin networks handle transaction processing fees. These costs, known as "gas" on the Ethereum network, are paid by Ethereum transaction participants. The costs connected with Bitcoin transactions are absorbed by the Bitcoin network as a whole. The charge, or pricing

value, needed to effectively conduct a transaction or execute a contract on the Ethereum blockchain platform is referred to as gas [20].

The gas, which is paid in tiny percentages of the cryptocurrency ether (ETH), is used to allocate money of the Ethereum virtual machine (EVM) so that decentralized applications like smart contracts could self-execute in a secured and decentralized manner. The real price of the gas is determined by the market among network miners, who might reject to perform a deal if the gas price falls below their threshold, and network users looking to front run the rest with higher gas bids to speed their transaction process [21].

The reason for this cause is that the size of the blocks themselves is limited. Each block has a goal size of 15 million gas, although the size of blocks will vary depending on network needs, up to the block maximum of 30 million gas (2x target block size). The total quantity of gas consumed in the block by all transactions must be less than the block gas limit. This is significant because it prevents blocks from becoming arbitrarily huge. If blocks could be arbitrarily huge, less performant full nodes would progressively lose their ability to keep up with the network owing to space and performance constraints [22].

3.4 Ethereum Transactions

As seen in Ethereum Whitepaper [3], a transaction in Ethereum is made up from the recipient address as well of the sender's signature and transaction amount. Also, it consists of gas price value which calculates the amount paid by the sender at each computational step, the start gas value which determines how many computing steps the transaction is permitted to do and an option field.

Most cryptocurrency transactions have the same top three values. Bitcoin transactions, for example, have all three data. However, the gas and start price numbers are distinctive to Ethereum transactions and play a significant role in preventing spam assaults on the network. Without strong defenses, bad actors might create smart contracts that use massive amounts of computing resources in order to overload the network. The Ethereum protocol assures that each calculation on the network has a cost by introducing the concept of gas. One computation cost one gas, as a matter of thumb. Because gas has a monetary value, such an attack would be prohibitively expensive. Furthermore, the Start gas value is supplied to restrict the number of calculations a transaction is permitted to run, which aids in the battle against spam attacks.

Before a transaction can be completed effectively, it must go through a sequence of procedures. The Ethereum blockchain verifies that the transaction contains all of the above-mentioned data and has a valid signature. If the nonce matches, the transaction proceeds to the next phase. The transaction charge is computed here. In layman's terms, this is accomplished by multiplying the Start gas by the gas Price value given in the transaction and adding one gas for every computation. When the charge is determined, it is applied to the sender's external account.

If the account cannot pay the fee, or if the transaction lacks a valid signature, the transaction fails and an error is generated. One of Ethereum's geniuses is its ability to totally rollback a transaction in the event of a mistake. If all of the requirements are satisfied, ownership is transferred from the sender to the receiver. If the receiving account is a contract account, the code is executed until the predetermined gas runs out.

3.5 Congestion of Ethereum

Congestion in the context of cryptocurrencies refers to a condition in which transactions are processed at a much slower rate, leading to the increase of the number of outstanding transactions. Ethereum network process 15 transactions per second on average. If a transaction is taking significantly longer than usual to be confirmed, or if the suggested gas charge is more than usual, the traffic is likely clogged. When traffic is heavy, miners may frequently favor transactions with greater gas prices. Those with lower gas prices will be stuck with a pending status [23].

High network demand might also have an impact on the constancy of gas fees. Currently, gas costs are determined by network demand, which means that fees can vary greatly depending on the time of day and the number of transactions moving through the network.

The charts in Figure 3.1 utilize the "standard" gas price. This pricing is recommended for those who want their transaction to be confirmed in less than 5 minutes and is a solid reflection of the current fair gas price. The heatmap computes an average of these standard prices for each 1 hour window using data from the preceding two weeks.

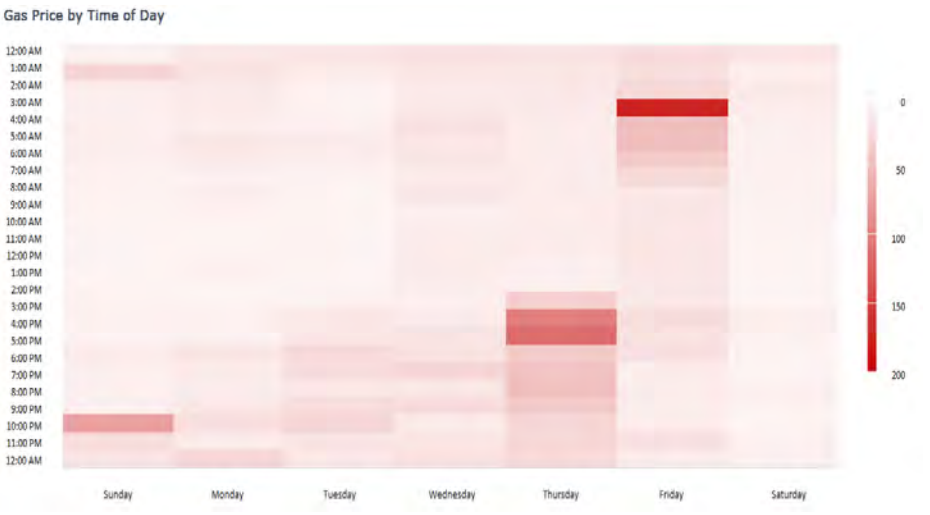

Figure 3.1: Gas Price by Time of Day (source B.2)

3.6 Smart Contracts

A smart contract is a self-executing agreement in which the buyer-seller deal terms are directly encoded into lines of code. The code and the agreements it contains are distributed and decentralized over a blockchain network. Transactions are easily traceable and unchangeable, and the programming executes them. Smart contracts enable for the execution of trustworthy transactions and agreements between different, anonymous persons without the need for a central system, legal system, or foreign means of enforcement. [24].

Nick Szabo [25], an American computer scientist who founded a virtual currency called "Bit Gold" in 1998, more than a decade before bitcoin, introduced smart contracts in 1997. According to Szabo, smart contracts are automatic transactional protocols that carry out the terms of a contract. He desired to digitalize the possibilities of online transaction platforms including such point-of-sale (POS) (point of sale).

Smart contracts may be used in a variety of contexts, including financial derivatives, insurance premiums, breach contracts, property law, credit enforcement, financial services, legal procedures, and crowdfunding agreements. Ethereum contracts have specific computer programming language. Solidity is the language utilized in this situation. While there are alternative programming languages that are compatible with smart contracts, Solidity is the preferred language. Solidity is a high-level, object-oriented programming language used to create smart contracts that are EVM-compatible (Ethereum Virtual Machine). Solidity is a curly bracket language that draws heavily on well-known programming languages such as JavaScript and C++. This implies that knowing JavaScript provides any programmer an ad-

vantage while studying Solidity [26].

3.6.1 ERC-20 Tokens

Although Bitcoin was the first cryptocurrency, Ethereum was the first cryptocurrency and blockchain to provide a variety of decentralized services within its network. To enable these services, the Ethereum network permits coins other than Ether to function on the network. These coins are created through smart contracts and referred to as ERC-20 tokens. ERC-20 tokens, like other coins, may be exchanged inside the network, which implies they can be profitable. However, ERC-20 tokens may also be used to run the Ethereum network's other decentralized services, such as developing and deploying Decentralized Applications (dApps), Decentralized Finance (DeFi), Decentralized Exchange (DEX), and many more.

ERC-20 tokens often have a limited quantity. This is done in order to avoid price inflation. Nonetheless, most ERC-20 tokens have a substantial supply, thus a scarcity is unlikely. Tokens based on the ERC-20 standard are likewise fungible. Fungibility indicates that these tokens are interchangeable with other tokens, which means that the price of one ERC-20 token may be comparable to the utility of another ERC-20 token. However, ERC-20 tokens are not typically private, thus if an ERC-20 token is used for illegal reasons, its value may differ from that of others.

ERC-20 tokens have reduced some of the restrictions that prevent projects from collaborating with one another, and their creation has enhanced and modified blockchain technology for good. Other networks, in addition to Ethereum, have begun to use these similar criteria in order to create their own coins. Binance blockchain, for example, employs BEP-20 tokens.

3.7 Utility of Ethereum

As we previously stated Ether is the Ethereum platform's native asset, which means it is utilized to complete every transaction or state change on the blockchain. Because Ether is utilized as network gas, it has utility as opposed to a pure money / store of value like Bitcoin. As a result, people desire to hold Ether in the same way as they want to hold oil in order to power equipment. As the Ethereum network grows in popularity, so will the need for Ether. In the Figure 3.2 we observe the high adoption recognized through frequent use of Ethereum network transactions over the past five years.

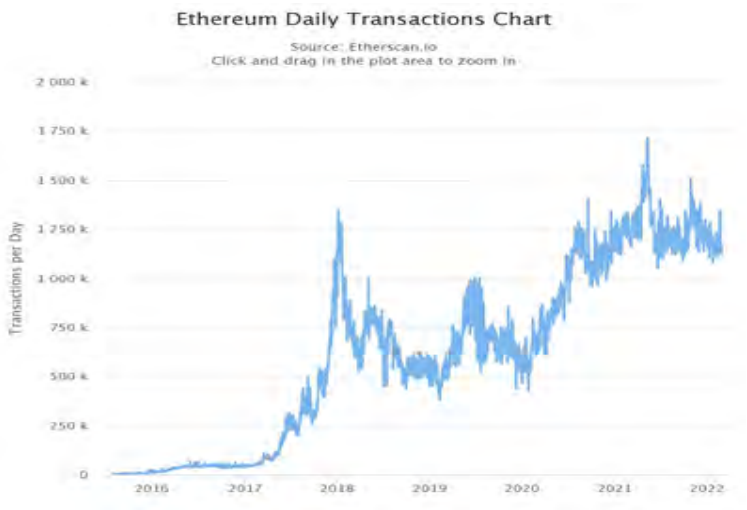

Figure 3.2: Ethereum Daily Transactions (source B.2)

3.7.1 Decentralized Finance

Vitalik and his team expanded the blockchain arena for Decentralize Finance by using Ethereum and its applications (DeFi). DeFi relating to money services and services are available to everyone who has an internet connection and can utilize Ethereum. With DeFi, the marketplaces are constantly open, and there is no central authority to halt payments or limit your access to anything. Services that were previously slow and susceptible to human error are now automatic and safer, owing to code that everyone can examine and assess [27].

While traditional finance includes difficulties, for instance, individuals who are denied the ability to open a bank account or utilize financial services, who do not have access to financial services because they may find it difficult to get work, information about personal data and block of payments are not a problem in the DeFi space. DeFi provides services without the need of middlemen by utilizing cryptocurrency and smart contracts.

In today's financial environment, financial institutions serve as transaction guarantors. Because your money flows through them, this gives these institutions enormous influence. Furthermore, billions of individuals throughout the world do not have access to a bank account. A smart contract substitutes the financial institution in a DeFi transaction. DeFi is used for numerous applications such as:

1. **Send money globally.** Ethereum, as a blockchain, is intended for transferring transactions in a safe and worldwide manner. Ethereum, like Bitcoin, enables transmitting money throughout the world as simple as sending an email. Simply provide your recipient's ENS name (such as bob.eth) or their wallet account address, and your money

will be sent immediately to them in minutes (usually).

2. **Flow money throughout the world.** You may also send money using Ethereum. This allows you to pay someone's income in a second, allowing them to access their money whenever they need it. Alternatively, you may lease anything in a second, such as a storage locker or an electric scooter.

3. **Stable coins access.** If you don't want to transfer or stream ETH due to the volatility of its value, there are substitute currencies on Ethereum called stablecoins. Volatility in cryptocurrencies is a concern for many financial products and ordinary spending. Stablecoins have been developed by the DeFi community to address this issue. Their value is fixed to another asset, generally a prominent currency such as the US dollar. Dai and USDC coins have a value that is within a few cents of a dollar. This makes them ideal for earning or selling. Many Latin Americans have adopted stablecoins to secure their assets during a period of significant uncertainty with their government-issued currencies.

4. **Borrowing.** Borrowing money from decentralized sources is classified into two types. Peer-to-peer means that a borrower will borrow directly from a lender and Pool-based lending, in which lenders contribute funds (liquidity) to a pool from which borrowers can borrow.

5. **Privacy.** Decentralized lending does not need either party to reveal oneself. Alternatively, the borrower must post collateral, which even the lender will seize if the loan is not repaid. Some lenders even accept NFTs as collateral. NFTs are the legal ownership of a one-of-a-kind item, such as an artwork.

6. **Access to global finances.** When you utilize a decentralized lender, you have access to money deposited from all over the world, not simply those held by your selected bank or institution. This increases the availability of loans and lowers interest rates.

7. **Tax efficiencies.** Borrowing can provide you with the money you demand without requiring you to sell your ETH (a taxable event). ETH, on the other hand, may be used as collateral for a stablecoin loan. This provides you with the necessary cash flow while allowing you to maintain your ETH. Stablecoins are tokens that are considerably better for when you need cash since their value does not vary like ETH.

8. **Flash Loans.** Flash loans are a more experimental kind of decentralized lending that allow you to borrow without giving any collateral or personal information. They are not generally available to non-technical people right now, but they hint to what everyone could be able to do in the future. It operates on the premise that the loan is obtained and repaid in the same transaction. If it is unable to be reimbursed, the transaction is canceled as though nothing happened. Liquidity pools house money that is often used (big pools of funds used for borrowing). If they are not being used at the moment, someone has the option of borrowing these funds, conducting business with them, and repaying them in full at the same time. This implies that a great deal of logic must be included in a highly tailored transaction.A simple example would be someone utilizing a flash loan to borrow as much of an asset as possible at one price in order to sell it on a different market at a higher price [28].

   As a consequence, you borrow X amount of asset from exchange A for $1.00, sell X asset for $1.10 on exchange B, refund the debt utilized to exchange A, and pocket the gain after reducing the transaction cost in a single purchase.

   The transaction would fail if the quantity of exchange B suddenly fell and the user was unable to acquire enough to pay off the initial loan. To carry off the above situation in the traditional banking business, you'd need a lot of money. These money-making strategies are only open to those with a lot of money. Flash loans are an example of a tomorrow in which having money isn't necessarily necessary to generate money. [29].

9. **Lending.** You may earn interest on your cryptocurrency by lending it, and you can see your funds increase in real time. Right now, interest rates are substantially greater than what you will find at your local bank (assuming you are lucky enough to have one). Here's an illustration:

   - You lend 100 Dai, a stablecoin, to a product such as Aave.Aave is a lending platform.
   - You are given 100 Aave Dai (aDai), which is a token that symbolizes the Dai you borrowed.
   - Your aDai will rise in line with interest rates, and you will notice an increase in your wallet balance. Your wallet balance will reflect something like 100.1234

within a few days or perhaps hours, depending on the APR (Annual Percentage Rate, more about definition here B.1).

10. **No loss lotteries.** PoolTogether and other no-loss lotteries are a fun and imaginative new way to save money. Your tokens are exchanged with the ticket tokens which are in for weekly lotteries and you have the ability at any point in time to withdraw. The prize pool is formed by all of the interest gained by lending the ticket deposits, as shown in the previous lending example.

Chapter 4

Blockchain Scalability problem

Ethereum developing dApps brought many users and developers into blockchain technology however, being a fully decentralized network comes with a cost. The ever-increasing number of nodes has resulted in the blockchain scalability issue. Even though blockchain has been available for more than a decade, issues with scalability might stymie blockchain adoption. In this chapter we will give a thorough examination of the primary scalability issues in blockchain, as well as an outline of applicable solutions.

4.1 Overview

Initially, blockchain technology was designed for the financial industry. The unchangeable ledger and decentralization of blockchain though, have made it a viable contender for non-financial applications. Blockchain, for example, has found interesting uses in the sphere of the Internet of Things (IoT) [30]. Furthermore, the ever-increasing sizes of prominent blockchain networks such as Ethereum exacerbate the blockchain scalability dilemma.

Take Bitcoin as an example to identify the best solution. On average, it handles about 7 transactions per second, whereas Visa processes over 1700 transactions per second. There is a noticeable performance gap between Visa and blockchain-based solutions. On the other hand, you must also deal with the issue of implementing new technologies. As a result, unsolved scalability problems on an architectural level complicate blockchain acceptance and practical implementations.

4.2 Scalability

When searching for scalability difficulties in blockchain, you must first understand blockchain scalability. Cost and capacity, networking, and throughput are some of the characteristics that define blockchain scalability [31].

The cost and capacity issue in scalability suggests that a considerable amount of data must be stored on the blockchain. You must store data beginning with the genesis block and ending with the most recent transactions. However, each node in the blockchain network lacks the necessary resources and capability to store such a large quantity of data.

In the event of a blockchain transaction, it is broadcasted to all nodes. When a block is mined, it is then broadcast to all nodes once more. As a result, the operation might consume significant network resources while increasing propagation latency. As a result, having a reliable and efficient data transfer system is critical. Another critical factor in the context of the blockchain scalability issue is throughput. Blockchain throughput refers to the time necessary to confirm a single transaction as well as the size of the transaction's block. With more transactions, the size of blocks grows, necessitating the use of greater resources.

4.2.1 Factors Affecting Scalability

Limitations

The limits are the most pressing issue in blockchain scalability. When a new transaction is processed, each node adds information about the transaction to the ledger. As a result, the growing transaction history has the potential to bring the entire system down. Furthermore, blockchain networks must keep all data accurate in order to maintain trust levels. Furthermore, blockchain is hampered by hardware constraints. The bulk of blockchain scalability issues are caused by physical limitations. As the blockchain network expands, it becomes increasingly difficult to install and operate the hardware required to run nodes.

Transaction Fees

The second significant aspect that contributes to serious scalability issues in blockchain is excessive transaction fees. Because of the increased need for more compute power for mining, the difficulties in procedures for verifying transactions have increased as the popularity of blockchain networks has grown. Users are required to pay a charge for the verification of

their transactions. With the ever-expanding blockchain networks, consumers are ready to pay greater transaction fees for transaction verification. However, it is equally crucial to realize that many other transactions linger in the queue for an extended period of time without being processed.

Block Size

Grasp why blockchain scalability is a concern requires an understanding of block size. Because of the increasing volume of transactions in blockchain networks, a time-consuming technique for transaction execution is required. In the early stages of the Bitcoin blockchain network, for example, each block was 1 Mb in size and had around 2,020 transactions. Nowadays, the increased amount of transactions in the chain has led in bigger block sizes, which are presently reaching 396 Gb with a daily fluctuation of +0,04 percent, affecting scalability [32].

4.3 Scalability Trilemma Problem

4.3.1 Overview

According to Geroni [33], before achieving viable solutions to blockchain scalability difficulties, we must first comprehend the blockchain scalability trilemma. When you improve scalability through a permissioned network, you sacrifice decentralization. The scaling trilemma is an imprecise idea that says blockchain networks can only have two of the three critical characteristics of decentralization, security, and scalability. To develop better answers to the blockchain scalability difficulty, let us first examine the relationship between the three separate components of this trilemma.

For the transaction to be settled, the blockchain network must reach a consensus on its legitimacy. In the event of a system with many users, the network may need longer time to achieve an agreement. As a result, it is apparent that as decentralization increases, scalability decreases. Consider two distinct Proof-of-Work-based blockchain networks with equivalent levels of decentralization, and consider security as the blockchain's hash rate. With a greater hash rate, you will have a shorter confirmation time as well as a significant increase in scalability and security.

As a consequence, with ongoing decentralization, security and scalability may have a direct proportional relationship. Reasonably, the blockchain scalability trilemma implies that a blockchain network cannot simultaneously guarantee decentralization, scalability, and security. The many issues for blockchain scalability, as well as the scaling trilemma, provide numerous major roadblocks to blockchain adoption. However, the following strategies can be used to overcome the numerous scalability difficulties in blockchain.

4.3.2 Improved Consensus Mechanisms

One of the most often touted solutions to the blockchain scalability problem is to improve consensus processes. Well-known blockchain networks, such as Bitcoin, employ the Proof of Work consensus system. While the Proof of Work consensus method provides reliable security, it is incredibly slow. As a result, many blockchain networks regard Proof-of-Stake consensus as a potential solution to blockchain scalability issues. The PoS consensus mechanism does not require miners to use massive computing power to solve cryptographic algorithms. On the contrary, it ensures agreement by selecting validators based on network stakes. Adoption of PoS consensus might dramatically enhance Ethereum network capacity while simultaneously improving security and decentralization.

4.3.3 Layer 1 Blockchain - Sharding

As an on-chain scaling solution, sharding is one of the traditional options for tackling the blockchain scalability challenge. Sharding, which is based on distributed databases, is now one of the most significant layer-1 scaling methods for blockchain networks. Sharding is the process of splitting transactions into smaller data sets known as “shards” [34].

The network then processes the shards in parallel, allowing for sequential work on many transactions. With the use of sharding, information might be distributed across several nodes while maintaining information consistency. Shards serve as evidence for the mainchain while interacting with one another to share addresses, general status, and balances via cross-shard communication protocols.

The adoption of L1 (Layer 1) solutions is one of the leading strategies for addressing the scalability challenge. A Layer 1 blockchain is a collection of solutions that enhance the fundamental protocol to make the whole system much more scalable. The consensus protocol and sharding are the two methodologies offered for achieving Layer 1 solutions. Layer 1

blockchains in use include Bitcoin, Ethereum, Binance Smart Chain (BSC), Litecoin, and Avalanche. However, Bitcoin continues to be the most affected by scalability difficulties, since the underlying network depends on an increase in the number of miners to provide increased transaction throughput and volumes.

4.3.4 Layer 2 Blockchain

Layer 2 is designed to run on top of the current base layer, easing the main chain of some responsibilities. In this case, the base layer will only be in charge of specified duties such as security and control. It should be noted that layer 2 blockchains must still report to the base layer. This guarantees that transactions are correctly verified while ensuring the security of the blockchain network. Layer 2 protocols on a blockchain run independently of the main chain. That's how the phrase "off-chain" came about [35]. The following are some of the layer 2 blockchain systems that are currently in use:

Nested blockchains

Nested blockchains are made up of the main chain and subsidiary chains that are constructed in such a way that one chain may run on top of the other. The main chain's role is to assign jobs and govern all parameters. The transactions are then carried out via the secondary chains. The layered blockchain guarantees that a primary chain can delegate work to numerous subordinate chains. After performing the specified assignment, the chains can submit a report for approval.

State channels

Parties engage directly in the blockchain network via state channels. Users of blockchains can conduct transactions without engaging the principal chains. The miners spend as little time as possible, resulting in quick processing rates. The transactions for state channels do not need to be verified by the layer-1 blockchain. This is due to the fact that resource validations are performed via the smart-contract mechanism. When the transaction is completed successfully, the resultant state is saved on the main layer. State channels safeguard the transaction information that is transferred between parties. The final transaction details, on the other hand, are recorded in the ledger and may be viewed publicly in order to keep records. Figure 4.1demonstrates a generic idea of the State Channels.

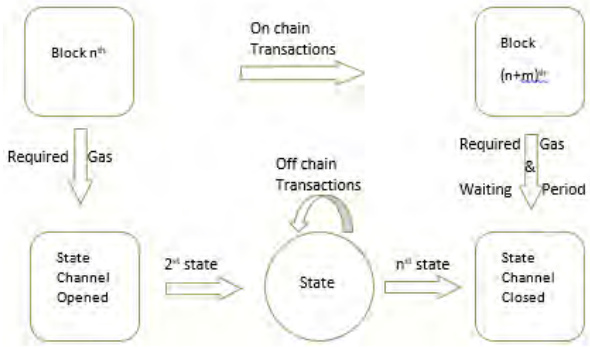

Figure 4.1: State Channels Process

Sidechains

A sidechain is a secondary blockchain that is linked to the parent chain by a two-way peg. We imagine it as a forest, with the trees serving as sidechains and the forest itself serving as the central chain. They are intended to manage a huge number of transactions. A sidechain supports the primary chain in verifying various blockchain transactions. The primary chain will then have plenty of time to deal with security and dispute resolution. State channels and sidechains are not the same thing. The reason for this is that they keep the transaction records on a public ledger. This implies that if the sidechain is attacked, the primary chain's activities will be unaffected. Sidechains, on the other hand, take a long time and a lot of effort to design and manufacture.

Rollups

These are layer-2 protocols that operate independently of the principal chain. In this blockchain, transaction data are sent after a certain time interval. This aids in the keeping of records.

Optmistic Rollups

Optimistic rollups assure the validity of every transaction executed on the blockchain. However, in most circumstances, optimistic rollups require some time to confirm the transactions. This waiting period allows rollups enough time to resolve a disagreement if one occurs.

Zero-Knowledge Rollup

Zero-Knowledge Rollups (ZK Rollups) do off-chain computations before submitting the primary chain's validity evidence. They occasionally utilize a smart contract to keep funds on the basic layer. Once the proof of validity has been presented and the transaction has been authenticated and approved by the primary chain, funds are released. Furthermore, rollups process transactions without interfering with the main layer. As a result, throughput is increased while transaction costs are kept to a minimum. Because the rollups' transaction information is maintained on the primary layer, the rollup's security can be assured.

Chapter 5

Blockchain Networks

The rise of Bitcoin has prompted a more in-depth examination of its underlying foundation: blockchain technology. This, in turn, prompted the investigation of decentralized applications for a variety of sectors.

Although Ethereum is one of the most well-known blockchain networks for the construction of decentralized applications, other blockchain networks have developed in recent years to redefine aspects such as scalability, security, and interoperability. Furthermore, the growth of the broader business has revealed the flaws in the Ethereum blockchain network, leading to the rise in importance of alternative networks.

In this chapter, we will look at the characteristics and functions of growing blockchain networks that are popular for dApp development.

5.1 Overview

With blockchain assets on decentralized finance (DeFi) platforms, several blockchain networks gained popularity. Despite the fact that Ethereum is the most widely used blockchain network in IoT, transaction costs remain rather expensive. This subject's innovation leads to the creation of hundreds, if not thousands, of blockchains. As blockchain technology is embraced and adapted to new use cases, the number will continue to rise. As a big number of investors flocked to such networks, BNB Chain (BSC), Terra (LUNA), Avalanche (AVAX), Solana (SOL), and a few others were investigated in this chapter.

5.2 Solana

Solana is a blockchain platform for hosting decentralized, scalable apps. Solana, which was founded in 2017, is an open-source project now managed by the Solana Foundation in Geneva, with the blockchain constructed by Solana Labs in San Francisco. Solana is quicker in terms of transaction processing capacity and offers significantly cheaper transaction costs when compared to other blockchains such as Ethereum. In November 2017, Solana co-founder Anatoly Yakovenko issued a white paper detailing the Proof of History (PoH) idea [36]. PoH is a proof for confirming the sequence and passage of time across events that is used to encode the trustless flow of time into a ledger.

According to Yakovenko's white paper, blockchains that were publicly available at the time did not rely on time, upon each node in the network depending by it's own local clock with out any knowledge of any other network members' clocks. Because there was no reliable source of time (i.e., a standardized clock), using a transaction timestamp to accept or reject a message did not guarantee that any network member would make the same decision. PoH removes this obstacle, allowing each node in the network to rely on the ledger's documented passage of time on a permissionless basis, which is crucial for blockchain to function.

Solana's design aims to show that there is a collection of software algorithms that, when combined to construct a blockchain, eliminate software as a performance barrier, allowing transaction throughput to expand proportionately with network capacity. Solana's design fits all three desirable blockchain characteristics: it is scalable, safe, and decentralized. According to Solana's architecture, the theoretical top limit on a typical gigabit network is 710,000 TPS and 28.4 million TPS on a 40-gigabit network.

Solana's blockchain employs both the Proof of History (PoH) and the Proof of Stake (PoS) models. PoS allows validators (those who authenticate transactions uploaded to the blockchain ledger) to verify transactions based on the number of coins or tokens they own; PoH allows those transactions to be timestamped and validated rapidly.

Much of the excitement around Solana in 2021 stemmed from its clear edge over Ethereum in relation to the market processing speed and transaction costs. Solana can handle up to 50,000 TPS at a cost of $0.00025 per transaction. Solana's status as a younger blockchain firm was further scrutinized after it experienced a network outage lasting more than 17 hours on September 17, 2021, due to an increase in transaction volume (which peaked at 400,000 TPS) and bot activity, which caused high memory usage. Though the SOL token originally

fell in value as a result of the announcement [37], it has subsequently recovered, hitting a high of more over $250 in November 2021 based on data from CoinMarketCap.

5.3 Avalanche

Avalanche is a blockchain that promises to integrate scalability with fast confirmation times via its Avalanche Consensus Protocol. It has a 4,500 TPS processing capacity (transactions per second). For Ethereum, this value is 14 TPS. Avalanche is being developed by Ava Labs, which is situated in New York. Emin Gün Sirer, a computer science professor at Cornell University, Kevin Sekniqi, a Ph.D. student, and Maofan "Ted" Yin, who created the protocol used in Facebook's unsuccessful digital currency project Libra, co-founded the firm.

According to Coinmarketcap statistics, Avalanche's native coin, AVAX, is the tenth-largest, with a market worth of $33 billion as of this writing in March 2022. Avalanche launched online in September 2020 and has since grown to become one of the most significant blockchains. According to Defi Llama statistics, it has over $14 billion in total value locked in its protocol, making it the fourth-largest DeFi-supporting blockchain behind Terra and Binance Smart Chain.

A blockchain, as a decentralized system, requires a mechanism to reach decisions among its globally dispersed members (validators) who update the public ledger - a technique to newline achieve consensus described by a protocol. The Avalanche Consensus Protocol, proposed in 2018 by a pseudonymous company called Team Rocket – a precursor of Ava Labs — plays that role in Avalanche. The Avalanche Consensus Protocol claims to bring together the benefits of two main consensus systems, Classical and Nakamoto.

- Classical protocols are quick, eco-friendly, and low-maintenance, but they are rarely decentralized or scalable. HotStuff, a Classical protocol, was well-known for its application in Meta Platforms' (previously Facebook) stablecoin project, Diem (formerly Libra).

- Nakamoto Protocols are pioneered by Bitcoin's pseudonymous creator Satoshi Nakamoto.They provide decentralized, resilient, and scalable blockchains — much like Bitcoin. However, the network is expensive to operate, and transactions are slow.

Avalanche is composed of three chains the C-chain, the X-chain and the P-chain. They are abbreviations for contract, exchange, and platform [38]. The C-chain contains Avalanche's

DeFi environment, which is where the bulk of users perform their transactions. It is a carbon clone of the Ethereum Virtual Machine. As a result, you will be able to copy and paste Ethereum dApps and start utilizing them on the Avalanche Network right now. The C-chain differs from the others in that it utilizes an Ethereum-style address with 0x at the start and can be added to MetaMask. The Snowman Protocol, a subset of the Avalanche Consensus Protocol, powers the C-chain.

The Exchange Chain (X Chain) is Avalanche's default asset blockchain, allowing for the production of new assets, asset exchanges, and cross-subnet transfers. The primary distinction between the X-chain and the C-chain is that the X-chain cannot be added in MetaMask or other similar wallets, and it cannot be used with DeFi. Your X-chain address is accessed through the Avalanche wallet, and you are assigned a new address with each deposit (although the old addresses remain valid too). The format differs from that of Ethereum-style 0x addresses. The Avalanche consensus protocol is used by the Exchange Chain. The main aim of the X-chain is to transfer and receive cash. The benefit of this method is that the X-chain is built particularly for transfers rather than attempting to be everything to everyone. Of course, cash may be sent on the more adaptable C-chain as well, but gas fees on the C-chain can reach several dollars when the network is busy, whereas the transaction charge on the X-chain is a set 0.001 AVAX, which is around $0.08 at current rates. Because to its streamlined form, the X-chain is likewise faster.

The P-chain is the final chain provided by Avalanche (P standing for platform). The primary purpose of this is to stake AVAX and act as a validator. If you are a validator (or are delegating to one), your AVAX incentives will be received on this chain. Transfers from the other two Avalanche chains are also feasible (X and C).

5.4 Polygon

Polygon, denoted by the symbol MATIC, is both a cryptocurrency and a technological platform that allows blockchain networks to communicate and expand. Polygon, called "Ethereum's internet of blockchains", debuted in 2017 as Matic Network. Jaynti Kanani, Sandeep Nailwal, Anurag Arjun, and Mihailo Bjelic co-founded Polygon. Over 7,000 blockchain-based projects are now supported by the platform [39].

The Polygon platform connects Ethereum-based projects by utilizing the Ethereum net-

work. Using the Polygon platform can boost a blockchain project's flexibility, scalability, and sovereignty while still providing the security, interoperability, and architectural benefits of the Ethereum blockchain. Polygon may be used to generate Optimistic Rollup chains, ZK Rollup chains, standalone chains, or any other type of infrastructure needed by the developer. Polygon essentially converts Ethereum into a multi-chain system (aka Internet of Blockchains).

MATIC is an ERC-20 token, which means it is interchangeable with other Ethereum-based digital currencies. MATIC is used to manage and protect the Polygon network, as well as to collect network transaction fees.Polygon employs a modified proof-of-stake consensus algorithm that allows for consensus with every block. (Achieving consensus with classical proof-of-stake necessitates the processing of several blocks.) The proof-of-stake mechanism requires network participants to stake—that is, pledge not to trade or sell—their MATIC in return for the ability to validate Polygon network transactions. Successful Polygon network validators are credited with MATIC.

As a supplementary scaling option, the Polygon network intends to overcome the Ethereum platform's constraints, especially high transaction fees and poor transaction processing times. Polygon is capable of deploying pre-existing blockchain networks and create custom blockchains, allow Ethereum and other blockchains to connect with one another and last but not least assist current blockchain networks in becoming Ethereum-compatible. [40]

Polygon can maintain rapid transaction processing speeds by utilizing a consensus technique that fulfills the transaction confirmation phase in a single block. The average block runtime for Polygon is 2.1 seconds. Polygon maintains its platform costs low, with an average transaction price of roughly $0.01 according to polygonscan.com.

5.5 Cosmos

Cosmos seeks to build "Internet of Blockchains", in which any blockchain may interact, share data, and interact with any other. At the moment, a blockchain acts as its own universe, with essentially no means to connect with the world beyond its network–at least without the assistance of a bridge. As a result, squabbling, tribalism, and maximalism among advocates of numerous blockchains have become the norm.

The goal of Cosmos is straightforward: to enable any blockchain to interact, share data,

and transact with any other. By enabling several blockchains to interact, there are lesser needs for these networks to compete viciously to be the one blockchain that rules them all. Instead, several separate blockchains may coexist, each with its own set of specialized use cases and benefits [41].

Cosmos is a whole technological stack that goes above merely connecting and sharing data between multiple blockchains. They have also developed a faster development system that enables developers to design their own unique blockchain in months, if not weeks, rather than years. Cosmos is built on Jae Kwon's Tendermint consensus mechanism, which he designed in 2014. Kwon was joined in developing the whole Cosmos interoperable ecosystem by Zarko Milosevic and Ethan Buchman; he subsequently stepped away from the project in 2020 [42].

Tendermint is a non-zero voting power Byzantine Fault Tolerance engine with two noteworthy qualities among many others: immediate finality, which means that once a transaction is included in a block, it cannot be canceled, and the light client, which is relatively straightforward to build on Tendermint. On Proof of Work blockchains, this is not the case. Another intriguing feature is that Tendermint lets you to create both public and private blockchains. So, whether you want to apply for a public blockchain in Proof of Stake, a private blockchain in Proof of Authority, or anything else, you can do it on Tendermint.

The Cosmos Hub is the Cosmos Network's first public blockchain, powered by the Tendermint BFT consensus algorithm. Cosmos created the Inter Blockchain Communication Protocol (IBC), which allows the ecosystem to link various blockchains that have the feature of finality with the Hub in a decentralized way.

While the Cosmos Hub is a multi-asset distributed ledger, it does include a unique native token known as the Atom. Atoms may be used in three ways: as a spam-prevention technique, staking tokens, and voting mechanisms in governance. Atoms are used to pay fees as a spam prevention technique. Similar to Ethereum's idea of "gas", the fee might be proportionate to the amount of computation performed by the transaction. Fee distribution occurs in-protocol, and a protocol definition is provided here.

Atoms can be "bonded" as staking tokens to obtain block rewards. The quantity of Atoms staked determines the economic security of the Cosmos Hub. The more Atoms collateralized, the more "skin" is at stake, and the higher the demand of attacking the network. As a result, the more Atoms that are joined, the better the network's economic security. Atom holders

can manage the Cosmos Hub by voting with their staked Atoms on proposals. Atoms are used as staking tokens to obtain block rewards. The quantity of Atoms staked determines the economic security of the Cosmos Hub.

5.6 BNB Chain

Binance Exchange is a significant cryptocurrency exchange that was created in Hong Kong in 2017. Binance Coin is the cryptocurrency issued by the Binance exchange, and it trades under the sign BNB. Binance Exchange is the world's largest cryptocurrency exchange, with over 1.4 million transactions per second as of June 2021. Binance launched Binance chain (BC) for governance (staking, voting) a year and a half later. Binance launched Binance Smart Chain in September 2020 and expanded in size and strength with the exchange. BSC was founded just in time for the DeFi revolution, as the public became more interested in alternative financial solutions and blockchain-powered application cases. In 15th of February 2022 the two chains became BNB Chain [34].

The objective of BNB Chain is to develop the infrastructure that will power the world's parallel virtual economy, and the company's pledge to the community is that it will be open, perpetually decentralized, permissionless and multi-chain network for creators and innovators setting goals for the next chapter MetaFi.

The term MetaFi is a combination of two words: 'Meta' for meta environment and 'Fi' for DeFi. MetaFi is a concept that brings together several initiatives such as Metaverse, DeFi, GameFi, SocialFi, Web3, and NFTs under one roof — MetaFi.

This is made feasible by the information that specifies asset ownership. MetaFi will enable the convergence of a wide spectrum of blockchain capabilities into a single meta ecosystem, and it will be compatible owing to set metadata standards utilized across many platforms and blockchains. MetaFi can comprise DeFi goods or a combination of fungible and non-fungible coins or assets, as well as community governance such as Decentralized Autonomous Organizations (DAOs).

MetaFi's mission is to create and develop new ecosystems rich in functionality, based on digital assets that enable widespread adoption of the metaverse while also providing users and participants with new use cases. By combining these several blockchain initiatives, a full-fledged alternative ecosystem servicing people from all over the world is created. None

of this will be achievable without the development of robust and interoperable projects with multi-chain capability and bridges to support the massive volume of asset and data transfers.

BNB Chain is a controlled blockchain in which Binance plays a major role in gatekeeping traffic and verifying transactions, while Bitcoin and Ethereum do not. Regardless the matter of how implausible the following scenario is, Binance might conceivably pull off the largest rug-pull in crypto history, and you should always bear that in mind while engaging with some of its so-called “decentralized” products.

5.7 Polkadot

Polkadot (DOT) is a third-generation blockchain that prioritizes interoperability and scalability. Polkadot like Cosmos is paving the way for interoperability by constructing a network that can sustain a constellation of separate blockchains. These self-governing blockchains are known as parachains. The Polkadot network’s fundamental backbone is the Relay Chain. Parachains generate transaction blocks that are submitted to validators on the Relay Chain. These validators affirm that the blocks may be added to the ledger permanently. As a result, all parachains benefit from the same degree of stringent security assurances.

Polkadot enables developers to create application-specific blockchains (parachains) that are suited to their individual requirements. These bespoke blockchains are intended to be compatible with one another, enabling smooth cross-chain communication and value transfers. Cross-Chain Message Passing (XCMP) enables communication, while transactions occur across bridge parachains in the network. Polkadot uses a sharded blockchain approach, which allows transactions to be handled in parallel rather than sequentially, resulting in a significant increase in the number of transactions per second.

Dr. Gavin Wood, a co-founder and former CTO of Ethereum, creator of the Solidity programming language, and author of the Yellow Paper, the first formal specification of a blockchain, spearheaded the Polkadot project [23]. While Dr. Wood’s seminal Solidity language set the groundwork for the usage of bespoke smart contracts on the Ethereum blockchain, Polkadot is taking it a step further by allowing any developer to construct their own unique blockchain.

While it is encouraging to learn about possible blockchain scaling solutions, most solutions are still in the experimental stage. It is obvious that scalability is a significant issue

for blockchain networks. Developers are attempting to address the scalability challenge from several angles. Increased block size, for example, might improve scalability. Such ideals, however, have not received widespread acceptance. Simultaneously, the installation of another layer atop the existing blockchain network with layer 2 solutions is a viable scaling option. On the other hand, it is too early to draw judgments about the most practical scalability alternatives.

5.8 Terra

Terra is an open-source PoS blockchain payment network for algorithmic stablecoins, or cryptocurrencies that monitor the value of currencies or other assets [43]. Terra stablecoins may be spent, saved, traded, or exchanged instantaneously on the Terra blockchain. Terra was created by Terraform Labs, a South Korean company launched in 2018 by Do Kwon and Daniel Shin. Kwon, the current CEO, formerly worked for Microsoft and Apple before launching Anyfi, a firm that provides decentralized wireless mesh networking solutions. Shin is the founder and CEO of Chai, an Asian fintech business that is a Terra partner, and a co-founder of TMON, better known as Ticket Monster, a Korean e-commerce startup.

The Terra protocol creates stablecoins that continuously monitor the price of any fiat currency (a government-backed currency like the U.S. dollar or euro). It is composed of two basic cryptocurrency tokens, Terra and Luna, each of which has the following properties.

Terra: These are stablecoins that are named after fiat currencies and track their prices. The base Terra stablecoin, for example, is dubbed TerraSDR or SDT and monitors the price of the IMF's Special Drawing Rights. TerraUSD (UST), which follows the US dollar, and TerraKRW (KRT), which monitors the South Korean won, are two more Terra stablecoin denominations. By burning Luna, users can create fresh Terra.

Luna: The Terra protocol's staking token, which absorbs the price fluctuation of Terra stablecoins, is used for governance and mining. Users stake Luna to Terra blockchain miners (dubbed "validators"), who log and confirm transactions on the blockchain and are compensated with transaction fees. Luna's value rises in tandem with Terra's utilization.

The Terra protocol ensures that supply and demand for the Terra stablecoin are continually balanced, as the basic value of stablecoins is predicated on the stability of the price peg, preventing the volatility prevalent with cryptocurrencies.

The variable counterbalance to the Terra stablecoin is Luna, which absorbs its volatility. To grasp how Terra operates, imagine the whole Terra "economy" as a Terra pool and a Luna pool. The Luna supply pool contributes to or deducts from Terra's supply to maintain Terra's price; users burn Luna to mint Terra and burn Terra to mint Luna. The protocol's algorithmic market module does this by incentivizing the minting or burning of Terra via arbitrage possibilities.

Expansion (of the Terra pool): According to the whitepaper, when Terra trades at a high proportion to its peg, it implies that demand for the stablecoin is greater than supply; this suggests that Terra supply should be raised to satisfy demand. The protocol encourages users to mint Terra and burn Luna, which lowers the Terra price (because to increased supply) while increases the Luna price (by reducing its supply). Users will continue to arbitrage until Terra reaches its goal peg price.

Contraction (of the Terra pool): The opposite situation happens when Terra trades at a low proportion to its peg, implying that there is more supply than demand for the stablecoin. This would involve limiting Terra supply until it met demand. The protocol then prompts users to burn Terra and mint Luna, which raises the Terra price (because to limited availability) while lowers the Luna price (by increasing its supply). Users will continue this arbitrage process until Terra trades at its goal price.

Terra Network has been through a hard fork lately, More information about this in the appendix section A.1.

Chapter 6

Cross Chain Transactions

Since the publication of the Bitcoin white paper in 2008, blockchain technology has gone a long way. Ever since then, there has been an explosion of blockchain networks with a wide range of designs and intended usefulness as we previously stated. The segmented form of today's blockchain networks violates the decentralization premise and re-establishes the Balkanization of the current centralized web (often called Web 2.0). While each year in cryptocurrency is unique, 2021 impacted the ecosystem in ways that have excited many people about crypto's potentially infinite future. This chapter will analyze the implemented solutions for cross chain transactions among variety of protocols

6.1 Overview

The term "cross-chain" refers to the fact that in cross-chain trade, the source and destination assets are deployed on two different blockchains [44]. At the same moment, execution takes place after traversing two or more distinct blockchain networks.

Asset spillover effects become increasingly visible when the Ethereum network experiences congestion and expensive fees. The introduction of the cross-chain bridge fractures the blockchain island and extends the area for DeFi ecological growth. The savvy money (or smart money, definition here B.1) can move back and forth in the public chains in quest of a higher-yielding "Bonanza". However, chances come at a cost. More than 100 cross-chain bridges supply a plethora of travel options and raise the complexity of choice for consumers as multi-chain ecosystem expands.

The year of the Layer 1s was 2021, which led in many people expecting a multi-chain

future for crypto, as opposed to the winner-take-all mindset that many people held previous to the development of these blockchains.

However, since the number and breadth of diverse blockchain ecosystems has grown dramatically, there is now a need for crucial infrastructure to connect them. Blockchain bridges came to help with this. According to Footprint Analytics as shown in Figure 6.1, DeFi have more than $100 billion in total locked up, up from $25 billion a year earlier. These estimates are expected to climb more as the crypto ecosystem develops. New ideas and technology may also provide additional possibilities in the long run, resulting in cheaper prices and improved dependability.

Figure 6.1: Decentralized Finance Total Value Locked (source B.2

6.2 Lifecycle of Cross chain Transaction

In this section we will analyze cross chain transactions through blockchain bridges. A bridge is essentially the interoperability of two separate blockchains. As far as blockchains share the same fundamental architecture, the technology has proven to be crucial in guaranteeing that blockchains can interact with one another. A straightforward explanation of Cross-chains is viewed as the final answer to improving interoperability across blockchains [45]. They will facilitate the exchange of information and value between blockchain networks. Consider the following example:

Alice has ETH on the Ethereum Mainnet that she wishes to utilize on Avalanche as shown 6.2. Because these two networks have their own protocols, laws, communities, and consensus procedures, interoperability is not conceivable. In such a circumstance, someone must stand in the intermediary and provide a means for information to be transferred from the Ethereum Mainnet to Avalanche. To accomplish so, Alice would most likely use a blockchain bridge to safely transfer the ETH from Ethereum Mainnet to Avalanche. Alice will be able to exchange ETH on Ethereum to wETH on Avalanche by using the bridge.

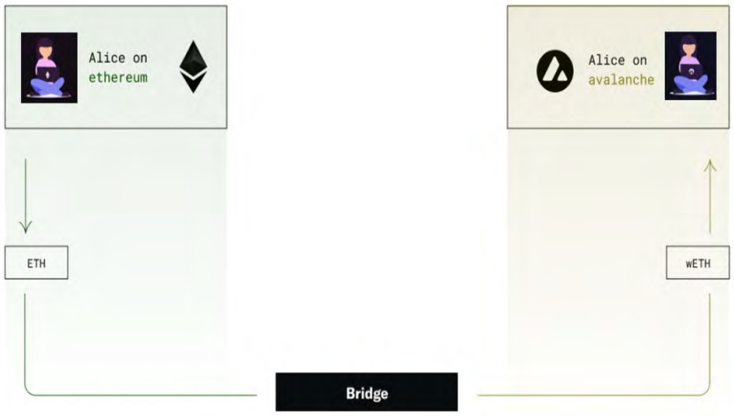

Figure 6.2: Cross chain swap of Eth from Ethereum Mainnet to Avalanche (ETH to wETH)

Interoperability refers to the capacity of blockchains to communicate with one another in order to facilitate information sharing. It is the capacity to observe and access data carried/stored in another blockchain. That is, if the information is delivered to another blockchain, a user on the other side may see it, read it, comprehend it, and react correctly while exerting the least amount of work throughout the process. Cross-chain technology aims to develop and improve interoperability across blockchains, removing the need for third parties to make such connections.

Several initiatives are tackling this issue as blockchain technology advances by constructing bridges across networks. As we advance toward a world where blockchains and systems are interoperable, apps will be able to leverage each other's services and skills. As a new, decentralized, and interoperable internet takes form, this will very certainly have a significant influence on a wide range of services. Increased liquidity and the capacity to establish a network of services that connect with each other across communities would assist applications such as decentralized finance (DeFi), growing their user base and extending the resources available.

6.3 Bridges

Bridges provide communication between multiple blockchains. And, as with hard math issues, there is no one technique to enable communication across blockchains when looking at multiple bridge solutions in the crypto ecosystem. Bridges have diverse designs with varied strengths and trade-offs, therefore there are several alternatives for which a bridge may be utilized to connect between two blockchain networks. Let's take a closer look at how communication works.

Bridges function by creating communication routes between two blockchains. In an ideal world, blockchains would simply communicate with one another, but this is not practical since one blockchain does not hold the state of the other.Obtain the following:

A Solana dApp wishes to interact with an Ethereum dApp. Because of the trust limits among Ethereum and Solana, they cannot easily communicate. These bounds of trust include, but are not restricted to:

- Ethereum and Solana are unaware of one other's existence.
- Both can only see what's going on on their own chain and have no idea what's going on elsewhere.

Receiving a message from the other blockchain is equivalent to having an encounter with the outside world about which they are unaware. As a result, trust cannot be formed in order to validate these communications.

Furthermore, blockchains can only transmit messages in one direction. That is, communication over a channel is only one-way. One blockchain can deliver a message to another over one channel, but the other blockchain cannot respond via the same channel and validate that the message was received.

To build confidence across blockchains and enable two-way communication, we want something in between, which can fill the gap between them. This is where blockchain bridges come in, allowing not just the transfer of messages, data, and resources between blockchains, but also the transfer of assets across blockchains. This changes things since blockchains are no longer confined to one-way communication because bridges allow them to speak back and forth with other blockchains.

Bridges employ various techniques, or actors (bridge node validators and multi-sig ones.Multi-sig is short for multiple signature validators), who function as verifiers across blockchains to

facilitate communication and overcome trust barriers. Communication between blockchains will be impossible without these off-chain players 6.3.

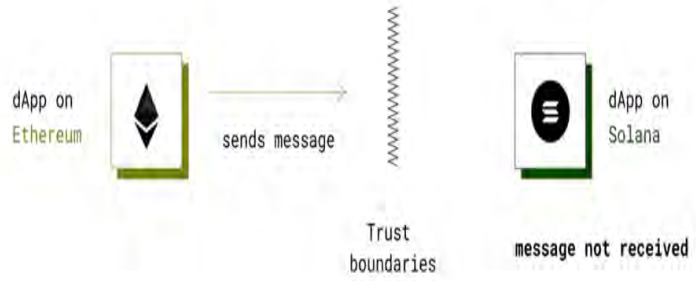

Figure 6.3: Without Off Chain Actors

However, by serving as a "man-in-the-middle" between the two blockchains, trust barriers may be overcome and communication becomes feasible 6.4.

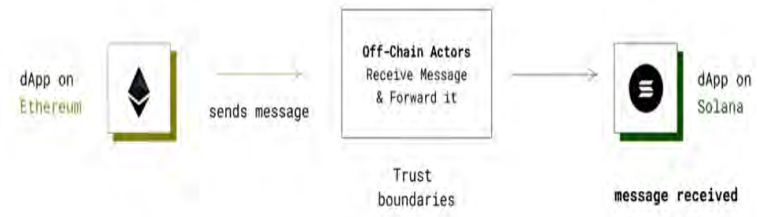

Figure 6.4: Off Chain

The function of validators is the primary distinguishing factor in how bridges function. Some bridges employ a trusted system, while others use a trustless system of verifiers. Furthermore, due to the crypto ecosystem's interoperability trilemma, we see a variety of bridge solutions.

In the Ethereum ecosystem, there is an Interoperability Trilemma 6.5, which is similar to the Scalability Trilemma. Interoperability protocols can only contain two of the three features listed below:

1. Trustlessness: having the same level of security as the underlying domains.

2. Extensibility: the ability to support any domain.

3. Generalizability: the capacity to handle arbitrary cross-domain data.

Interoperability is essential for a number of use cases:

- Collateral - Without an effective DeFi ecosystem, many blockchains, such as Bitcoin, maintain substantial value, restricting the potential to make income from any assets. Cross-chain bridges might make it easier for anybody to gain access to DeFi capabilities.
- Scalability - Many proof-of-stake blockchains are experiencing scalability concerns, especially as the volume of transactions continues to grow. Cross-chain and sidechain bridges might help relieve these concerns without totally switching networks.
- Efficiency - In addition to increased scalability, crypto users may want to execute transactions on blockchains with cheaper fees, reducing congestion on parent blockchains and saving large sums of money on gas fees.
- Web3 - To foster acceptance, Web3 will rely on interoperability across multiple blockchains. Users, for example, will want to preserve their avatars, currencies, and other non-transferable and fungible assets across games and experiences.

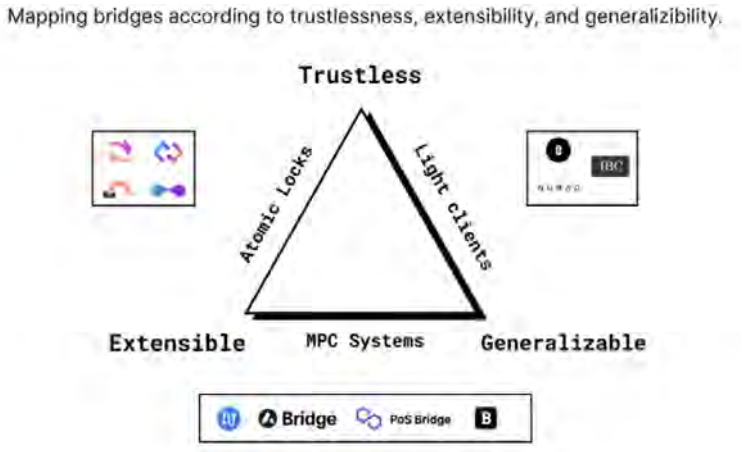

Figure 6.5: Interoperability Trilemma

In addition, in this study, bridges are categorized as natively, externally or locally certified systems. Different bridge solutions focus on different variables from the three outlined above, each with their own set of advantages and disadvantages. As a result, many bridge designs with distinct value propositions exist.

The preceding considerations explain the reasons we have various bridge designs. However, many types of bridges exist based on the kind of what they connect and their primary use-cases. This will be discussed further in the section "Classification Of Bridges According On Their Functionality".

6.3.1 Classification Of Bridges According On Their Functionality

While the goal of all blockchain bridges is the same (allowing communication across various blockchains), the methods through which they do this differ. Bridges are grouped into three types based on how they function:

- Trusted Bridges — These bridges are operated by a central authority. They are known as "trusted bridges" because users must rely on a third party to use the bridge and keep their payments safe. Trusted bridges include multichain and chain-specific bridges such as the Binance to Ethereum bridge.

- Trustless Bridges – These bridges eliminate the need for a trusted third party by utilizing smart contracts and algorithms. They are known as trustless bridges because they do not require users to trust a central authority in order to utilize the bridge. As a result, the user is always responsible for the protection of their cash. Connext, cBridge, and Hop are examples of trustless bridges.

6.3.2 Bridge Classification Based on What They Connect

Bridges can be categorised into the following categories based on what they link, in addition to how they work:

- Bridges from L1 to L1 — These bridges connect distinct L1 blockchains. The Avalanche Bridge (AB), for example, connects Ethereum and Avalanche.

- L1/L2 from/to L2 Bridges — These bridges connect the Mainnet to various L2 solutions and the L2s to one another. Across, for example, is a bridge that connects Ethereum Mainnet to L2s such as Arbitrum and Optimism. Hop Protocol is a bridge that connects multiple L2s while also linking them to the Ethereum Mainnet.

Bridges, like highways that connect multiple cities, might be compared to Haseeb Qureshi's conceptual image of blockchains as cities [46]. Roads are categorized into the following types based on what they connect:

- National Highways are the routes that link all major cities.
- State Highways — These are the routes that link major portions of the city.

L1 to L1 bridges are found on national highways. If Ethereum represents New York City and Avalanche represents Chicago, the Avalanche Bridge (AB) is the National Highway that links the two cities as shown in the Figure 6.6.

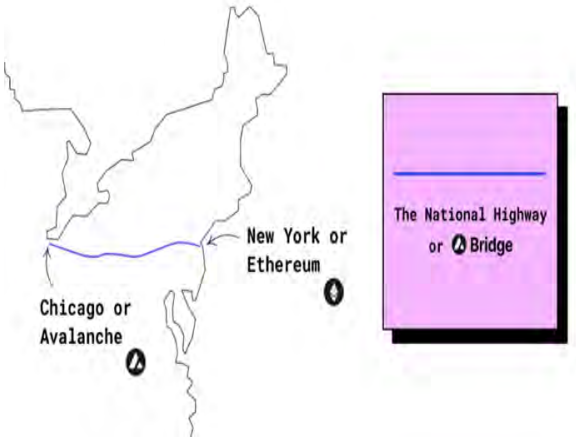

Figure 6.6: L1 from/to L1 Bridges or National Highways

State highways are L1/L2 bridges that connect to L2 bridges. If L2s and rollups like Arbitrum and Optimism are two buildings on Ethereum, then Hop Protocol is the state highway that connects them in New York City. Figure 6.7 shows an example.

6.3.3 Bridge Classification Based on Asset Movement

Bridges can also be categorised according to the technique they utilize to transfer assets between chains. Bridges are classified into the following categories based on how they transport assets:

- Lock & Mint - These bridges lock assets on the source chain and mint assets on the destination chain. Polygon's PoS bridge, Avalanche Bridge (AB), wrapped BTC, and wMonero are other examples.

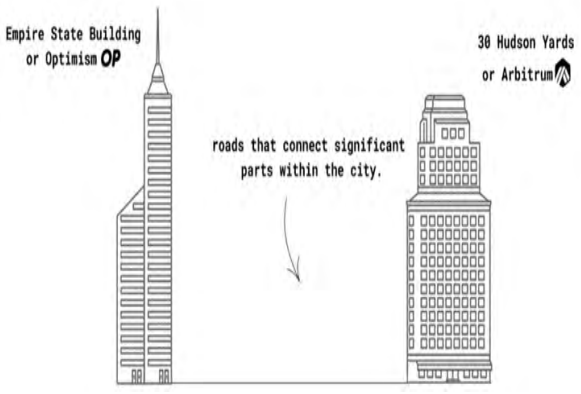

Figure 6.7: L1/L2 from/to L2 Bridges or State Highways

- Burn & Mint — These bridges mint assets on the destination chain while burning assets on the source chain. Examples are Hop and Across.

- Atomic Swaps - are bridges that exchange assets from the source chain for assets from the destination chain. They are more trustless in general because they rely on self-executing smart contracts for asset exchanges, eliminating the need for a trusted third party that is required in lock & mint or burn & mint processes [47]. cBridge and Connext are two examples.

Let's look at an example.

Assume you are driving from City A to City B, which are connected by a bridge. When you are at the bridge, preparing to depart City A for City B, you have three alternatives for crossing:

1. If you leave your automobile at a warehouse in City A, you will receive an identical car in City B. When you return to City A, just return the automobile you received in City B and pick up your original car. Bridges employ a lock and mint system similar to this 6.8.

2. To exit City A, you must wreck your automobile, in exchange for an identical car in City B. When you return to City A, the same procedure will be repeated: you must destroy your automobile in City B in order to receive an identical car in City A. Bridges employ a burn and mint technique similar to this 6.9.

3. Trade in your automobile in City A for a new car in City B. When you wish to return

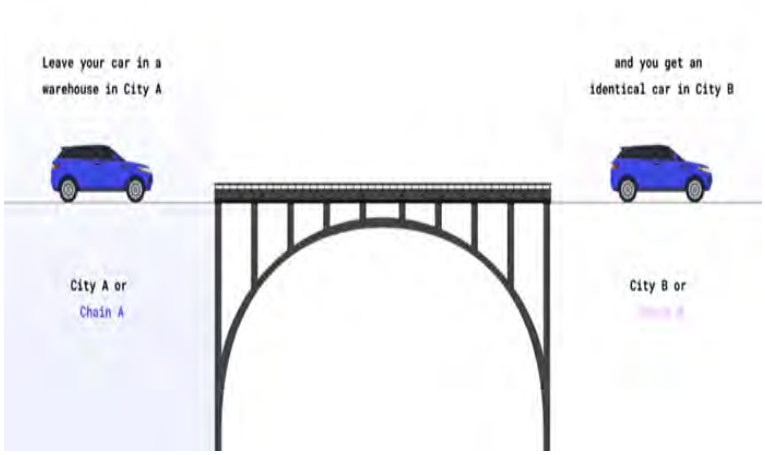

Figure 6.8: Lock and Mint

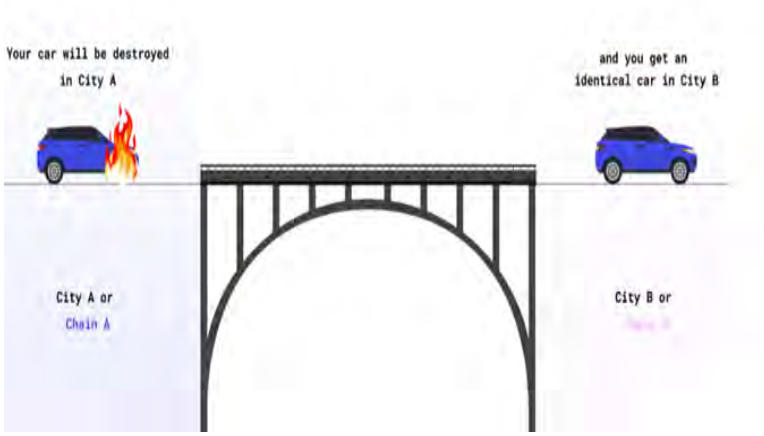

Figure 6.9: Lock and Burn System

to City A, simply repeat the procedure of exchanging your automobile in City B for another car in City A. Bridges employ an atomic swaps method similar to this6.10.

Figure 6.10: Atomic Swaps

Bridges Classified Based On Their Function

The above mentioned classes differentiate bridges fairly substantially. When considering different bridge kinds and designs based on how bridges are utilized, things might become difficult. Therefore, based on their functionality, bridges are categorised into the following:

- Chain-to-Chain Bridges: These bridges are primarily intended to facilitate the transfer of assets between two blockchains. In most cases, such bridges employ the lock and mint system. Native bridges such as Polygon's PoS Bridge, Binance to Ethereum Bridge, and Avalanche Bridge (AB) are examples.

- Multi-Chain Bridges: These bridges are used to move assets between blockchains. They are designed to be implemented on any type of L1 or L2 blockchain. Connext, cBridge are two examples.

- Specialized Bridges: These bridges are oriented on certain ecosystems and are meant to facilitate asset mobility across specific locations. Because of their expertise, these bridges may often permit quicker and cheaper cross-chain transactions. Examples: Hop is a rollup-to-rollup bridge that allows assets to be transferred between the Ethereum Mainnet and L2s, whereas Across is a bridge that focuses on allowing assets to be transferred quickly and cheaply from L2 rollups to the Ethereum Mainnet.

- Wrapped Asset Bridges: These bridges are especially built to allow the movement of non-native assets across blockchains. They do this by producing wrapped assets on the destination chain that correspond to the original asset on the source chain. Wrapped BTC, Interlay, and wMonero are among examples.
- Data Specific Bridges: This type of bridges are interoperability protocols that are especially built for moving arbitrary data across several blockchains. In general, these protocols serve as the foundation for dApps, allowing them to be cross-chain composable. Celer's inter-chain Message Framework, IBC, Nomad, and Data Movr are a few examples.
- dApps Specialized Bridges: These are not bridges from a technical standpoint. These dApps have created an ecosystem that allows value to be exchanged between blockchains in a manner similar to bridges by connecting to multiple blockchains. Examples: Thorchain is a decentralized cross-chain AMM that provides cross-chain liquidity capabilities which allow assets to be exchanged between blockchains. Anyswap, Wanchain, and Synapse are some other examples.

6.4 Bridges as a Spectrum of Trust

After analyzing the diverse types of bridge designs, trust, as a spectrum in bridges, boils down to the following:

- External validators and federations — Externally Verified
- Optimistic bridges — Optimistically Verified
- Liquidity networks — Locally Verified
- Light clients and relays + ZK Bridges

In Figure 6.11 there is a chart that shows where each bridge design stands on the trust scale .

Only people make trust assumptions; code does not. In Figure 6.11, as we travel from left (trusted or trust the person) to right (trustless or trust the code), the systems become less trusting as they remove the requirement for users to rely on humans and either disperse it across the system or replace it with code.

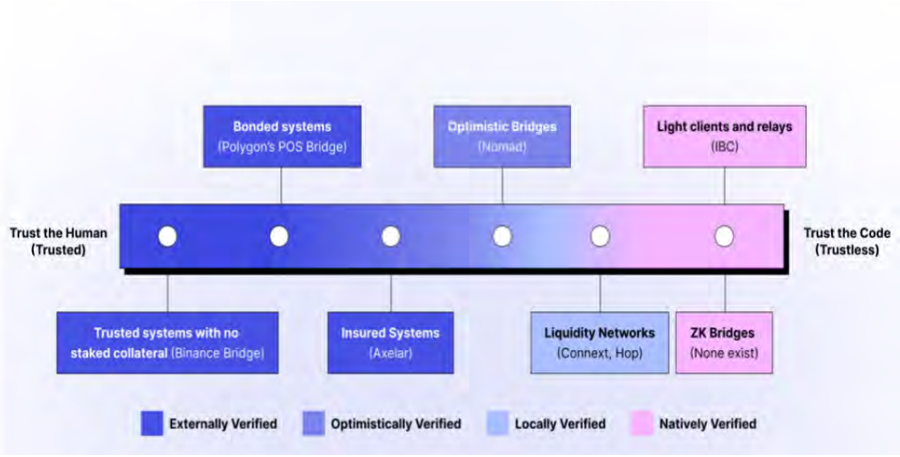

Figure 6.11: The ”Trust Spectrum” in Bridges

Let’s take a look at how these distinct systems work and why one has more or less trust than the other.

6.4.1 External Validators and Federations — Verified Externally

A group of validators is in charge of confirming any transactions in externally verified systems. This collection of validators is not associated with either of the two blockchains involved in the cross-chain interaction. Instead, the bridge introduces it to allow communication between the two chains. The bridge’s validator set is distinct from the underlying blockchains in terms of trust assumptions. As a result, users must trust a new system rather than the more secure validator set of the underlying blockchains.

These bridging solutions typically operate by storing users’ assets in a wallet on the source chain and minting an identical amount on the destination chain. External validators and federations manage and administer this wallet and consensus to mint new assets. Examples:

- A multi-party custody scheme is used by Multichain [48].
- Before the $625 million breach, Ronin Bridge had a 5/9 threshold multi-sig [49].

Even within the subset of systems that employ external validators, other crypto-economic processes may be leveraged to reduce confidence even more (moving closer to the effectively trustless end of the spectrum). Here are a few instances in decreasing order of trust minimization:

- **No Staked Collateral Trusted Systems:** Validators are not required to post any collateral. Users must rely on the bridge builders’ reputation and the widespread goodwill

that all validators will operate honestly to ensure the security of their cash. Users cannot retrieve their payments in the event of malicious activity. Binance Bridge is an example.

- **Burned Collateral Bonded Systems:** Validators must post collateral, which is destroyed in the event of harmful activity. Incentivizing malevolent behavior reduces trust. The method, however, does not ensure that user cash would be refunded if something goes wrong. Polygon's PoS Bridge is an example.

- **Insurance Systems with Reduced Collateral:** Validators must provide collateral, which is reduced in the event of harmful activity. This cut collateral is used to repay users if assets are taken as a result of the validators' fraudulent acts. Trust is undermined by disincentivizing harmful behavior and compensating users when things go wrong. Axelar is an example.

- **Systems Using Native Tokens as Collateral** Several bridge systems employ their native token. These systems operate in the same way as insured and bonded systems, but the sort of collateral employed differs. When malicious actions occur in such systems, the bridge system faces cascade failures across the design since the token is often a key aspect of the whole system's security. Trust is effectively leveraged up with token-based bridges, where the bridge's security is likewise dependent on the price of a token, making them less trustable.

  For example, Thorchain asks validators to stake RUNE tokens to assure the system's economic security. In the event of malicious activity, this collateral is cut and used to recompense consumers. As a result, RUNE, Thorchain's native token that was being staked as collateral, will have to be released to compensate the impacted users. In such a case, the selling pressure on RUNE may intensify, with cascade repercussions across the Thorchain architecture as a result of the falling price of RUNE. Such actions took place on 16 of July 2021 with $7.6M stolen [50].

6.4.2 Bridges that are optimistically verified

Optimistic bridges work in the same way as Optimistic Rollups. They deploy honest system observers to monitor operations and detect fraud. A single honest verifier is a separate trust vector with optimistic bridges. To validate changes, optimistic bridges require one

watcher in the system. As a result, while optimistic bridges allow fraud, an attacker can never be certain of stealing funds since there is no way of knowing whether a single honest observer is watching the system at any given time. This style of design mechanics dramatically raises the economic cost of attacking the system, thereby reducing trust to zero. Nomad is an example [51].

Optimistic vs. Externally Verified Systems Comparison

Optimistic bridges are fundamentally different and, by definition, have less trust than bridges with external validators. Let's have a look at an example to see how this works.

Assume a security breach occurs and the private keys of the vast majority of validators in an externally verified system are hacked (ex: Ronin bridge hack). Because he now has control of the system, the attacker will be able to take all of the bridge's cash. In an optimistically verified system, however, even if the attacker has the private keys of all validators, he is not assured to steal the funds as long as there is one honest observer in the system who may 'catch the fraud' and deny the attacker's access to the funds. As a result, the assumptions in both configurations are fundamentally different, and optimistic bridges are naturally less trusted than externally verified bridges.

6.4.3 Locally Verified Liquidity Networks

Locally verified systems use the validator set of the underlying blockchains in a particular cross-chain exchange. Instead of a transaction being verified by the whole validator set on both chains, two validators (one from each side) validate the counterparty on the other chain like in Figure 6.12.

These two validators serve as "routers" in the liquidity networks, ensuring that:

1. Maintain liquidity pools across each chain
2. Independently check each other (the counterparty)
3. Make atomic swaps easier.

To maintain the safety of the users' cash, such systems often include lock/unlock mechanisms and dispute resolution processes, essentially leaving no method for the validators on

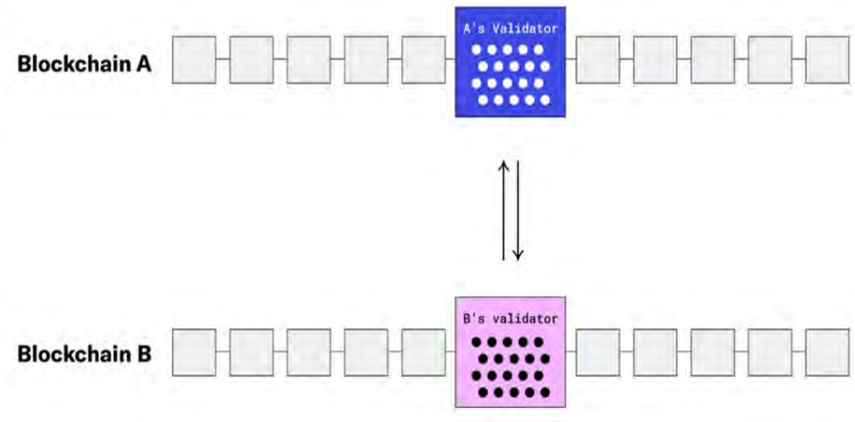

Figure 6.12: Locally Verified Liquidity Networks

each chain to coordinate and steal funds. Systems that have been locally verified are effectively trustless. Connext and Hop are two examples.

Trustlessness in bridges is not definite, as evidenced even by bridges in the same category. For example, trustlessness differs across various liquidity network solutions such as Connext and Hop.

6.4.4 Natively Verified - Light Clients and Relays Plus ZK Bridges

All validators of the underlying blockchains are accountable for maintaining the system in natively certified systems as seen by Figure 6.13. These are the most trustless bridging systems since users rely on the chains' own verifiers for bridging. Cosmos IBC is an example.

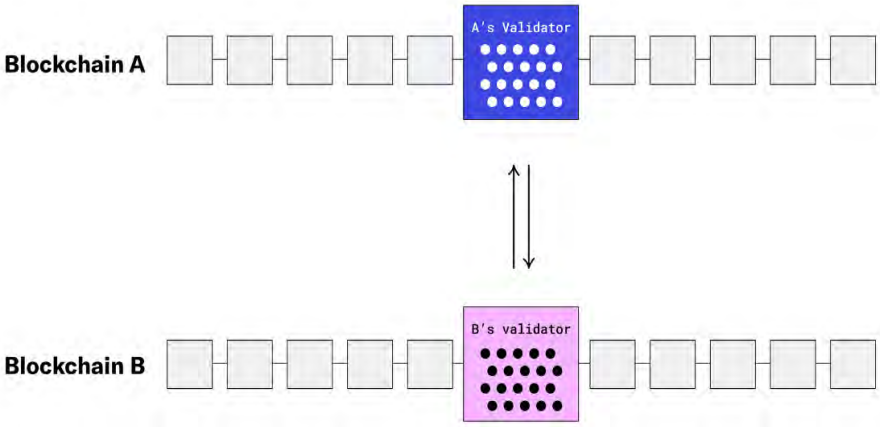

Figure 6.13: Natively Verified - Light Clients and Relays Plus ZK Bridges

Bridges based on Zero-Knowledge (ZK) proofs are another trustless approach that em-

ploy light clients and relays to confirm cross-chain transfers. However, no trustless ZK bridges are currently in production [52]. Furthermore, establishing bridges based on ZK proofs is an unexplored topic, and as we go farther down the rabbit hole, we may discover additional tradeoffs, trust assumptions, and downsides.

6.5 Cross Chain aggregators

6.5.1 Overview

A Cross Chain aggregator thrives in the noumerous blockchains of the DeFi ecosystem. Consolidates trades from numerous decentralized financial platforms (DeFi DEXs) into a single place, saving customers time and enhancing cryptocurrency trade efficiency. DeFi, as the name implies, is distributed across many blockchains, including Ethereum, Binance Smart Chain, Avalanche and Solana. Each blockchain has an ecosystem of distinct financial protocols.

Cross Chain aggregators gather the best rates from DEXs, loan services, and liquidity pools in one spot, allowing users to maximize their deals. Without an aggregator, customers must go to each platform individually to compare costs and choose the best offer for them. The user must then manually execute each transaction via smart contracts. While this technique is good for recreational crypto trading, it significantly hinders anyone wanting to execute complex trading strategies.

Aggregators not only extract the best prices, but certain Cross Chain aggregators also provide a unique, user-friendly approach to examine and integrate other users' trading strategies using a straightforward drag and drop process.

The cross-chain infrastructure is one of the most basic components of a multi-chain and multi-layer design. In the cross-chain region, the cross-chain aggregator plays an essential part in the transaction function of cross-chain aggregation. Its explicit purpose is to minimize transaction difficulty through the algorithm that may provide reduced transaction costs, faster screening, stronger security, and other benefits of the way for users to carry out the ideal cross-chain transaction path.

The aggregators provide more than just a bridge. The primary function of cross-chain aggregators is "bridging plus aggregation transaction", which opens up transaction functions with financial qualities such as liquidity mining and loan facilitation at the asset swap level,

allowing users to aggregate liquidity from multiple ecosystems. It is the foundation of a multi-chain world. Cross-chain aggregation is another approach for on-chain liquidity management, in addition to boosting capital efficiency.

Furthermore, what is the purpose of a cross-chain aggregator and what are the distinct advantages of cross-chain aggregators? How do they meet their cross-chain asset needs? With these questions in mind, let's look at the current five cross-chain aggregators. We examine the present state of cross-chain aggregators and speculate on how they enlarge the development area. In addition, we open up assets and data based on asset cross-chain aggregate transactions, moving toward a multidimensional, multi-chain, and multi-layer ecological cosmos.

6.5.2 Competitive Distinction of Aggregators

Li.Finance

Li.Finance works as a cross chain function and an aggregator transaction. In one word, the features of Li.Finance (Li.Fi) include paraswap(DeFi swap aggregator) and 1inch(DeFi yield farming) with cross-chain bridge functionality [53]. Li.Fi fulfills the twin functionalities of cross-chain swap and cross-chain yield farming schemes when combined with the DEX aggregator and cross-chain bridge. It performs the cross-chain function of the cross-chain bridge's on-chain assets. To summarize, you may exchange any token from any (supported) chain for any token from another chain. .

This procedure is relatively expensive. Assume a user wishes to exchange ETH from Ethereum for BNB on the BNB chain as seen in 6.14. The user must first swap ETH for USDC, then move assets to the BNB chain via the bridge, and finally convert USDC into BNB. The cross-chain bridge handling charge and gas fee that consumers must pay are not insignificant costs.

Consider the Li.Fi transaction flow and consider the hidden expenses. When users confirm the purchase, they have the following options: Which cross-chain bridge to choose as the cross-chain path; which DEX to trade on; is there a more efficient, easier, and cheaper method to trade after all of these cost considerations? Finally, another aspect is the security of the smart contract for the cross-chain bridge and DEX.

To reduce the difficulties in choosing, Li.Fi integrated cross-chain bridge capital resources and linked DEX and DEX aggregator. Li.Fi will automatically analyze the likelihood of a user's transaction request and rate the security, speed, and other elements of the path based

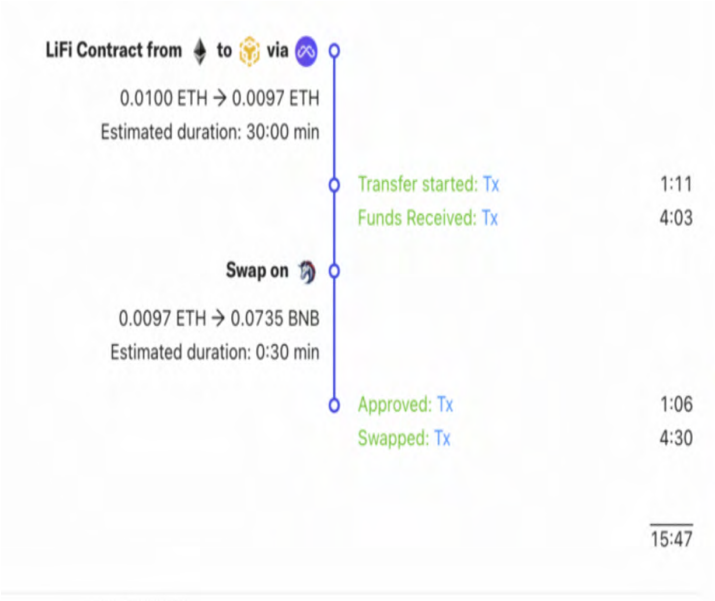

Figure 6.14: Li.Fi Transaction Route (source B.2

on many indications to provide the best way.

At the user level, the procedure is as follows: enter the transaction, wait a few seconds, obtain an asset transfer and exchange method, verify the transaction progress, sign numerous times to confirm the cross-chain and asset swap, and finish the transaction. Li.Fi also allows users to customize the slippage setting, cross-chain bridge, and DEX scheme as showcased in 6.15. Li.Fi delivers a more effective use of capital after lowering the cost of "option" for consumers.

In comparison to cross-chain bridges, Li.Fi emphasizes the following benefits of cross-chain aggregators:

- More diverse cross-chain trade paths: Because cross-chain bridge now only enables stablecoin and relatively original assets on a single public chain, cross-chain asset trading frequently falls short of user demand. When users exchange assets across chains, the function of DEX and DEX aggregators cannot be abolished. Li.Fi incorporates the three cross-chain bridge parties, DEX and DEX aggregator, and provides DEX for token exchange in both the source and destination chains. The transaction path of necessary tokens is more likely to succeed with a greater variety of cross-chain currency transactions.

- Breaking the liquidity impasse and increasing capital efficiency: At the moment, DEX contains duplicates of identical liquidity pools on each public chain. Users will dis-

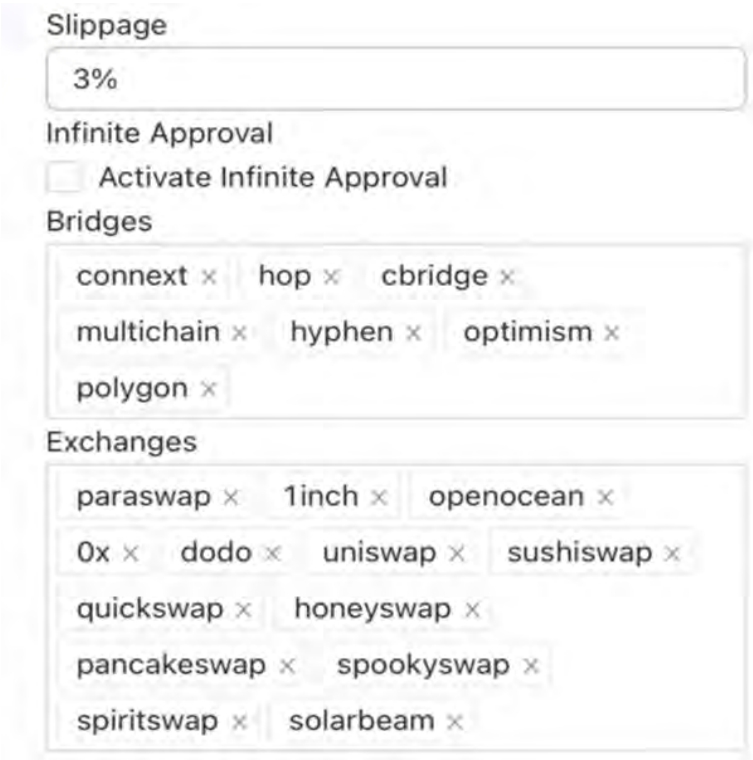

Figure 6.15: Li.Fi Slippage (source B.2

cover that this approach is exceedingly inefficient and fragmented if the number of copies of liquidity pools is multiplied by the number of distinct AMMs on each chain. Cross-chain aggregators provide deeper pools of liquidity within the same ecosystem by merging transaction data from various platforms, completing the present inefficient and fragmented structure.

- The transaction flow becomes more efficient after optimizing transaction security: When integrating with cross-chain bridge, DEX, and other partners, Li.Fi will first conduct technical evaluation and review, which is equivalent to reducing certain "systemic risks" such as smart contract security; second, the context technology is used at the bottom of Li.Fi, and the algorithm is used to score the security, gas fees, speed, and other influencing factors of each path, in order to provide a smoother and optimal trading path.

Li.Fi presently obtains liquidity from external methods. In other words, the existing integrated public chain, DEX, and DEX aggregator are the key components for providing cross-chain route trade benefits. In some ways, we believe Li.Fi represents the tipping point in the realm of cross-chain aggregators. After all, as compared to the other four aggregators, it

concentrates solely on cross-chain aggregate transactions.

When given the option between security and decentralization, Li.Fi chooses the latter. The algorithm assessment criteria used by Li.Fi to calculate the best route were never revealed. The ideal path is known to users following a "centralized evaluation". Furthermore, while the Li.Fi smart contract is open source, the API is not. There are two "killer" termination switches on the Li.Fi back-end interface. The first is at the API level, where path computations explicitly disregard bridges under assault, and the second is at the "risk" level. The second is on the smart contract layer, where Li.Fi or the project can disable the integration interface if a hacker attacks the protocol party.

Cross-chain aggregator measures with stronger smart contract security are supposed to guard against hacker assaults, however cross-chain aggregator protocols increase counter-party risk. Due to a weakness in the swap function of Li.Fi contracts, hackers stole around $600,000 in tokens from 29 wallets on March 20, 2022 [54]. In retrospect, Li.Fi was not the only stolen cross-chain aggregator.

XY Finance

The XY Finance project includes the twin functionalities of X Swap and Y Pool. X Swap in XY Finance is responsible for cross-chain swapping and aggregated trading capabilities, akin to Li.Fi [55]. When a user requests a transaction, XY Finance will construct a single transaction from the source chain to the destination chain, searching for the best path, and the transaction's security is dependent on the decentralized consensus method. XY Finance cross-chain transaction path is shown in Figure 6.16.

Figure 6.16: XY Finance cross-chain transaction path (source B.2

XY Finance's Y Pool is an asset liquidity upgrade that varies from Li.Fi in terms of liquidity. Y Pool is a single currency liquidity management pool capable of managing the liquidity of a single asset across numerous chains. Y Pool now supports the USDT and USDC cryptocurrency. The USDT Y Pool, for example, may accept USDT assets from several chains, including ERC-20 USDT, BEP-20 USDT, and Polygon USDT. Users can deposit ERC-20 USDT, BEP-20 USDT, and Polygon USDT into the USDT Y Pool and get the Pool token xyUSDT. These various USDTs will be utilized to create liquidity for the X Swap transaction. By staking xyUSDT, xyUSDT holders can earn swap fees generated by X Swap and receive XY tokens as a reward.

The demand for trade will most likely move most of the liquidity to another chain, culminating in an imbalance in the percentage of assets in each chain of the pool. As a result, XY Finance has instituted rebalancing incentives. Users can use the rebalance function to rebalance liquidity on each chain in the Y Pool. Users that assist in rebalancing liquidity in the Y Pool will also be rewarded with XY tokens as shown in XY Finance rebalancing incentive formula in the next paragraph.

Assume that the asset percentage in the USDT Y Pool is uneven, the Ethereum USDT is 0.1 million, the USDT on BSC is ten million, and the USDT on Polygon is fifty million:

- There are n different chains, which has its pool supported tokens
- Token on each chain is represented as a1, a2, a3, ... an
- Max XY token rewards each time = m

Formula

$$A = \frac{\alpha_1 + \alpha_1 + \ldots + \alpha_n}{n}$$

$$balanceratio : R = \frac{\alpha_1 * \alpha_2 * \ldots * \alpha_n}{A^n}$$

Reward

$$reward = (R_2 - R_1) * m$$

1. If Alice invokes the re-balancing function and sends 20 million USDT from Polygon to the Ethereum pool, the balance in each chain will be: Ethereum: 20.1 million, BSC: ten million, and Polygon: thirty million.

2. The balancing ratio is R2 = 0.75 = 75% according to the formula;

3. Assume the highest XY token award amount (m) is 1,000; Alice will get (0.75–0.0062) * 1,000 = 748.3 XY tokens.

4. USDT Y Pool will re-balance the percentage of USDT on different networks in the pool based on the algorithm formula.

The purpose of the X Swap and Y Pool mechanisms is to manage the liquidity of multiple chains and to encourage users to become providers and balancers of the liquidity of assets on the chain. Y Pool established its liquidity pool to suit the trading demands of X Swap, and X Swap's trading fees fund Y Pool's liquidity suppliers. Figure 6.17 is the X Swap and Y Pool mechanisms work in tandem.

Although XY Finance cannot personalize the slippage and charges for customers, after understanding the cross-chain exchange path, users may pick the most appropriate path to trade based on their specific needs and preferences as shown in the XY Finance Trading User Interface 6.18.

Figure 6.17: The X Swap and Y Pool complementing mechanisms (source B.2

The XY coin is another important component of XY Finance. The original XY Finance token is XY token, while veXY is a typical ve-Model token. Staking allows XY token holders to engage in different governance ideas. Locking XY tokens boosts liquidity mining results. The longer the lock, the greater the return.

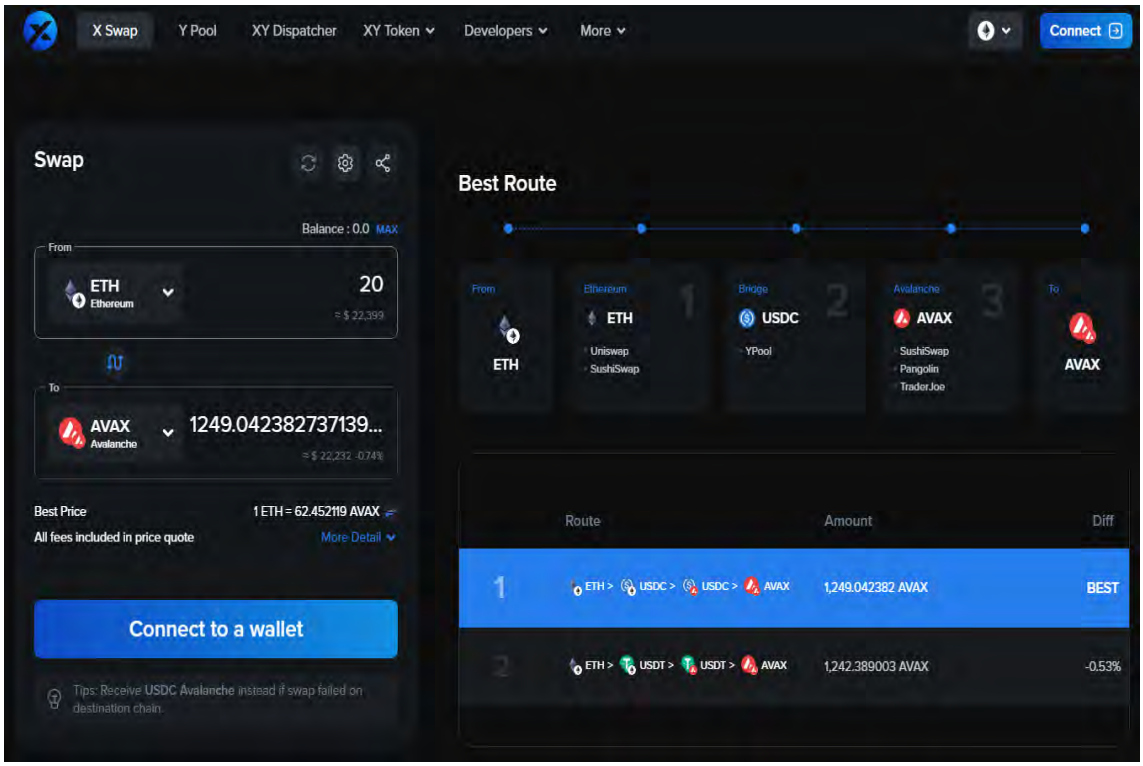

Figure 6.18: XY Finance Trading UI (source B.2

In general, X Swap and Y Pool have created a fully functional cross-chain trading mechanism for XY Finance. With the addition of governance token XY, users are not only motivated to supply liquidity but are also tied to the agreement's long-term interests. XY Finance demonstrates the zealous aim of connection Metaverse and financial company growth under the two enterprises of GalaXY Kats of Play-to-Earn and NFT Satellite.

O3 Swap

O3 Swap is a cross-chain transaction aggregator akin to XY Finance. O3 Swap is a cross-chain aggregation mechanism based on PolyNetwork that was developed by O3 Labs in 2017 [56]. O3 Swap's primary function modules are O3 Aggregator and O3 Hub, which are layered to provide cross-chain aggregation transaction service. O3 Aggregator acts as a transaction aggregator and is in charge of combining DEX across many chains. O3 Hub is a cross-chain liquidity hub that allows users to provide on-chain asset liquidity showcased in Figure 6.19.

Liquidity providers, similar to XY Finance's Y Pool, can deposit single or multiple identical assets on various chains in O3 Hub and receive O3 tokens as a return by staking LP tokens. O3 Hub currently provides a plethora of options as it shows in Figure 6.20.

It is easy to observe that O3 Swap performs the basic duties of a cross-chain aggregator,

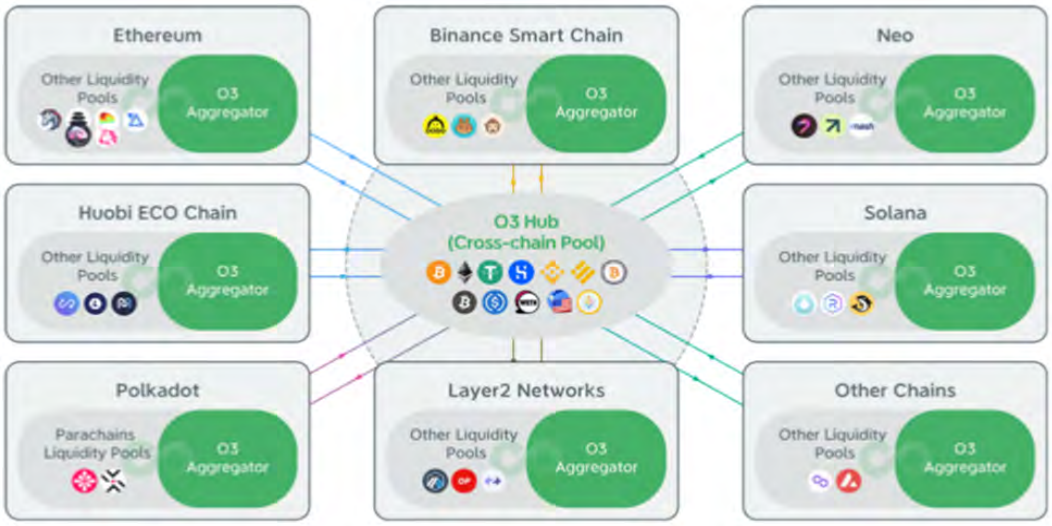

Figure 6.19: O3 Hub Architecture (source B.2

namely liquidity aggregation and cross-chain exchange. With the introduction of the O3 Swap token, the route to decentralized governance and community-driven growth is obvious. Only the aforementioned two traits allow XY Finance to compete in a very unique manner. So, what distinguishes O3 Swap?

Firstly, the architecture's four-tier design 6.21. The recently published O3 Swap V2 (O3 Interchange) release demonstrates O3 Labs' desire to provide a one-stop cross-chain transaction.

Architecturally, the V2 design is more complicated. O3 Swap is in charge of aggregating DEX and DEX aggregators on the input and output chains, resulting in a more diverse selection of tokens available for cross-chain trading. O3 Bridge is made up of two parts: PTMCs (linked Token Management Contracts) on the protocol layer and NPAPs Pools (NativeToken & PeggedToken AMM Pools) on the liquidity layer, which serves as a cross-chain asset trading channel. Swap and bridge enable single-click transactions. Users may also buy gas at O3 Gas Station. The transverse line expansions improve the app's playability and provide customers a one-stop trading experience.

Furthermore, the V2 version of the liquidity layer features a new breakthrough. The liquidity layer is divided into two parts: one is DEX integrated by O3Aggregator, which is identical to Li.Fi, and the other is Li.Fi. SushiSwap, PancakeSwap, and other DEX will be in charge of the same chain exchange function. The other is O3's one-of-a-kind NPAPs pool, an AMM pool made out of tokens and anchored tokens (pToken) that use a burning-minting method. Tokens enter the Liquidity Entry Chain, and users can mint similar quantities of

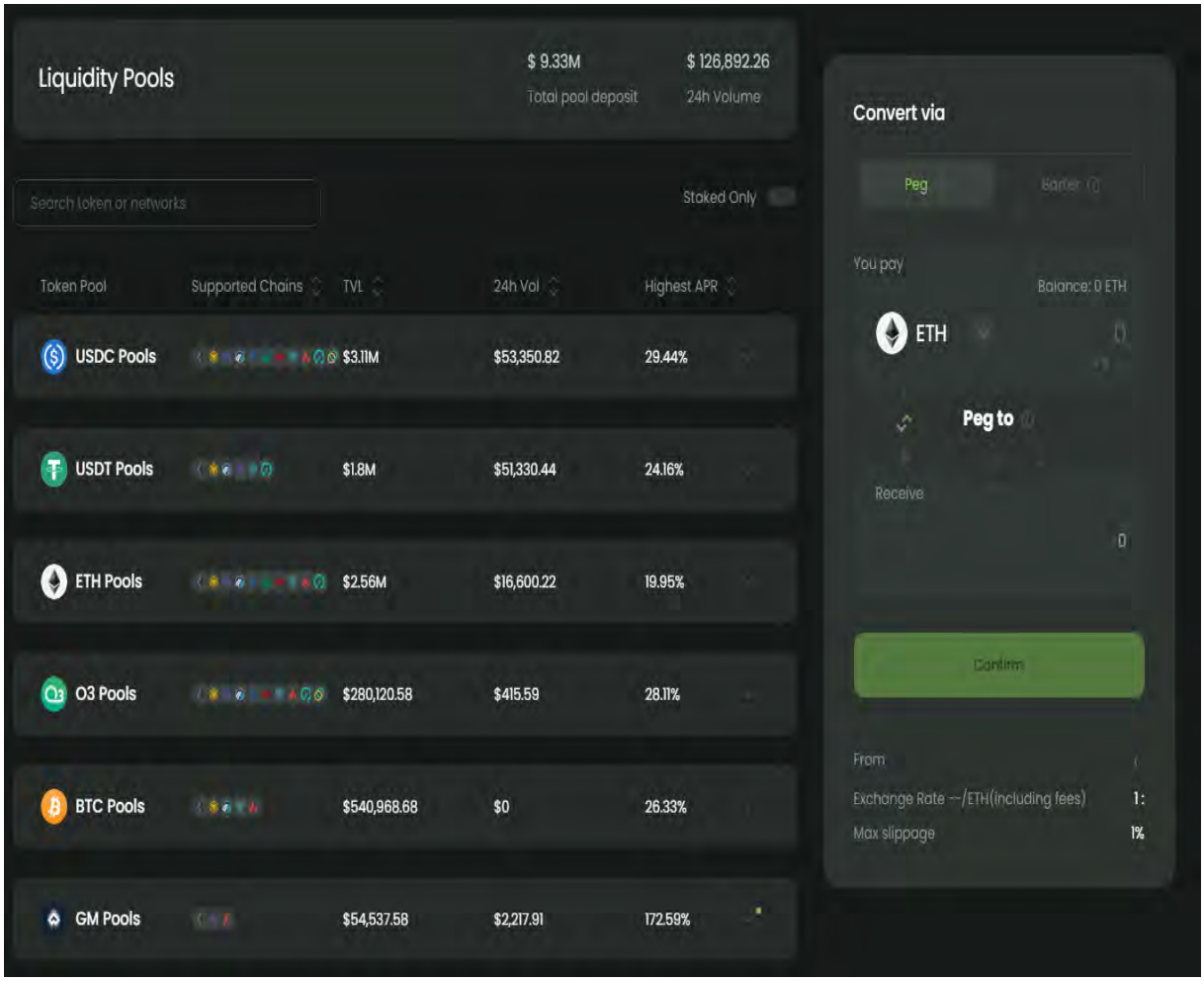

Figure 6.20: O3 Hub Cross-chain Pool (source B.2

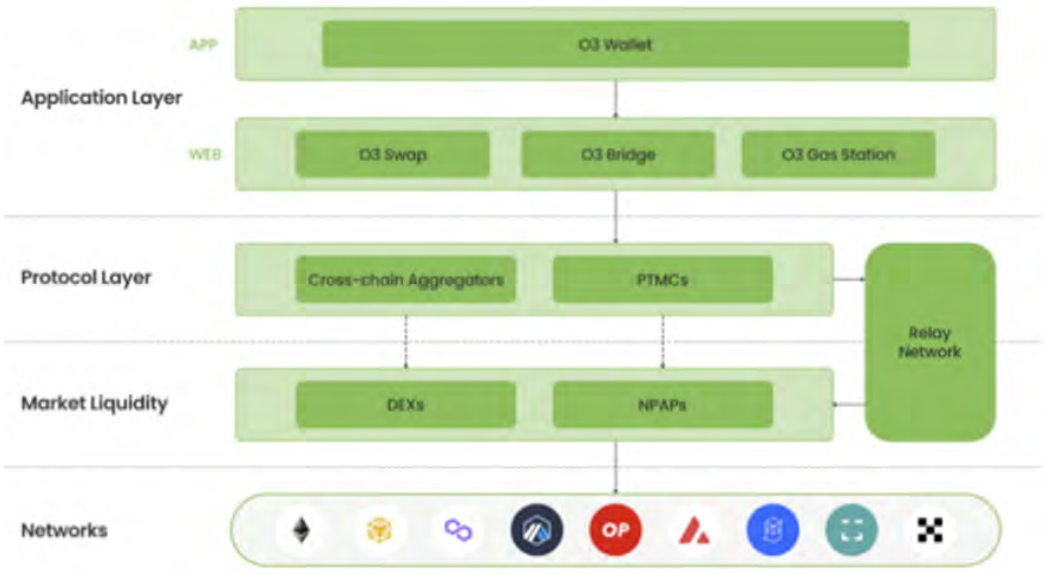

Figure 6.21: O3 Swap V2 design (source B.2

pToken on the same or other chains. Each pToken on each chain corresponds to a distinct PolyNetwork PTMC.

It should be noted that liquidity providers have two trading patterns. The first is Peg, in which users get pTokens via the liquidity input chain or other chains; alternatively, users can unbind the pToken from the liquidity entry chain to redeem the token. Another transaction type is barter, in which users swap tokens and pTokens directly in the same chain's AMM pool. Liquidity solution for O3 V2 is shown in Figure 6.22.

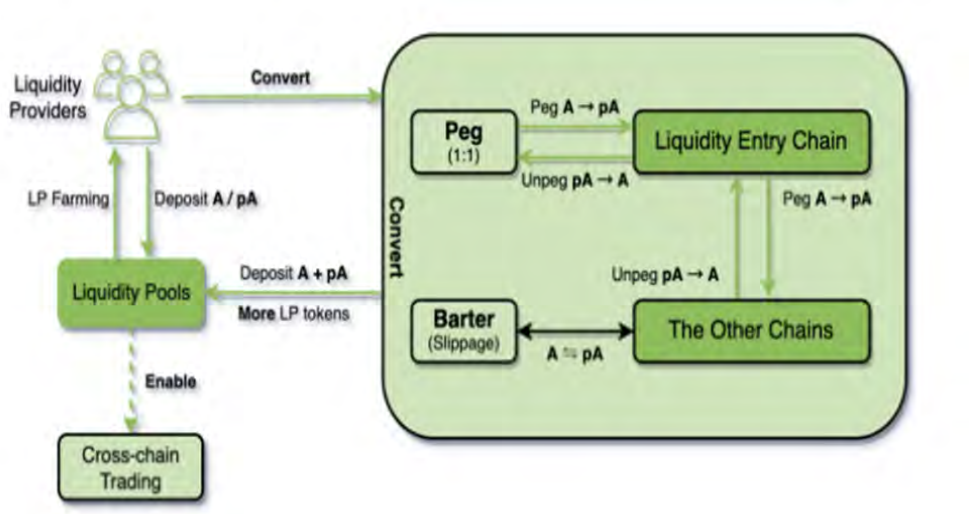

Figure 6.22: Liquidity solution for O3 V2 (source B.2

Token: the initial ratio of pToken in the AMM pool is 1:1. However, as users conduct Barter trades to arbitrage, the pool's equilibrium is disrupted. Users' arbitrage behavior, on the other hand, has become a mechanism of adjusting the balance of the O3 liquidity pool.

1. Assume that the primary network of Ethereum is token A's liquidity entry chain, and that the quantity of token A in the pool is more than the number of pA at the present.

2. The user later discovers that the quantity of token A in the BNB chain pool (m) is less than that in pA (n);

3. The user elects to swap m token A for n pA, then unpeg the n pA from the Ethereum main network to receive n token A.

4. The Ethereum and BNB pools will be rebalanced, and users will profit from "(n-m) *token A" arbitrage. The mechanism design of V2 is obviously more sophisticated, and it has been considerably enhanced and improved in the liquidity layer. The more

flexible and diverse company classification enhances O3 Swap's distinctive one-stop aggregate trading advantage.

ChainSwap

Up to this point, it is apparent that XY Finance and O3 Swap's cross-chain aggregating business is a strong point for them to build a footing in the multi-chain cosmos. ChainSwap is the same thing. Moreover, in combination to multi-chain and multi-asset cross-chain aggregation, they intend to construct a massive cross-chain ecological Hub called ChainSwap Hub.

ChainSwap's four pillars enable an ultimate cross-chain ecosystem, from assets to apps, from proxy networks to intermediary chains that facilitate cross-chain functionality.

Bridging aggregation is handled by the ChainSwap Bridge Aggregator. API collect data and back-end work from multiple cross-chain solutions presently supported by AnySwap, PolyNetwork, Wormhole, and cBridge, just like other cross-chain aggregators. Integration with Rango, a multi-chain DEX aggregator, demonstrates how ChainSwap enables apps and provides a knowledge hub.Of course, ChainSwap's UI 6.23is more similar to DEX Uniswap's.

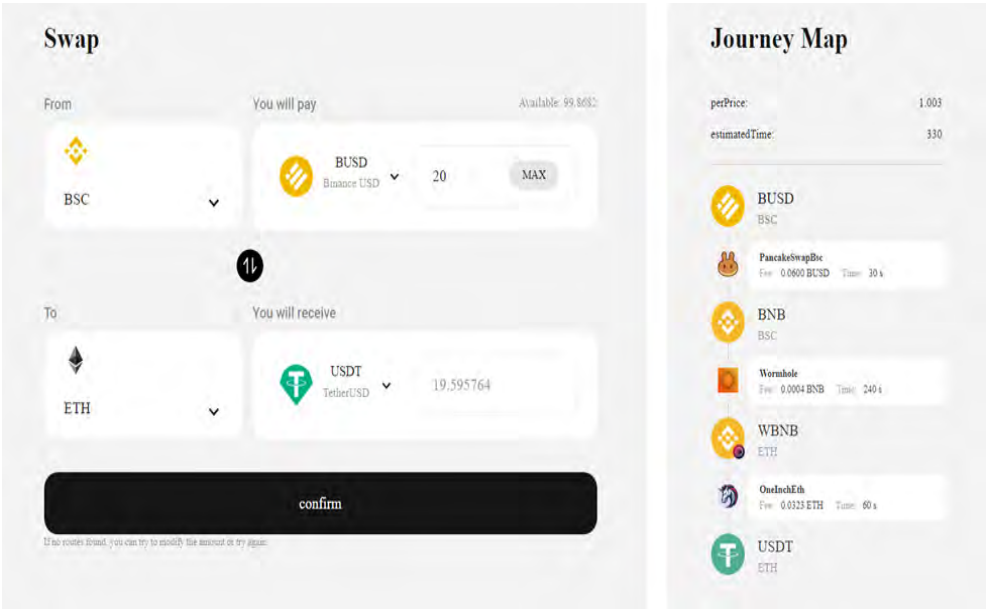

Figure 6.23: ChainSwap UI (source B.2

ChainSwap Bridge Aggregator also aggregates ChainSwap's native projects, such as ChainSwap native bridge V2 [57]. Its decentralized pre-set coin-issuing mode can streamline the administration process and boost coin-issuing efficiency. Of fact, according to ChainSwap's

whitepaper, the Liquidity Bridge they want to develop is a “Burn/Mint” mechanism that would enable cross-chain services for mainstream assets and allow liquidity providers to stake single tokens [58].

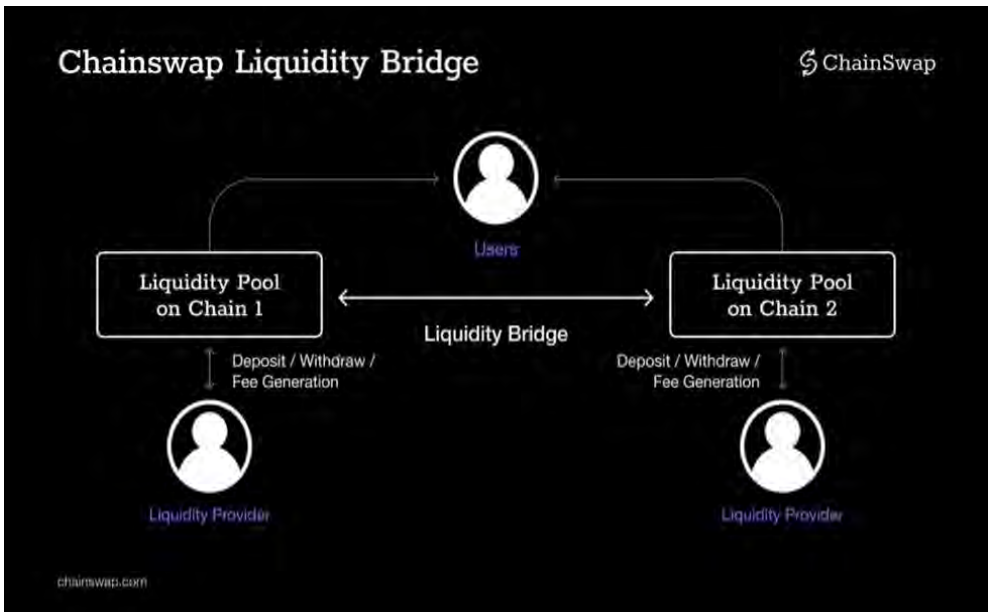

Figure 6.24: Chainswap Liquidity Bridge (source B.2

At the moment, I believe ChainSwap is distinct from XY Finance and O3 Swap. It opts to begin with the initial project of the cross-chain bridge in order to address a key issue of insufficient liquidity at the cross-chain asset end. After all, the ultimate aim is ChainSwap Hub. ChainSwap connects loan and derivative transactions from asset and data levels by aggregating numerous public chains and on-chain dApps such as cross-chain aggregator, cross-chain DEX, NFT cross-chain, and so on. As a consequence, an intelligent platform that combines apps and tools across chains will be created, as well as a parallel hub that will allow users to access and finish multi-chain transactions with a single click.In Figure 6.25 falls the project’s business model.

Bungee

FundMovr changed their name to Bungee in February 2022 after completing its makeover. The product is straightforward. The benefits of cross-chain aggregators include the ability to aggregate cross-chain bridges, DEX, and DEX aggregators in order to locate open pathways. It can satisfy bridging criteria such as highest output of the destination chain, lowest gas charge for transactions and transfers, shortest bridging time, and other aspects [59].

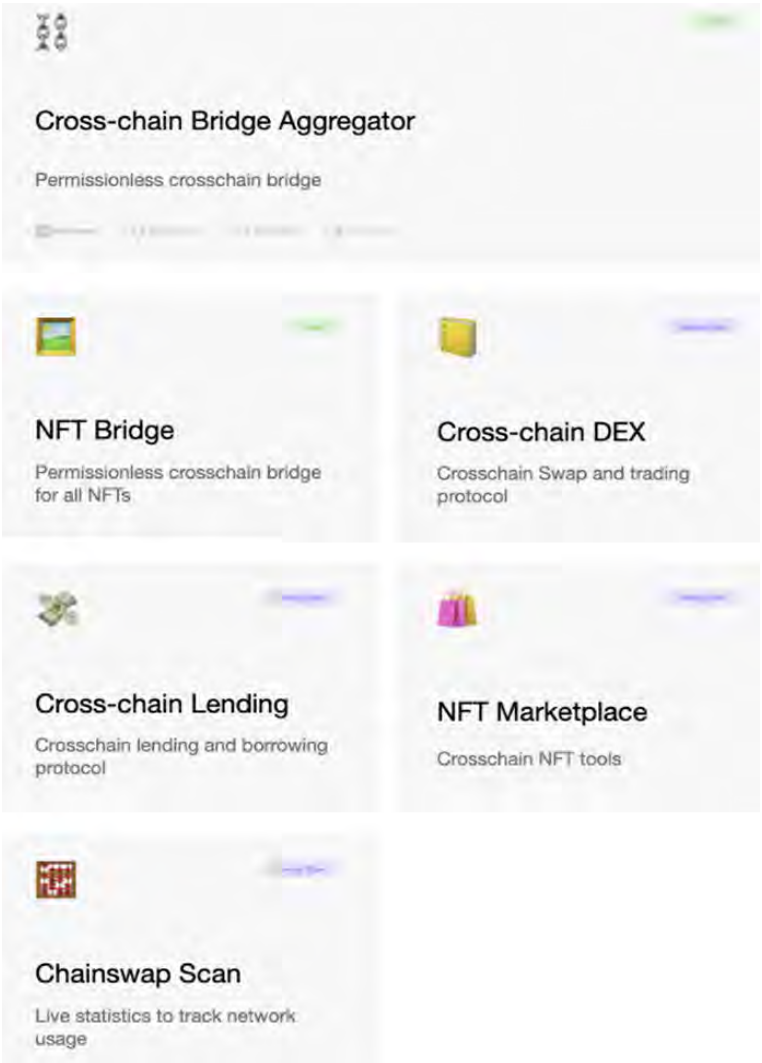

Figure 6.25: ChainSwap's business model (source B.2

Bungee's user experience strength is that it has put out three suitable pathways for consumers as shown in Figure 6.26. In comparison to previous cross-chain aggregators, the path selection option "truly" returns to the user. For your personal desire, you can select any of the three pathways with the fastest speed, lowest gas expense, and highest rate of return, such as Li.Fi, Bungee presently charges no fees.

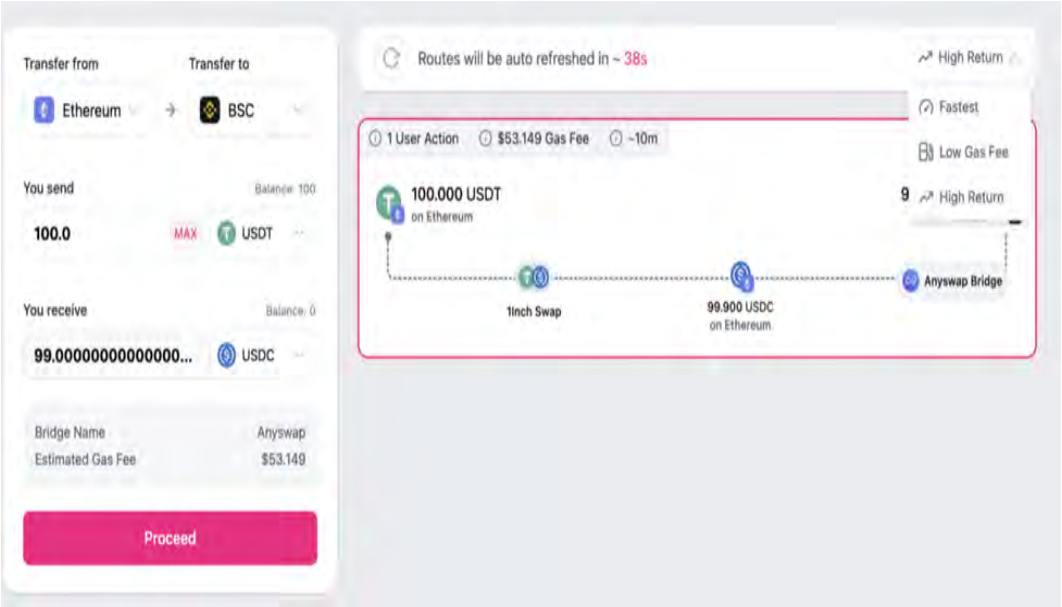

Figure 6.26: Bungee's trading interface (source B.2

Bungee enhanced Li.Fi with a point-to-point settlement methodology to enable bridge trade. Assume Alice wants to move 100 DAI from Optimism to Arbitrum, and Bob wants to move 50 DAI from Arbitrum to Optimism. Bungee will settle DAI in the same manner as the order book. It just needs to transfer the remaining 50 DAI from Optimism to Arbitrum in Alice's transaction. This method enhances the liquidity pool's efficiency and is a cost-effective choice. However, it is also a test of liquidity depth. Such a model cannot take use of its advantages if the chain trade volume is insufficient. The distribution of the Socket liquidity layer is shown in Figure 6.27.

Bungee's route options were restricted because the project was in beta, and funding was insufficient. Furthermore, I examine Bungee's rich business logic from the standpoint of sockets.

Socket takes a technological approach to multi-chain ecology. It establishes a meta-layer to enable multi-chain shared liquidity and dApp state unification [60]. Protocols can incorporate API interfaces to facilitate two-way asset transfer and information bridging. The Socket

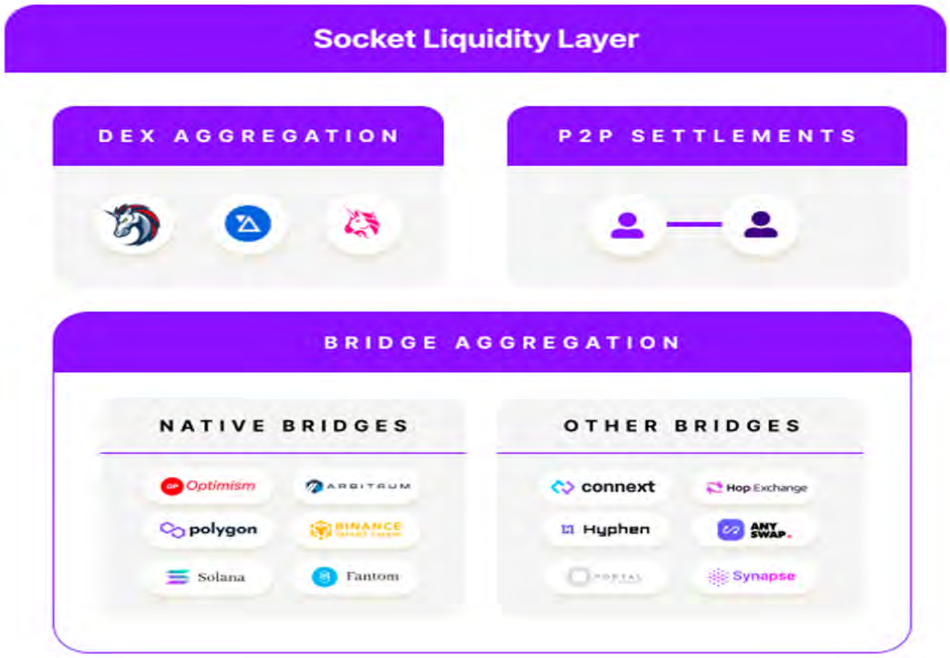

Figure 6.27: The Socket liquidity layer's distribution (source B.2

API currently supports low-level sockets such as Zapper, Zerion, and Ambire Wallet. Developers may also use the Socket as the foundation of their technological architecture to create an interoperable dApp after customizing it.

Bungee, as a native project of the Socket team, is, in my perspective, an external output of the team to demonstrate the fundamental technology. A brand like this can serve as a starting point for cross-chain communication protocols.

Chapter 7

Results

7.1 Cross Chain Adoption

Blockchain interoperability will be critical to the long-term viability of cryptocurrencies, non-fungible tokens, and other blockchain use cases. When developing apps, playing games, or investing money, most consumers and developers do not want to select between platforms. Interoperability adds benefit for everyone.The business implementation and key aspects of these five cross-chain aggregators have been accomplished. Following that, we'll take a quick look at the project status of these five cross-chain aggregators, taking into account the presently supported public chain / DEX / DEX aggregators, changes in transaction functionalities, user experience, and other issues.

Taking a look at October's adoption in 2021, Fantom's TVL showed a substantial increase, gaining 31.21 percent more in TVL. Meanwhile, Solana and Terra had far lower improvements, with Solana gaining 0.44 percent and Terra gaining 0.79 percent. Arbitrum experienced a TVL rise of around 24.58 percent, while Polygon (MATIC) increased by 4.41 percent. The Binance Smart Chain (BSC) TVL fell 6.15 percent but remained the second-largest defi TVL behind Ethereum. The recent collapse of Terra network created a domino effect within all DeFi products as seen from Figure 7.1

The chart 7.2 showcase a sample of the volume of transactions per day within a range of 20 days gathered across the above cross chain bridges

The quantity of Bitcoins locked on Ethereum serves as a proxy for Bitcoin's use in DeFi protocols. Tokenized Bitcoin may be utilized in a variety of ways on Ethereum, from lending collateral to earning a dividend on top of it. As a result, the quantity of Bitcoin on Ethereum

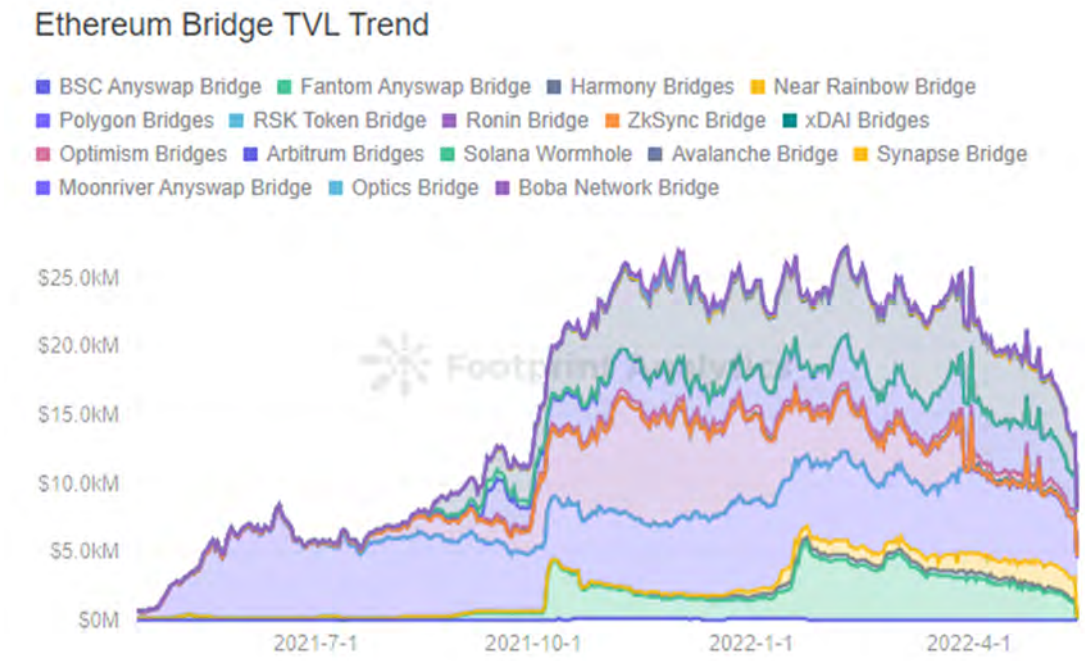

Figure 7.1: Ethereum Bridge Total Value Locked (source B.2

Figure 7.2: Volume/Transaction per Day(ntxp)

demonstrates Bitcoin holders' support and acceptance of the DeFi ecosystem.

Wrapped BTC, for example, may be used as collateral in a variety of Decentralized Finance (DeFi) protocols on the Ethereum network, including Uniswap, Aave, Maker DAO, Compound, Synthetix, Curve, Sushiswap, Balancer, 0x Protocol, and many others. Arbitrum, Polygon, Cronos, Metis Andromeda, Boba, and Aurora Network can also be used to stake WBTC. The graph below depicts the conversion of Bitcoin balances held in centralized exchanges to WBTC based on on-chain statistics from Glassnode 7.3.

Figure 7.3: Bitcoin transition to WBTC (source B.2

The big drop of Bitcoin Balance stored in all Cexs fell from 3,15M BTC to 2,5M BTC at 13 of March 2020 and the rise of WBTC adoption happened in late February of the next year. In early July 2020 WBTC went live on Compound DeFi protocol with 40% collateral factor, that is users may only lend 40% of the value of any WBTC they choose to use as collateral. Wrapped Bitcoin was added to Compound in response to a community suggestion made to Compound holders in May 2020. On May 12, after two months of discussion, the Compound community voted 533,899 to 523,974 in support of introducing WBTC to the lending protocol. [61].

Further investigation from ethercan 7.4 WBTC token holders addresses reveals that three of the eight addresses belong to lending protocols, including Aave, Compound, and Maker. This significant concentration of deposits on lending processes demonstrates the existing need for investors to leverage their holdings and maximize the value of their assets.

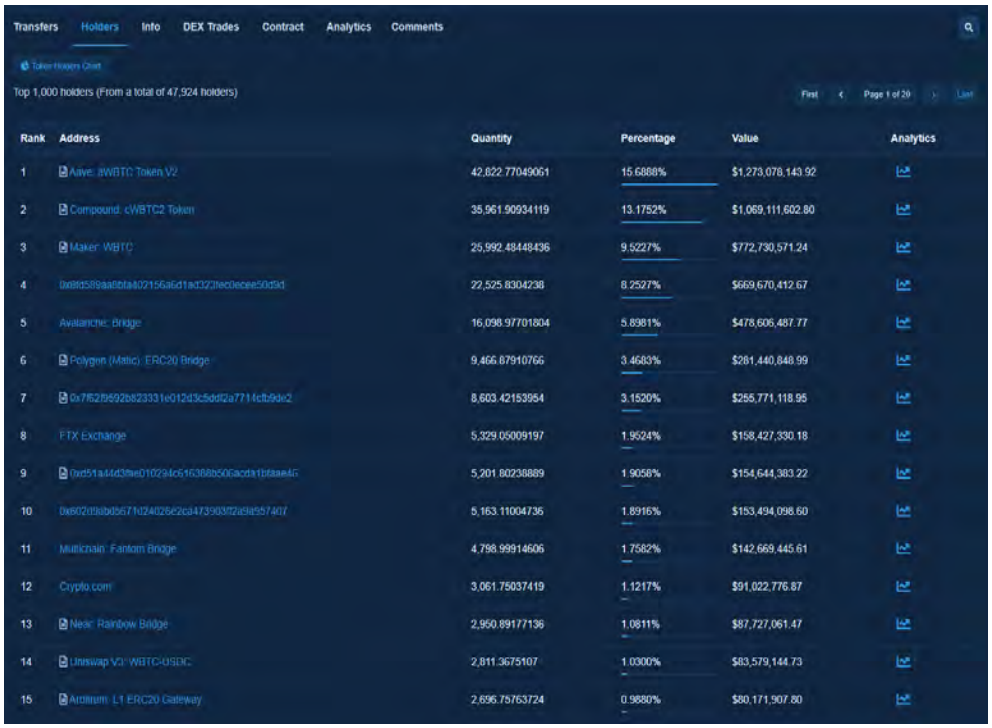

Figure 7.4: WBTC Top Holders (source B.2)

Two of the rest eight addresses belong to blockchain bridges: the Avalanche and Polygon bridges. This bridge consolidation lets us to assess and consider the expanding demand for WBTC in other new blockchains. In this situation, consumers are most likely bridging in order to participate in fresh current investing possibilities. The remaining three addresses in the group are identified as Nexo and an unnamed address that appears to be a personal account and the last belongs to FTX Exchange. Finally, the highest personal degree of concentration goes to this undisclosed address (0xB60C61DBb7456f024f9338c739B02Be68e3F545C), which has obtained around 5% of WBTC's current supply.

7.1.1 Risks Associated with Bridges

There has been a huge dilemma trusting a bridge. As previously noted, TVL plays an important role in bridge protection. Bridges function by utilizing a smart contract on both blockchains. The bridge employs a relay to send messages back and forth between the smart contracts on each blockchain. The Ethereum Virtual Machine is unable to send messages over the Internet. As a result, the relay for a bridge is a centralized entity — a handy bridging API or an "oracle" server dedicated to this one task. Centralized entities supply the APIs. These are sometimes referred to as "decentralized" since they guarantee not to interfere with the

communications. For that reason, if there are vulnerabilities on the smart contract, hackers can break in and steal enormous amount of funds [62].

On March 23, the Ronin Network's bridge to Ethereum was hacked, and $625 million in Ether and USDC were taken from the blockchain game Axie Infinity [49]. The hack was discovered on March 29. The Ronin chain of Sky Mavis presently has 9 validator nodes. Five of the nine validator signatures are required to acknowledge a Deposit or Withdrawal event. The attacker gained control of Sky Mavis' four Ronin Validators as well as a third-party validator run by Axie DAO. The validator key mechanism is designed to be decentralized, limiting an attack vector similar to this one, however the attacker discovered a backdoor via the gas-free RPC node, which they exploited to obtain the signature for the Axie DAO validator.

The Multichain attack, in which $7.9 million was taken as a result of a hacker reversing the private key. In addition, the hack had far-reaching consequences. As a result, O3, a trading pool that leverages Poly Network to transfer tokens between blockchains, has forced to halt its cross-chain functionality.

Wormhole Portal, a DeFi bridge connecting Solana and other blockchains, has been compromised, with 120,000 Ethereum (ETH) valued around $325 million hacked. Wormhole's backend architecture failed to adequately confirm its guardian accounts, according to a thorough study provided by Samczun on Twitter [63] a few hours after the robbery on February 3rd 2022. The hacker or hackers behind the scam produced 120,000 ETH tokens on the Solana chain by creating a bogus signature account, valued about $323 million at the time of the transactions. According to blockchain research firm Elliptic, the hackers then performed a series of transfers that deposited around 93,750 tokens into a secret wallet housed on the Ethereum network. In total, over 1,67 billion were stolen from cross chain attacks in two years. Is it true that cross-chain protocols are more prone to attack? The massive volume of assets gathered in the chain is the primary cause for the frequent occurrence of cross-chain protocol assaults. When faced with enormous incentives, hackers are forced to develop new ways to attack. Furthermore, because cross-chain projects include not only smart contracts on the chain but also code off chain, hackers will attack any flaw in the project.

Cross-chain bridges are becoming more popular, but that doesn't imply they're without danger. Cross-chain bridges, for example, claim Ethereum's Vitalik Buterin, raise security concerns when transferring assets by expanding the surface area for attack. These issues grow

when the number of chains increases from two to three or even a hundred.

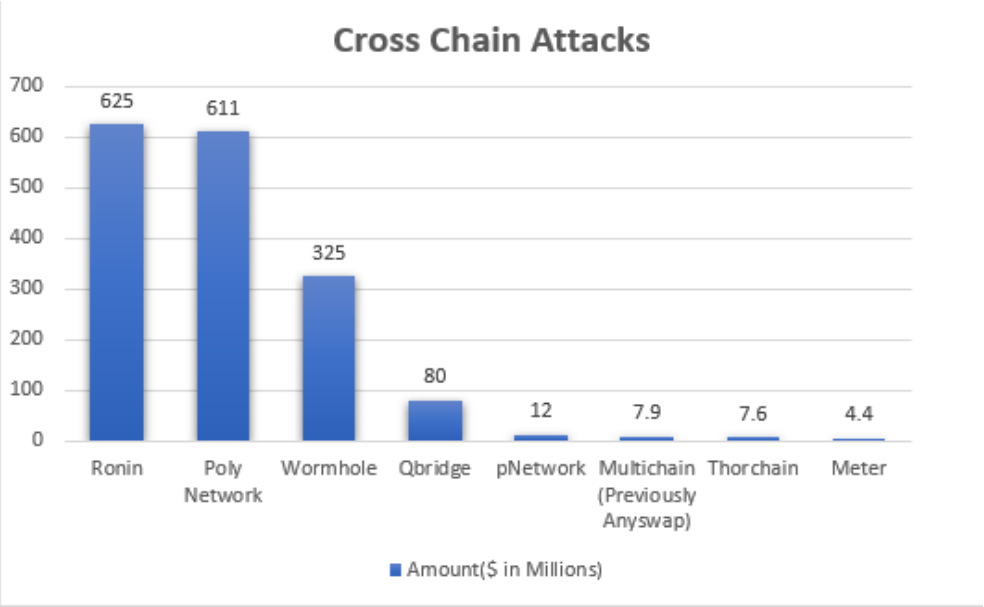

Figure 7.5: Cross Chain Damage in Millions

In a recent tweet [64] Vitalik, he stated it this way: “Imagine what happens if you move 100 ETH onto a bridge on Solana to get 100 Solana-WETH, and then Ethereum gets 51% attacked. The attacker deposited a bunch of their own ETH into Solana-WETH and then reverted that transaction on the Ethereum side as soon as the Solana side confirmed it. The Solana-WETH contract is now no longer fully backed, and perhaps your 100 Solana-WETH is now only worth 60 ETH. Even if there’s a perfect ZK-SNARK-based bridge that fully validates consensus, it’s still vulnerable to theft through 51% attacks like this.”

Multi-chains, such as Cosmos or Polkadot, overcome these issues by utilizing a common security mechanism as well as cross-chain bridges. Developers can build their own unique parachains on top of these sorts of services, relying on them to manage security and asset transfers across parachains.

Finally, cross-chain bridges may have tax consequences [65]. Axie Infinity, for example, is developed on Ethereum’s Ronin sidechain. When you sell ETH to buy an Axie, you must pay tax on any ETH appreciation since you bought it. You may also owe taxes if you profitably sell an Axie, earn SLP, or breed Axies.

To make this situation worse, uninformed web3 users may feel safer while utilizing higher TVL/TVB (Total Value Locked/ Total Volume Balance) bridges since these bridges appear to be sturdy enough to manage massive rates of token transfers; yet, there is no apparent

association between TVL/TVB and security. In fact, one might argue that as the TVL/TVB grows, the security of the bridge becomes more vulnerable since a hostile actor has a higher economic incentive to uncover a flaw.

When transferring payments, it is important to understand the underlying security system of the bridge. If a retail trader has to deposit 0.5 ETH rapidly to assure an NFT mint, security should not be a key priority.Conversely, if a DAO intends to move 10,000 ETH to a contract on a separate chain, the bridge's underlying security should be thoroughly scrutinized.

7.1.2 Aggregators Comparison

The content in the table is current as of April 22nd, 2022.Returning to another question we set in the beginning, why is a cross-chain aggregator required? The following are the important points summarized in this section:

1. **Effective liquidity reduces the transaction costs of cross-chain aggregators**

   The cross-chain bridge serves a single purpose and can only be responsible for "transportation" between stablecoin and native token. Users' true demands will be far from met if there is a lack of composability. When cross-chain bridges employ the wrapped token as the medium token to overcome liquidity difficulties, the extra transaction complexity is passed on to the user in the form of needless overhead and a bad user experience. More significantly, when users weigh the benefits and drawbacks of each chain bridge and DEX, they incur recurring and wasteful effort expenses.

2. **Cross-chain aggregators provide a more pleasant user experience**

   The cross-chain aggregator combines the cross-chain bridge, links the DEX and DEX aggregator, and reduces the time necessary to query the token exchange path. Users can carry out the complete asset exchange procedure in whatever way they see fit. Cross-chain aggregators have substantially improved in terms of usability, convenience, and cost efficiency for users. All cross-chain bridges, DEX, and DEX aggregators may be combined to determine all accessible routes. They may then assist users in optimally transferring assets across block-chains depending on parameters such as maximum output on the destination chain, minimal gas prices for transactions and transfers, minimum bridging times, and so on.

	Li.Finance	XY Finance	O3 Swap	Chainswap	Bungee (Fund Movr)
Team	PhiliPP Zentner;Max Kenk	Taiwan team	O3 Labs(Tokyo,2017)	CEO:Dmitry Atlasman	Socket
Found time	2021	Aug.,2021	N/A	2020	Oct.,2021
Token	None	XY	O3	ASAP	None
Project volume	N/A	$111.44M	$1.53B	$175.45M	N/A
Token Market Cap	N/A	$3,156,969	$15,180,310	$1,016,437	N/A
Public chains supported	12	7	8(Swap)	10(Swap)	8
DEXs supported	13	N/A	N/A	N/A	N/A
Bridge supported	9	N/A	N/A	4	N/A
Token supported	more complete	fewer	fewer	967	fewer
Business line	Assets Swap	X Swap&Y Pool (DeFi);GalaXY Kats(GameFi); NFT Satellite(NFT)	Bridge, Swap, Hub(Cross-chain liquidity mining),Vault(Stake LP/Token To Earn O3)	Cross-chain Bridge Aggregator; To be released:Cross-chain DEX, Cross-chain Lending, Cross-chain NFT tools, statistics	Assets Swap
Wallet supported	Metamask	Metamask, imToken, BitKeep, ThunderCore Hub Wallet , QubicWallet ,Walet Connect	Matamask , Coinbase Wallet , OntoWalet, CloverWallet	Metamask , Coinbase Wallet , WaletConnect , For matic , Portis	Metamask
Business progress	Swap Beta Version ;add newly module "Help Ukraine"	Swap Beta Version, "NFT" module to be released;	V2 interchange	The Cross-chain Bridge Aggregator Has been launched Bridge Aggregator, Swap . NFT Bridge	beta V1

Figure 7.6: Aggregators Comparison part 1

Trading Experience	1) The website has a dashboard function to provide a visual interface for wallet currency. 2) You can customize the slippage fee, Bridges, and DEX. 3) After the transaction is submitted, the system will automatically display the transaction process, and the whole process will be visible. 4) The user needs to confirm the next step of the transaction manually. 5) Li.Fi is free.	1)1-click Transaction takes about 10 minutes: the progress of the Transaction process can only be obtained by clicking on the Transaction History section of Vaults. 2) Y Pool now only supports USDT and USDC, and USDT APY is about 12.37%. 3)DAO provides XY mining. The fifth installment is about to begin; XY can earn money for a maximum lock-in period of 104 weeks and can also stake veXY with voting rights.	1) The optimal path selection will be updated within 30 seconds. 2) The currency selection is less concentrated on stablecoins and wrapped tokens. The mainstream public chains' original assets are not covered yet; If you Swap the ETH of Ethereum to the BNB chain, only BTCB, BUSD, ETH, USDT, and USDC can be selected. BNB cannot be selected. 3) Fees include 0.3% O3 Swap fee and Poly Network Fee.	1) The data provided by the website Dashboard is the most intuitive and clear. 2) The SWAP process does not support ETH of Ethereum. 3) To confirm the delivery, you need to confirm the path, wallet and cost again: after the transaction is confirmed, a pop-up box will show the transaction process.	1) The interface and functions of the website are single. 2) Simple operation, you can choose the fastest/lowest path. 3) Multiple path choices for point-to-point settlement mode; After approval, the selected bridge + fee and estimated time spent will be presented. 4) Bungee charges no fees.
Solution	The liquidity comes from the integrated DEX, DEX aggregator, and cross-chain bridge, and the back-end centralized switch improves security.	X Swap Y Pool model: X Swap is used to provide cross-chain transfers and transactions; Y Pool motivates users to provide liquidity.	The FOUR-tier architecture of O3 V2 provides one-stop trading. O3 Aggregator is responsible for aggregating transactions, and O3 Hub is responsible for asset liquidity. Liquidity generation mainly comes from two aspects: one is the external DEX, and the other is the native NPAPs pool.	Another function of ChainSwap Bridge Aggregator is to aggregate ChainSwap's native projects, such as ChainSwap native bridge V2.	Cross-chain assets + cross-chain communication protocol;Laid out three applicable routes for users. The liquidity layer introduces the point-to-point settlement mode.

Figure 7.7: Aggregators Comparison part 2

3. **Cross-chain aggregators lower development, decision-making, and administrative expenses.**

   Cross-chain bridge development is still in its early stages, which entails safety issues, illiquidity, and high maintenance costs. The cross-chain aggregator, as a third party, retains all cooperative cross-chain bridging features and handles user selections programmatically. For technology developers, cross-chain aggregators provide a "backup" solution.

4. **The cross-chain aggregator business is not restricted to asset cross-chain transactions**

   Cross-chain aggregators refer to the liquidity aggregation and cross-chain aggregation bridge protocols provided by asset cross-chain. When XY Finance, O3 Swap, linkage metaverse, or a one-stop trading platform is built, they also point to data, application, and other cross-chain interactions. In addition to providing a compensation for liquidity providers, the currency created by XY Finance and O3 Swap shows the development of decentralized governance and a community-driven paradigm.

5. **With two-way asset and information transfer, the cross-chain aggregator is an essential component of the multi-chain cosmos**

   In the context of Web 2, a cross-chain aggregator is a bridging form of an online shopper website, a minor portion of a multi-chain ecosystem. It removes the obstacles to the smooth two-way exchange of assets and information, resulting in a more versatile user experience. The cross-chain aggregator is not restricted to the asset's cross-chain part, but functions more like a function key. Whether at the technical level, focused on cross-chain convergent transactions, or business development based on this, it is attempting to open the door to the multi-chain trading world. As we all know, DeFi has a lot of energy, and asset efficiency is the most logical requirement.

As stated in the beginning, cross-chain aggregators offer a clear benefit in meeting user asset transformation requirements. Non-technical user pictures can be locked by convenient trading of hot assets, simple trading processes, greatly decreased transaction costs, and good capital efficiency. The flaws of early cross-chain aggregators are also visible. Poor user experience is caused by function flaws and a lack of liquidity. One of the primary reasons consumers employ cross-chain aggregators is to increase transaction efficiency. However, when

making a transaction request with the expectation of immediate success, it is frequently discovered that the right trade channel cannot be established, heightening the sensation of loss.

When Bungee exchanges Ethereum's USDT for BNB's BNB, the inability to confirm the transaction route is not specific to Bungee. The cross-chain bridge track is being redesigned, and the possibility is increasing.

The hot project LayerZero broke the present cross-chain bridge's impasse from the underlying architecture. The rise of cross-chain bridge comparison tools like BridgeEye strengthens the cross-chain infrastructure. THORChain is the foundation for the cross-chain DEX THORSwap, which Ryan Watkins describes as a decentralized cross-chain liquidity mechanism that can replace exchanges and custodians [66]. Fresh initiatives, like as Swim Protocol, which combines Wormhole bridging technology with an AMM mechanism, offer new development concepts for cross-chain liquidity to break down blockchain islands. Managing on-chain liquidity is an inescapable subject for future cross-chain aggregator growth.

Li.Finance has XY Finance and O3 Swap as liquidity sources, which choose external agreements or establish the original liquidity pool. ChainSwap and Bungee, the former decided to boost token supply by refining origin cross-chain bridges, while the latter selected point-to-point settlement to improve capital efficiency. Other than Li.Finance, the four cross-chain aggregators continue to study the combinable route of cross-chain liquidity with cross-chain aggregation transactions as the point cut.

Simultaneously, hacking attacks caused by contractual flaws are common. In addition to Li.Fi, ChainSwap and O3 Swap experienced comparable shocks to varied degrees. ChainSwap was hacked for $8 million on July 10, 2021 [67]; on August 1, 2021, as the underlying protocol Poly Network was compromised by hackers, $610 million was robbed, and the market-making funds were locked in O3 Swap also experienced huge losses [68]. When considering the future growth route, we discover that one of the most pressing issues for cross-chain aggregators is how to successfully avoid security vulnerability assaults.

Chapter 8

Conclusion

8.1 Conclusion

DeFi's novel yield bearing techniques and prospects boosted Ethereum's activity to previously unheard-of heights. Because Bitcoin is one of the most important cryptocurrencies on the market, the need for an Ethereum alternative has increased. With Ethereum's expanding usability and Bitcoin's market importance, WBTC plays an important role in the connectivity and interoperability of the blockchains. The creation, use, and adoption of WBTC demonstrates the growing demand for blockchain interoperability. Its introduction aided DeFi's expansion while also providing Bitcoin investors with access to a variety of yield-generating tactics not available on the Bitcoin Blockchain. WBTC's success shows that further interoperability in the crypto industry is still required. This will enable users to have access to the most recent market changes and opportunities.

WBTC has won the process of tokenizing BTC, and it has been the primary driver of Bitcoin acceptance on the Ethereum Blockchain thus far. Each tokenized BTC has certain fundamental peculiarities that impact its network acceptance. The primary ones are user confidence in the custodian, which is vital since the custodian is the one who locks the real asset on the Bitcoin blockchain, from whence the value is generated. Second, the degree of decentralization in the process of transforming BTC into a tokenized ERC-20; the more decentralized the process, the less control the custodian has over the locked assets.Finally, the amount of acceptance on the DeFi network is crucial since it broadens the use case alternatives.

Cross-chain bridges and aggregators allow currencies, smart contracts, and other data to be transferred across blockchains. The bridges might enable lower-cost transactions, collat-

eralized assets, higher scalability, and, ultimately, unleash the potential for Web3—the next iteration of the internet and commerce—by linking various networks.

Once again, one approach to "trustlessness" does not apply to bridges. There is no such thing as pure trustlessness. Trust is a spectrum with bridges, and there are compromises made for certain use cases that effect trust reduction. Bridges do not lend themselves to a one-size-fits-all solution. There is no ideal answer; only trade-offs for certain use cases – Each bridge has its own set of strengths and limitations, and as we learned from the interoperability trilemma, all bridges must pick between trustlessness, extensibility, and generalizability. While trust is a continuum, and one bridge may be more trust-minimizing than another, each bridge has its own set of strengths and flaws. Some bridges, for example, can provide faster and cheaper cross-chain swaps by using a more trustworthy technique.

The cross-chain aggregated transaction is a future path of capital efficiency and on-chain liquidity management for DeFi, but it is not the only one. Its and DeFi's development are mutually beneficial. Cross-chain aggregation transactions are anticipated to become a regular activity of DeFi ecology as more public chain ecology grows and multi-chain becomes viable. Cross-chain liquidity mining incentive rules, "active market maker" trading mechanism, LaaS (Liquidity as a Service), and other DeFi innovation trends may drive the future growth route of cross-chain aggregation.

8.2 Future Additions

Cryptocurrencies began with Bitcoin, but have evolved into much more. In a few years, billions of users will cross chain transacting on hundreds of chains, utilizing thousands of applications. Here's a my thoughts of a multichain future expansion:

I believe many large IT businesses will likely develop bridges in order to obtain power and influence. Advantages of having a bridge:

- You have control over assets coming in and leaving out
- You can collect statistics on popular coins/chains
- Simple integration into current payment apps
- Insurance for bridged assets.

More technology will be closed source and centralized as we grow more multichain. Decentralization is the fundamental spirit of crypto, however actual decentralization is incompatible with how the world works. The future will most likely be distributed rather than decentralized.

A decentralized world vs a distributed world is a possible tale to study and unfold: Users own their private keys in a decentralized society, are totally accountable for theft/loss, have no insurance, and are difficult to utilize, while in a distributed world, users can opt out of centralized systems if they like, although a mix of both is preferred for ease.

Another consideration is if Metamask will be completely supplanted as the top wallet by a better, easier-to-use wallet within the next five years. To avoid losing market share, wallet firms will combine and consolidate. Will we progress from having hundreds of different wallets to only 5 for popular for cross-chain use?

Are we going to have wallets that allow you to switch NFTs between chains with the press of a button? Is it possible to create massive pools where anybody, anywhere may borrow money at cheap interest rates without the requirement for a credit score or personal identity? Bridges and Oracles may power all of this.

Crypto 'wins' when it powers practically every program, is incorporated into our daily lives, and is so simple to use that most people don't notice. We are one step closer to making all of this a reality by working together and rejecting maximalism. The universe will be tokenized.

At the end of the day, the chains who listen to their customers, cherish their communities, and consistently innovate will win. We're so early in the game that the best ideas and companies haven't even been established yet—which is amazing. Let us toast to a multichain future.

Bibliography

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

[2] A Antonopoulos. *Mastering Bitcoin*. O'Reilly Media Inc, 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2 edition, 2017.

[3] V Buterin. Ethereum.org. *Ethereum Whitepaper*, 2014, February 4.

[4] David Easley, Maureen O'Hara, and Soumya Basu. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, 134(1):91–109, 2019.

[5] H. Sparks. Bitcoin pizza guy who squandered $365m has no regrets. https://nypost.com/2021/05/24/bitcoin-pizza-guy-who-squandered-365m-has-no-regrets/, 2021, May 24.

[6] R. Stevens. As bitcoin price rises, more investors are buying in. https://decrypt.co/45724/bitcoin-price-rises-more-investors-buying-in, 2020, October 20.

[7] Franz J. Hinzen, Kose John, and Fahad Saleh. Bitcoin's limited adoption problem. *Journal of Financial Economics*, 144(2):347–369, 2022.

[8] A. Pokima. Public companies hold a combined $11.8 billion worth of btc on their balance sheet. https://zycrypto.com/public-companies-hold-a-combined-11-8-billion-worth-of-btc-on-their-balance-sheet-see-the-leading-firms/, 2022, January 2.

[9] J. Benson. Microstrategy ceo: Bitcoin the solution to $250 trillion problem. https://decrypt.co/46809/microstrategy-ceo-bitcoin-solution-250-trillion-problem, 2020, October 31.

[10] Goland T. & Schiff R. Chaia A. Counting the world's unbanked. https://www.mckinsey.com/industries/financial-services/our-insights/counting-the-worlds-unbanked, 2010, March 1.

[11] M. Grenier. The worst currency performers in 2020. https://airshare.air-inc.com/the-worst-currency-performers-in-2020, 2020, July 2.

[12] J. Mariathasan. Are cryptocurrencies an asset class for institutional investors? https://www.ipe.com/current-edition/are-cryptocurrencies-an-asset-class-for-institutional-investors/10043517.article, 2020, February 1.

[13] E. Cheng. Cme, world's largest futures exchange, launches bitcoin futures. https://www.cnbc.com/2017/12/17/worlds-largest-futures-exchange-set-to-launch-bitcoin-futures-sunday-night.html, 2017, December 17.

[14] CFTC. Cftc charges bitmex owners with illegally operating a cryptocurrency derivatives trading platform and anti-money laundering violations. https://www.cftc.gov/PressRoom/PressReleases/8270-20, 2020, October 1.

[15] S. Klemens. Ethereum review: Ethereum use cases, advantages & disadvantages. https://www.exodus.com/blog/ethereum-review/, 2020, September 16.

[16] A. Gulley. Understanding ethereum. a simple explanation of ethereum and…. https://allan-gulley.medium.com/understanding-ethereum-819c2096b613, 2021, March 27.

[17] TheLuWizz. What are smart contracts? | definition and explanation. https://medium.com/coinmonks/what-are-smart-contracts-definition-and-explanation-e96cb879a8cb, 2021, February 22.

[18] T. Akintade. Ethereum migration to pos: Becoming eth 2.0 validator. https://cryptotvplus.com/2022/01/ethereum-migration-to-pos-becoming-eth-2-0-validator/, 2022, January 30.

[19] B. Polanco. Ethereum's move to proof of stake - what does it mean? https://www.coinreview.com/ethereums-proof-of-stake/, 2018, June 17.

[20] Arnaud Laurent, Luce Brotcorne, and Bernard Fortz. Transaction fees optimization in the ethereum blockchain. *Blockchain: Research and Applications*, 3(3):2, 2022.

[21] B. Nibley. What is ethereum gas? how eth gas fees work. https://www.sofi.com/learn/content/what-is-ethereum-gas/, 2021, October 5.

[22] Ethereumprice. Ethereum gas price charts & historical gas fees. https://ethereumprice.org/gas/, 2021, February 12.

[23] G. Wood. Polkadot whitepaper. *Polkadot Whitepaper - Whitepaper.Io*, 2020, April.

[24] M. Isler. Smart contracts explained | the ultimate beginner's guide. https://imiblockchain.com/smart-contracts-explained/, 2021, February 5.

[25] N. Szabo. Smart contracts: Building blocks for digital markets. *Phonetic Sciences*, 1996.

[26] Moralis Blog. Solidity explained - what is solidity? https://moralis.io/solidity-explained-what-is-solidity/, 2021, May 22.

[27] R. Sharma. Decentralized finance (defi). https://www.investopedia.com/decentralized-finance-defi-5113835, 2022, January 14.

[28] A. Hertig. What is a flash loan? https://www.coindesk.com/learn/2021/02/17/what-is-a-flash-loan/.[Accessed:Jun.25,2022], Feb. 17, 2021.

[29] I Vasile. What is a flash loan. https://beincrypto.com/learn/flash-loan/#h-how-do-flash-loans-work, 2022, January 11.

[30] H. Anwar. Blockchain and iot: The dynamic duo. https://101blockchains.com/blockchain-and-iot/, 2019, July 23.

[31] G. Anwar. State channels: An introduction to off-chain transactions. https://www.talentica.com/blogs/state-channels-an-introduction-to-off-chain-transactions/, 2020, June 19.

[32] Statistics YCharts. Bitcoin blockchain size. https://ycharts.com/indicators/bitcoin_blockchain_size, 2022, April.

[33] D. Geroni. Blockchain scalability problem - why is it difficult to scale blockchain. https://101blockchains.com/blockchain-scalability-challenges/, 2021, September 30.

[34] Binance Blog. Layer 1 blockchain tokens: Everything you need to know. https://www.binance.com/en/blog/fiat/layer-1-blockchain-tokens-everything-you-need-to-know-421499824684903155, 2021, December 13.

[35] L. Hoang. What is a 'layer 2 blockchain,' and what does it mean? https://bestarion.com/what-is-a-layer-2-blockchain-and-what-does-it-mean/, Dec. 29, 2021.

[36] A. Yakovenko. Solana: A new architecture for a high performance blockchain v0.8.13. *Solana Whitepaper*, pages 2–4, 2017, November.

[37] J. Ponciano. Solana's market value plunges $20 billion after outage—is this good for ethereum? https://www.forbes.com/sites/jonathanponciano/2021/09/17/solanas-market-value-plunges-20-billion-after-outage-is-this-good-for-ethereum/?sh=3d490b02e4e2, Sep. 17, 2021.

[38] DeFi Decrypted. What's the difference between the avalanche c-chain, x-chain, and p-chain? https://medium.com/@defidecrypted/whats-the-difference-between-the-avalanche-c-chain-x-chain-and-p-chain-9af28f6524d8, 2021, December 10.

[39] Polygon. Polygon litepaper. *polygon*, 2021, February.

[40] Polygon. Matic network becomes polygon, ethereum's internet of blockchains—expands mission and tech scope. https://blog.polygon.technology/matic-network-becomes-polygon-ethereums-internet-of-blockchains%E2%80%8A-%E2%80%8Aexpands-mission-and-tech-scope-364932c02cd0/, 2021, February 9.

[41] & Buchman E. Kwon J. Cosmos whitepaper - whitepaper.io. *Cosmos Whitepaper*, 2017, February 10.

[42] A. Hamacher. Cosmos founder jae kwon is stepping down. https://decrypt.co/17993/cosmos-founder-jae-kwon-is-stepping-down, 2020, January 29.

[43] Di Maggio M. & Platias N. Kereiakes E., Kwon D. Terra whitepaper, 2019, April.

[44] Narges Shadab, Farzin Houshmand, and Mohsen Lesani. Cross-chain transactions. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–9, 2020.

[45] Babu Pillai, Kamanashis Biswas, and Vallipuram Muthukkumarasamy. Cross-chain interoperability among blockchain-based systems using transactions. *The Knowledge Engineering Review*, 35:e23, 2020.

[46] H. Qureshi. Blockchains are cities. will we live in a multi-chain world, or…. https://medium.com/dragonfly-research/blockchains-are-cities-564327013f86, 2022, January 18.

[47] Peter Robinson, Raghavendra Ramesh, and Sandra Johnson. Atomic crosschain transactions for ethereum private sidechains. *Blockchain: Research and Applications*, 3(1):100030, 2022.

[48] Multichain Docs. How it works - multichain. https://docs.multichain.org/getting-started/how-it-works, 2020, July.

[49] Ronin Network. Community alert: Ronin validators compromised. https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=w, 2022, March 29.

[50] J. Lyanchev. Another defi hack: Thorchain compromised with up to $7.6m stolen. https://cryptopotato.com/another-defi-hack-thorchain-compromised-with-up-to-7-6m-stolen/, 2021, July 16.

[51] Nomad. The nomad design philosophy. https://blog.nomad.xyz/the-nomad-design-philosophy-6fc0eacf3263, 2022, February 7.

[52] D. Stone. Trustless, privacy-preserving blockchain bridges. https://arxiv.org/pdf/2102.04660.pdf, 2021.

[53] Li.Finance. Overview - li.fi documentation. *docs.li.fi*, 2022, April.

[54] BowTiedPickle. Li.fi protocol hacked for $600k. https://bowtiedisland.com/li-fi-protocol-hacked-for-600k/, 2022, March 21.

[55] XY Finance. Introduction - xy finance. *XY Finance*, 2022, April.

[56] O3 Swap. Litepaper v1 - o3 docs. https://docs.o3swap.com/o3-swap-litepaper, 2021, June 15.

[57] ChainSwap. Chainswap progress updates. https://chain-swap.medium.com/chainswap-progress-updates-e9fe960797c0, 2021, November 21.

[58] Chainswap. Liquidity bridge - chainswap. https://docs.chainswap.com/mechanism/liquidity-provision-bridge-solution, 2021, July.

[59] S. Vasudevan. Introducing bungee: Seamless cross-chain bridging. *Bungee-Exchange*, 2022, March 10.

[60] Socket. What is socket? https://docs.socket.tech/socket-overview/what-is-socket, 2022, April.

[61] G. Thomson. Wrapped bitcoin goes live on compound defi protocol - decrypt. https://decrypt.co/35357/wrapped-bitcoin-goes-live-on-compound-defi-protocol, 2020,Jul. 13.

[62] Simon Joseph Aquilina, Fran Casino, Mark Vella, Joshua Ellul, and Constantinos Patsakis. Etherclue: Digital investigation of attacks on ethereum smart contracts. *Blockchain: Research and Applications*, 2(4):8–10, 2021.

[63] Samczsun[@samczsun]. How did the @wormholecrypto exploit work? https://twitter.com/samczsun/status/1489044939732406275, 3 Feb 2022.

[64] Vitalik Buterin]. My argument for why the future will be *multi-chain*, but it will not be *cross-chain*: there are fundamental limits to the security of bridges that hop across multiple ”zones of sovereignty”. https://twitter.com/VitalikButerin/status/1479501366192132099, 7 Jan 2022.

[65] ZenLedger. 3 types of crypto taxes you'll pay in 2021. https://www.zenledger.io/blog/3-types-of-crypto-taxes, 2021, November 9.

[66] Ryan Watkins. We live in a multichain world. today there are 10 blockchains storing more than $10 billion in assets, as well as several ecosystems with meaningful development and activity. thorchain is vying to sit at the center of this world as infrastructure for cross-chain finance. https://twitter.com/RyanWatkins_/status/1404795233997557770, 15 June 2021.

[67] S. Cooling. Chainswap hackers steal $8m and crash token prices. https://finance.yahoo.com/news/chainswap-hackers-steal-8m-crash-121056965.html, 2021, July 12.

[68] Min.News. Poly network, a cross-chain protocol, was attacked, and o3 swap, which was on the altar, was looted. https://min.news/en/tech/4eebf1f343c816c1b7f3579dc1e799c7.html, 2021, August.

[69] Carlos Bellón and Isabel Figuerola-Ferretti. Bubbles in ethereum. *Finance Research Letters*, 46:102387, 2022.

APPENDICES

Appendix A

Current Affairs

A.1 The Crash of Terra Network

At the time of writing this subsection in May 2022, the cryptocurrency market is in a brutal state. Bitcoin has now been in the negative for nine weeks in a row, a cryptocurrency record, while Ether is at its lowest level since 2018. While the drop is distressing for crypto investors, it is not wholly uncommon. Cryptocurrencies are notorious for their volatility, and volatile economic conditions are pulling down not just crypto but also the stock market.

The collapse of the Luna cryptocurrency and its accompanying terraUSD stablecoin, dubbed UST, is unprecedented. UST had a significant story. Billions of dollars in cryptocurrency riches have vanished, sending shockwaves across the whole market. Some critics predicted a bubble blow up few months back

There are two connected tales here: the UST stablecoin's and Luna's, both of which are part of the Terra network. The UST coin is supposed to be worth $1 at all times, but it was depegged on May 9 and has subsequently dropped to 7 cents. Then there's Luna, Terra's ecosystem's focal point. Its value has plummeted in one of the most spectacular crypto collapses ever witnessed as seen in the chart A.1 [69]. All Luna pairs for trade were removed from TradingView as well as every centralized and decentralized exchange because of the hard fork two weeks later to LUNC (Luna Classic) and LUNA (Luna 2.0).

The value of the coin has dropped from $116 in April to a fraction of a penny at the time of writing. Such a crash has already occurred in small-cap memecoins, but never for a currency the scale of Luna, which had a market valuation of more than $40 billion only last month based.

Figure A.1: Luna/USD Price

As it was previously mentioned, you must burn Luna to make UST. In early May, for example, you could exchange one Luna token for 85 UST (because the Luna was valued $85), but the Luna would be destroyed "burned") in the process. This deflationary technique was designed to safeguard the long-term growth of the Luna. As more individuals invest in UST, more Luna will be burnt, increasing the value of the remaining Luna supply.

To attract traders to burn Luna to generate UST, the Anchor Protocol provided a ridiculous 19.5 percent yield on staking – which is effectively crypto terminology for earning 19.5 percent interest on a loan. Instead of putting your money in a bank for a 0.06 percent interest rate, the pitch is to put it in UST, where it may yield over 20 percent. Prior to the depegging, this scheme held over 70% of UST's circulating supply, or over $14 billion.

Do Kwon, the founder and CEO of Terraform Labs, established the Luna Foundation Guard, a coalition tasked with protecting the peg. The LFG had around $2.3 billion in bitcoin reserves, with intentions to increase this to $10 billion in bitcoin and other digital assets. If UST fell below $1, bitcoin reserves would be liquidated along with the money used to purchase UST. If UST rises over $1, creators will sell UST until it returns to $1, with the proceeds used to purchase additional bitcoin to replenish reserves. Everything makes sense. However, at the time of writing, UST is worth 7 cents.

It all began on Saturday, May 7. Over $2 billion of UST was unstaked (taken out of the Anchor Protocol), with hundreds of millions of dollars sold instantly. It's unclear if this was

a reaction to a tumultuous era – the rise in interest rates has had a particular impact on bitcoin values – or a more purposeful attack on Terra's infrastructure. Such massive sales drove the price down to 91 cents. Traders attempted arbitrage by swapping 90 cents worth of UST for $1 worth of Luna, but a speed bump emerged. Only $100 million of UST can be burnt every day for Luna.

Investors, already jittery in the current bear market, hurried to sell their UST after the stablecoin failed to maintain its peg. It fluctuated between 30 cents and 50 cents in the week following the first depeg, but has since dropped to a consistent low of less than 20 cents. Its market capitalization has dropped from over $18 billion in early May to $770 million currently.

It's much worse for Luna owners. The value of Luna tokens has nearly vanished: after peaking at just under $120 in April, the current price is less than a fiftieth of a penny. Users of the network were desperate in need of a centralized exchange or a cross chain solution to jump out to another network before Terra collapsed.

Appendix B

Definition and Figure Sources

B.1 Definitions

- Satoshis: The base unit of bitcoin is the satoshi.It is named after Satoshi Nakamoto, the creator(s) of the blockchain system and the bitcoin cryptocurrency. The satoshi to bitcoin ratio is one bitcoin for every 100 million satoshis.
- Bitcoin URI: The term URI stands for Unique Resource Identifier. It is a protocol used by your web browser to identify resources on your computer. It is usually in the form of a link (URL) that, when activated, executes the stated action.
- Savvy/smart money: These are the crypto world's top wallets. These wallets have a track record of making wise financial decisions and staying one step ahead of the competition.
- APR: The annual percentage rate (APR) is the interest earned by an amount charged to borrowers or paid to investors each year. APR is a number that shows the real yearly cost of money throughout the life of a loan or the revenue received on an investment. This includes any fees or other costs linked with the transaction but excludes compounding. The APR offers consumers with a single number that they may use to compare lenders, credit cards, and investment products.

B.2 Source of Figures

2.2 source: `https://paybis.com/blog/what-is-a-blockchain-nonce/`

2.3 source: https://developer.bitcoin.org/devguide/transactions.html

2.4 source: https://developer.bitcoin.org/devguide/transactions.html

2.5 source: https://developer.bitcoin.org/devguide/transactions.html

2.6 source: https://developer.bitcoin.org/devguide/transactions.html

2.7 source: https://developer.bitcoin.org/devguide/transactions.html

2.8 source: https://www.buybitcoinworldwide.com/volatility-index/

3.1 source: https://ethereumprice.org/gas/

3.2source: https://etherscan.io/chart/tx

6.1 source: https://www.footprint.network/@KikiSmith/Cross-Chain-Bridge-Dashboard

6.14 source: https://transferto.xyz/swap?fromChain=eth

6.15source: https://transferto.xyz/swap?fromChain=eth

6.16 source: https://docs.xy.finance/products/x-swap

6.17 source: https://docs.xy.finance/products/y-pool

6.18 source: https://app.xy.finance/

6.19 source: https://docs.o3swap.com/o3-swap-v1/o3-swap-litepaper

6.20 source: https://o3swap.com/hub

6.21 source: https://docs.o3swap.com/o3-interchange-v2

6.22 source: https://docs.o3swap.com/o3-interchange-v2

6.23 sourcehttps://exchange.chainswap.com/#/swap

6.24 source: https://docs.chainswap.com/mechanism/liquidity-provision-bridge-solution

6.25 source: https://chainswap.com/

6.26 source: https://www.bungee.exchange/

6.27 source: https://docs.socket.tech/socket-overview/how-socket-works

7.1 source: https://www.footprint.network/@KikiSmith/Cross-Chain-Bridge-Dashboard

7.3 source: https://studio.glassnode.com/workbench/455cdff8-202a-4b3a-741c-26a6e9fd1ba6

7.4 source: https://bit.ly/3aC4Ulc