FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Assignment of master's thesis

Title:	Analysis of blockchain bridge networks in decentralized finance
Student:	Bc. Martin Kupka
Supervisor:	Ing. Josef Gattermayer, Ph.D.
Study program:	Informatics
Branch / specialization:	Managerial Informatics
Department:	Department of Software Engineering
Validity:	until the end of summer semester 2022/2023

Instructions

It is possible to exchange tokens between individual blockchains through exchanges, but those are centralised and complicated. For this reason, "bridges" are being created, which are projects that aim to enable direct mirroring of transactions on two different blockchains. The technological solutions, business models, implementations, and functionalities of individual solutions differ. This thesis aims to analyse and document the current state of blockchain bridges.

Instructions:
- Study and analyse blockchain technology.
- Study and analyse the technologies used in DeFi.
- Along with the supervisor, select individual bridges that you will focus on in the thesis.
- Compare the selected bridges in terms of business model, technology, and functionalities.
- Evaluate the quality of the development team and the quality of the code.

Electronically approved by Ing. David Buchtela, Ph.D. on 29 October 2021 in Prague.

FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Master's thesis

Analysis of Blockchain Bridge Networks in Decentralized Finance

Bc. Martin Kupka

Department of Software Engineering
Supervisor: Ing. Josef Gattermayer, Ph.D.

May 4, 2022

Acknowledgements

First and foremost, I want to thank my supervisor, Ing. Josef Gattermayer, Ph.D. for the time he dedicated to answering my questions and providing helpful guidance. I would also like to thank my family, friends, and classmates who have supported me during my studies.

Declaration

I hereby declare that the presented thesis is my own work and that I have cited all sources of information in accordance with the Guideline for adhering to ethical principles when elaborating an academic final thesis.

I acknowledge that my thesis is subject to the rights and obligations stipulated by the Act No. 121/2000 Coll., the Copyright Act, as amended. In accordance with Article 46 (6) of the Act, I hereby grant a nonexclusive authorization (license) to utilize this thesis, including any and all computer programs incorporated therein or attached thereto and all corresponding documentation (hereinafter collectively referred to as the "Work"), to any and all persons that wish to utilize the Work. Such persons are entitled to use the Work in any way (including for-profit purposes) that does not detract from its value. This authorization is not limited in terms of time, location and quantity. However, all persons that makes use of the above license shall be obliged to grant a license at least in the same scope as defined above with respect to each and every work that is created (wholly or in part) based on the Work, by modifying the Work, by combining the Work with another work, by including the Work in a collection of works or by adapting the Work (including translation), and at the same time make available the source code of such work at least in a way and scope that are comparable to the way and scope in which the source code of the Work is made available.

In Prague on May 4, 2022 . . . . . .

Czech Technical University in Prague
Faculty of Information Technology

Citation of this thesis

Kupka, Martin. *Analysis of Blockchain Bridge Networks in Decentralized Finance*. Master's thesis. Czech Technical University in Prague, Faculty of Information Technology, 2022.

Abstract

This thesis introduces the core concepts of blockchain, decentralized finance, and cross-chain interoperability. The crucial properties of blockchain technology and the scalability trilemma is explained. The main applications of decentralized finance technology and how they differ from traditional solutions are highlighted. The importance of cross-chain bridges is explained, and the different models and properties of cross-chain bridges are discussed. A framework for comparing and evaluating bridges is presented, and Axelar, IBC and LayerZero are compared.

Keywords blockchain, cryptocurrencies, crypto, decentralized finance, DeFi, bridges, cross-chain, interoperability

Abstrakt

Tato práce představuje základní koncepty technologie blockchainu, decentralizovaných financí a interoperability mezi blockchainy. Vysvětluje klíčové vlastnosti blockchainu a trilema jeho škálovatelnosti. Dále zdůrazňuje hlavní možnosti využití decentralizovaných financí a jak se liší od tradičních řešení. Je vysvětlena důležitost cross-chain bridgů a diskutovány různé modely a vlastnosti těchto bridgů. Vytváří rámec pro porovnávání a hodnocení bridgů a aplikuje jej na tři vybrané bridge - Axelar, IBC a LayerZero.

Klíčová slova blockchain, kryptoměny, krypto, decentralizované finance, DeFi, interoperabilita

Contents

List of Figures

List of Tables

Introduction

Over the past few years, cryptocurrencies have become too big to ignore. The total marketcap has grown from less than 100 million dollars in 2017 to over 1.5 trillion [1]. Major institutions [2], well known investors [3] and even nation states [4] have recognized the immense potential cryptocurrencies bring. Cryptocurrencies have also moved from being used as a speculative asset class to becoming stores of value, or programmable money [5], allowing users to earn yield or lend against their assets. With the increasing popularity of Bitcoin and Ethereum, many new cryptocurrencies were created, trying to offer better speed, lower transaction fees, or new use cases [1]. This has led many to believe a muli-chain future is coming [6].

The goals of this thesis are to study and analyze blockchain technology, decentralized finance, cross-chain bridges, and create a framework based on the knowledge obtained and compare and evaluate the selected bridges.

In the first chapter, readers are introduced to the blockchain technology itself. What a blockchain is and how it differs from traditional databases is explained. The various properties of a blockchain are presented, what a typical blockchain structure looks like is described, and the blockchain scalability trilemma is discussed. A brief history of Bitcoin and altcoins is mentioned, and some crucial concepts are described – smart contracts, oracles, and layer 1 and layer 2 blockchains.

The second chapter describes decentralized finance. The main applications are listed and described. The importance of stablecoins in decentralized finance is mentioned, along with a description of how lending, borrowing, and decentralized exchanges work. Finally, the advantages, risks, and challenges of interacting with decentralized finance protocols are discussed.

In the third chapter, the concept of cross-chain bridges and why they are becoming increasingly important is explained. The interoperability trilemma is presented and the different verticals on how bridges can be classified are introduced. The open issues, risks, and the future of blockchain bridges is mentioned. At the end of the chapter, two of the most notable cross-chain

protocol hacks are discussed.

I have been interested in cryptocurrencies for the past two years, and the speed at which the whole space progresses and evolves is breathtaking. There is an abundance of information available online, but it is fragmented and sometimes hard to find. This thesis should give the reader a high-level overview of the essential concepts in blockchain and decentralized finance and explain why the existence of reliable cross-chain bridges is crucial and what are the benefits and drawdowns of current leading solutions.

Chapter 1

Blockchain Technology

This chapter explains the basics of blockchain technology. It introduces the main properties of blockchain, its structure, the blockchain scalability trilemma, and a brief history of Bitcoin and altcoins. Afterward, it explains smart contracts and why blockchains need oracles to access real-world data. In the end of this chapter, the differences between layer 1 and layer 2 blockchains is explained.

1.1 What is a Blockchain?

A blockchain is a distributed database shared among the nodes of a computer network [7]. The main advantage over classical databases is the fact that the fidelity of the data records is provable and verifiable without the need for a trusted third party. Any data can be stored using a blockchain, but the most common use has been a distributed ledger for transactions. New transactions are transmitted to the network, clustered into a block that is then appended to all the previous blocks. All of the blocks are chained together using cryptographic hashes of the previous block – each new block contains information about all the previous blocks. A simplified view of a distributed ledger is shown in Figure 1.1, and Figure 1.2 represents how are the blocks chained together.

1.1.1 Blockchain Properties

Three main properties make blockchains unique and separate them from classical databases.

- **Immutability** – Once a block is appended to the chain, it is impossible to edit or roll back the transaction inside.
- **Transparency** – All transactions are public and can be viewed by anyone.

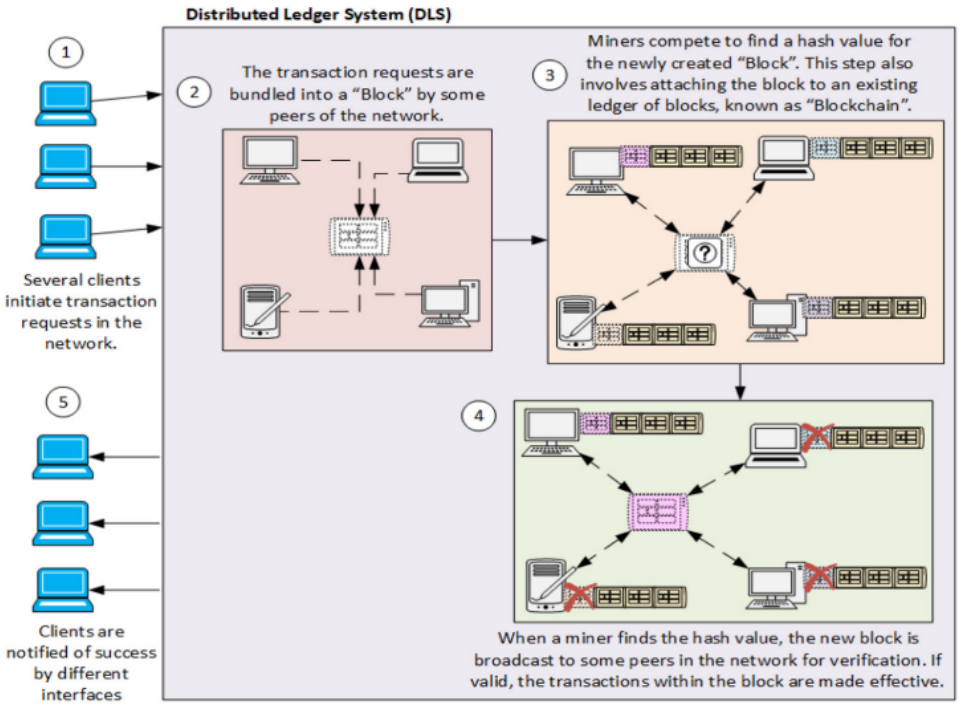

Figure 1.1: Distributed Ledger System [10]

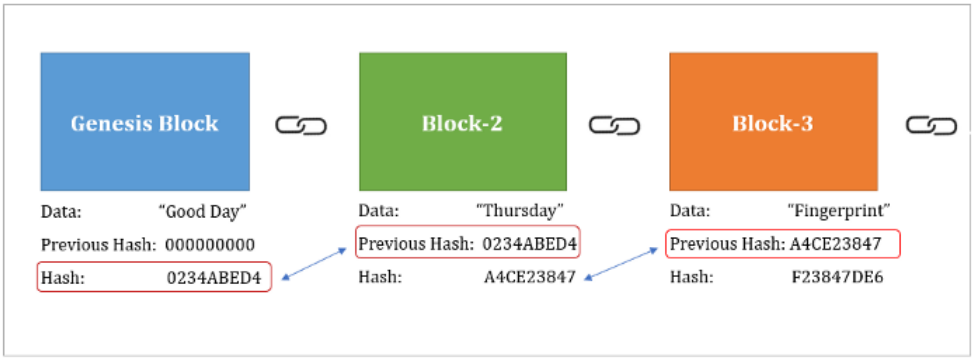

Figure 1.2: Blocks in a Blockchain [11]

- **Security** – Thanks to the decentralization of the network, there is no trusted entity responsible for running the blockchain. It allows any two parties to transact without the need for a middle man or a trusted third party.

These properties make blockchain perfect for cryptocurrencies – digital money designed to be used over the internet [12]. Yet blockchain use case is not limited to just money. It can store medical records, votes in elections, or track goods along the supply chain and prove their authenticity.

1.1.2 Blockchain Structure

Most blockchains consist of several layers [13]:

- **Infrastructure/Hardware** – The hardware on which the peer-to-peer network is run. Different blockchains have vastly different requirements for the hardware required to participate in the network.

- **Network** – The network of nodes, miners, or validators that discover new nodes, relay information (transactions) and verify them.

- **Consensus** – There are different ways that blockchains networks reach a consensus – determining which transactions are legit and which will be included in the next block. They are designed in such a way to make attacks on the network unfeasible - mainly the 51% percent attack. If an attacker were to gain control of at least 51% of the nodes in the blockchain network, he could control the consensus and insert invalid transactions for his own benefit. The main goal of a consensus mechanism is to incentivize all actors to act honestly, because it is more profitable for them to do so. Many different consensus mechanisms exist, the most popular being proof of work (used by Bitcoin) and proof of stake (a newer, more energy-efficient way of reaching consensus).

  Proof of Work is a cryptographical way to prove that a certain amount of specific computational effort was performed. The downside of this approach is that it is very resource (energy) intensive. The participants who actively participate in the computational effort are called miners and get rewarded if they successfully mine a block [8].

  Proof of Stake is an alternative consensus mechanism – validators are selected in to validate (mine) a block in proportion to how much cryptocurrency they have staked. A delegated proof of stake systems are also common, where the role of stakers and validators is separated – stakers can choose to which validator they want to delegate their coins. Once again, successful validators are rewarded for mining new blocks [9] .

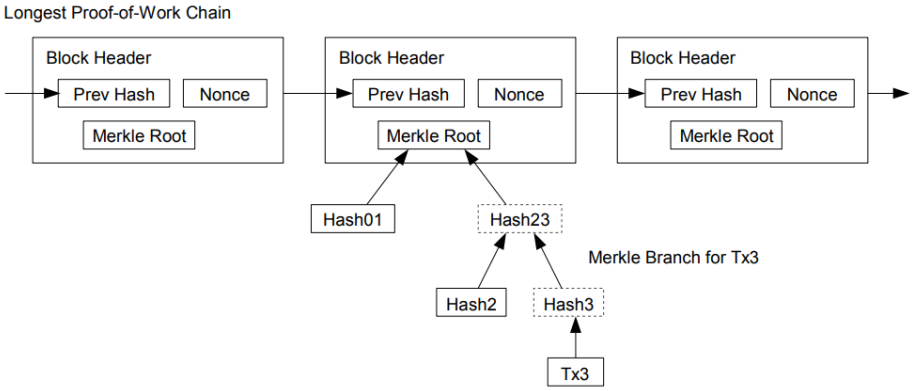

Figure 1.3: Blockchain Structure [8]

More consensus algorithms exist - proof of history, proof of authority, proof of burn, proof of reputation, and many others [27], with each of them having a distinct set of benefits and drawdowns.

- **Data** – The blocks of transactions chained together. The blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree [14]. Each block also includes a cryptographic hash of the previous block – the link between block that creates a chain. The blocks are linked all the way back to the genesis (inception) block. An illustration of such a structure is shown in Figure 1.3.
- **Decentralized Applications (dApps)** – Blockchains can have decentralized applications running on top of them.

1.1.3 The Blockchain Scalability Trilemma

The term scalability (or blockchain) trilemma was coined by Vitalik Buterin, the creator of the second-largest cryptocurrency by market cap, Ethereum [31]. It states that blockchains strive be decentralized, scalable, and secure, but can only achieve two out of these three properties. The scalability trilemma is represented in Figure 1.4.

- **Scalability** – The number of transactions the chain can process can scale along with the traffic on the chain.
- **Decentralization** – The chain can run without a trust dependency on a small group of large centralized actors. The barrier to running a node in the network should be low.
- **Security** – The chain can resist a large percentage of nodes trying to attack it, ideally at least 50%.

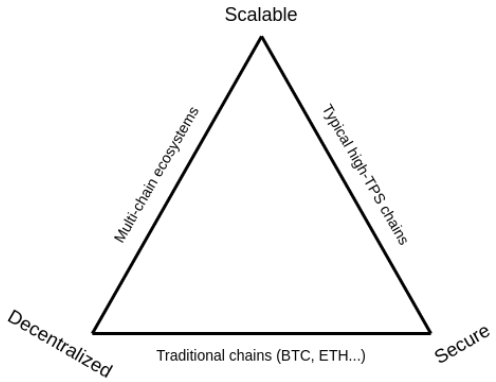

Figure 1.4: The Scalability Trillema [31]

Figure 1.5: Bitcoin's Marketcap [1]

1.2 Bitcoin

Blockchain technology was first outlined in a 1991 paper by Start Haber, and W. Scot Stornetta called How to Time-Stamp a Digital Document [16]. Bitcoin became the first real-world implementation of blockchain almost two decades later, in 2009. The original Bitcoin whitepaper was published a year earlier by Satoshi Nakamoto, a pseudonym for a person or a group of people – the real identity is unknown to this date and has been subject to many speculations.

Since its inception, Bitcoin's market cap grew to over $700 billion. Its exponential growth can best be seen in a logarithmic chart in Figure 1.5.

1.3 Altcoins

As Bitcoin's popularity rose, more cryptocurrencies were created. Currently, there are almost 19 000 cryptocurrencies [22], the growth is shown in Figure

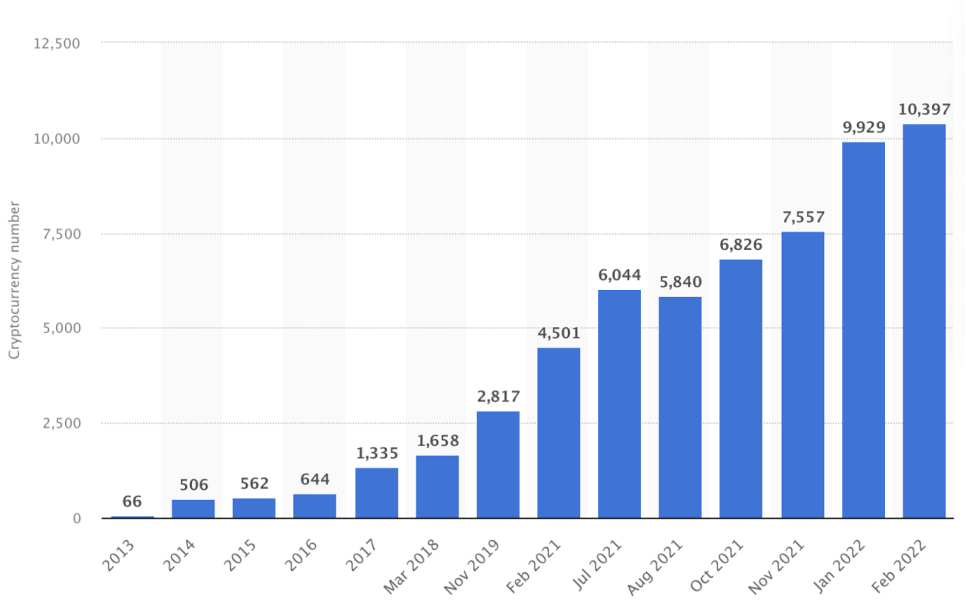

Figure 1.6: Total Number of Existing Cryptocurrencies [26]

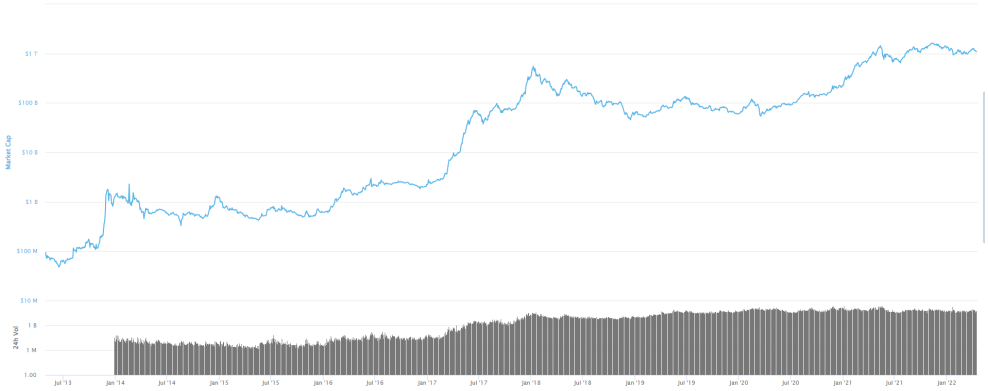

Figure 1.7: Total Cryptocurrency Marketcap Excluding Bitcoin [1]

1.6. The first altcoins were just forks of Bitcoin with some parameters changed, affecting the transactions fees, speed, and security of the network [15]. Some of the cryptocurrencies in this category are Bitcoin Cash, Bitcoin Satoshi Vision, and Litecoin. All of them have underperformed Bitcoin significantly.

Ethereum was the first cryptocurrency that propagated the idea of "programmable money" using smart contracts, instead of being just a currency [5]. With the rise of its popularity, many additional Layer 1 blockchains with various specifications and use cases were created.

The rising popularity of altcoins and the diminishing dominance of Bitcoin can be seen in Figures 1.7 and 1.8

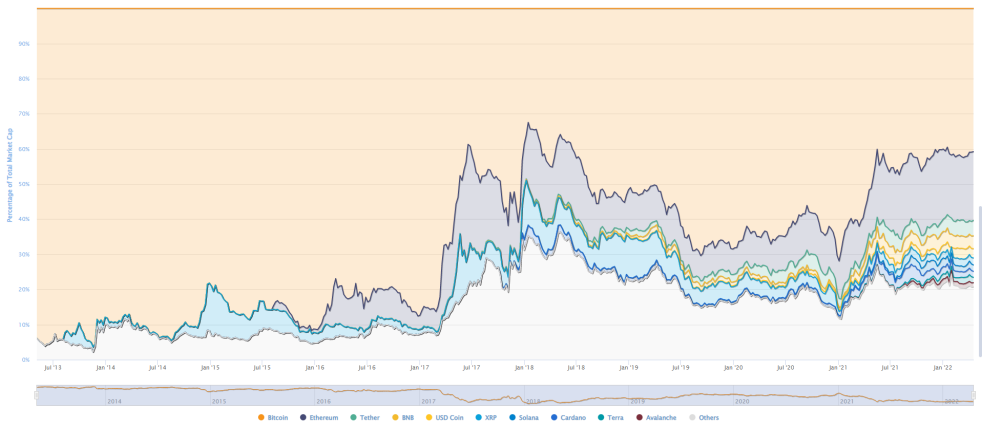

Figure 1.8: Major Cryptoassets By Percentage of Total Market Capitalization [1]

1.4 Smart Contracts (SCs)

Smart contracts are executable programs stored on the blockchain that get executed when predetermined conditions are met [17]. Because they are on-chain, they are immutable and distributed. Their main proposition is that they are executed and enforced without the need for human interaction or a trusted third party. They are also a part of the public blockchain record, so anyone can verify that they are programmed to do what they are supposed to before they choose to interact with the smart contract. Another benefit of smart contracts is their composability – they can work like lego blocks, other people can build on top of already deployed SCs.

One of the commonly used analogies for smart contracts is the vending machine analogy. A vending machine works similarly to a smart contract – specific inputs guarantee predefined outputs. The user chooses which product he wants go get and inserts the required amount of money. The machine verifies that the requirements for obtaining the products were met and dispenses the product along with any excess cash paid. If the requirement were not met, the vending machine returns the money and keeps the product [17].

1.5 Oracles

One of the main limitations of smart contracts (and blockchains in general) is the fact that they cannot, by design, get access to any "off-chain" data, such as asset price feeds or outcomes of certain real-world events. This decision for blockchains to be siloed from outside information is made deliberately because being open to off-chain data could jeopardize the consensus mechanism [20].

Oracles are the link that connect smart-contract enabled blockchains to off-chain data. They act as on-chain APIs that can be queried to get information inside smart contracts. Common use cases include price-feeds of different

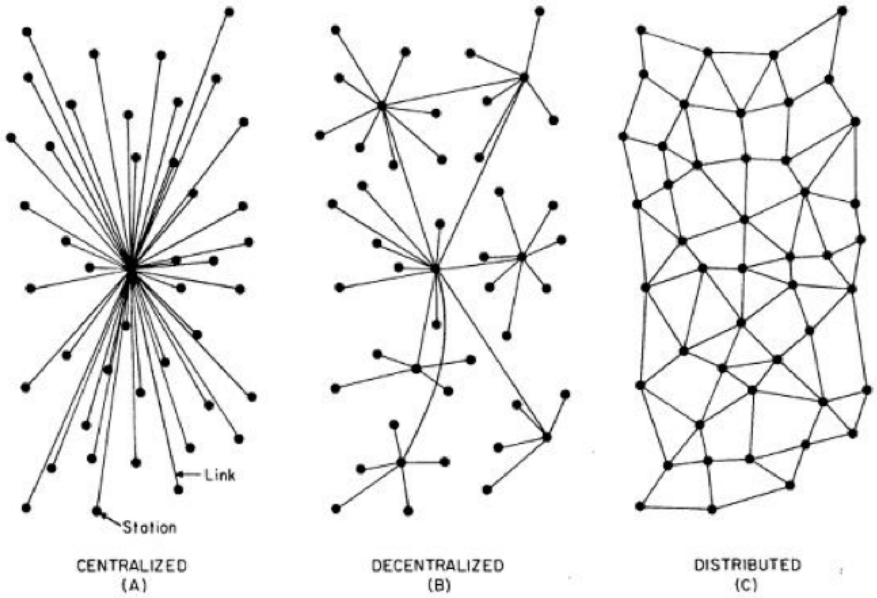

Figure 1.9: Different Types of Software Applications [18]

assets, random number generation, or the outcome of real-world events (sports matches, election results).

1.6 Decentralized Applications

The three different architecture models of software applications are shown in Figure 1.9. Currently, centralized systems are the most widespread. Distributed systems spread the computation across multiple nodes instead of just one to speed it up. However, the whole distributed system can still be controlled by one central node – meaning that systems can be centralized and distributed simultaneously. Decentralized applications (dApps) have no node instructing the other nodes about what to do [18]. They also leverage the decentralization and immutability of the underlying blockchain to function. The main benefits of dApps are that they are open source, censorship free and have no single point of failure [19].

1.7 Layer 1 and Layer 2

Layer 1 network is another name for a base blockchain such as Bitcoin or Ethereum. They are referred to as layer 1 because they are the main networks within their ecosystem. A common problem with the layer 1 networks is their inability to scale and process transactions in times of increased demand. This is why layer 2 solutions were created [21].

Layer 2 protocols are blockchains built on top of a Layer 1 that leverage the underlying chain's security and consensus. Their goal is to offer faster transaction times and lower fees while not sacrificing the security of the main chain. An example of a layer 2 built on top of Bitcoin is the Lightning network that enables near-instantaneous transactions at a fraction of Bitcoin's blockchain fee. Similarly, the Polygon network is a layer 2 solution for Ethereum [21].

Chapter 2

Decentralised Finance

In this chapter, the term Decentralized Finance is introduced. Its main use cases – stablecoins, lending, borrowing, and decentralized exchanges are discussed. Then the advantages and risks of interacting with decentralized finance protocols compared with traditional finance.

2.1 Decentralized Finance

Decentralized Finance (DeFi) is a broad term for an ecosystem of financial applications that are developed on top of blockchain networks. It also refers to a movement that aims to create open-source, permissionless, and transparent financial services that are open for anyone to use and that operate without any central authority. This ecosystem is enabled by blockchains, smart contracts, and decentralized applications.

DeFi saw a massive rise in total value locked (TVL) of assets inside various DeFi smart contracts since 2020 – from less then a billion dollars to over $200 billion [39]. This growth is illustrated in Figure 2.1.

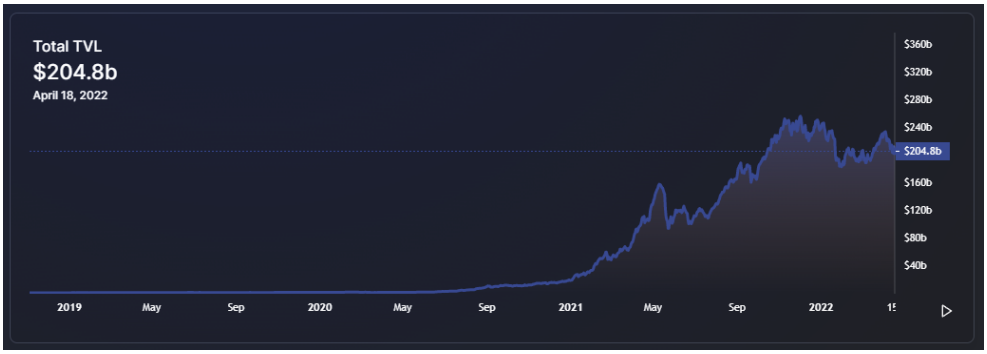

Figure 2.1: Total Value Locked in DeFi [39]

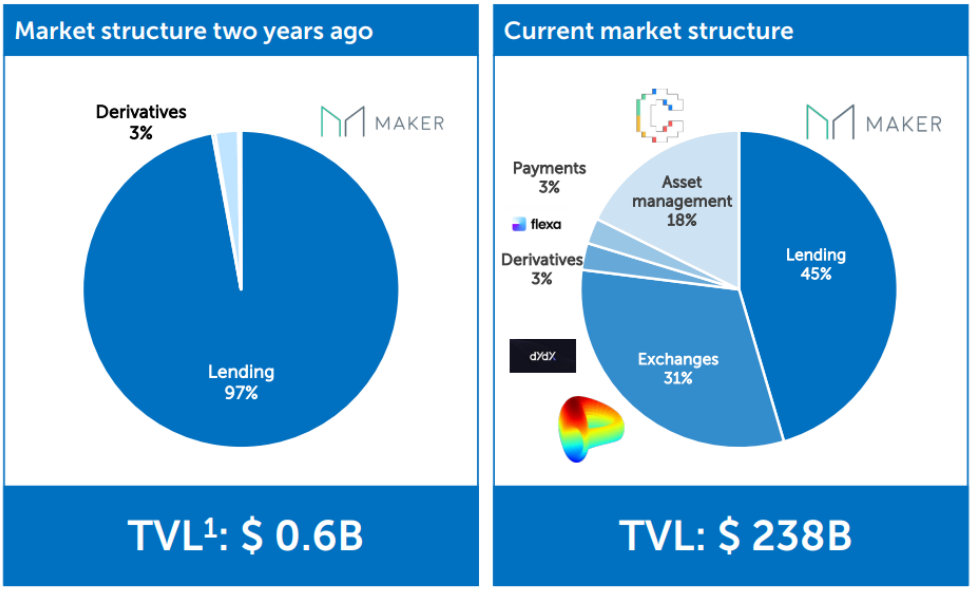

Figure 2.2: DeFi Market Structure [40]

2.2 Main DeFi applications

DeFi is still in its infancy, and the landscape has changed significantly since 2020, as illustrated in Figure 2.2. In this section, the main use cases are discussed.

2.2.1 Stablecoins

One of the crucial reasons for DeFi's success are stablecoins – coins designed to maintain a stable market price. Most commonly, these are pegged to the US dollar but can be pegged to any currency, asset, or commodity. There are various mechanisms for maintaining the 1:1 price peg, from being collateralized by actual USD and other assets (USDC stablecoin), to maintaining the peg via an arbitrage opportunity (UST stablecoin). Stablecoins allow users to hedge against the volatility of the cryptocurrency market and are often used for taking out loans against provided collateral.

2.2.2 Lending and Borrowing

The very first popular DeFi use case was lending and borrowing of assets. Using protocols such as Aave or Compound, users can lend their assets for interest or rewards in tokens issued by the protocol. The other option is to borrow against held assets, either to be able to gain leverage or to get fiat money without incurring tax gains from selling the underlying cryptocurrency.

The loans can be taken instantaneously and because most DeFi protocols use over-collateralization, so no credit checks are required.

2.2.3 Decentralized Exchanges

Decentralized exchanges (DEX) can be split into two types:

- **Order Book Exchanges** – These work similar to classical centralized exchanges – users are able to put limit orders into the orderbook or execute market orders. However, this means that every order, alteration or cancelation has to be recorded on chain. This makes it expensive, because a transaction fee has to be paid for every interaction with the exchange. However, on chains with high transaction-per-second (TPS) and low transaction fees, like Solana, this model works and the user experience is comparable to using a centralized exchange.
- **Automated Market Makers (AMM)** – The primary decentralized exchange model - they allow for on-chain trading without the need for an order book or a direct counterparty to execute the trades. Instead of trading peer-to-perr, AMMs allow users to trade peer-to-contract [24].

  Users can lock a pair of assets into a liquidity pool to create a market. For doing so, they are rewarded with trading fees collected by the the pool proportional do their share of the total pool liquidity. The largest DEX on Ethereum called Uniswap charges users 0.3% fee that is split directly between the liquidity providers (LPs).

  A diagram of a an AMM trade is shown in Figure 2.4. An algorithm prices the assets in the pool – the simplest one being $x * y = k$, where x is the amount of one token in the pool, y is the amount of the second token and k is a fixed constant, the total value of assets in the pool. This equation is visualised in Figure 2.3 Different protocols use different variations of the formula.

  One of the main advantages of AMMs over order book exchanges is the fact that it allows seamless liquid trading even for the long-tail assets without the need to pay expensive market-making fees.

2.2.4 Other Usecases

- **Derivatives** – Various derivatives platforms like dYDx, Synthetix, or Mirror allow users to trade synthetic assets that mimic the price of traditional assets such as stocks or commodities, various indexes, or more advanced instruments like options.
- **Decentralized Insurance** – Users can get insured in case of a hack due to a smart contract vulnerability.

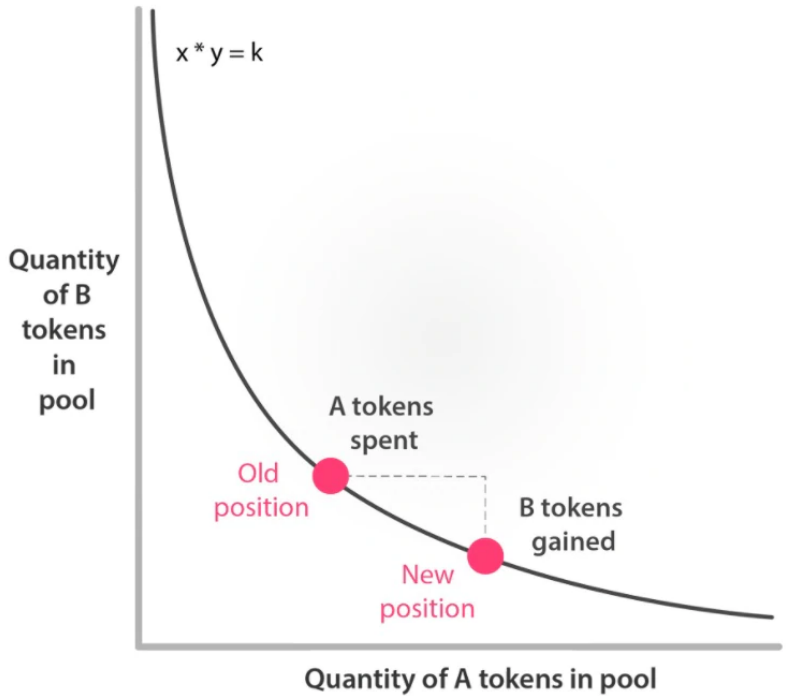

Figure 2.3: AMM Formula Visualized [41]

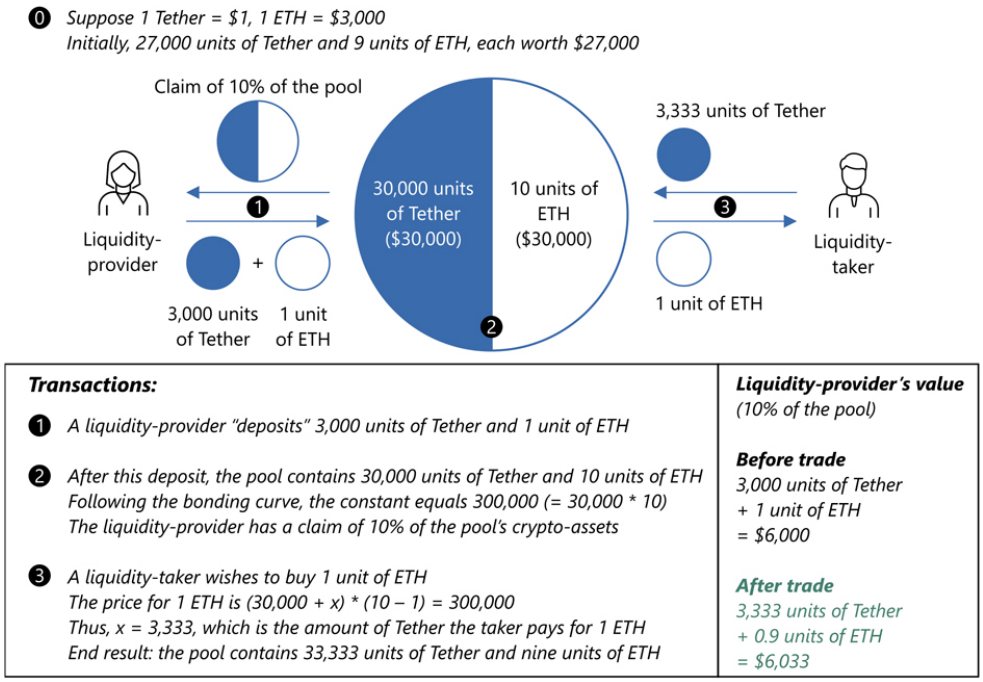

Figure 2.4: AMM Trade Explained [25]

- **Yield Farming** – Yield farming is a term used for various strategies created to maximize yield on users' assets. It often includes providing liquidity into new protocols that offer high rewards and a high risk of security vulnerabilities or providing liquidity for exotic, extremely volatile pairs. Another common strategy is lending against an asset, buying more of said asset, and lending against it again, effectively leveraging the user's capital. However, if the price of the assets drops, the user can get liquidated and lose all their collateralized assets.

2.3 DeFi Advantages

DeFi has many advantages when compared to traditional finance (TradFi) [42, 43, 45]:

- **Trustlessness** – TradFi relies heavily on institutions to act as intermediaries and courts for arbitration. DeFi removes the need for both intermediaries and arbitrators – everything is immutably defined in the smart contract. The need to trust a third party is removed. Users maintain the control of their assets, and every possible outcome has a defined solution.

- **Security** – Because DeFi is deployed on top of a blockchain, a single point of failure is eliminated (as long as we assume the smart contracts themselves do not contain any vulnerabilities). The data is immutable and censorship-resistant.

- **Transparency** – Because all the transaction data is available on-chain, everything can be verified immediately and it is not possible to fake transactions.

- **Permissionless** – Anyone with internet access can interact with the available protocols.

- **Composability** – Developers can utilize existing dApps and start building on top of them, opening up new use-cases.

- **Availability** – DeFi is available to use 24/7.

- **Speed** – DeFi allows transactions to execute immediately instead of taking hours or days.

- **Cost** – No need for a trusted third party to transact reduces the costs of providing and using the financial products, resulting in better conditions for both users and developers.

- **Yield** – One of the main benefits that attract users to DeFi is the attractive yields. It is possible to achieve a double-digit annual percentage yield (APR) on stablecoins – Anchor protocol gives 19.5% APR on the UST stablecoin with almost $20 billion of TVL [49].

2.4 DeFi Risks and Challenges

There are plenty of areas where DeFi interacting with DeFi comes with risk or uncertainity [42, 45]:

- **Regulatory Unclarity** – Currently, DeFi protocols operate with almost no government oversight or regulations. It is impossible to predict when the regulation will come and what it will bring when it is created [48].

- **Governance Risk** – Decentralized governance proposals control the behavior of many DeFi protocols and can often alter essential parameters, such as the loan-to-value (LTV) ratio – the minimal value of collateralized assets required for the user not to get liquidated. If this ratio changes without the user's knowledge, they can be unwillingly exposed to more risk.

  Smaller or lesser-known protocols can be more prone to governance attacks if a small number of parties hold enough voting power to influence the proposal's outcome [46].

- **Smart Contract risk** – Common characteristic of DeFi is that the code is open-sourced. This transparentness allows anyone to check and verify that the smart contracts are bug-free and that the protocol works as intended. In theory, this also means that bugs or vulnerabilities can be discovered and fixed quickly. However, this also allows malicious actors to search for protocols with vulnerabilities and try to exploit them. Because most users do not have the skills or time required to check all smart contracts before interacting with them, security audits are often performed to give protocols credibility [47].

- **Exogenous Protocol Risk** – DeFi users are also exposed to the risks outside of the protocol they are interacting with. DeFi protocols use oracles to get price feeds of different assets. If the oracle gets attacked or manipulated, user's positions can be liquidated, even if the actual asset's price never reached the liquidation threshold.

  If a successful attack on the underlying blockchain happens, the DeFi protocols functions may halt. Finally, DeFi users are often exposed to the extreme volatility of cryptocurrencies. Even if they choose only to

use stablecoins, there is the risk of de-pegging – losing the 1:1 peg to USD (or some other fiat currency). [48].

- **Scams** – Due to the anonymity and immutability of DeFi, some protocols are created solely for the purpose of stealing users' assets. The "rug pull" is when a protocol purposely has a backdoor implemented, allowing the creators to withdraw all locked assets. Another common trick is the "pump-and-dump" scheme – the creators hold a large supply of the token and then use influencers or celebrities to attract new investors to the project. Then they immediately sell all of their token holdings, dumping the price and securing a profit.
- **Bad User Experience** – Currently, the DeFi space is very fragmented. The number of different ecosystems, cryptocurrencies, and protocols can be overwhelming for a newcomer. Some protocols miss sufficient documentation or tutorials on using them. At the same time, if a user makes an error, it might lead to a complete loss of funds.

The explosive rise of DeFi since 2020 has challenged a lot of the status quo in traditional finance. Many innovative ideas were conceived in such a short period of time, and there are many challenges the DeFi space needs to overcome to continue its growth in user adoption.

Chapter 3

Bridges

This chapter describes what blockchain bridges are, where the need for them comes from, and what benefits they bring. The interoperability trilemma is explained, and the different ways to classify the bridges are demonstrated. Open issues, the future, and the risks of using bridges are discussed. Finally, the most notable bridge hacks are described.

3.1 What Is a Bridge?

A blockchain bridge is an application that transfers information between two or more blockchains. Most commonly, the information mentioned refers to assets. However, it can also refer to smart contract calls, proofs, or the state of the chain [28]. Blockchains are passive in communication by nature, but cross-chain communication must be active. There are trust boundaries between chains, as we can see in Figure 3.1. Blockchain bridges are the needed outside actor between the source chain and the destination chain that monitors, verifies, and relays the message. The schema, including the off-chain actor(s), is visible in Figure 3.2.

The bridge acts as the man-in-the-middle, facilitating the transition from passive one-way communication to two-way active back and forth communication. Most complex problem that bridges need to solve is that the verification of message they are relaying is valid and not forged. We can classify blockchain bridges into multiple categories based on how they tackle this problem.

Most bridges have the following structure [28]:

- **Monitoring** – An actor (oracle, validator, or relayer) monitors the source chain state.
- **Message Parsing and Relaying** – After a message or event from the source chain gets picked up by the monitoring actor, it must be parsed and relayed to the destination chain.

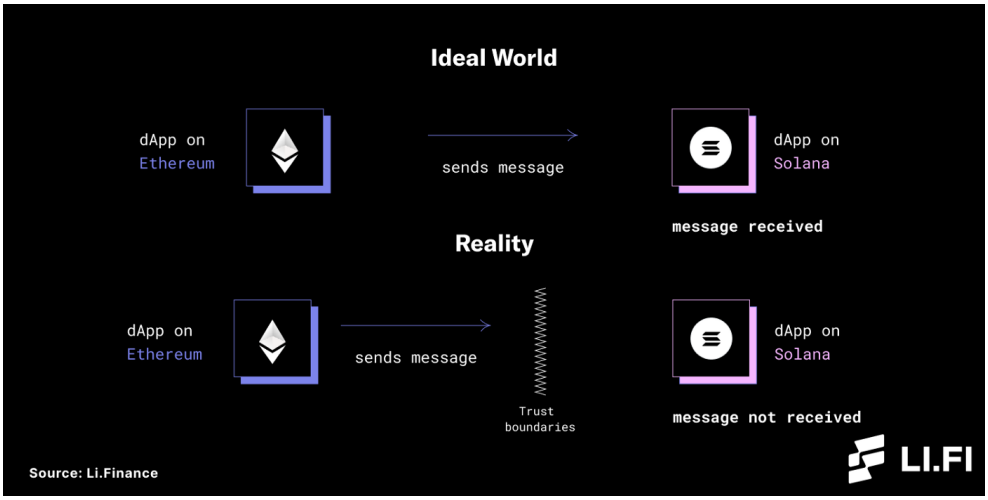

Figure 3.1: Visualisation of Trust Boundaries [30]

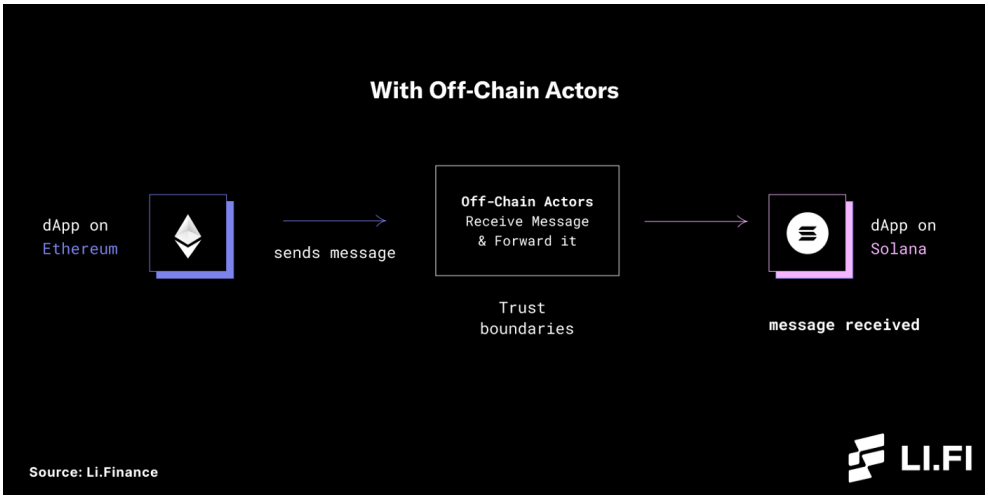

Figure 3.2: Role of off-chain actors visualised [30]

- **Consensus** – If multiple actors monitor the source chain, they first need to reach a consensus before the message is relayed to the destination chain.

- **Signing** – If the message has been received, parsed, and verified, the actor(s) need to cryptographically sign the information sent to the destination chain.

An example of the entire bridging process is shown in Figure 3.3.

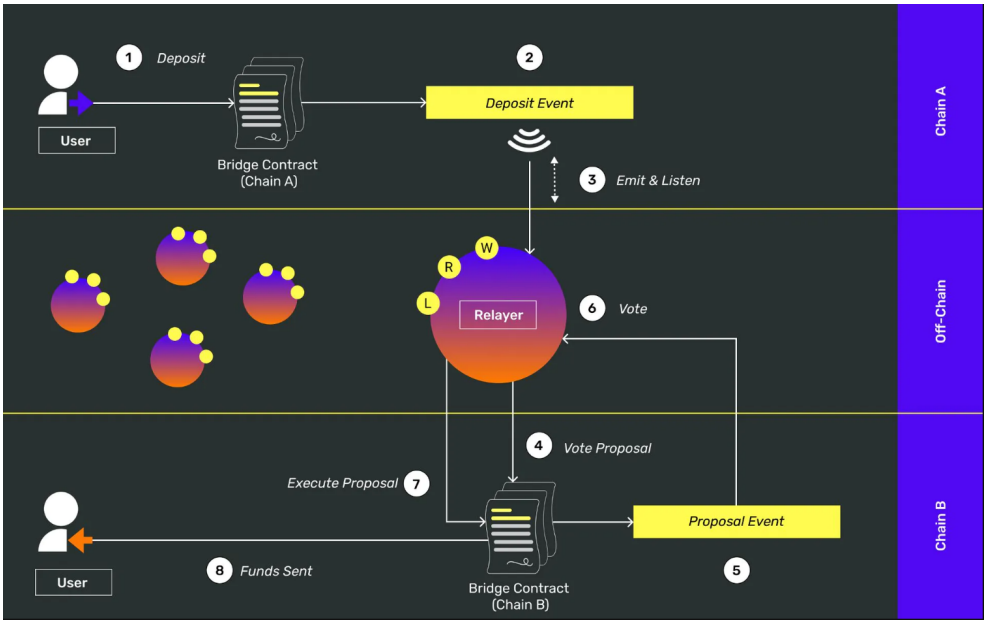

Figure 3.3: The Bridging Process [55]

3.2 Why Do We Need Bridges?

Currently, there are over 100 active public blockchains [23]. Out of the top 100 biggest cryptocurrencies by market cap, around 45 of them are independent blockchains [1]. We can imagine different blockchains like cities [29] – but they are isolated. Also, like cities, they are not infinitely scalable without trade-offs. As the number of decentralized applications and their users grows, it becomes crucial to be able to represent assets across multiple chains while also decreasing the friction of doing so. In the same way cities need roads to stay connected, blockchains need bridges to be able to communicate.

Blockchains, by nature, cannot communicate with each other. They are not aware of what is going on off-chain. That is where bridges come in – at the very basic layer, they are applications that transfer information between two or more blockchains. As of September 2021, there were over 40 different bridge projects [28], so the demand for bridges is apparent.

3.3 The Benefits of Bridges

The main advantage of bridges is that they allow interoperability between different chains, which benefits both the users and the whole crypto ecosystem. The benefits include:

- **Discovery** – Enabling users to access new platforms, protocols, and dApps.

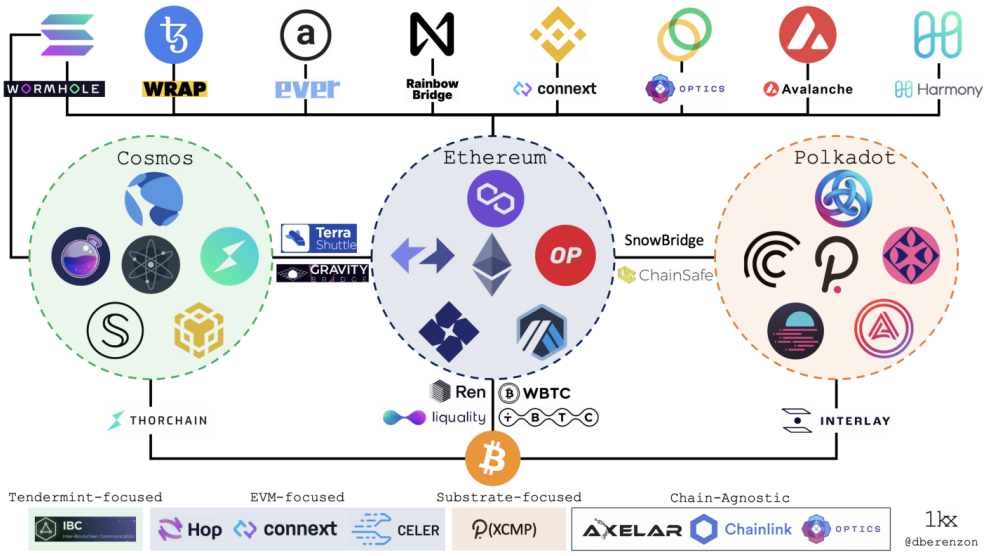

Figure 3.4: Some of the Existing Bridges Visualised [28]

- **Collateral** – Use of assets as a collateral cross-chain (using Bitcoin to take out a loan on Aave, which is built on Ethereum).
- **Scalability** – Bridges help blockchains facing heavy loads scale better by redirecting part of the traffic of the main chain (Polygon as a Layer 2 for Ethereum)
- **Decentralization** – Allows users to move ecosystems without selling their assets to fiat or interacting with a centralized entity (centralized exchange like Binance, FTX, or Coinbase).
- **More Opportunities** – Cross-chain arbitrage becomes possible. Cross-chain order books for DEXes and NFT marketplaces can be created to enable bidding from different chains.
- **Innovation** – Developers can use each chain's unique features to develop dApps without worrying about onboarding users.

3.4 The Interoperability Trilemma

Equivalent to how blockchains try to solve the scalability trilemma [31], there exists the interoperability trilemma for bridges as shown in Figure 3.5.

The trilemma states that bridges can only achieve two out of the three properties without compromising on the third [32].

- **Trustlessness** – Is the bridge as secure as the underlying chains? Is there a third party that needs to be trusted?

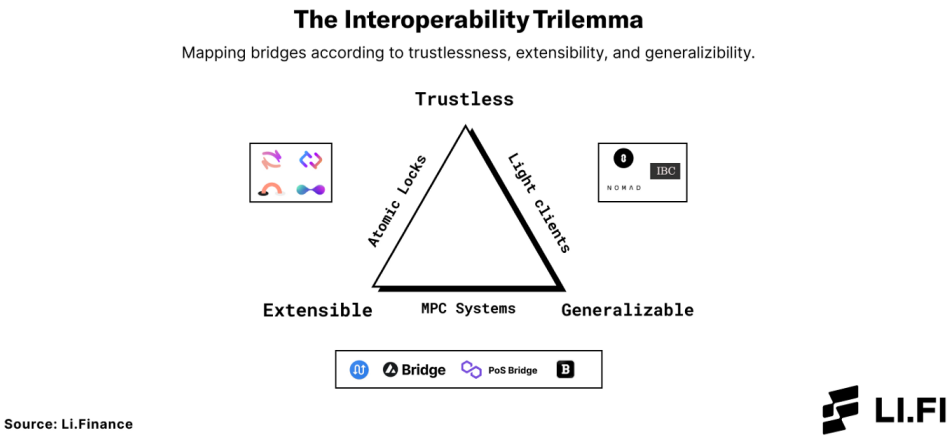

Figure 3.5: The Interoperability Trilemma [30]

- **Extensibility** – Can it support any chain? How difficult will be the integration?

- **Generalizeability** – Is it capable of handling arbitrary cross-chain data, not just asset swap/transfer?

3.5 Bridge Classification

We can classify bridges based on how they approach the interoperability trilemma or how they validate the cross-chain transactions [28, 30, 33].

3.5.1 Trustlessness

An illustration of bridges classified by how trustless they are is shown in Figure 3.6.

- **Trusted Bridges** – The bridge depends on a central entity that users need to trust. It is moving away from the security of the underlying chains toward trust assumptions for the external verifiers. The actors do not need to post collateral, and there is no way for users to recover funds in case of bridge failure or hack. Users have to rely on the bridge operator's reputation. These solutions are often the easiest to implement.

- **Bonded** – In case of bonded bridges, the actors have to post collateral that gets burned in case of malicious actions.

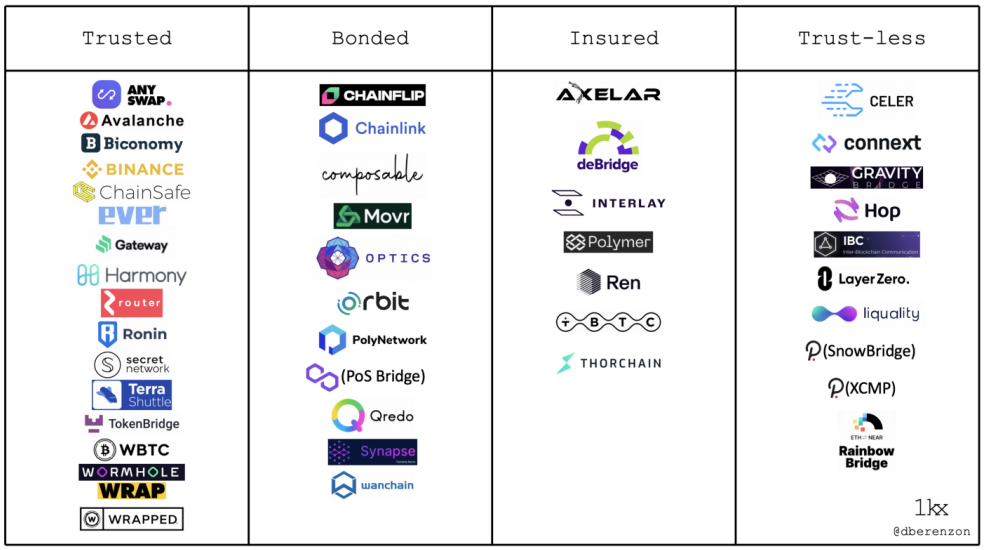

Figure 3.6: Bridges Classified by Trust [30]

- **Insured** – As with bonded bridges, validators must post collateral. If the actor acts maliciously or makes an error, his stake is used to reimburse the lost fund instead of being burnt.
- **Trustless Bridges** – Trusted third party is replaced with smart contracts and algorithms. Funds remain under the user's custody. The security of the bridge is equal to the chains it is bridging. Unless there is a consensus-level attack on the underlying chain, the funds cannot be lost or stolen. However, a complete state of trustlessness can never be achieved because there will always be trust assumptions – we trust that the code has no bugs or that the hashing algorithm will not get broken.

3.5.2 Generalizability

We can also classify bridges by what kind of information they can communicate between the chains. An example of bridges classified by this metric is shown in Figure 3.7.

- **Asset-specific** – The most basic and straightforward communication to implement. Solely serves to provide access to a specific asset from a foreign chain. The user often receives a "wrapped" asset collateralized 1:1 by the underlying in asset (wBTC on Ethereum backed by BTC) a custodial or non-custodial manner. Bitcoin is the most commonly bridged asset, with seven [34] representations on Ethereum alone. The downside to this approach is limited functionality and the need for re-implementation on each destination chain.

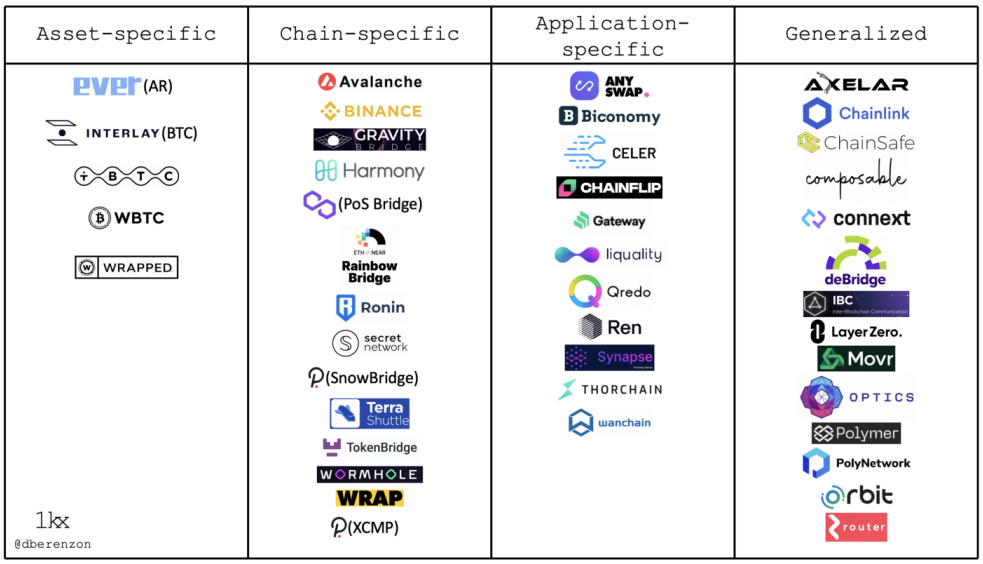

Figure 3.7: Bridges Classified by Generalization [30]

- **Chain-specific** – Bridge between two blockchains that support simple locking assets on the source chain and minting wrapped assets on the destination chain. If the user decides to bridge back, the minted assets are burned, and the original assets get unlocked. These bridges have only a limited complexity but are not easily scalable. The most well-known example of this type of bridge is Polygon's proof-of-stake bridge that connects Ethereum to its layer 2, Polygon.

- **Application-specific** – Bridge that provides access to two or more blockchains but solely for one application. The application benefits from having a smaller code-base and adapters for each blockchain instead of building the application separately for each chain. Additional chains can connect to the application by implementing the adapter, making it easier to achieve a network effect. However, extending the bridge's functionality to other applications is hard. Notable examples of this approach are Thorchain (cross-chain decentralized exchange) and Compound (cross-chain lending protocol).

- **Generalized** – These are protocols specifically designed to transfer information across multiple blockchains. This allows them to achieve a strong network effect – single integration of the protocol gives access to the entire ecosystem within the bridge. However, this amount of generalization often comes with security and decentralization trade-offs. A remarkable example of this is the Inter-Blockchain Communication Protocol (IBC).

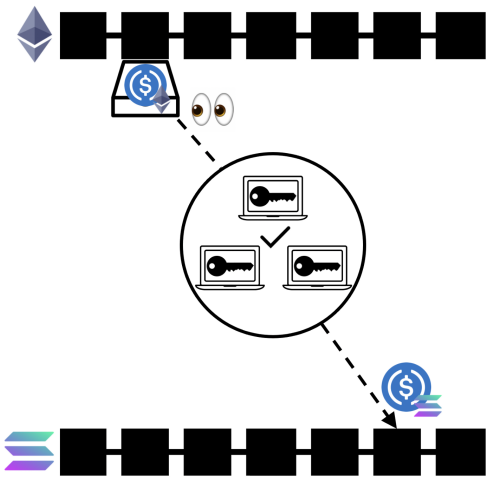

Figure 3.8: A High-Level Illustration of an External Validator or Federated System [30]

3.5.3 Validation

We can split bridges into three categories based on how they validate the cross-chain transactions:

- **External Validators and Federations** – A group of validators (federation) monitors a "mailbox" address on the source chain. If the federation reaches a consensus on the action that happened on the source chain, they perform the appropriate action on the destination chain. The federation members are often bonded validators using a separate token as a security model. An illustration of this model is shown in Figure 3.8.

- **Light Clients and Relays** – Actors continuously monitor events on the source chain and generate cryptographic proof about all past events recorded on that chain. These proofs and block headers are then forwarded to the lite client (smart contracts) on the destination chain. The client verifies that a particular event was recorded on the source chain and executes a corresponding action on the destination chain. There is a liveness assumption that some actor will continuously relay the block headers and proofs. It is one of the trustless bridge designs because it guarantees valid delivery without the need for a trusted third party. The drawdown is that it is not easily scalable, because a new smart contract needs to be built on each destination chain that parses state proofs from the source chain. Also, the continuous validation can become expensive if the chain has high gas fees – transaction fees paid for computational resources needed to conduct a transaction successfully [44]. This solution is illustrated in Figure 3.9.

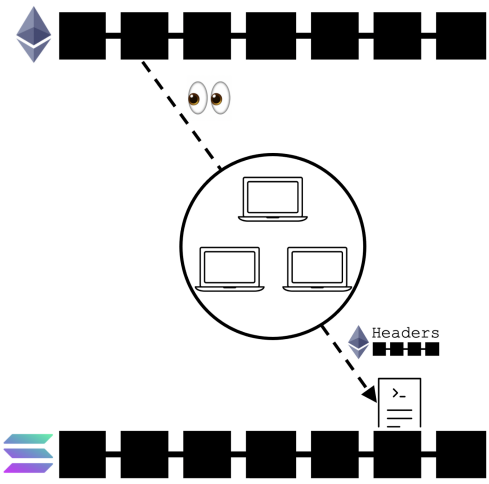

Figure 3.9: A High-Level Illustration of a Light Client and Relay System [30]

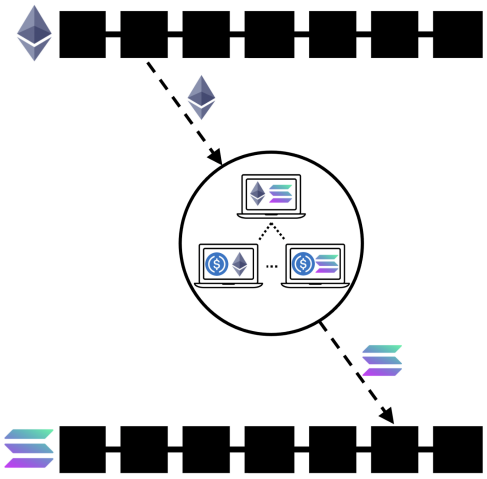

Figure 3.10: A High-Level Illustration of a Liquidity Network [30]

- **Liquidity Networks** – A peer-to-peer network where each node holds assets both on the source and the destination chain. These networks leverage the security of underlying chains, and because there is no trusted entity, users are guaranteed that the nodes cannot steal the assets or act maliciously. These networks are also advantageous for cross-chain asset swaps because users can receive assets native to the destination chain instead of wrapped assets. However, this solution only allows for asset transfers or swaps, not for complete interoperability.

It is important to note that each bridge is a two-way communication channel. Each channel can use a separate communication model, so this classification does not accurately represent bridges that use the hybrid model. For

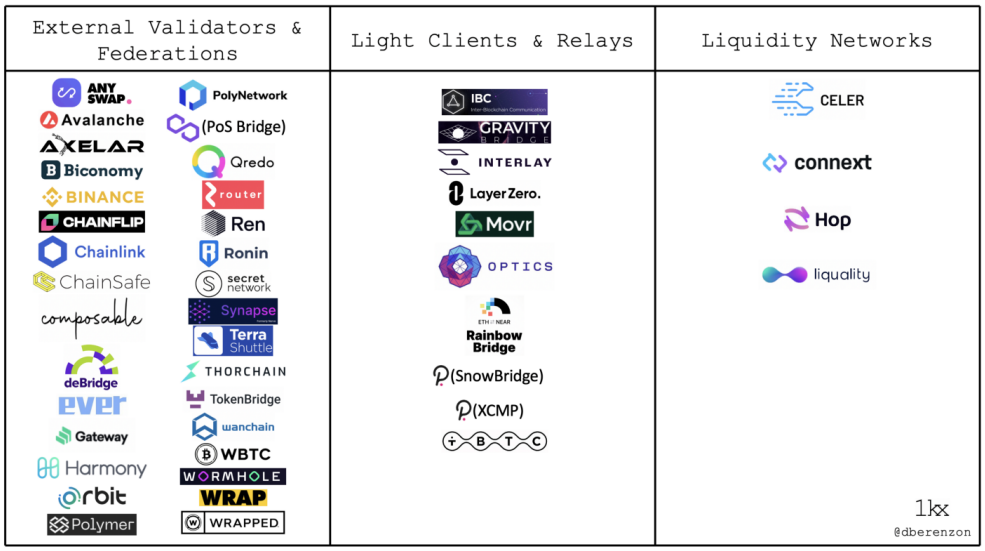

Figure 3.11: Bridges Classified by Approach to Validation [30]

example, the Gravity and the Interlay bridge use light clients in one direction and validators in the other.

3.6 Open Issues and the Future

There are still open issues with bridges and cross-chain communication. [30].

- **Finality and Rollbacks** – What happens to the user's assets if either the source or destination blockchain experiences a rollback (Ethereum after the DAO hack [35])?
- **Non-fungible Tokens (NFT) Transfers and Provenance** – What if one NFT is bridged over to another chain, listed across multiple marketplaces, and eventually sold? How will the transfer of ownership be represented and recorded?
- **Stress Testing and Vulnerability** – A lot of the bridges have not been stress tested enough, and it is yet to be seen how they will perform under network congestion or protocol level attacks.
- **Running Light Clients is Expensive** – Constant monitoring of the source chain and writing the proofs and block headers on the destination chain incurs high gas fees.
- **Shift From Trusted Models to Insured Models** – While insured models are less capital efficient, they assure the user's assets are collateralized and can be reimbursed in case of error or malicious actors.

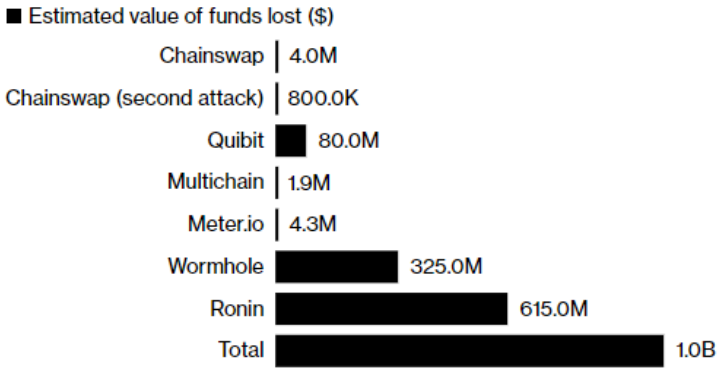

Figure 3.12: Biggest Bridge Hacks [36]

- **Bridge Aggregation and User Experience** – Bridging assets can still be a complex task even for an experienced user. There is plenty of room to improve the user experience – bridge aggregators like Li Finance can make the process more streamlined.

3.7 Risks of Using Bridges

Interacting with blockchain bridges exposes users to multiple types of risk [33]:

- **Smart Contract Risk** – User's assets can be lost or stolen due to a bug, vulnerability, or a backdoor left by the creator.
- **Custodial or Censorship Risk** – While using trusted bridges, assets are under the trusted third party's custody. The trusted party can also censor some or all users from transferring their assets.
- **User Error** – if the user makes an error while transacting with the bridge, all of his assets can be lost irrecoverably.

The users should be acquainted with these risks before using bridges and understand the different trade-offs of different bridge models.

3.8 Notable Hacks

As of April 2022, over $20 billion is currently locked in Ethereum bridges alone[37]. This, combined with how complex the bridging infrastructure is, makes bridges a very lucrative target for hackers. In total, over 1 billion dollars worth of assets were stolen from various bridges, shown in Figure 3.12, with the two biggest hacks happening in February and April of 2022.

3.8.1 The Wormhole Hack

Wormhole is a bridge connecting six blockchains together: Ethereum, Solana, Terra, Binance Smart Chain, Avalanche, and Polygon. As of April 2022, the total value locked is almost $4 billion [38]. The bridge is controlled by a set of Guardians that observe and attest to events and data on its connected chains [50]. When at least two-thirds of the Guardians agree, it is sufficient for an attestation to be created.

The attacker exploited a vulnerability on the Solana side of the bridge that allowed him to forge a fake signature set, which made it appear that his transaction to mint 120 000 wrapped Ether (wETH) without providing the necessary collateral was valid. This led to breaking the 1:1 peg of wrapped wETH to the underlying Ether. The hacker was able to withdraw 93 750 ETH (worth $320 million) back to the Ethereum chain. It is possible that the hacker was able to find the security issue when the fix was uploaded to the public Wormhole Github repository but was not deployed yet [51]. The hack occurred just hours after the publication.

However, all of the stolen assets were replenished by Jump Crypto, a crypto venture capital firm that owns Certus One, the developer of the Wormhole token bridge, so no loss has been incurred to the users of the bridge [52].

3.8.2 The Ronin Hack

The Ronin blockchain is an Ethereum side-chain created specifically for Axie Infinity, one of the most popular blockchain games. The chain has nine different validator nodes in total, and at least five of them need to sign the transaction before it is approved.

However, the security setup of the validator nodes was far extremely centralized – four of the validator keys were held by Sky Mavis, the company behind Axie Infinity. One of the remaining five keys was held by the Axie DAO Validator, but it lent its key to Sky Mavis in November 2021. Sky Mavis decided to do this so they could authorize transactions quicker (having control of the five keys necessary for transactions to be signed) due to a high number of users. The key was returned to the Axie DAO validator later but was never deleted from Sky Mavis servers. This meant that all five were still under the control of one centralized entity.

All that the hacker needed to do to be able to sign any transaction at will was to get access to Sky Mavis servers, which he managed to do via social engineering, as confirmed by a member of the Axie Infinity team [53]. The hacker managed to withdraw assets worth around $600 million, and it took almost a week before anyone noticed that it had happened.

This case showcases how trading decentralization and security for additional speed can lead to massive vulnerabilities. Sky Mavis has promised

to reimburse all the affected users and has raised $150 million from various investors to cover the losses [54].

Chapter 4

Selected Bridges

In this chapter, the criteria used for selecting the bridges for comparison is introduced. Afterward, the selected bridges and their infrastructure is described in detail.

4.1 Selection Criteria

For a system to become truly interoperable, it should satisfy the following criteria [93]:

- **Plug-and-Play Connectivity** – Each distinct network should stand on it its own, and no internal changes should be required for the network to be connected to other ecosystems. If one of the chains connected to the network makes any changes, no additional work from other chains connected to the network should be required to maintain the interoperability.
- **Best-effort Intermediate Communication** – If a cross-chain communication packet is dropped, no one should lose their assets, and they should be either refunded or be able to re-send them again. The transfers of the state and assets must be atomic to prevent double-spending.
- **Gateway-Based Connectivity to All Blockchains** – The individual blockchains should connect to other chains via black boxes. Each chain should host a gateway account, and all information from applications on that chain should be routed to that account. These accounts should be easy to instantiate and should not be dependent on other blockchains.

The mentioned properties can be satisfied by using a centralized system – creating a database between the networks with an interface queriable by the users. However, that goes against one of the main benefits that blockchains bring – decentralization and trustlessness.

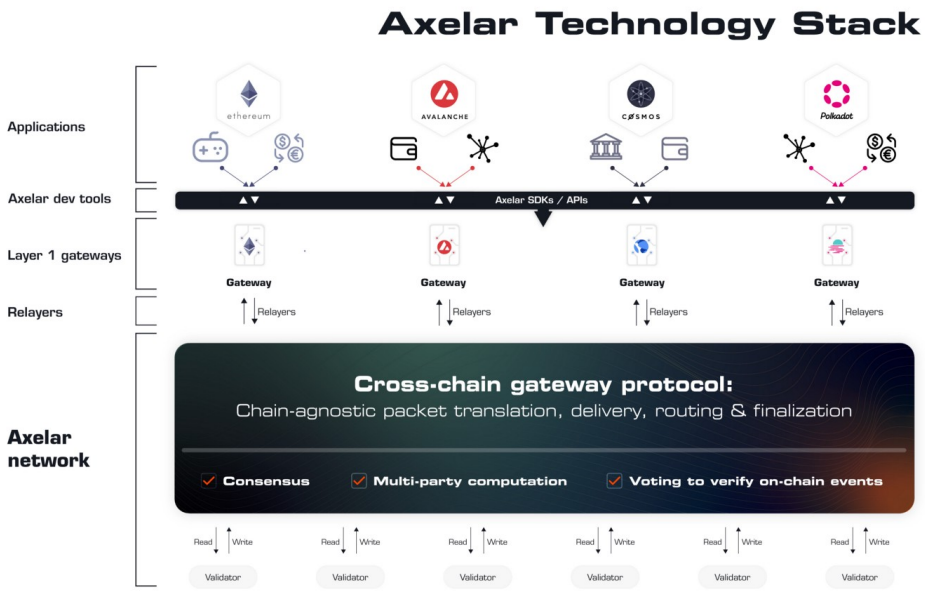

Figure 4.1: The Axelar Technology Stack [56]

The following protocols were selected for comparison because they try to accomplish true interoperability by satisfying the criteria above in a trustless, decentralized, yet secure manner.

4.2 Axelar

Axelar is a universal overlay network that aims to securely connect all blockchain ecosystems, applications, assets, and users to allow full Web3 interoperability. To achieve this goal, Axelar team plans to [56]:

- Make it easy for blockchain developers to plug in new blockchains into the interoperable network.
- Provide dApp developers with cross-chain composability.
- Allow seamless cross-chain interaction for users.

4.2.1 Components

The Axelar network has three key components across two functional layers. A diagram of the Axelar network's technology stack is shown in Figure 4.1.

- **A Decentralized Network** – A blockchain with Delegated Proof-of-Stake (DPoS) model. Members of the network elect validators who have

to lock their stake to participate in the consensus. The validators run the cross-chain gateway protocol, a multi-party cryptography overlay that sits on top of Layer 1 blockchains. They perform read and write operations through the gateway smart contracts deployed on the connected external chains. Once a sufficient number of validators have voted and attested to events on the monitored chains, the state of the chains gets stored on the Axelar blockchain.

- **Gateway Smart Contracts** – These smart contracts provide connectivity between the Axelar network and its interconnected Layer 1 blockchains. Validators monitor the gateways for incoming transactions from the source chains. After they see a message, they read it and start to form a consensus on the validity of the transaction. The consensus is managed via threshold cryptography – a majority of the validators need to agree and collectively approve any transaction [57]. If a consensus is reached, the validators write to the destination chain's gateway to execute the cross-chain transaction.

- **Developer Tools** – The network and gateway smart contracts compose the core infrastructure layer of Axelar. On top of the validators and gateways are the APIs and SDKs – the developer tools that enable easy access to the interoperable network of blockchains that Axelar connects. It is an application-development layer that developers can use to add universal interoperability to their blockchains and dApps. It abstracts the complexity of cross-chain communication into simple API calls that can lock, unlock and transfer assets between any two addresses on any two blockchains, execute cross-chain applications trigger and handle any cross-chain request in general [56].

4.2.2 Protocols

There are two foundational decentralized protocols at the core of the Axelar network:

- **Cross-Chain Gateway Protocol (CGP)** – Handles the routing of data across multiple autonomous blockchain ecosystems. The CGP does not require blockchains to parse the state of each other and supports any consensus protocol, finality rules, smart contract language, or even chains without smart contracts.

- **Cross-chain Transfer Protocol (CTP)** – This protocol serves as the gateway itself, allowing applications to perform simple queries via a unified API, similar to HTTPS or FTP, to facilitate cross-chain operations. Decentralized applications can send CTP queries to gateways on

different blockchains, and CGP is responsible for the cross-chain delivery to the destination chain and returning the transaction results to the sending application [57, 58].

4.2.3 Interacting with Axelar

There are four primary ways to interact with the axelar network catered both to the users and developers.

- **Retail Users** – Axelar has published a proprietary asset transfer application called Satellite that enables easy transfers between different blockchains. Satellite is just the first application, and as more developers and blockchains join the network, users will benefit from being able to easily transfer and utilize their assets in DeFi cross-chain.
- **Application Developers** – Through interaction with a dedicated SDK, developers are able to host their dApps anywhere, transfer assets and ensure interoperability with all chains currently connected to the Axelar network.
- **Platform Developers** – Platform developers will be able to simply connect their products to all popular blockchains just by integrating Axelar instead of having to integrate all platforms separately, saving them from solving substantial engineering work. As of April 2022, adding new blockchains is not openly available for Axelar network users, but a demo on testnet shows the simplicity of the process [59].
- **Validators and Node Operators** – Anybody can set up a node or a validator to help the network security and decentralization and get rewarded in AXL token for doing so.

4.3 IBC

Inter-Blockchain Communication protocol is an interoperability layer for communicating arbitrary data between arbitrary state machines (blockchains). It consists of two distinct layers: the transport (IBC/TAO) layer and the application (IBC/APP) layer [60]. The IBC is one of three layers that are a part of the Cosmos stack.

4.3.1 Cosmos Layers

- **IBC/TAO** – The lower transport, authentication, and ordering layer of IBC. Its goal is to relay packets between two blockchains in a reliable manner. It is implemented as a set of smart contracts (modules) that operate on both the source and destination chains connected via

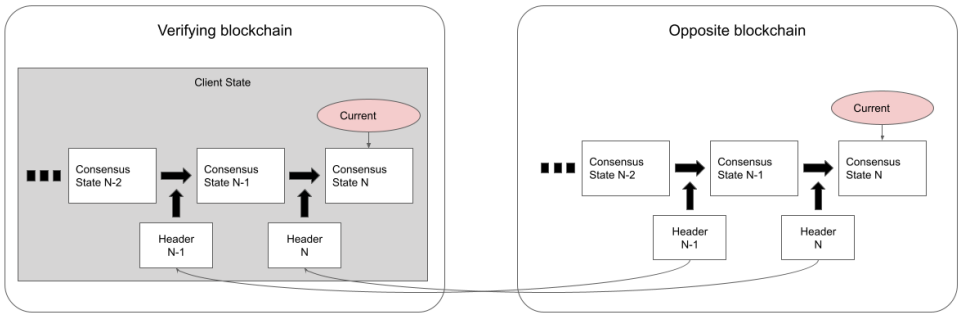

Figure 4.2: IBC Light Client [62]

IBC. The modules consist of three components: on-chain light client, connection abstraction, and channel abstraction.

The light client is the core component that verifies that the states presented actually exist on the source blockchain by checking the block headers. A diagram of this verification is shown in Figure 4.2.

The two connection and channel abstraction components are defined and used to connect two smart contracts on two blockchains and relay packets between them [62].

- **IBC/APP** – The applications that are built on top of IBC/TAO can leverage the simplified inter-chain communication that comes from implementing the IBC/TAO layer.

4.3.2 Cosmos Stack

Cosmos is an ecosystem of independent interconnected blockchains built using the Cosmos SDK or connected to Tendermint, and IBC handles the cross-chain communication [61].

- **IBC** – The most generalized layer of the stack. It is a general-purpose interoperability protocol for different blockchains. It defines how data is sent and acknowledged across blockchains but does not define what the data is or how it should be structured.

- **Tendermint** – Tendermint is a general-purpose consensus engine. Application in any programming language can be built on top of Tendermint. The main ICB implementation uses Tendermint, but as long as a

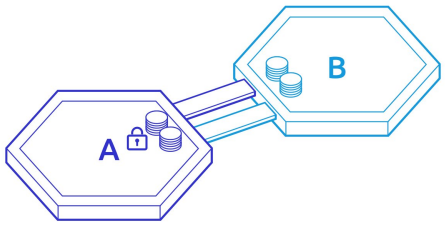

Figure 4.3: Interoperability Between Homogenous Chains [64]

client for Tendermint is implemented, the IBC can work with different kinds of consensus algorithms.

- **Cosmos SDK** – The framework for building application specific blockchains. Many well-known blockchains are built using the Cosmos SDK (Binance Chain, Terra, Crypto.com, Cosmos Hub, and more). In the Cosmos ecosystem, each application has its own blockchain that can be customized for the intended use-cases and retains its sovereignty. Contrary to Ethereum, for example, where all applications are built on top of the same blockchain and have to follow the same rules. Cosmos SDK is written in Go, but it is possible to build blockchains on top of Tendermint without Cosmos SDK. For example, the Nomic bridge that allows the bridging of Bitcoin to Cosmos is built using Rust instead [63].

4.3.3 Interoperability

Cosmos is often described as the "internet of blockchains". If we continue with that analogy, IBC works as the TCP/IP layer, ensuring that messages are being delivered. This also means that it cannot connect nodes that do not have compatible protocols installed. The interoperability of IBC depends on specific properties of the chains being connected [64].

- **Homogenous Chains** – Connecting with other homogenous (Tendermint-based) blockchains is supported by IBC out of the box without the need for a middle man, illustrated in Figure 4.3. IBC enables the transfer of assets and value.
- **Heterogenous Chains** IBC can directly enable value transfer between fast-finality chains (with deterministic finality). However, Bitcoin, for example, is not a fast-finality chain. Instead, it is a probabilistic finality chain - the deeper down the chain a block is, the less likely the chain will get reorganized.

  Peg zones are a solution to this problem. They are an account-based blockchain that acts as an adapter zone and translates probabilistic finality to pseudo-finality by imposing a finality threshold at some arbitrary

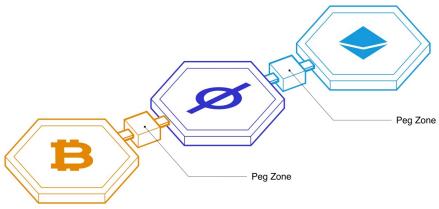

Figure 4.4: Interoperability Between Heterogenous Chains [64]

number of blocks. The peg zones are application-specific and have to be developed for every non Tendermint blockchain that wants to connect to Cosmos. Representation of the two-way peg is shown in Figure 4.4.

4.4 Layer Zero

LayerZero is an omnichain interoperability protocol that uses Ultra Light Nodes (ULN) to achieve cheap yet secure cross-chain communication. There are two models that most cross-chain bridging and messaging protocols use [65].

- **Middle Chain** – This model uses a separate blockchain to receive, validate and forward messages between all the interoperable chains. The middle chain has the full power of signing all messages – thus making it a single point of failure. If a consensus corruption happens, all liquidity locked can be immediately drained. Even if the chain uses the bonded or insured model, if the total value locked inside is higher than the stake of the validators, they have an incentive to act maliciously. Axelar is an example of a middle chain solution.
- **On-Chain Light Node** – On-chain light nodes are a more secure solution, leveraging the security of the underlying blockchains. They receive and validate every block header for each integrated chain. Transaction proofs containing the cross-chain messages are forwarded and validated against the block headers. However, running light nodes is by far the most expensive solution. Running an on-chain light node on Ethereum can cost tens of millions of dollars per day for each pairwise chain [65]. IBC is an example of a solution using light nodes.

4.4.1 Ultra Light Node

The solution used by Layer Zero combines the security of the light node with the cost-effectiveness of middle chains. It is achieved by performing the same validation as an on-chain light node (validating the block headers) but only

doing it on demand by decentralized oracles instead of keeping all the headers [65].

4.4.2 Infrastructure

Layer Zero is a User Application (UA) configurable on-chain endpoint that runs a ULN. The infrastructure diagram can be seen in Figure 4.5. Instead of relying on one party to transfer the message between the on-chain endpoints, it is routed through two parties – the Oracle and the Relayer. When a UA sends a message from chain A to chain B, the endpoint on chain A notifies the Oracle and the Relayer of the message and the intended destination chain. The Oracle forwards the block header to the endpoint on chain B, and the Relayer submits the transaction proofs. The proof is validated on chain B and the message is relayed to the destination address [65].

LayerZero composes of:

- **Endpoints** – The user-facing interface to LayerZero. Each chain in the LayerZero network has one endpoint. Its purpose is to allow the user to send a message and guarantee a valid delivery.
- **Oracle** – The Oracle is a third-party service, independent of other LayerZero components. It reads a block header from the source chain and sends it to the destination. LayerZero leverages the security properties of established oracles Chainlink and Band, but in theory, it can be any third-party service.
- **Relayer** – The Relayer is an off-chain service that fetches the proof for a specified transaction. The protocol itself does not requrie any specific implementation of the Relayer, so even the users of LayerZero can implement their own relayers if needed [66].

With the breaking up of responsibilities between the Oracle and Relayer, LayerZero can leverage the security properties of the established oracles with an added layer of security via the open relayer system. This has the following implications :

- In the worst case, the network's security reduces to being as secure as the Oracle the network uses.
- Even if the Oracle's consensus is corrupt, the Relayer needs to be actively colluding with the corrupted oracle in order for a malicious transaction to go through.
- Furthermore, even if this happens, only the UA's accepting messages from the corrupted Oracle and the corrupted Relayer are at risk. All other UA's using other Relayers, running their own Relayers, or using a different Oracle remain unaffected.

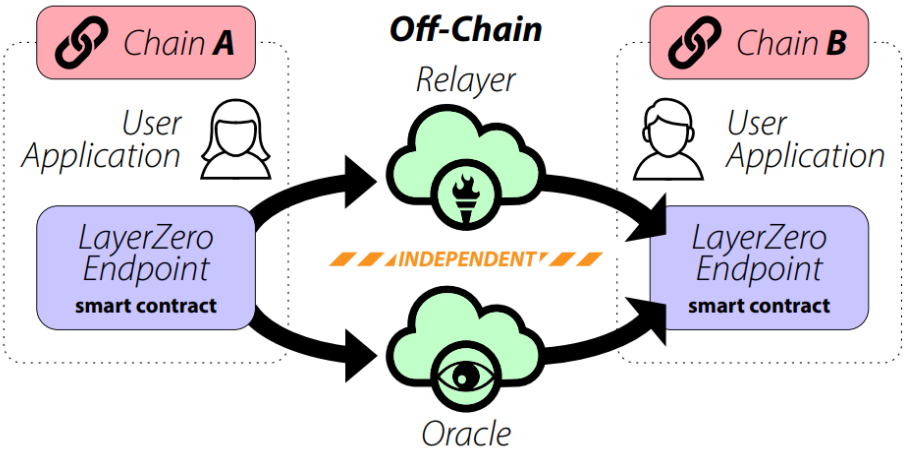

Figure 4.5: LayerZero infrastructure [65]

Figure 4.6: Worst Case Scenario in Layer Zero and in Middle Chains [65]

A representation of how even in the worst-case scenario, only a part of the TVL is affected is shown in Figure 4.6

4.4.3 Additional Security Layers

LayerZero is implementing a 2 phase security mechanism in the LayerZero Labs Relayer for Stargate. Stargate is the first live implementation of LayerZero – it is a fully composable liquidity transport. It allows users to transfer native assets cross-chain while accessing the protocol's unified liquidity pools with instant guaranteed finality [68].

The Dome, the first phase, is a system that deflects attacks from malicious external smart contracts at the Relayer level [67].

Pre-crime, the second phase, provides an additional level of security for UAs. It forks the destination blockchain and runs the transaction locally. Afterward, it can check the state of the forked blockchain in relation to other connected blockchains to verify that no malicious action has occurred. The asserts are defined by the UA and enforced by the Relayer. If running the transaction results in a compromised state of the forked blockchain, Relayer will not deliver the message and stop a potential attack.

Chapter 5

Bridge comparison

In this chapter, the selected methodology for comparing bridges is explained. Then the chosen bridges are evaluated and compared based on the methodology.

5.1 Comparison Methodology

The selected bridges are compared based on multiple criteria explained in the rest of this section. There are six categories: team quality, code quality, business model, infrastructure, community, and user experience. The infrastructure category is broken down further into: security, scalability, capital efficiency, and functionalities.

5.1.1 Team Quality

The quality of the founders of the project is evaluated based on their previous accomplishments, academic background, published articles, and the popularity of their published open-source repositories.

5.1.2 Code Quality

If the code is publicly available or has been audited, its general quality is assessed based on code readability, documentation, test coverage, and reported vulnerabilities.

5.1.3 Business Model

The different business models of the bridges and the cost of interacting with the bridges are compared.

5.1.4 Infrastructure

Under the Infrastructure, the following categories are compared:

- **Security** – Different trust and liveness assumptions, tolerance for malicious actors, and the safety of user funds.
- **Speed** – The times needed to complete the transaction as well as finality guarantees.
- **Scalability and Connectivity** - The number of chains the bridge is connecting and the complexity of integrating additional chains.
- **Capital Efficiency** – The costs of bridging for the user and the capital required to make the system secure.
- **Functionalities and Statefulness** – The ability to transfer assets, more complex states, and the ability to execute cross-chain smart contract calls

5.1.5 Community

The size and activity of different communities are compared to each other.

5.2 Comparison

In this section, the bridges are compared based on the selected criteria.

5.2.1 Team quality

The previous experience and academic background of the founders is described.

5.2.1.1 Axelar

Axelar has two co-founders:

- **Sergey Gorbunov** – Currently an Assistant Professor at the University of Waterloo. He was the Head of Cryptography and a member of the founding team of Algorand, one of the top 50 cryptocurrencies by market cap. He received a Ph.D. from MIT, the top-ranked university in the world [69], and he received Sprowls Doctoral Thesis Prize for best Ph.D. thesis in computer science at MIT. He has published 36 articles that were cited over 3500 times [70].
- **Georgios Vlachos** – Previously the Head of Mathematics and founding team member at Algorand, holds a master's degree from MIT. Winner of a Gold Medal at the International Math Olympiad.

5.2.1.2 IBC

Originally, Cosmos was founded by Jae Kwon and Ethan Buchman. They are the sole authors of the Cosmos whitepaper, in which the idea of Cosmos, Tendermint, and IBC was first described. However, Jae Kwon resigned from the role of CEO of Cosmos in 2020 to focus on a Cosmos-based project Virgo.

Ethan Buchman holds a BSc in Physical Science and a MASc in Engineering Systems and Computing, both from the University of Guelph, ranked 581-590 in the QS World University Rankings [69]. He has published 23 articles that were cited over 700 times [71].

5.2.1.3 LayerZero

LayerZero has three co-founders, Bryan Pellegrino, Caleb Banister, and Ryan Zarick. All of them studied at the University of New Hampshire, ranked 800-1001 in the QS World University Rankings [69]. Ryan holds a Master's degree in Computer Science, Caleb a Bachelor's degree, and Bryan has dropped out.

Bryan has previous experience as a founder of two start-ups in online fantasy sports and predictive AI. He also used to be a professional poker player. Ryan was a CTO of one of the start-ups and has co-founded three blockchain and AI-related companies with Caleb.

5.2.1.4 Evaluation

Looking at the founders, Axelar has the most experienced team in mathematics and cryptography. Cosmos (IBC) founder also has a strong academic background. It is important to note that the development of IBC is completed, and now it is up to new chains to implement it or build two-way pegs for heterogenous chains. LayerZero founders are lacking academic background compared to the other founding teams.

5.2.2 Code Quality

5.2.2.1 Axelar

Axelar has undergone security audits by NCC, Cure53, and Oak Security audits as of April 2022 and the team plans to continue testing the network throughout its development [72]. However, these audits are not available to the public.

The code is open-source and available on Github. The Axelar core module has received 18 stars and the community tools 41 stars. It is well organized, formatted, and documented by plenty of comments, and documentation is available for developers, node operators, and validators. As of April 2022, some parts of the documentation are still under construction (network design and gateway contracts) [73].

Axelar is also running a bug bounty program with rewards up to $1 million focused on finding security vulnerabilities in the Axelar blockchain, smart contracts, website, and app [74].

5.2.2.2 IBC

Cosmos (including IBC) has undergone seven security audits as of 2019 [75], with some of the audits being available to the public. A published security audit by Least Authority found the codebase to be well organized, with a clean and succinct coding style. Tests were available for all major modules and some of them had a 100% test coverage. The audit hasn't identified any issues [76]. The code is open-source and available on Github.

The Cosmos SDK has received over 3800 stars and the IBC over 500 stars. All interchain standards are clearly documented with lengthy explanations, code snippets, and graphs. Cosmos is also running multiple bug bounty programs. In October 2021, a high-severity vulnerability was reported in the Cosmos SDK. It made the network vulnerable to a consensus halt due to a non-deterministic behavior of nodes. However, this vulnerability was patched before anyone used it to attack the chain [77].

5.2.2.3 LayerZero

Zokyo, Slowmost, and Ackee Blockchain have audited LayerZero. All of the audits are publicly available.

Zokyo has rated the security of the code with 98 out of maximal 100, with the percentage of testable code being 86.23%. It identified two high severity issues that were resolved based on the findings. Some less severe issues were also found, all of which were resolved or clarified by the LayerZero team [78].

Audit conducted by Slowmost discovered three low severity vulnerabilities that were acknowledged by the LayerZero team [79].

Ackee Blockchain review rated the architecture of the protocol and overall quality of the code as very good. The code is well documented in code, Gitbook, and the whitepaper. One high severity issue was found related to the possible conspiracy between the Relayer and the Oracle, but it was acknowledged by the team, and the probability of it happening was classified as extremely low. Other than that, no issues with the code were found [80]. The code is available on Github and has received 76 stars.

5.2.2.4 Evaluation

All of the projects were audited multiple times. IBC has undergone most audits, and the code has been deployed live for the longest time without any significant issues. Many third-party developers have also implemented and used it, unlike Axelar and LayerZero, which have only one live application each (StarGate and Satellite) built by the original team of developers. Both

Asset symbol	Ethereum	non-Ethereum EVM	Cosmos Chains	Decimals	Unit
UST	20 UST	1 UST	0.5 UST	6	uusd
LUNA	0.2 LUNA	0.01 LUNA	0.005 LUNA	6	uluna
ATOM	0.7 ATOM	0.04 ATOM	0.02 ATOM	6	uatom
USDC	20 USDC	1 USDC	0.5 USDC	6	uusdc
FRAX	20 FRAX	1 FRAX	0.5 FRAX	18	frax-wei
DAI	20 DAI	1 DAI	0.5 DAI	18	dai-wei
USDT	20 USDT	1 USDT	0.5 USDT	6	uusdt
NGM	16 NGM	0.8 NGM	0.4 NGM	6	ungm
EEUR	20 EEUR	1 EEUR	0.5 EEUR	6	eeur

Figure 5.1: Axelar Fees [82]

of these applications were deployed just recently (January 2022 for Satellite, March 2022 for StarGate), while Cosmos with IBC has been live since April 2021.

5.2.3 Business Model

The business models of selected solutions are explained in this section.

5.2.3.1 Axelar

The Axelar network leverages transaction fees depending on the destination chain. There is a base fee for all-cross chain transfer, and it depends only on the source and destination chain. The fee is a sum of the source and destination chain fees for that asset. The table with the fees is shown in Figure 5.1.

The base inflation of 10%-15% (based on the amount of delegated stake) is split evenly between participating in the underlying Tendermint consensus and signing multi-party signing protocols [81]. Then for each external chain, there is additional inflation of 2% split between the validators that maintain nodes for that chain. Cosmos-based chains are supported natively through IBC, so there is no additional support needed from the validators. The distribution of inflation is shown in Figure 5.2 and Figure 5.3

To incentivize validators to avoid undesirable behavior (losing liveness, failing to vote correctly, double signing), reward slashing is implemented. For the consensus, standard Tendermint slashing reward rules are used. For multiple-

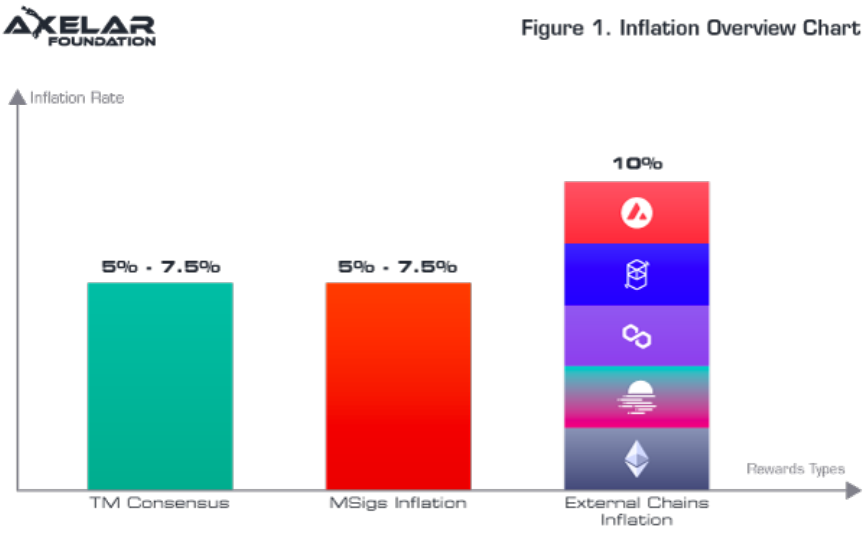

Figure 5.2: Inflation Overview Chart [81]

party signing protocol, validators are slashed and suspended for a period of time if they are not active [81].

These parameters put the inflation at around 22% per anum, not counting any additional chains connected to the network. However, they are subject to change and are set up in such a way to bootstrap the protocol and incentivize validators to keep the network secure.

5.2.3.2 IBC

There are no fees or a business model associated with IBC itself. The only fee required is the source chain's standard fee for initiating the transaction. Each chain in the Cosmos ecosystem can independently set up the transaction fee structure. Also, it is possible to use IBC without integrating with the Cosmos ecosystem at all, although the main advantage of using it (and Tendermint) is the immediate interoperability it allows.

5.2.3.3 LayerZero

In every LayerZero transaction, there are three fees the sender has to pay [94]:

- Fee for oracles for moving the block data between the chains.
- Relayers for delivering the message along with a cryptographic proof.
- LayerZero for developing the messaging protocol.

Figure 5.3: Inflation Distribution [81]

The UA's can choose any Oracle and Relayer combination available on the market. This open market approach was chosen to incentivize the participants to provide the best service they can. UA can estimate what will the total fee be by calling a designated function, but there is no exact value (percentage or flat fee) given in the documentation. The entire fee can be paid in the native token of the source chain [94].

Using Stargate for transferring other tokens than the Stargate token (STG) incurs a 0.06% fee. This fee is split between the liquidity providers for the destination pool, which take 0.045%, and protocol treasury, which takes the remaining 0.015% [95].

Partners that integrate Stargate in production and have significant transaction volume can apply to participate in the Stargate whitelist partner program, which rewards them with 0.003% of the transaction volume they have sent through Stargate.

5.2.3.4 Evaluation

Axelar has changed its model from taking a percentage of the transaction volume (0.1% from transfer to Ethereum and 0.05% to other destination chains) to a flat fee. That makes it a lot more attractive for users wanting to transfer high volume of assets through Axelar over LayerZero. However, these business models are subject to change as both protocols are new and are trying to attract as many users and liquidity as possible.

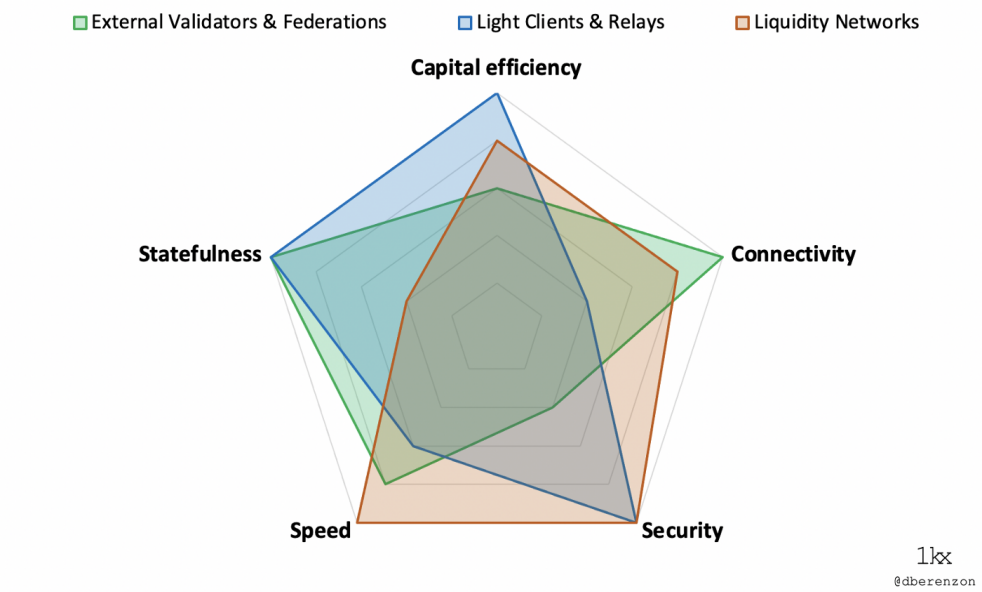

Figure 5.4: Infrastructure Trade-offs [28]

5.2.4 Infrastructure

The trade-offs of different infrastructure solutions are shown in Figure 5.4. Axelar uses the external validator model, IBC the light client model, and LayerZero a tweaked version of the light client model.

5.2.4.1 Security

- **Axelar** – The Axelar network relies on its validators to stay secure. Anyone can become a validator so that the network is as decentralized as possible. The validators need to stake tokens and if they act maliciously, their stake gets slashed [89]. This should make it unprofitable for validators to try to steal any funds because their collateral is at stake. Axelar implements a Delegated Proof-of-Stake model that allows community members to elect a set of validators to run the consensus. The safety threshold on consensus is set at 90% on the primary validator set. This means that almost all validators must agree before any funds locked in the network are withdrawn.

  If the Axelar network should stall as a result of the high consensus threshold, each threshold bridge account on a given blockchain has an emergency unlock key. Secret shares of the key are generated and each validator shares a random value and by summing these values, the recovery key is generated.

  In the case one of the blockchains connected to the Axelar network fails, limits on the dollar value of the assets moving in and out can

be imposed to prevent the malicious chain from stealing a significant fraction of assets before being detected. Then a vote through the Axelar governance module can determine the following steps [89].

- **IBC** – The security of IBC is equal to the security of the underlying blockchains connected to the Cosmos network. The only way user assets can be stolen is if a successful consensus-level attack happens on one of the chains. However, the only way to connect IBC to heterogenous (non-Tendermint) chains is to use peg-zones. The peg-zone itself is a translator blockchain that allows users to query and perform transactions [90]. Each additional peg-zone brings a security risk since they have to be written and tested separately for each non-Tendermint chain.

- **LayerZero** – The security of LayerZero relies on two actors – the Oracles and the Relayers [65]. The Ultra Light Node leverages the security of the Oracle, which can be chosen by the LayerZero UA. Even if the Oracle gets compromised, the Relayer that the UA has chosen would have to be compromised at the same time, only the assets of UA's using this exact pair of Relayer and Oracle would be in danger. This effectively reduces the chance of any malicious actions, and even if it happens, only a fraction of the assets in the network are compromised. LayerZero also has the Pre-Crime functionality that simulates the transaction before it goes live, and if a malicious action is detected, the transaction is never performed.

It is challenging to compare the different security models since many variables exist. Even if the proposed model is perfect, there can still be a security vulnerability in the smart contracts implementing the model. The IBC model is the safest with leveraging the security of the underlying blockchains, but connecting more chains outside of the Cosmos zone brings additional points of vulnerability. The Axelar only has one point of failure, the consensus mechanism. However, attacks on consensus are complicated once the network reaches a sufficient size and a state of decentralization. LayerZero, in the worst case, leverages the security of the chosen Oracle.

5.2.4.2 Speed

- **Axelar** – Depending on the selected source and destination chains and the current load on the network, the transfer can take anywhere between 5 to 20 minutes [83].

- **IBC** – The transfers within the Cosmos ecosystem take around 10 seconds. However, transactions between non-Tendermint chains can take minutes [84].

- **LayerZero** – The speed once again depends on the selected chains, but in general, the swaps take 30 to 90 seconds [85].

5.2.4.3 Scalability / Connectivity

- **Axelar** – Axelar currently supports nine chains: Ethereum, Avalanche, Cosmoshub, e-Money, Fantom, Moonbeam, Osmosis, Polygon, and Terra [83]. Currently, adding new chains is not open to everyone, but adding new EVM-based chains is a simple process. There are no requirements for the consensus protocol, finality rules, smart contract language, or even the need for the chain to have smart contracts. The new blockchain only needs to deploy the Axelar Gateway and it will immediately become a part of the ecosystem.

- **IBC** – There are currently 43 blockchains in the native Cosmos ecosystem connected via IBC [84]. Any blockchain built using the Cosmos SDK or the Tendermint consensus can is cross-chain compatible with the Cosmos network. However, integrating chains that do not use the Tendermint directly with IBC is time-consuming, and a new peg zone has to be built for each chain. Replacing the peg-zones with the integration of Axelar or LayerZero seems to be a better, more efficient solution.

- **LayerZero** – LayerZero currently supports Ethereum, Avalanche, Polygon, BNB Chain, Fantom, Arbitrum, and Optimism. Support for Solana, Terra, Cosmos Hub and Osmosis should begin in May-June 2022 [91]. The goal of LayerZero is to replace the IBC's transport layer, lifting the finality restrictions IBC imposes and making IBC compatible with all kinds of consensus mechanisms without the need for chain-specific peg zones.

IBC works perfectly with chains using Tendermint, but adding support for different consensus mechanisms is complicated. Running light nodes for EVM chains is cost-prohibitive. Both Axelar and LayerZero solve this problem, but LayerZero has been able to onboard more chains in a shorter period, and the transactions happen faster than on Axelar.

5.2.4.4 Capital Efficiency

- **Axelar** – Axelar is not very capital efficient since it requires a lot of staked capital to be secure – ideally, the amount of staked capital has to be higher than the total value locked in the network [28].

- **IBC** – IBC is very capital efficient within the Cosmos ecosystem because it does not require any capital staked to secure the network. However,

running light nodes on EVM compatible systems is very cost-prohibitive [65].

- **LayerZero** – LayerZero does not need any additional capital to be secure since it leverages the security of the Oracle networks [65].

LayerZero is the most capital-efficient in general of the compared solutions.

5.2.4.5 Functionality

All of the compared chains models are not limited to specific assets and can transfer the state of one blockchain to another, including cross-chain smart contracts calls. However, the available functionalities and dApps built on top of these protocols differ:

- **Axelar** – Currently offers cross-chain swaps of stablecoins, ATOM, and LUNA between the available chains. There is also the top flows feature that showcases the most common flows of assets via the Axelar network [83].
- **IBC** – Chains that implement the Cosmos Interchain module can interact with each other seamlessly. This allows complete composability and aggregates the flow into one transaction for the user, instead of having to do a cross-chain transaction via IBC first and then perform the desired action on the destination chain [92].
- **LayerZero** – Stargate allows users to transfer stablecoins and the STG token cross-chain. Users can also deposit stablecoins into the various pools to earn a cut from the transaction fees and also stake their LP-tokens to earn yield in STG for providing liquidity. Finally, the Walk-through mode guides the user through the cross-chain transfer in a simple, user-friendly way [85].

5.2.5 Community

5.2.5.1 Axelar

Axelar has over 43 thousand members on Discord and over 50 thousand on Twitter. The Axelar Academy also provides plenty of material for anyone to learn more about the network. It also includes two video courses, an introduction to Axelar Network, and an explainer of the core network protocols. Besides the Axelar Academy, the Quantum Community Program gives anyone from the community a chance to get AXL tokens as a reward for submitting educational material [86]. Axelar is also running the Axelerator Multichain Grant Challenge, with $2.3 million split across the best submissions that build a cross-chain native application using the Axelar network [87].

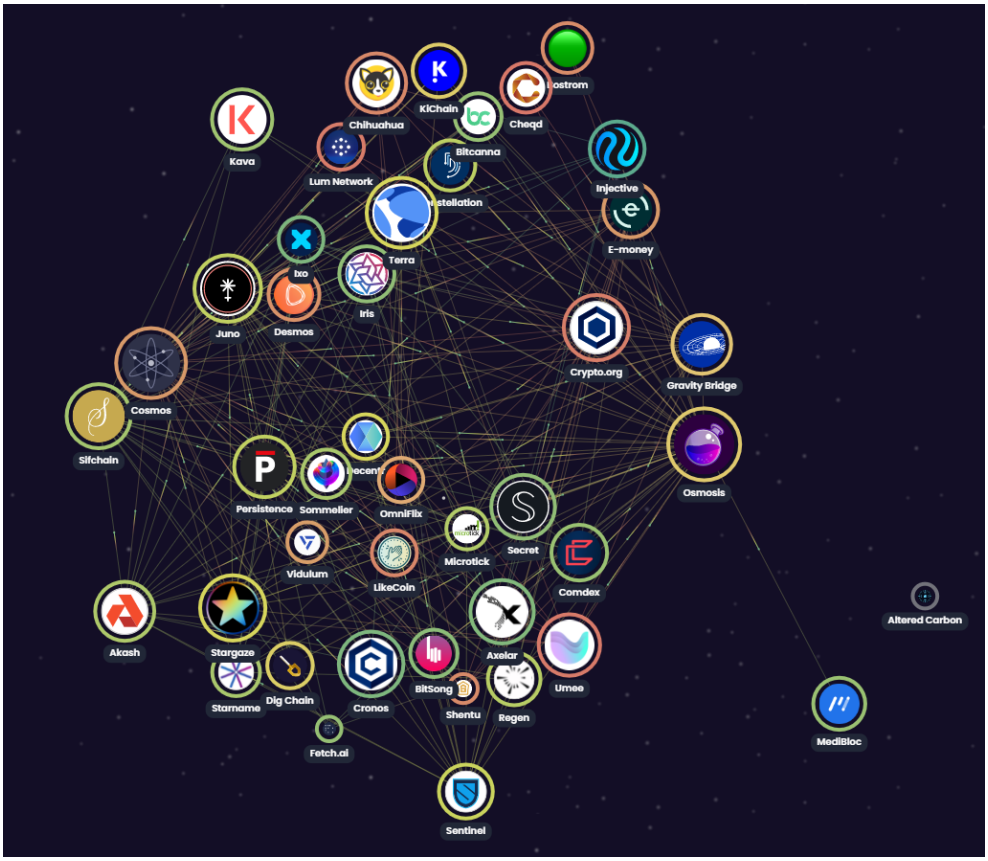

Figure 5.5: The Zones of Cosmos [88]

5.2.5.2 IBC

The Cosmos network has over 400 thousand followers on Twitter but only 20 thousand members on Discord. However, there are already 43 chains connected via IBC. The zones in Cosmos and their communication is shown in Figure 5.5.

5.2.5.3 LayerZero

LayerZero has 86 thousand followers on Twitter and 23 thousand on Discord.

5.2.5.4 Evaluation

The Cosmos ecosystem currently has the highest community but has also been around for the longest time. The Cosmos SDK makes it easy to create a new blockchain that is interoperable with all the existing blockchains in the ecosystem immediately. Axelar is doing a great job of engaging the community members and rewarding them for their contributions. LayerZero has a good

amount of traction, but developers have no monetary incentives to build on LayerZero as of April 2022.

5.3 Evaluation

In this section, the table containing the evaluation is presented. The purpose of this table is to provide a quick overview of the compared criteria.

- **Team Quality** – The total number of times the founders were cited in academic papers.
- **Code Quality** – The number of security audits and cumulative Github stars received.
- **Business Model** – Where applicable, the fees charged by the protocol.
- **Security** – The number of validators validating the Axelar network is compared with the number of validators on the Cosmos Hub – the main chain of the cosmos ecosystem, and with the number of validator nodes Chainlink has – the primary oracle used by LayerZero.
- **Speed** – The average times per cross-chain transaction are compared. However, once non-finality chains (such as Ethereum) are on either part of the transaction, the bridging can take up to 20 minutes.
- **Scalability** – The number of supported chains.
- **Capital Efficiency** – The need for staking external capital to secure the network.
- **Functionality** – The functionalities that the protocols currently offer.
- **Community** – The combined sizes of the Twitter and Discord communities.

Criteria/Project	Axelar	IBC	LayerZero
Team Quality	∼3500 citations	∼700 citations	0 citations
Business Model	3 security audits ∼60 Github stars	7+ security audits ∼4300 Github stars	3 security audits ∼80 Github stars
Business Model	$1-$20 flat fee	-	0.06% fee from the total volume
Security	42 validators	385 validators on Cosmos Hub	344 validators on Chainlink
Speed	5-20 minutes	within Tendermint <10 seconds, up to 20 mins for ETH	on average 30-90 seconds up to 20 minutes for ETH
Scalability	9 chains	43 chains	7 chains 4 more being implemented
Capital Efficiency	requires staked capital	does not require any staked capital	oracles require staked capital not LayerZero itself
Functionality	cross-chain swaps	cross-chain swap Cosmos Interchain integrated chains seamless interoperability	cross-chain swaps cross-chain liquidity pools
Community	∼90000	∼420000	∼109000

Table 5.1: Overview Comparison Table

Conclusion

The first goal of this thesis was to study and analyze blockchain technology – the first chapter is dedicated to describing what a blockchain is and its essential properties. A brief history of Bitcoin and altcoins is presented, and fundamental terms used in the world of cryptocurrencies are explained.

The second goal was to study and analyze technologies used in decentralized finance. The second chapter explains the term DeFi and what are the main applications of the technology, and the advantages and risks of using DeFi compared to traditional financial instruments are presented. The third chapter explains what cross-chain bridges are – one of the critical components of fully interoperable DeFi. The interoperability trilemma, which discusses how bridges try to become trustless, extensible, and generalizable at the same time, is introduced. Building on top of this concept, various ways by which cross-chain bridges can be classified are proposed. The different issues, risks, and the most significant hacks are mentioned at the chapter's end.

The criteria used for selecting the bridges for comparison is presented in the fourth chapter. Then the three selected interoperability protocols, Axelar, IBC, and LayerZero are introduced in detail. This accomplishes the goal of documenting the current state of blockchain bridges and selecting the individual bridges for the comparison.

The fifth chapter lays out the framework constructed for comparison of the bridges. The different bridges are compared and evaluated based on the discussed criteria – the technology model used, the functionalities the bridges offer, their business model, and the quality of the code and the team. Finally, a table for a quick overview of the comparison is attached and described.

This thesis should provide enough information about blockchain technology and the technology used in decentralized finance for anyone interested in learning the different complexities and challenges of trustless yet secure cross-chain interoperability and to prepare the reader a further research of the topic.

Bibliography

[1] CoinMarketCap [online]. [cited 2022–04–06]. Available at: https://coinmarketcap.com/.

[2] ZMUDZINSKI, Adrian. Institutional Investors Now Hold $70B Of Bitcoin: Report [online]. [cited 2022–04–06]. Available at: https://finance.yahoo.com/news/institutional-investors-now-hold-70b-122022840.html.

[3] Top 5 Bitcoin Investors [online]. [cited 2022–04–06]. Available at: https://www.investopedia.com/articles/people/091516/top-5-investors-investing-bitcoin.asp.

[4] HERNANDEZ, Joe. El Salvador Just Became The First Country To Accept Bitcoin As Legal Tender [online]. [cited 2022–04–06]. Available at: https://www.investopedia.com/articles/people/091516/top-5-investors-investing-bitcoin.asp.

[5] What is Ethereum? [online]. [cited 2022–04–06]. Available at: https://ethereum.org/en/what-is-ethereum/.

[6] Multi-chain future likely as Ethereum's DeFi dominance declines [online]. [cited 2022–04–06]. Available at: https://www.bloomberg.com/professional/blog/multi-chain-future-likely-as-ethereums-defi-dominance-declines/.

[7] NOFER, Michael; GOMBER, Peter; HINZ, Oliver; SCHIERECK, Dirk. Blockchain [online]. [cited 2022–04–06]. Available at: http://cs.unibo.it/~danilo.montesi/CBD/Articoli/2017Blockchain.pdf.

[8] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. [cited 2022–04–17]. Available at: https://bitcoin.org/bitcoin.pdf.

[9] PROOF-OF-STAKE (POS) [online]. [cited 2022–04–17]. Available at: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[10] LEON, Daniel; STALICK, Antonius; JILEPALLI, Ananth; HANEY, Michael; SHELDON, Frederick. Blockchain: properties and misconceptions [online]. [cited 2022–04–17]. Available at: https://www.emerald.com/insight/content/doi/10.1108/APJIE-12-2017-034/full/pdf?title=blockchain-properties-and-misconceptions.

[11] KASTHALA, Venkat. Blockchain key characteristics and the conditions to use it as a solution [online]. [cited 2022–04–17]. Available at: https://medium.com/swlh/blockchain-characteristics-and-its-suitability-as-a-technical-solution-bd65fc2c1ad1.

[12] What is cryptocurrency? [online]. [cited 2022–04–17]. Available at: https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency.

[13] A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses [online]. [cited 2022–04–17]. Available at: https://arxiv.org/pdf/1908.04507.pdf.

[14] BECKER, Georg. Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis [online]. [cited 2022–04–17]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.7879&rep=rep1&type=pdf.

[15] HEASMAN, Will. More Than 430 Altcoins Are Now Derived From Bitcoin [online]. [cited 2022–04–17]. Available at: https://decrypt.co/42736/more-than-430-altcoins-are-now-derived-from-bitcoin

[16] HABER, Stuart; STORNETTA, W. Scott. How to Time-Stamp a Digital Document [online]. [cited 2022–04–17]. Available at: https://link.springer.com/content/pdf/10.1007%2F3-540-38424-3_32.pdf.

[17] Smart Contracts [online]. [cited 2022–04–17]. Available at: https://ethereum.org/en/smart-contracts/.

[18] RAVAL, Siraj. Decentralized Applications [online]. [cited 2022–04–17]. Available at: https://www.oreilly.com/library/view/decentralized-applications/9781491924532/ch01.html.

[19] What are Dapps? All you need to know about the Decentralized Applications [online]. [cited 2022–04–17]. Available at: https://thedapplist.com/learn/what-is-dapp/.

[20] Introduction to Smart Contracts [online]. [cited 2022–04–17]. Available at: https://ethereum.org/en/developers/docs/smart-contracts/.

[21] Layer-1 and Layer-2 Blockchain Scaling Solutions [online]. [cited 2022–04–17]. Available at: https://www.gemini.com/cryptopedia/blockchain-layer-2-network-layer-1-network.

[22] CoinMarketCap [online]. [cited 2022–04–17]. Available at: https://coinmarketcap.com/.

[23] All layer 1 blockchain protocols [online]. [cited 2022–04–06]. Available at: https://blockchain-comparison.com/blockchain-protocols/.

[24] What Are Liquidity Pools in DeFi and How Do They Work? [online]. [cited 2022–04–18]. Available at: https://academy.binance.com/en/articles/what-are-liquidity-pools-in-defi.

[25] ARAMONTE, Sirio; HUANG, Wenqian; SCHRIMPF, Andreas. Trading in the DeFi era: automated market-maker [online]. [cited 2022–04–18]. Available at: https://www.bis.org/publ/qtrpdf/r_qt2112v.htm.

[26] SILVESTRI, Michaela. A deep look into the cryptocurrencies that survived the Bitcoin market crashes [online]. [cited 2022–04–06]. Available at: https://wire.insiderfinance.io/a-deep-look-into-the-cryptocurrencies-that-survived-the-bitcoin-market-crashes-5d172b73569.

[27] SAINI, Vaibhav. ConsensusPedia: An Encyclopedia of 30+ Consensus Algorithms [online]. [cited 2022–04–17]. Available at: https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f.

[28] BERENZON, Dmitriy. Blockchain Bridges: Building Networks of Cryptonetworks [online]. [cited 2022–04–06]. Available at: https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8.

[29] QURESHI, Haseeb. Blockchains are cities [online]. [cited 2022–04–06]. Available at: https://medium.com/dragonfly-research/blockchains-are-cities-564327013f86.

[30] CHAND, Arjun. What Are Blockchain Bridges And How Can We Classify Them? [online]. [cited 2022–04–06]. Available at: https://blog.li.finance/what-are-blockchain-bridges-and-how-can-we-classify-them-560dc6ec05fa.

[31] BUTERIN, Vitaly.Why sharding is great: demystifying the technical properties [online]. [cited 2022–04–06]. Available at: https://vitalik.ca/general/2021/04/07/sharding.html

[32] BHUPTANI, Arjun. The Interoperability Trilemma [online]. [cited 2022–04–06]. Available at: https://blog.connext.network/the-interoperability-trilemma-657c2cf69f17

[33] Blockchain bridges [online]. [cited 2022–04–07]. Available at: https://ethereum.org/en/bridges/

[34] BTC on Ethereum [online]. [cited 2022–04–07]. Available at: https://dune.xyz/eliasimos/btc-on-ethereum_1

[35] What Was The DAO? [online]. [cited 2022–04–08]. Available at: https://www.gemini.com/cryptopedia/the-dao-hack-makerdao#section-the-dao-hack-remedy-forks-ethereum

[36] KHARIF, Olga. Understanding Crypto Bridges and $1 Billion in Thefts [online]. [cited 2022–04–08]. Available at: https://www.bloomberg.com/news/articles/2022-04-02/understanding-crypto-bridges-and-1-billion-in-thefts-quicktake

[37] Bridge Away [online]. [cited 2022–04–08]. Available at: https://dune.xyz/eliasimos/Bridge-Away-(from-Ethereum)

[38] Wormhole [online]. [cited 2022–04–08]. Available at: https://defillama.com/protocol/wormhole

[39] DeFi Dashboard [online]. [cited 2022–04–18]. Available at: https://mcusercontent.com/d3ae2759971a9a026c8999c2c/files/cece4879-d1f1-d087-0ef3-d26eeec0d609/RBF_Investor_Summit_II_vpostsummit.pdf?mc_cid=957b5fef4e

[40] Role of DeFi: Development [online]. [cited 2022–04–18]. Available at: https://defillama.com/

[41] SERGEENKOV, Andrey. What Is an Automated Market Maker? [online]. [cited 2022–04–18]. Available at: https://www.coindesk.com/learn/2021/08/20/what-is-an-automated-market-maker/

[42] The Complete Beginner's Guide to Decentralized Finance (DeFi) [online]. [cited 2022–04–21]. Available at: https://academy.binance.com/en/articles/the-complete-beginners-guide-to-decentralized-finance-defi

[43] How Blockchain Technology Will Impact the Banking Industry [online]. [cited 2022–04–21]. Available at: https://academy.binance.com/en/articles/how-blockchain-technology-will-impact-the-banking-industry

[44] GAS AND FEES [online]. [cited 2022–04–18]. Available at: https://ethereum.org/en/developers/docs/gas/

[45] What Is DeFi 2.0 and Why Does it Matter? [online]. [cited 2022–04–21]. Available at: https://academy.binance.com/en/articles/what-is-defi-2-0-and-why-does-it-matter

[46] What are the risks of DeFi? [online]. [cited 2022–04–21]. Available at: https://www.futurelearn.com/info/courses/defi-exploring-decentralised-finance-with-blockchain-technologies/0/steps/256218

[47] RODRIGUEZ, Jason. The 5 Big Risk Vectors of DeFi [online]. [cited 2022–04–21]. Available at: https://www.coindesk.com/layer2/2022/02/03/the-five-big-risk-vectors-of-defi/

[48] DeFi Investment Risks [online]. [cited 2022–04–21]. Available at: https://help.coinbase.com/en/coinbase/trading-and-funding/advanced-trading/defi-investment-risks

[49] Anchor Protocol Dashboard [online]. [cited 2022–04–23]. Available at: https://app.anchorprotocol.com/

[50] Introducing Wormhole [online]. [cited 2022–04–08]. Available at: https://wormholecrypto.medium.com/introducing-wormhole-32b16d795c01

[51] Wormhole Github [online]. [cited 2022–04–08]. Available at: https://github.com/certusone/wormhole/commit/7edbbd3677ee6ca681be8722a607bc576a3912c8#diff-0d27d8889edd071b86d3f3299276882d97613ad6ab3b0b6412ae4ebf3ccd6370L92-R101

[52] SUN, Zhiyuan. Jump Crypto replenishes funds from $320M Wormhole hack in largest-ever DeFi 'bailout' [online]. [cited 2022–04–08]. Available at: https://cointelegraph.com/news/jump-crypto-replenishes-funds-from-320m-wormhole-hack-in-largest-ever-defi-bailout

[53] Ronin hack statement [online]. [cited 2022–04–08]. Available at:
https://twitter.com/Psycheout86/status/1509134629009342467?s=20&t=D-MnRql0umqssHWTuVJ3ag

[54] Sky Mavis raises 152$Matnearly$3B valuation for Axie Infinity play-to-earn NFT game [online]. [cited 2022–04–15]. Available at:
https://venturebeat.com/2021/10/06/sky-mavis-raises-152m-at-nearly-3b-valuation-for-axie-infinity-play-to-earn-nft-game/

[55] DOYLE, Megan. Blockchain Bridges And Interoperability: Overview, Roles, and Integrations [online]. [cited 2022–04–09]. Available at:
https://hackernoon.com/blockchain-bridges-and-interoperability-overview-roles-and-integrations-r64433i2

[56] An Introduction to the Axelar Network [online]. [cited 2022–04–09]. Available at:
https://medium.com/axelar/what-is-axelar-network-5ba423a3594c

[57] GORBUNOV, Sergey. A Technical Introduction to the Axelar Network [online]. [cited 2022–04–09]. Available at:
https://medium.com/axelar/a-technical-introduction-to-the-axelar-network-3c4bf9fe4dc3

[58] SHIYANOK, Denis. The Essentials You Need to Know About Axelar [online]. [cited 2022–04–09]. Available at:
https://medium.com/@denisshiyanok/the-essentials-you-need-to-know-about-axelar-a8c39a92fb4a

[59] Onboarding Avalanche to the Axelar Network [online]. [cited 2022–04–09]. Available at:
https://www.youtube.com/watch?v=iZgqneh7s88&ab_channel=Axelar

[60] Inter-Blockchain Communication Protocol [online]. [cited 2022–04–09]. Available at:
https://ibcprotocol.org/

[61] Cosmos Intro [online]. [cited 2022–04–09]. Available at:
https://cosmos.network/intro

[62] How Cosmos's IBC Works to Achieve Interoperability Between Blockchains [online]. [cited 2022–04–16]. Available at:
https://medium.com/@datachain/how-cosmoss-ibc-works-to-achieve-interoperability-between-blockchains-d3ee052fc8c3

[63] Cosmos Co-Founder Ethan Buchman on Building an Internet of Sovereign Blockchains [online]. [cited 2022–04–09]. Available at:
https://newsletter.thedefiant.io/p/-cosmos-co-founder-ethan-

buchman?token=eyJ1c2VyX2lkIjo0MjQ4NjI4MSwicG9zdF9pZCI6NTE2MDI0NzMsIl8iOiJPRWFuSiIsImlhdCI6MTY0OTU5NzY1OSwiZXhwIjoxNjQ5NjAxMjU5LCJpc3MiOiJwdWItMTEyNTkiLCJzdWIiOiJwb3N0LXJlYWN0aW9uIn0.XVs0ChRvk4t47R5UpRN7TY7evqyQVWM0Dvwmbs_Piyc&s=r

[64] BIRCH, Gavin. Inter-Blockchain Communication (IBC) is Coming to Cosmos [online]. [cited 2022–04–09]. Available at: https://www.figment.io/resources/inter-blockchain-communication-ibc-is-coming-to-cosmos

[65] ZARICK, Ryan. LayerZero- An Omnichain Interoperability Protocol [online]. [cited 2022–04–10]. Available at: https://medium.com/layerzero-official/layerzero-an-omnichain-interoperability-protocol-b43d2ae975b6

[66] ZARICK, Ryan; PELLEGRINO, Bryan; BANISTER, Caleb. LayerZero: Trustless Omnichain Interoperability Protocol [online]. [cited 2022–04–10]. Available at: https://arxiv.org/pdf/2110.13871.pdf

[67] ZARICK, Ryan. LayerZero Security Update — April 2022 [online]. [cited 2022–04–10]. Available at: https://medium.com/layerzero-official/layerzero-security-update-april-2022-4c27a22380b4

[68] Stargate Finance [online]. [cited 2022–04–10]. Available at: https://stargate.finance/

[69] QS World University Rankings 2022 [online]. [cited 2022–04–10]. Available at: https://www.topuniversities.com/university-rankings/world-university-rankings/2022

[70] Sergey Gorbunov [online]. [cited 2022–04–10]. Available at: https://scholar.google.com/citations?user=joZ7vIgAAAAJ&hl=en

[71] Ethan Buchman [online]. [cited 2022–04–10]. Available at: https://scholar.google.com/citations?user=bdovc6EAAAAJ&hl=en

[72] Axelar FAQ [online]. [cited 2022–04–10]. Available at: https://axelar.network/faq

[73] Axelar Network Documentation [online]. [cited 2022–04–10]. Available at: https://docs.axelar.dev/

[74] Axelar Network Bug Bounty [online]. [cited 2022–04–10]. Available at: https://immunefi.com/bounty/axelarnetwork/

[75] KIM, Christine. Tendermint Says Last Month's Cosmos Vulnerability Exposed Security Loophole [online]. [cited 2022–04–10]. Available at: https://www.coindesk.com/markets/2019/06/17/tendermint-says-last-months-cosmos-vulnerability-exposed-security-loophole/

[76] Final Security Audit Report [online]. [cited 2022–04–10]. Available at: https://leastauthority.com/static/publications/LeastAuthority-Cosmos-SDK-Audit-Report.pdf

[77] Cosmos-SDK Vulnerability Retrospective: Security Advisory Jackfruit, October 12, 2021 [online]. [cited 2022–04–10]. Available at: https://forum.cosmos.network/t/cosmos-sdk-vulnerability-retrospective-security-advisory-jackfruit-october-12-2021/5349

[78] Smart Contract Audit by Zokyo [online]. [cited 2022–04–10]. Available at: https://assets.website-files.com/5f99eb79d508ca853be5f2e8/619b7ccefe06e2014bd61ddf_Layer%20Zero%20SC%20Audit.pdf

[79] Smart Contract Security Audit Report [online]. [cited 2022–04–10]. Available at: https://github.com/LayerZero-Labs/LayerZero/blob/main/audit/SlowMist%20Audit%20Report%20-%20LayerZero-2022.03.15.pdf

[80] LayerZero Audit [online]. [cited 2022–04–10]. Available at: https://github.com/LayerZero-Labs/LayerZero/blob/main/audit/Ackee%20Audit%20Report%20-%20LayerZero-2022.03.15.pdf

[81] Rewards and Transaction Fees for the Axelar Network [online]. [cited 2022–04–11]. Available at: https://medium.com/@axelar-foundation/inflation-and-transaction-fees-on-the-axelar-network-d56ea9e2c142

[82] Cross-chain Transfer Fee [online]. [cited 2022–04–11]. Available at: https://docs.axelar.dev/resources/mainnet

[83] Satellite by Axelar [online]. [cited 2022–04–11]. Available at: https://satellite.money/

[84] Emeris [online]. [cited 2022–04–11]. Available at: https://app.emeris.com/

[85] Stargate Transfer [online]. [cited 2022–04–11]. Available at: https://stargate.finance/transfer

[86] Axelar Community [online]. [cited 2022–04–11]. Available at: https://axelar.network/community

[87] The Axelerator Multichain Grant Challenge: Build the Web3 Super App [online]. [cited 2022–04–11]. Available at: https://axelar.network/multichain-grant-axelerator-program

[88] The Cosmos Zones [online]. [cited 2022–04–11]. Available at: https://www.notion.so/Cosmos-Zones-map-85819147febb4eabb77137187642d1f7

[89] Technical Details of the Axelar Network [online]. [cited 2022–04–11]. Available at: https://axelar.academy/ecosystem/technical-details/

[90] The Technicals of Interoperability—Introducing the Ethereum Peg Zone [online]. [cited 2022–04–11]. Available at: https://blog.cosmos.network/the-internet-of-blockchains-how-cosmos-does-interoperability-starting-with-the-ethereum-peg-zone-8744d4d2bc3f

[91] ZARICK, Ryan. The Omnichain Future is Here [online]. [cited 2022–04–12]. Available at: https://medium.com/layerzero-official/the-omnichain-future-is-here-74389f6d70c3

[92] LEE, Josh. Why Interchain Accounts Change Everything for Cosmos Interoperability [online]. [cited 2022–04–12]. Available at: https://medium.com/layerzero-official/the-omnichain-future-is-here-74389f6d70c3

[93] GORBUNOV, Sergey. The Foundation of Cross-Chain Communication [online]. [cited 2022–04–15]. Available at: https://medium.com/axelar/the-foundation-of-cross-chain-communication-291f5a4f9879

[94] Economic and Fees [online]. [cited 2022–04–15]. Available at: https://layerzero.gitbook.io/docs/faq/ultra-light-node/economic-and-fees

[95] Protocol Fees [online]. [cited 2022–04–15]. Available at: https://stargateprotocol.gitbook.io/stargate/v/user-docs/tokenomics/protocol-fees

Appendix A

Acronyms

PoW Proof of Work

PoS Proof of Stake

dApps Decentralized applciations

SC Smart Contract

DeFi Decentralized Finance

TVL Total Value Locked

DEX Decentralized Exchange

TPS Transactions Per Second

AMM Automated Market Maker

LP Liquidity Provider

TradFi Traditional Finance

APR Annual Percentage Yield

LTV Loan To Value

IBC Inter-Blockchain Communication Protocol

NFT Non-fungible Token

CGP Cross-Chain Gateway Protocol

CTP Cross-chain Transfer Protocol

ULN Ultra Light Node

UA User Application

Appendix B

Contents of enclosed CD

`Kupka_Thesis.pdf` ..... the thesis text in PDF format