.

Router Chain: Tendermint-based Interop Layer

Vatsal Gupta, Abhishek Somani, Shubham Singh, Mankena Venkatesh

May 2023

Abstract

Over the past few years, we have witnessed web3 evolve from a novel innovation to an ethos defining the new era of computation and digital governance. The maturity of Ethereum's infrastructure and ecosystem fostered true innovation, which has paved the way for a variety of decentralized applications. However, increased adoption by users led to scalability issues, resulting in the emergence of multiple layer1 and layer2 networks. Trilemma design trade-offs in most of these solutions have been focused on reduced gas costs and improved throughput. While these new networks have played an essential role in onboarding new users to the DeFi ecosystem, their proliferation has resulted in the fragmentation of liquidity, user base, and activity across multiple networks. Due to these factors, interoperability is no longer a luxury; it is a requirement for any dApp seeking to capitalize on the subsequent adoption wave. Attempts have been made in the past to solve this problem by enabling communication across chains, but their usability is limited by a number of issues. Towards this end, this paper introduces the Router chain, an interoperability hub built at a crucial intersection of decentralization, scalability, and security. With an architecture enabling communication between various blockchain ecosystems - EVM & non-EVM, support for middleware contracts and application-specific bridging logic, provision for adding custom security measures, and a developer tooling suite facilitating continuous integration and development of cross-chain dApps, the Router chain will catalyze the growth of the cross-chain ecosystem.

Contents

Glossary

atomicity If an operation is atomic, it will either be seen as yet to be started or as completed and not in any partially completed state. In other words, either all the sub-operations in that operation will be successful, or none of them will be successful.

block headers The part of the block which includes all the metadata, including block height, block hash, the Merkle root of all the transactions included in the block, and the timestamp at which the block was mined, amongst other things. They act as a summary of the block.

blockchain trilemma The idea that finding the right balance between security, decentralization, and scalability is very hard in a blockchain.

composability The ability to use existing components and resources as building blocks for new applications.

layer 1 Base layer blockchain architecture, e.g., Bitcoin, Ethereum. In recent years, multiple layer 1 alternatives to Ethereum have come to the fore. Most of these blockchains have made certain changes to Ethereum's existing infrastructure, like introducing sharding or implementing a different consensus mechanism.

layer 2 Blockchain networks implemented as smart contracts on top of another blockchain (layer 1). Layer 2 networks do not make any changes to the underlying blockchain architecture. For example, layer 2 networks on Ethereum take advantage of Ethereum's decentralized security model while negating its scalability constraints by adding another layer of transactions on top of it. There are mainly three ways in which layer 2 scaling solutions are exercised - State Channels, Plasma, and Rollups. Popular examples of layer 2 blockchains include Polygon, Optimism, and Arbitrum.

Merkle root The hash of all the hashes of all the transactions included in a block. It is part of the block header.

multisig A special type of digital signature that requires two or more users to sign.

nonce A pseudo-random number that can only be used once. It is used by blockchains primarily as a counter.

oracles Data feeds that bring information from external sources and provide it to smart contracts on chain. Decentralized oracles play a significant role in any blockchain system since blockchains cannot access off-chain information on their own.

pseudo RNG Defined by the use of deterministic algorithms to generate random numbers.

siloed Refers to something that is isolated from other.

state proof A cryptographic proof delineating all the state changes that happened in a specific set of blocks.

stateful In the context of decentralized systems, a stateful entity is one that can maintain past data. Smart contracts are considered stateful because they can store data in the form of variables.

tendermint An open-source blockchain protocol that allows developers to build secure decentralized applications.

true RNG Defined by the use of external physical attributes such as radioactive decay, airwave static, and atmospheric noise, among others, to generate random numbers.

Web 3.0 Third generation of internet services built on top of decentralized data networks with the aim to make the internet more open and trustless.

Acronyms

ASM Additional Security Module.

BFT Byzantine Fault Tolerant.

ECDSA Elliptic Curve Digital Signature Algorithm.

EVM Ethereum Virtual Machine.

HTLCs Hash Time-Locked Contracts.

IBC Inter-Blockchain Communication Protocol.

PoA Proof of Authority.

PoS Proof of Stake.

RNG Random Number Generator.

SBT Soulbound Token.

1 Introduction

1.1 Background

It has been well established that the cornerstone of innovation is rooted in iteration as much as it is in invention. In 2008, Bitcoin's whitepaper [1], which was later abstracted to build the first blockchain network, was an instance of an inimitable invention. It challenged existing archaic institutions from their very foundations and provided a viable alternative to the traditional norms of transaction, computation, and communication. The evolution and subsequent maturity of the whole Web 3.0 ecosystem has been a process of iterative innovations. It has involved isolating the caveats of existing technical architecture and building viable products to address them. Bitcoin's technical restraints to build and run dApps gave birth to the Ethereum network. In turn, Ethereum's scalability constraints gave way to multiple layer 1 and layer 2 blockchains, each trying to carve out a niche for themselves by capitalizing on a core competency to onboard new applications and attract developers, users, and liquidity providers. A few of these blockchains have been able to achieve this goal by committing strategic trade-offs to balance the blockchain trilemma. While their developments have played a vital role in onboarding new users onto Web 3.0, it has also amplified a foundational quandary of a blockchain network. The absence of interoperability.

Up until now, every blockchain ecosystem has operated and matured in silos. A trait that gave them gravitas and catalyzed their initial usage is now becoming the primary factor for limiting their developer ecosystem and, subsequently, their user base. The time and effort required to explore various blockchain ecosystems impede most users from tapping into the benefits of different blockchains. Blockchain interoperability will, therefore, play a pivotal role in the holistic evolution of the Web 3.0 ecosystem and will subsequently facilitate the next wave of Web 3.0 adoption. It is no longer a cosmetic add-on feature that serves as a means to impress the end users. It has become a must-have - without a robust mechanism that extends the composability of DeFi and promotes communication among various blockchains, the success of current and upcoming L1s/L2s is a non-starter.

The self-evident and almost natural solution to the problem of blockchain interoperability is cross-chain bridges. Over the past few months, there has been a sudden influx of cross-chain bridges with varying capabilities - some only allow for the transfer of tokens, whereas some also provide support for message passing between independent platforms. And even though these bridges have made significant strides towards achieving an interoperable ecosystem, they suffer from varying issues that hamper their usability. From doubts about their security and decentralization to their inability to simplify cross-chain integrations, existing cross-chain platforms have often come short of the expectations placed upon them.

1.2 Intro to Sygnal Chain

To strike the perfect balance between security, decentralization, and scalability/throughput - we introduce a first-of-its-kind interoperability solution powered by a tendermint-based Router chain. A blockchain focused primarily on enabling state transitions across chains, the Router chain will sit as a hub between various EVM and non-EVM ecosystems. Features that set Router chain apart from other interoperability solutions include, but are not limited to:

1. **Support for middleware contracts:** Maintain states and implement custom business logic directly in the bridging layer.

2. **Plug-and-play for developers:** Sygnal has a transcendent open-source developer tooling suite to assist with the continuous integration and development of cross-chain dApps.

3. **CrossTalk:** Developers looking to build cross-chain applications without any custom bridging logic can leverage Sygnal's easy-to-integrate smart contract library, CrossTalk.

4. **Support for various kinds of use cases:** Batching, sequencing, and atomicity can be enforced directly from the Router chain.

5. **Flexibility:** Sygnal provides developers with the utmost flexibility over their bridging model (stateless or stateful), security model, and smart contract platform (EVM or CosmWasm):

6. **Data aggregation:** Contracts on the Router chain can serve as data aggregation modules for various cross-chain and multi-chain applications.

7. **Cross-chain meta transactions:** By leveraging Sygnal as their cross-chain infra provider, applications can enable gasless cross-chain transactions by delegating the execution of a request to a third-party service.

8. **Composability:** The Router chain will have inbuilt support for global applications such as oracles and liquidity pools/bridges, to name a few, which will help in easier integration of other applications.

1.3 Organization

In the sections that follow, we will first comprehend the shortcomings of the existing bridging technologies, followed by a deep dive into the Router chain's architecture, working, transfer flows, and security considerations. Following that, we'll explore the CrossTalk framework that abstracts Router chain's architecture into an easy-to-use smart contract library. Next, we will expand upon Sygnal's fee model for various flows, followed by a look into the features afforded by Sygnal. In drawing the paper to a close, we will briefly touch upon other facets that can be added to the Router chain in the future.

2 Existing Solutions

The problem of blockchain interoperability has become impossible to ignore as more siloed ecosystems emerge across the DeFi space. As mentioned above, to solve this issue, multiple bridging technologies have come to the fore in recent times. Based on the level of trust required, these solutions can be classified into three broad categories:

- **Trustless:** These systems do not require their users to place any trust in third-party actors.
- **Centralized Trust-based:** The system's control rests with a few external actors, and users must assume that they are not malicious.
- **Decentralized Trust-based:** The system is governed by an extensive network of third-party actors; users have to trust that the majority of them are not malicious.

Examples of trustless bridging technologies include Optimistic bridges, and light-client-based bridges, whereas PoA bridges come under the category of centralized trust-based bridges. Chain-based approaches fall into the third category, i.e., they follow a decentralized trust-based model. In this section, we will examine some of the widely deployed cross-chain technologies and their advantages/shortcomings.

2.1 Hash Time Locked Contracts (HTLCs)

One of the earliest models developed to enable cross-chain operations was Hash Time-Locked Contracts (HTLCs), which employs hash locks [2] and timelocks [3] to ensure that the operations remain atomic. Even though HTLC implementations differ across projects, the overall concept remains the same [4]. Let us understand the working of HTLCs using the following example:

Step 1: Alice hashes a secret code to obtain hash lock h_1. Alice also generates a timelock t_1 corresponding to an upper bound in which the hash lock can be unlocked.

Step 2: Alice uses these locks to create a smart contract c_a on chain A and locks her funds in that contract.

Step 3: Bob acknowledges that Alice has locked her funds.

Step 4: Bob uses the same hash lock h_1 and a different timelock t_2 to create a contract c_b on chain B. To ensure that Bob gets adequate time to claim funds from contract c_a, t_2 will be less than t_1.

Step 5: Alice unlocks Bob's funds from contract c_b thereby revealing the secret code.

Step 6: Bob uses the revealed secret to unlock Alice's funds from contract c_a on chain A.

Step 7: If the swap does not go through, Alice and Bob can claim their funds back once the timelock on the individual contracts expires.

One upside of using HTLC techniques is that they do not introduce any trust assumptions. However, they suffer from a range of issues that limits their efficacy:

- They require all the concerned parties to always be online. Both the sender and the receiver need to monitor the involved blockchains during execution actively.
- They are very slow and inefficient since every cross-chain swap requires a total of four transactions (two on each blockchain) [5].
- Given the high fees and waiting periods involved with HTLC-based swaps, the scalability of this approach is also a concern.

2.2 Proof of Authority (PoA) Bridges

Proof of Authority (PoA) bridges rely on a small set of outside actors that listen to events on the source chain, validate them, and relay them to the destination chain. Incentivization and slashing mechanisms are often kept in place to ensure the integrity of these actors. For the most part, PoA solutions work well -

- Since few validators are involved, the consensus can be achieved in very little time, ensuring a low-latency transfer of funds/messages.
- Adding support for new chains is straightforward - the validators can simply update their configuration to subscribe to events coming from the newly supported chain.

The only, albeit quite a significant, drawback of PoA bridges is that they are trust-based, not trustless. PoA bridges necessitate that their users place trust in a federation of third-party validators. Since the number of entities at play in a PoA system is relatively low compared to a Proof of Stake (PoS) system, there is a possibility of collusion; a dishonest majority of the authorities can manipulate the system to their advantage and to the detriment of the end user.

2.3 Light Client Node Approach

A light client can be defined as a smart contract that parses source chain block headers on the destination chain. Since a light client node maintains a record of historical block headers, it can verify that a particular event has indeed taken place on the source blockchain. In a light-client-based bridge, external actors named relayers forward events from the source chain to the destination chain, including block headers, state proofs, and other relevant data. Following this, the source chain's light client node on the destination chain cross-references its records to verify that a particular event was recorded on the source chain before executing a corresponding action on the destination chain. When compared to PoA bridges (Section 2.2), light-client-based bridges have two main advantages:

- There is no need to maintain a new validation layer [6].
- There are no trust assumptions - even though a third-party actor forwards an event from the source chain to the destination chain, light clients can independently validate the event's existence using the block headers it holds.

However, light-client-based approaches also suffer from a few issues:

1. **Light client nodes can be incredibly expensive to operate:** Due to the costs associated with executing gas-intensive validation logic, updating block headers is a costly affair, especially for light clients running on Ethereum [7]. To combat this, some bridges batch these block headers before relaying them to Ethereum, which can be problematic for time-sensitive applications. For example, Rainbow bridge, one of the most popular implementations of a light client node, batches Near block headers and sends them to Ethereum after a period of 12-16 hours. This can lead to long waiting times when bridging assets from Near to Ethereum.

2. **Adding a new chain to the mix is resource-intensive:** For every new chain, (a) a new light client has to be deployed on all the existing chains, and (b) light clients of all the existing chains need to be deployed on the new chain [8].

2.4 Ultra Light Client Node with Oracle-based Bridge Adaptors

To alleviate the concerns surrounding the costs involved in running a light client node, a few projects opt to replace a light client node with an ultra-light client node. An ultra-light client interface is similar to a light client node in that it also validates whether a transaction has been committed on the source chain. However, unlike a light client node, an ultra-light client node does not keep track of block headers; it cannot compute the transaction proof on its own - an external actor is required to forward the transaction proof. To prevent any single party from tampering with the block headers and transaction proofs to include a malicious transaction, the entity relaying the block headers and the entity relaying the transaction proof must be different. A prominent implementation of this approach uses an oracle to relay the block headers and a relayer to forward the transaction proofs.

Although such a model addresses the cost constraints of a light-client-based model, it introduces a new trust assumption - the oracle and the relayer will not collude. Although this problem is unlikely to arise while using reliable decentralized oracles, finding such oracles is not an easy task. In addition to this, as with light-client-based bridges, including a new chain into the mix can be quite challenging with this approach.

2.5 Relays/Sidechains

Another prominent strategy to achieve interoperability is based on relays/sidechains. Relays are abstractions (often a smart contract or a script) deployed on some chain A with light-client-like verification capabilities over chain B [9]. Sidechains, on the other hand, can be defined as independent blockchain networks that are connected to another blockchain, typically called a mainchain or a parent chain, via a two-way bridge. Their functioning is similar to that of relays in the sense that every sidechain can read and verify the information on the main chain. The block data is passed onto the sidechain for each new block appended to the main chain. The sidechain itself implements the standard verification mechanism of the mainchain's consensus algorithm and can therefore verify the block's validity. Cosmos and Polkadot are two of the most active projects using this technology to achieve cross-chain interoperability.

One issue with sidechain-based projects is that the inconsistency of consensus rates between different blockchains can impact the validity of cross-chain transactions. Another major drawback with sidechain implementations is that they typically have the ability to read and interpret data only from their parent chain or other sidechains connected to the parent chain, i.e., there is no support for communication with other blockchains.

2.6 Optimistic Bridges

Optimistic verification of cross-chain requests is another technique that has gained much traction in recent months. It is one of the more secure approaches to interoperability. Here is how optimistic bridges generally work:

Step 1: A user or an application posts data to a contract on the source chain.

Step 2: A third-party entity validates this data by signing a Merkle root containing the aforementioned data and committing it to the source chain. Some implementations of optimistic bridges require these entities to bond funds while signing the Merkle root. In the case of a fraudulent Merkle root, these funds are slashed.

Step 3: The root committed in the previous step is read by relayers and submitted to the destination chain.

Step 4: Following data submission to the destination chain, a challenge period starts wherein anyone watching the system can provide a fraud-proof and stop the transaction from going through.

Step 5: If no one flags the transaction as a fraud during the challenge period, the data is considered valid, and the transaction can be executed on the destination chain.

Optimistic bridges are considered trustless because they require only one honest node to watch the network to ensure no malicious activity occurs. However, the foundation of its core competency also gives rise to its most significant drawback - high latency. Any cross-chain request sent via an optimistic bridge cannot be executed with instant finality, i.e., applications/users will have to wait for the challenge period to end before their request is marked as completed. Such a solution is suboptimal for any user/application needing a low-latency solution, whether for asset transfer or a generic message transfer.

2.7 Existing Chain-based Approaches

To address the diverse variety of issues plaguing existing interoperability solutions, a few chain-based technologies have come forward in the past few months. Such solutions deploy a dedicated PoS blockchain that acts as a hub connecting various blockchains. During a cross-chain transaction, transactions mined on the source chain are validated on this hub chain by a dedicated network of validators. Following this, the transactions are relayed to the specified destination chain for the corresponding action.

Even though certain trust assumptions are involved in a chain-based interoperability solution, specifically on the chain's PoS validators, they have proved to be one of the most elegant interoperability solutions to date by finding a good balance between decentralization, security, and throughput. That being said, chain-based solutions have not been able to realize their full potential - the lack of support for a stateful middleware limits the features and use-case they can enable.

- **Application-level security and infrastructure-level security are tightly coupled:** Since dApps cannot deploy any middleware logic, they cannot enforce their own security mechanisms. All dApps have to rely on the underlying security mechanism of the blockchain.
- **No support for application-specific bridging logic:** Applications cannot persist any states in the middleware, limiting them from referring to historical information and implementing the "If this, then that" kind of logic in their applications.
- **Code redundancy:** The same business logic has to be implemented on contracts deployed across the chains.

3 Sygnal Chain

3.1 What is Sygnal Chain?

The Router chain is a layer 1 blockchain that leverages tendermint's Byzantine Fault Tolerant (BFT) consensus engine. As a Proof of Stake (PoS) blockchain, the Router chain is primarily run by a network of validators with economic incentives to act honestly. The Router chain is built using the Cosmos SDK and encapsulates all the features of Cosmos, including fast block times, robust security mechanisms, and, most importantly, CosmWasm - a security-first smart contract platform. In addition to CosmWasm, the Router chain also ships with Ethermint [10] - a Cosmos library with support for EVM smart contracts. By leveraging the CosmWasm and Ethermint toolkit, developers can start building secure blockchain applications on the Router chain from scratch or port their existing applications to the Router chain with minimal overhead.

In addition to its functionalities as a blockchain network, the Router chain provides an innovative solution to the problem of blockchain interoperability. Apart from validating state changes on the Router chain, validators running on the Router chain also monitor state changes on other chains. Applications on the Router chain can write custom logic to trigger events in response to these external state changes. Additionally, applications on the Router chain can leverage a trustless network of relayers to update states on external chains directly from the Router chain. Simply put, the Sygnal architecture allows contracts on one chain to interact with contracts on other chains in a secure and decentralized manner. More details regarding the Router chain and how it enables cross-chain communication are given in the following sections.

3.2 Characteristics

3.2.1 Decentralized Trust-based

With Sygnal, we chose a decentralized trust-based approach over a trustless approach due to the inability of the latter to support application-specific bridging logic, which would have restricted the types of applications that could be built using Sygnal. In the new approach, any cross-chain request initiated from a third-party chain has to go through the Router chain's tendermint-based PoS consensus mechanism. With multiple independent validators securing the network and a minimum validation requirement of two-thirds plus one vote (on the basis of voting power), the Router chain minimizes the amount of trust required by the user on the system. Furthermore, any validator having excessive downtime or engaging in any kind of malicious activity will be penalized by having a portion of their staked tokens slashed. This mechanism will ensure that validators have no economic incentive to carry out a malicious transaction or disregard a valid transaction.

Having said that, we recognize the need for some applications to have a trustless security layer. To that end, Sygnal ships with support for Additional Security Modules (ASMs), using which developers can add custom security measures like optimistic verification, m-out-of-n multisig, among others. More about this is given in Section 5.3.

3.2.2 Support for Middleware Contracts

One of the main characteristics of Sygnal is its ability to support middleware contracts. For the uninitiated, in the current interoperability setups, applications cannot enforce an "If this, then that" logic, as all transactions initiated on the source chain are routed to the destination chain as is. To add any application-specific bridging logic, applications must refactor their code and deploy it on multiple chains, which is both inconvenient and inefficient.

With Sygnal, applications can leverage the middleware contract capability to implement custom business logic directly in the bridging layer:

- Features such as batching, sequenced transactions, and atomicity can be enforced directly from the Router chain.
- With stateful middleware in place, case-based routing is possible.
- Limited code redundancy - no need to duplicate computation logic; only the final execution function needs to be deployed on all external chains.

3.2.3 Sygnal Chain as a Data Aggregation Layer

The Router chain can serve as the accounting and data aggregation layer for various cross-chain and multi-chain applications. For example, cross-chain governance can be carried out directly via a governance contract on the Router chain, which can allow users to create and vote on proposals. The contracts on the Router chain will serve as a cross-chain synchronizer to communicate data and voting results between other chains (Ethereum, Polygon, BSC, etc.) and the Router chain.

3.2.4 Multilayer Security

Applications building on the Router chain do not need to rely solely on the Router chain's security measures to secure their applications - applications can deploy and leverage a custom security layer on top of the infrastructure level security provided by the Router chain. For instance, before a cross-chain request is picked up by the relayer, an application can enforce an MPC-based or multisig verification of the incoming request on the middleware contract. In fact, applications can also implement custom security checks once the request reaches the destination chain. More about application-level security is given in Section 3.5.3.

3.2.5 Flexibility

As the cross-chain domain evolves further, new applications will come to the fore, each with a different set of requirements. In our endeavor to build a future-proof interoperability infrastructure, we provide

developers the utmost flexibility over their bridging model (stateless or stateful), security model, and smart contract platform (EVM or CosmWasm).

3.2.5.1 Support for Multiple Languages

The Router chain has native support for both the CosmWasm and EVM compiler to accommodate developers with varying degrees of experience and programming language preferences. As per their comfort, developers can build and deploy middleware contracts on Sygnal in Rust, Solidity, or Vyper.

3.2.5.2 Modular Security

Applications can implement their own security measures on top of the baseline security model provided by the Router chain. This security layer can be configured based on different parameters, such as the source chain, transfer value, and latency sensitivity. For example, an application can place a condition that transactions with a transfer value greater than $50,000 must be verified using an optimistic model. Applications can use this modular security mechanism to include additional safeguards and provide a more secure environment to their end users.

3.2.5.3 Infra-level Flexibility

With Sygnal, developers are not confined to a single type of bridging infrastructure. Depending on their requirements, they can build cross-chain applications using Sygnal's stateful infra (using middleware contracts) or stateless infra (CrossTalk framework).

3.2.6 Composability

Any infrastructure that encourages developers to build applications on top of it should be highly composable. Keeping that principle in mind, we have ensured that various out-of-the-box applications on the Router chain provide components and functionalities that developers can freely integrate into their applications.

3.2.6.1 Global Liquidity

Several use cases of a bridging solution, including but not limited to cross-chain staking, cross-chain prediction markets, and cross-chain lending/borrowing, depend directly on its ability to transfer funds across chains securely and efficiently. To that end, the Router chain ships with an inbuilt asset-swapping engine that acts as the gateway to the liquidity managed by Sygnal. Any application requiring access to Sygnal's fund transfer capabilities can tap into these liquidity pools to move funds.

Consider a project that wants to move funds from one chain to another along with an instruction to mint an NFT using the transferred funds. To do this, the application can create a sequenced request with two contract calls - the first call will unlock funds on the destination chain using Sygnal's asset transfer bridge, and the second call will take the unlocked funds and execute the function to mint the user-specified NFT on the destination chain. Additional details about Sygnal's asset-swapping capabilities will be unveiled in a separate paper, due to be published soon.

3.2.6.2 Oracles

One of the most critical requirements while building a dApp is that of a decentralized oracle - not just for price feeds of different assets, but for gas price estimation and other data feeds (based on application-specific use-case). To spare the developers from the painstaking process of sourcing and integrating reliable oracles, the Router chain will have a smart contract module that maintains multiple price feeds. This contract will fetch the price feed from reliable oracle providers, such as the Band Protocol, at regular time intervals.

3.2.6.3 Inter-Blockchain Communication Protocol (IBC)

IBC is a communication standard that allows applications built on any Cosmos-based chain to interact with each other. Since the Router chain is built using the Cosmos SDK, any application built on it can use IBC to interact directly with applications on other Cosmos blockchains like Injective, Osmosis, and others. This interaction can be a token transfer or an instruction transfer.

3.3 Message-passing Library (CrossTalk)

3.3.1 What is CrossTalk?

Sygnal's CrossTalk library is an extensible cross-chain framework that enables seamless state transitions across multiple chains. In simple terms, this library leverages Sygnal's infrastructure to allow contracts on one chain to pass instructions to contracts deployed on another chain. The library is structured in a way that it can be integrated seamlessly into your development environment to allow for cross-chain message passing without disturbing other parts of your product. CrossTalk supports both stateful and stateless bridging:

- **Stateless:** For dApps that do not require any custom bridging logic or any data aggregation layer in the middle, no middleware contract is required.
- **Stateful:** For cross-chain dApps that require custom bridging logic between any two chains, developers can build and deploy middleware contracts on the Router chain. All cross-chain requests originating from the dApp's source chain contract will come to this middleware contract, where some actions can be performed before they are forwarded to the intended destination chain.

3.3.2 Stateless CrossTalk Workflow

Now that we have a basic understanding of what the CrossTalk library is, let's examine the overall lifecycle of passing a cross-chain request via the Router chain and receiving an acknowledgment back on the source chain.

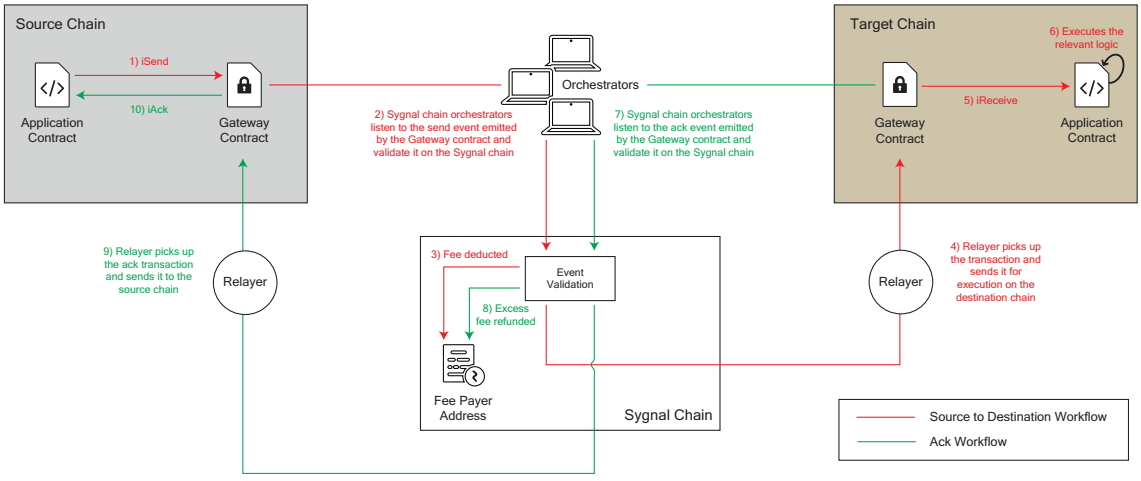

Figure 1: CrossTalk Workflow between Two External Chains

Step 1: **a)** A user initiates a cross-chain action on an application's smart contract on the source chain.

b) The application contract calls the `iSend()` function on the Sygnal Gateway contract.

Step 2: The Gateway contract on the source chain emits an event that is listened to by the orchestrators on the Router chain.

Step 3: Once the event is validated, the Router chain will deduct the fee from the `feePayerAddress` for that dApp on the Router chain. A dApp's fee payer is its designated entity on the Router chain that is responsible for paying the fees for all of its cross-chain requests. The `feePayerAddress` can be set by the dApp using the `setDappMetadata()` function on the Sygnal Gateway contract. More details about the fee payer are given in Section 4.1.

Step 4: Once the fee is deducted successfully, the relayers pick up the transaction signed by the orchestrator and forward the message to the destination chain's Sygnal Gateway contract.

In case the destination chain is not a third-party chain but the Router chain itself, the request is sent to the designated contract on the Router chain instead of being picked up by the relayers. Once the request is processed by the contract, it generates an acknowledgment which is validated by the orchestrators. Finally, the acknowledgment is sent back to the source chain.

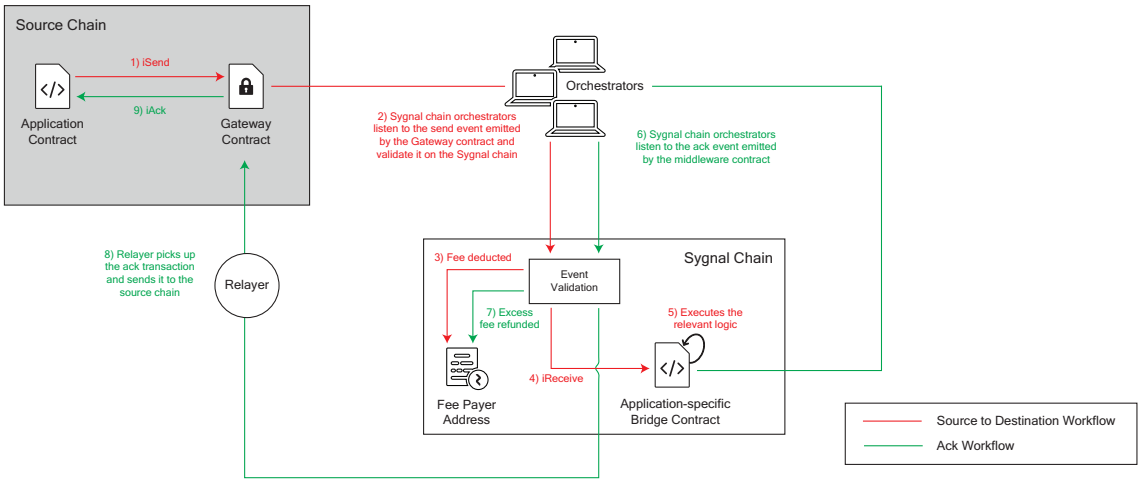

Figure 2: CrossTalk Workflow between an External Chain and the Sygnal Chain

Step 5: The Gateway contract on the destination chain calls the `iReceive()` function on the application contract on the destination chain.

Step 6: The application contract on the destination chain will take appropriate actions based on the data transferred.

Step 7: After the `iReceive()` function execution is complete on the destination chain, the destination chain's Gateway contract emits an acknowledgment event that is listened to by the orchestrators on the Router chain.

Step 8: Once the acknowledgment event is validated, it is processed on the Router chain, i.e., the cross-chain request corresponding to the ack is marked as completed and excess fee is paid back to the `feePayerAddress`.

Step 9: If the dApp had opted to receive the ack back on the source chain, the relayers send it to the source chain's Gateway contract. If not, it is discarded.

Step 10: The Gateway contract on the source chain sends the ack to the application's source chain contract.

Note: In case there is a need for application-specific bridging logic, applications can include a bridge contract on the Router chain (refer to Section 3.3.3 for the middleware workflow).

3.3.3 Stateful CrossTalk Workflow (Middleware Workflow)

Middleware workflow entails sending a request from an external source chain to an external destination chain via a middleware contract on the Router chain. This workflow consists of two legs: 1) a CrossTalk request from the source chain to the Router chain and 2) a CrossTalk request from the Router chain to the destination chain.

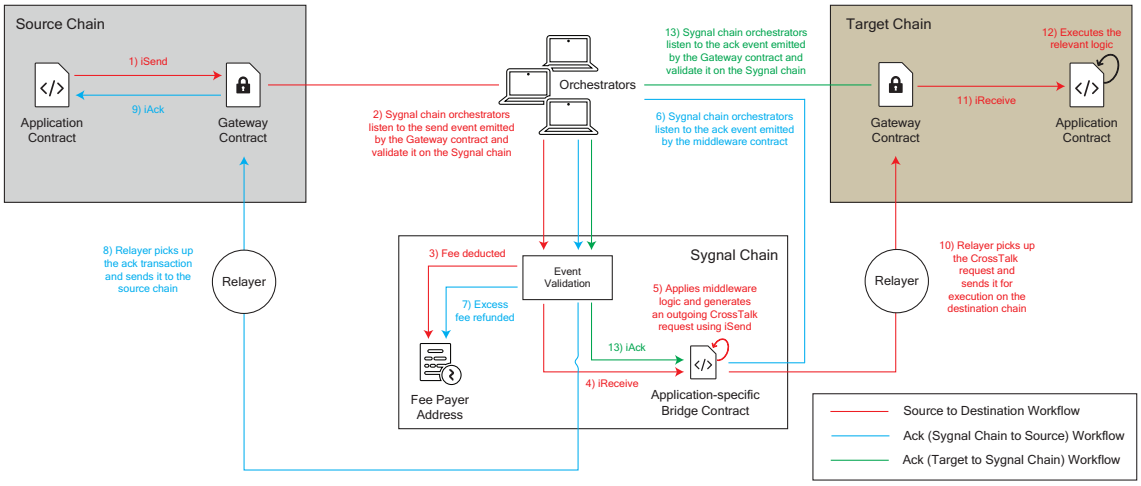

Figure 3: Workflow with Middleware Contracts

Note: Even though the steps in the figure are numbered sequentially, the ack workflow from the Router chain to the source chain happens parallelly with the Router chain to destination workflow.

3.3.4 Different Types of CrossTalk Requests

Now that we have an understanding of the CrossTalk workflow, let us take a look at the different types of requests that can be sent using CrossTalk. We will be categorizing the requests based on two different properties:

1) Number of Contract Calls

Depending on the number of contract calls present in a cross-chain request, a CrossTalk request can be categorized into two types:

- **Single-call Request:** A request that includes only one contract call for execution on the destination chain.
- **Multi-call Request:** A request that includes multiple contract calls for execution on the destination chain.

Consider an application that allows users to transfer their ERC20 tokens from one chain to another. If only one ERC20 token is being transferred, then the request will fall under the former category. However, if multiple tokens are transferred in a single request, it will be categorized as a multi-call request.

2) Acknowledgment Requirement

Depending on the need for an application to receive an acknowledgment for its request on the source chain, a CrossTalk request can be split into two types:

- **Requests Without Acknowledgment:** An acknowledgment is not required on the source chain after the request is executed on the destination chain.

- **Request With Acknowledgment:** If an acknowledgment is required on the source chain, developers need to specify whether they want an acknowledgment only in the case of a successful call, a failed call, or in both cases.

If an acknowledgment is anticipated on the source chain, an acknowledgment handler function with the relevant logic to handle the acknowledgment on the source chain has to be implemented by the application in their contract. If an acknowledgment is not anticipated, the acknowledgment handler function can be left empty, as it will never get invoked.

3.4 Architectural Components

3.4.1 Application Contracts

These are contracts deployed by applications on third-party chains and serve as the intermediary between end users of the application and the Sygnal cross-chain infra. In the lifecycle of a cross-chain transaction, these contracts are responsible for making the `iSend()` function call to the Gateway contracts on the source chain by passing the address of the bridge contract on the Router chain as well as the relevant payload. On the destination chain, application contracts will execute the instructions forwarded by the Gateway contract.

3.4.2 Gateway Contracts

As their name implies, Gateway contracts serve as the interface for application contracts to interact with Sygnal's bridging infrastructure. Gateway contract functions include:

- `iSend()` - The application contract on the source chain can call its corresponding bridge contract on the Router chain by invoking `iSend()` on the Gateway contract with the relevant parameters. Upon receiving this function call, the Gateway contract emits an event that is listened to by the Router chain orchestrators.
- `iReceive()` - The bridge contract on the Router chain can call its application contract on the destination chain by submitting an outbound request with the relevant parameters. Relayers will eventually submit the outbound request to the destination chain by invoking the `iReceive()` function on the Gateway contract, which will subsequently pass the payload to the destination contract.
- `setDappMetadata()` - To facilitate cross-chain transactions, a `feePayerAddress` needs to be set for paying the fees on the Router chain. This can be achieved using the `setDappMetadata()` function available in the Gateway contracts.

  Note: Once the `feePayerAddress` is set, the designated fee payer must approve the request to act as the fee payer on the Router chain. Without this approval, dApps will not be able to execute any cross-chain transactions.

3.4.3 Orchestrators

Sygnal orchestrators are entities that listen to incoming cross-chain requests from other chains, attest their validity, parse them into a unified format and post them on the Router chain. These attested requests can then be picked up by the relayers and forwarded to the destination chain. All validators must run an orchestrator instance to be a part of the Router chain ecosystem.

Working

At a high level, a Sygnal orchestrator works like a funnel that gathers events from various chains and posts them to the Router chain. To do so, an orchestrator uses a listener and dispatcher model wherein the listener module aggregates events while the dispatcher module forwards these events to the Router chain [11].

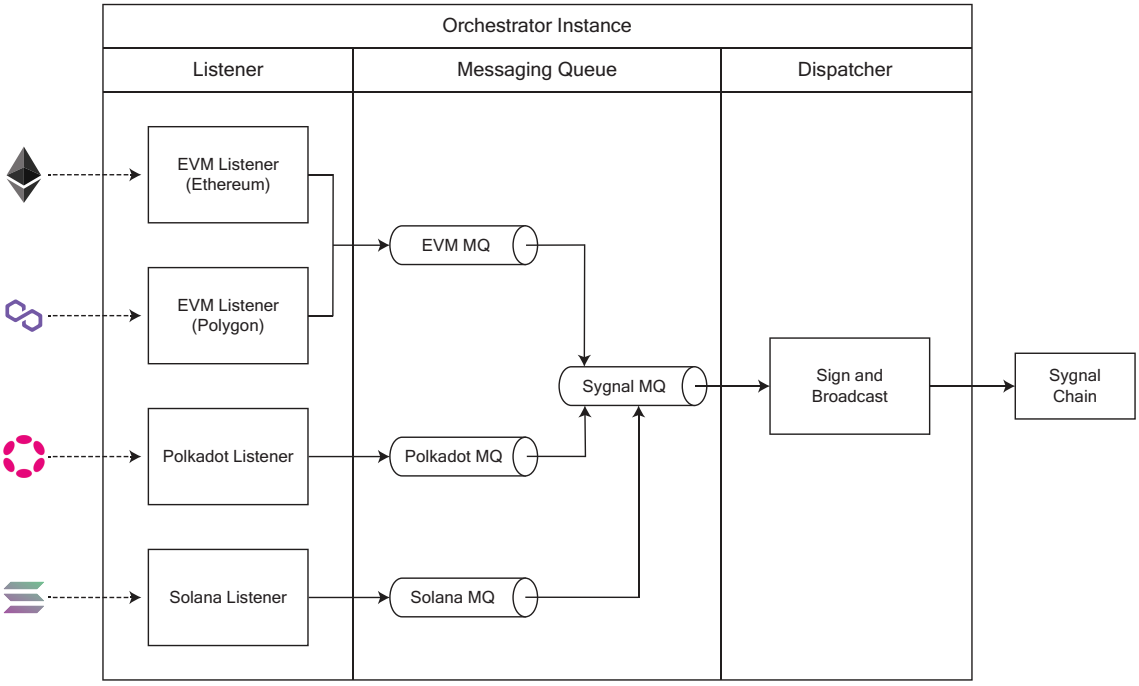

Figure 4: Orchestrator Architecture

- **Listener:** The listener module of an orchestrator listens to events emitted from specific chains based on the `chainType` parameter in the configuration provided to it. Listeners operate as threads (goroutines) under an orchestrator. All listeners subscribe to multiple types of events - a regular `iSend()` (cross-chain send) event, an `iRecieve()` (cross-chain receive) event, and an `iAck()` (acknowledgment) event. Once the listener module receives an event, it waits for the preconfigured amount of network confirmations (for example, three network confirmations for requests originating from Mumbai/Fuji) before parsing it into a message. Once the message is prepared, the listener adds it to a queue.
- **Queue:** The queue is used to store and deliver transformed messages to consumers (dispatchers) in a first-in-first-out manner while ensuring that duplicate messages are automatically discarded.
- **Dispatcher:** The dispatcher module is essentially responsible for streamlining the incoming requests by (a) listening to the queue, (b) signing the messages, and (c) broadcasting them to the Router chain.

Besides verifying the incoming requests to the Router chain, orchestrators also verify the outgoing requests from the Router chain.

3.4.4 Validator Set (Valset)

Each validator set consists of a nonce, a list of validators, and the height on the Router chain at which the valset is created. The validator set on the Router chain should be consistent across all the Gateway contracts.

Updating the Valset

Here is how the valset is updated on all the third-party chains:

Step 1: At the end of each block, the Router chain checks if the valset power has changed by more than 5%. If it has, the Router chain creates a new valset request.

Step 2: Orchestrators will query the chain for the latest valset request and confirm the new valset request by sending a `MsgValsetConfirm` tx.

Step 3: Once the $\frac{2}{3}+1$ majority has approved the new valset request, the relayer will pick the valset request and send the `updateValset()` contract call on all the Gateway contracts of all the configured chains in the Multichain module.

Step 4: The Gateway contracts will verify the signatures, replace the old valset with the new valset and emit a `ValsetUpdate` event.

Step 5: The orchestrators will listen to the `ValsetUpdate` event and submit a tx to the Router chain, confirming that the valset has been updated on all the chains.

Step 6: On receiving the confirmation from the $\frac{2}{3}+1$ majority, the Router chain will update the valset nonce in the Multichain module.

3.4.5 Multichain Module

The Multichain module persists the configuration of all the external chains supported by the Router chain and provides APIs to query the `ChainConfig`, which consists of the following:

- **chainID:** Network ID of the supported blockchain, for example, 1 for Ethereum mainnet, 137 for Polygon, etc.
- **chainName:** Name of the chain (Polygon, Ethereum, etc.)
- **symbol:** Native gas token symbol for the supported chain (ETH for Ethereum, MATIC for Polygon, etc.)
- **nativeDecimals:** Number of decimal places in supported by the chain's native token
- **chainType:** EVM, Cosmos, Solana, Polkadot, etc.
- **confirmationsRequired:** To make sure that the tx is finalized, the orchestrator has to wait for a specified number of network confirmations on each blockchain, which is determined by this parameter
- **gatewayContractAddress:** Sygnal Gateway contract address
- **gatewayContractHeight:** Sygnal Gateway contract deployment height
- **sygnalContractAddress:** SGN ERC20 contract address on the chain
- **lastObservedEventNonce:** Nonce of the latest event that was observed on the chain (initially, it will be set to zero)
- **lastObservedValsetNonce:** Nonce of the latest `ValsetUpdate` event (initially, it will be set to zero)

Adding a New Chain

To add a new chain in Sygnal's interoperability mesh, the following steps need to be followed:

Step 1: Deploy a Sygnal Gateway contract on the new chain with the current validator set.

Step 2: Create a chain integration governance proposal and send it to the Multichain module.

Step 3: If not already present, deploy a SGN token contract on the new chain.

Step 4: Once the governance proposal is passed, the requested chain config is added to the Multichain module.

3.4.6 Application-specific Bridge Contracts

The application-specific bridge contracts are middleware contracts deployed on the Router chain that include the logic required to process the incoming request from a third-party chain and generate an outoging request to another third-party blockchain. These contracts can be written in either Rust (compiled using CosmWasm) or Solidity (compiled using the EVM compiler provided by Ethermint).

To ensure that a faux contract doesn't execute any of the functions in these contracts, a bridge contract should always maintain a mapping of the `chainId` and addresses of all the application contracts (deployed on the third-party chains) that can execute its functions. Along with the payload, the Gateway contract will always pass the `msg.sender` parameter, which can be cross-referenced by the bridge contract to determine whether the source chain application contract is genuine or not.

3.4.7 Token and Gas Price Oracles

For a bridge contract to create and submit a cross-chain request from the Router chain to any external destination chain, it should be aware of the current gas price on the destination chain. Additionally, a bridge contract may require the price of any external chain's native gas token for internal calculations. To address this, we need oracles on the Router chain, which provides the token and gas prices of various chains.

3.4.7.1 Gas Price Oracle

The steps involved in querying gas prices and providing a generalized gas price oracle to the contracts on the Router chain are as follows:

Step 1: A simple microservice will be used to query the gas price on different chains and submit the same in the form of a transaction on the Router chain.

Step 2: The Router chain, upon receiving the gas prices from multiple providers, will take a median and update the oracle module state with the gas price.

Step 3: At any given time, application-specific bridge contracts can query the oracle module for the latest gas prices of external chains and pass the `gasLimit` parameter for the outbound request accordingly.

3.4.7.2 Token Price Oracle

Token prices of all the native tokens of all the chains in the Multichain module will be fetched from the Band Protocol via Cosmos' IBC. The system has been designed in a way that different types of providers can be supported in the long term. The steps involved in querying price feeds and providing a generalized token price oracle to the applications on the Router chain are as follows:

Step 1: At regular intervals, the Router chain will generate a Band IBC oracle request to the oracle module on the Router chain. The length of these intervals is decided using governance and added to the chain configuration.

Step 2: Upon receiving the request, the module will query the Band Protocol for the latest price feed of all the assets specified in the multichain module.

Step 3: Upon receiving the Band IBC price feed, the oracle module will update the latest price of the assets in its contract state.

Step 4: At any given time, any application can query the oracle module for the latest price feed of any chain's native asset. Upon receiving the request, the oracle module will return the most recent price of the specified asset from its contract state.

Note: In addition to the bridge contracts, the token price oracle is also used by the Router chain to estimate the outbound transaction fee in SGN tokens.

3.4.8 Relayers

Relayers are permissionless entities that relay executable proposals from the Router chain to a specific destination chain. The Router chain has a set of relayers operated by various third parties, which distributes the responsibility. In the set, each relayer listens to the Router chain and relays data to the destination chains as and when required. These relayers also carry out subsequent actions based on the events that have been transmitted.

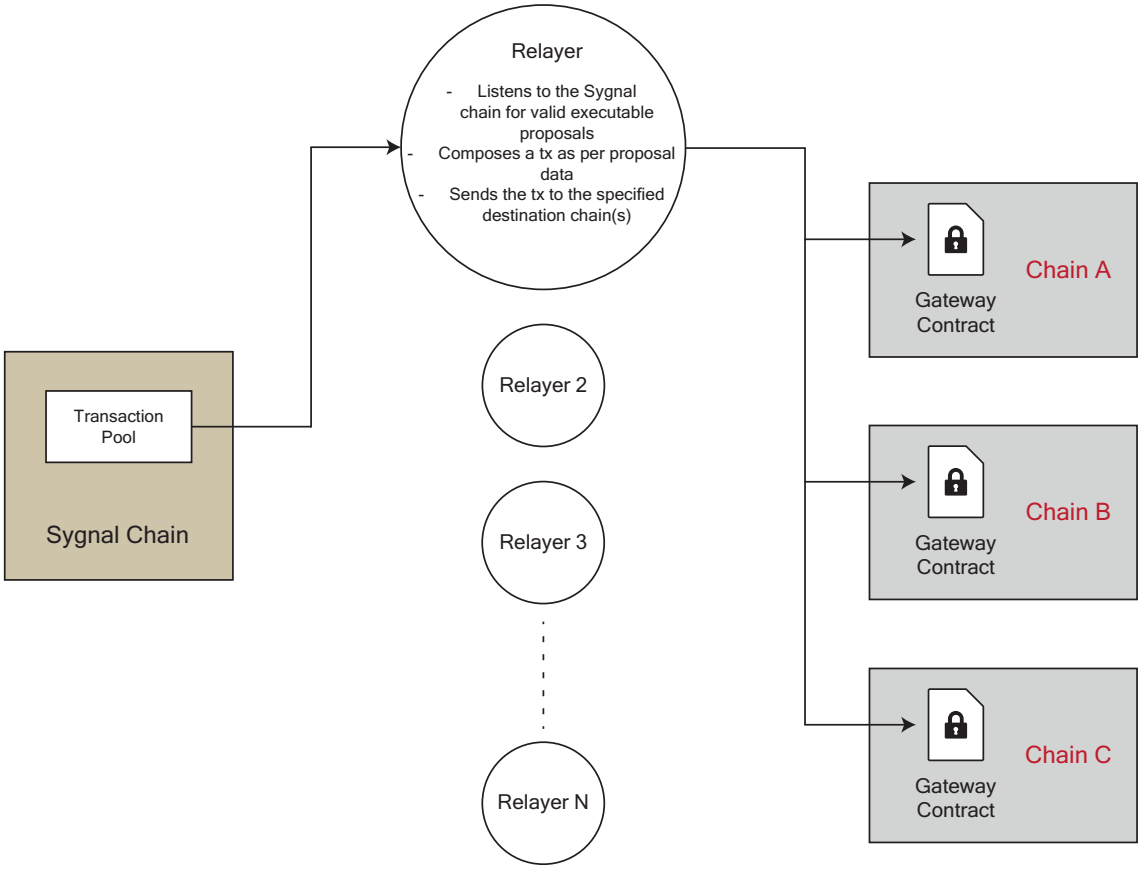

Figure 5: Relayer Functioning

Functionalities

1. The relayer will be able to submit cross-chain requests from the Router chain to other chains.
2. The relayer can choose to whitelist bridge contract addresses and process outgoing requests originating from only those addresses.
3. The relayer will be able to make a `updateValset()` call to all the Gateway contracts configured in the Multichain module.
4. The relayer will securely hold the private keys to wallets on different chains. These chains can be of distinct types, such as EVM, Cosmos, and Substrate, among others.

3.4.8.1 Working

Step 1: The listener interface of the relayer will listen to the transaction pool on the Router chain for unprocessed requests and add them to a tx queue.

Step 2: The processor interface of the relayer will fetch all the unprocessed requests from the tx queue.

Step 3: The relayer will transform the request into a defined message format where it queries the Router chain and fetches:

a) the current valset

b) payload from the request

c) signatures of validators who signed the request

Step 4: The relayer validates if the request has received $\frac{2}{3} + 1$ votes. If it has, it will estimate the gas price required to submit the request to the destination chain and check if sufficient gas price is provided by the bridge contract to execute the request.

Step 5: Finally, the request is relayed to the destination chain defined in the request.

Step 6: Once the request is successfully executed on the destination chain and an acknowledgment is received for the same, the relayer receives the fee it incurred in posting the tx on the destination chain and an additional fee on top of it.

3.4.8.2 Addressing Relayer Collisions

In some cases, multiple relayers may pick up the same request. To avoid collisions while submitting the transaction on the destination chain, relayers may choose to implement collision prevention strategies at their end. For example, relayers can include a specified time offset within their logic to ensure they wait for a certain amount of time before delivering the transaction to the destination chain. If another relayer submits the transaction within this time frame, they can simply discard it. Even if relayers do not implement any collision prevention strategy, no transaction that has already been executed will ever get replayed thanks to the event nonce-level validation done by the Sygnal Gateway contracts on the destination chain. The Gateway contracts always maintain a mapping of the most recent event nonce that has been executed. Since event nonces are incremental, if any request with an event nonce equal to or less than the mapped event nonce is received, it is ignored by the Gateway contract.

3.4.8.3 Addressing Scalability Constraints via the Use of Application-specific Relayers

Scaling issues might arise if we process the requests sequentially, i.e., in the order of event nonce. To address this, the Router chain's relay architecture allows for the parallel execution of requests. Since the relayer network is permissionless, each application can run its custom relayer to process its requests. This way, an outgoing request from one application bridge contract does not affect an outgoing request from another.

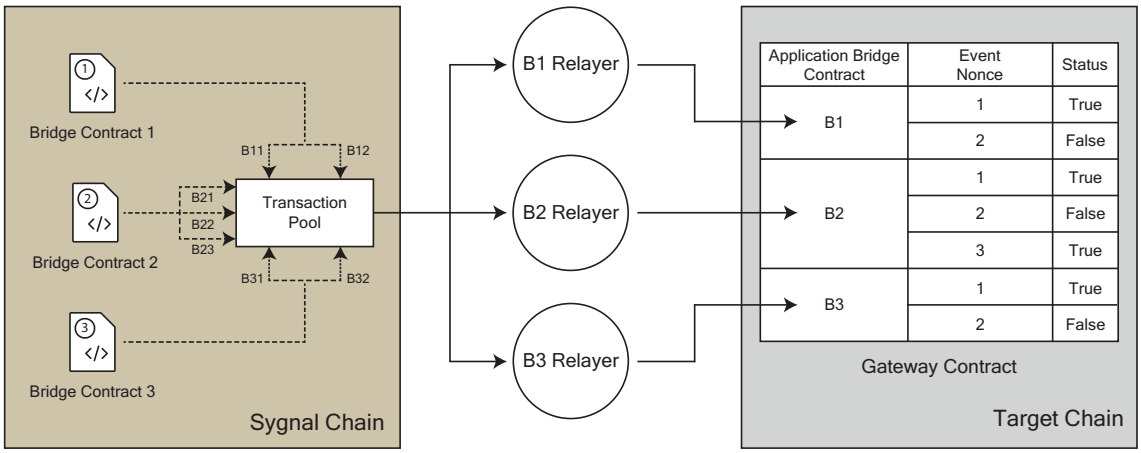

Figure 6: Improved Scalability using Application-specific Relayers

3.4.8.4 Gas Estimation

All relayers will need to run a `GasEstimator` module to estimate the gas price required to submit a request to the destination chain. If a third-party estimator service like Owlracle, Eth Gas Station, or others is available, the relayer will estimate the gas using that; if not, the relayer will estimate using an RPC endpoint.

3.4.8.5 Trustlessness

To ensure that the data forwarded by the relayer is not tampered with, the Gateway contract on the destination chain decodes the signed call data to verify the validator signatures. Upon ensuring the authenticity of the request, the call data is executed.

3.4.8.6 Manual Relaying using Sygnal's Web Relayer

Web relayer is a user interface provided by the Sygnal team using which a tx payload can be manually relayed on the destination chain.

- If anyone wants faster execution for their request on the destination side, they can manually increase the gas price and perform the tx from their wallets using the web relayer.
- Transactions stuck on the Router chain for any reason can be replayed using the web relayer.

3.5 Network Security

3.5.1 Infrastructure-level Security

Security is an essential aspect of any blockchain network. The Router chain derives its security from its underlying tendermint consensus engine.

Decentralized Network of Validators

For any block to be mined, $\frac{2}{3} + 1$ validators by voting power will be required to achieve consensus, meaning the network can only be compromised if validators holding a combined voting power of more than 67% decide to collude and engage in malicious activities.

PoS Economics

Any node having excessive downtime or engaging in any kind of malicious activity will be penalized by having a portion of its staked tokens slashed. This mechanism will ensure that the validator nodes have no economic incentive to carry out a malicious transaction. Moreover, all validators who are properly aligned with the network will be eligible for a portion of the block rewards. More about the validator economics will be disclosed in the subsequent versions of this paper.

Byzantine Fault Tolerance

The Router chain can tolerate up to $\frac{1}{3}$ of its validator nodes being faulty. This includes both inactive nodes and malicious nodes.

ED25519 Signature Scheme

All communication between the Router chain validators is secured by ED25519 [12], an elliptic curve-based encryption scheme [13], considered one of the fastest and most secure authentication mechanisms.

Decentralized Governance

Any updates on the Sygnal blockchain will be made after a governance decision undertaken by the community.

3.5.2 Bridge-level Security

Any cross-chain request from an external chain to the Router chain undergoes a validation process wherein the orchestrators attest to the presence of the request's corresponding source chain transaction. Similarly, before an outgoing request from the Router chain is picked up by a relayer, the orchestrators verify if the event's corresponding transaction on the Router chain has been mined. For signing the attestations during the validation, the orchestrators use the Elliptic Curve Digital Signature Algorithm (ECDSA) [14].

3.5.3 Application-level Security

3.5.3.1 On Sygnal Chain

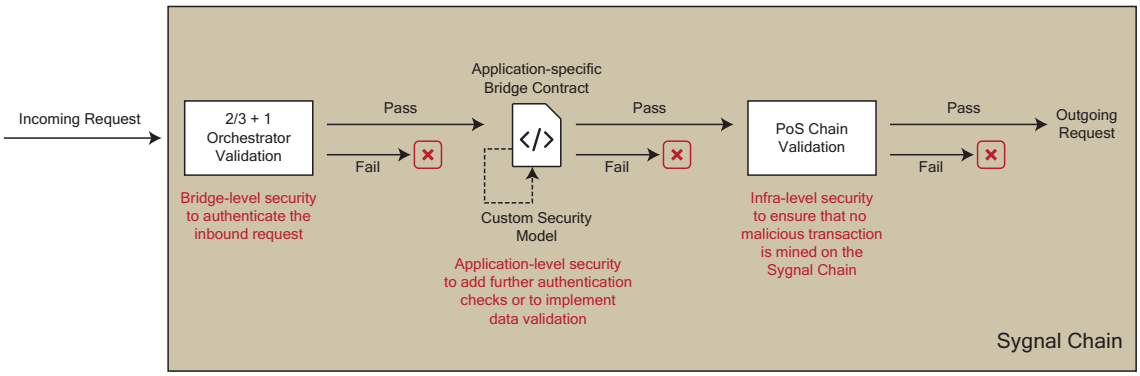

Figure 7: Multilayer Security on the Sygnal Chain

The Router chain provides generic message-passing bridge security - it ensures that the data reaching the destination chain is authentic, i.e., the data/instruction generated by the application on the source chain reaches unaltered to the destination chain. However, to add another layer of security - whether to check the validity of the data or to have an additional authenticity check, applications can put in smart contract-level checks like having their own validators sign the contract on the Router chain before the data is forwarded to the destination chain.

Additionally, applications can design and implement their custom governance strategies to handle updates to the application. In fact, due to the ability of Router chain contracts to change the state of contracts deployed on external chains, the governance decisions taken on the Router chain can be broadcasted and executed on other chains.

3.5.3.2 On Destination Chain

For developers who do not wish to implement application-level checks on the Router chain itself or who are looking to leverage Sygnal's CrossTalk framework instead of the middleware flow, we have introduced the concept of an Additional Security Module (ASM). Akin to Hyperlane's Sovereign Consensus [15], this module layer enables applications to incorporate their own security standards, such as an m-out-of-n multisig or a fraud-proof-based authentication model (optimistic approach), among others. More details about Sygnal's ASM feature are given in Section 5.3.

4 Fee Management

4.1 Fee Payer Considerations

The fee associated with any cross-chain request initiated by a dApp is paid by the dApp's corresponding fee payer account on the Router chain. This fee payer account is set by the dApp for all the integrated chains and can be changed anytime. Any fee refunds are also credited to this account.

- To designate the fee payer for any chain or to modify the fee payer address, the application must invoke the `setDappMetadata()` function on that chain's Gateway contract and provide a valid address on the Router chain.
- To prevent unauthorized usage of someone else's address as the fee payer, the designated fee payer address must perform a fee payer approval transaction on the Router chain.
- The approval as a fee payer can be provided by accessing the explorer.

4.2 Gas Considerations

- The gas price for the execution of incoming cross-chain transactions on the Router chain is decided via governance and included directly in the chain configuration.
- To ensure the proper execution of CrossTalk requests on the destination chain, users must specify the gas price and gas limit in their request metadata. This information is used to calculate the fees required for the transaction. If the gas price is not specified, the gas price oracle on the Router chain will estimate it.
- While exercising the option to run their own relayer, applications might want to leave the task of gas limit estimation to the relayers. In such a scenario, they can pass the gas limit as 0.

4.3 Incoming Request Fee Structure

To execute an incoming request on the Router chain, users are required to configure a `gasLimit` parameter in their request metadata. This `gasLimit` is multiplied by the `gasPrice` present in the Router chain configuration to calculate the amount of SYGNAL tokens to be deducted from the user-specified `feePayerAddress`. This fee is used to cover the cost of transaction execution (bridge contract call) on the Router chain. Note that if your fee payer does not have sufficient SGN balance, the transaction will not be executed. Since the `feePayerAddress` cannot be changed once set, you will have to top up the `feePayerAddress` to ensure the execution of your request.

4.4 Outgoing Request Fee Structure

The bridge contract must pass reasonable `gasPrice` and `gasLimit` parameters to cover the cost of executing any outgoing cross-chain request on the destination chain. Once the Router chain receives the outgoing request, it queries the oracle module for the latest price of the SGN token and the native gas token of the specified destination chain. It uses the gas price fetched using the gas price oracle, and the token prices fetched using the token price oracle to convert the gas cost involved in the execution of the outgoing request from the destination chain native token to the SGN token.

4.5 CrossTalk Fee Structure

CrossTalk works on a prepaid fee model. Upon receiving a CrossTalk request, the Router chain will calculate the estimated fee for executing the transaction on the destination chain in terms of SGN and deduct the fee plus incentive from the `feePayerAddress` upfront.

```
EstimatedFeeInSGN = EstimatedFeeInDestNativeToken * PriceRatio
```

where:

```
EstimatedFeeInDestNativeToken = DestGasLimit * GasPriceInDestNativeToken
```

```
PriceRatio = DestNativeTokenPrice / SGNTokenPrice
```

4.6 Other Fee Considerations

- Fee and relayer incentive for any cross-chain request on Sygnal have to be paid in SGN tokens only.
- To prevent Sybil attacks on the Router chain, Sygnal's Gateway contract on the source chain charges a minimal fee from the application contract to cover the cost of orchestrator validation. This fee is paid in the source chain's native token.

4.7 Handling Refunds

Once the Router chain receives the acknowledgment generated by the destination chain's Gateway contract, it (a) pays the fee used along with the relayer incentive to the relayer from the already deducted fee, and (b) refunds the surplus fee back to the `feePayerAddress`. This mechanism ensures the following:

- The relayers receive their incentive automatically without any delay.
- The applications can send extra gas limit as a buffer since they will get automatic refunds in case of a surplus fee.

5 Features

5.1 Cross-chain Meta Transactions

With Sygnal, we are coming up with a first-of-its-kind cross-chain meta-transaction capability. As mentioned in the previous sections, the fee for any application's cross-chain request is deducted from that application's `feePayerAddress`. Applications can use this feature to delegate the execution of cross-chain requests to a third-party service and enable feeless cross-chain transactions for their end users.

5.2 Decentralized Cross-chain Read Requests

One of the most underrated, albeit important, aspects of blockchain interoperability is being able to read the state of contracts present on one chain (say chain A) from a different chain (say chain B). A good example of this could be a Soulbound Token (SBT). Let us assume that every user gets a SBT on chain A, which contains the user's Date of Birth (DoB) information. This information can come in handy for multiple dApps that want to restrict users below a particular age. Creating this SBT on multiple chains will not make sense, but having the information of the SBT across multiple chains is essential for dApps to be able to access this information and use it. To achieve this, applications can use Sygnal to generate a decentralized read request between two chains. This request will include (a) the contract state to read on the destination chain (in this case, the user's age) and (b) the operation to be performed when the data is received back on the source chain (in this case, it could be to accept/deny user's request to access a gambling application). More details in regards to generating, sending, and handling a cross-chain read request are given in our documentation.

5.3 Additional Security Modules

Security is all-important in a cross-chain infrastructure. As a PoS network built on Tendermint, the Router chain's baseline security model is one of the most robust. However, at Sygnal, we believe that applications leveraging our infrastructure should be able to implement their own safeguards on top of our baseline model if they so require. In fact, we have already alluded to the fact that a modular security mechanism is one of the core facets of Sygnal. Applications utilizing Sygnal's middleware flow can already take advantage of this option by coding custom security logic on their Router chain contracts.

As noted in Section 3.5.3.2, we also provide a customizable security layer on external chains in the form of Additional Security Modules (ASMs). Integrating an ASM can enhance a dApp's ability to

mitigate potential security threats at an application level and maintain the overall system's security. We support a few modules out of the box, but developers are free to add their own implementations. This can include security measures such as a waiting period similar to optimistic roll-ups, rate-limiting, or other relevant features that can be seamlessly integrated into the dApp to provide an additional layer of protection.

When to Use an ASM?

There are no fixed criteria that applications need to satisfy to implement an ASM. Applications can choose to configure additional security measures based on various parameters:

1. **Type of call:** Applications might not want an additional security layer for a read request. However, for a cross-chain write, an application might require a few further checks.
2. **Source chain:** An application might want higher security for transactions originating from specific chains.
3. **Transfer value:** In case of asset transfers, or sequenced asset and instruction transfers, an application might want to place additional safeguards if the ticket size of the transfer is above a certain threshold.
4. **Latency sensitivity:** For transactions that need to be executed in a low-latency environment, applications can impose a timestamp check by adding a custom module that reverts a transaction if the transaction is not received within the expected duration.

How Does an ASM Work?

- An ASM can be added to a chain's Gateway contract via the `verifyCrossChainRequest()` function. This function returns a boolean value, based on which the Gateway contract decides whether to proceed with the transaction request or not.
- When the function returns `true`, the request is deemed valid, and the Gateway contract proceeds with its execution. Conversely, if the function returns `false` due to transaction tampering or any other issue, the request is rejected, and an acknowledgment is sent back to the Router chain for the same.
- In case the request to the ASM module reverts, the transaction call to the Gateway contract will also be reverted, and no state changes will be recorded on the Gateway contract. As a result, relayers can try to execute the request again since there will be no changes in the Gateway contract's state. However, the Gateway contract will not execute the request until the ASM implementation returns either `true` or `false`. Once the request is executed, an acknowledgment event will be generated to convey this information.
- These functions can be called by the Sygnal Gateway contract only. Developers have to integrate these functions with the same selector in their ASM module implementation.

5.4 Transaction Batching

Transaction batching can help a lot of applications cut costs for their cross-chain operations. Depending on the requirement of the application, Sygnal can be asked to execute batches of transactions either directly on the Router chain or on the destination chains.

5.4.1 Batching at the Sygnal Chain

Sygnal enables applications to batch and execute transactions directly on the Router chain. Consider a scenario wherein users want to mint an NFT on Polygon from various chains. We can aggregate users' requests from different chains on the bridge contract, i.e., collate all the requests in a single payload and then execute that call when a certain number of requests are received. This kind of system will save costs involved in (a) executing individual transactions on the Router chain and (b) relaying separate

transactions to the destination chain, in this case, Polygon. The entire step-by-step flow of batched cross-chain NFT minting can be found in Appendix B.

5.4.2 Batching at the Destination Chain

For executing a transaction batch on the destination chain(s), the bridge contract will create and send a `BatchRequests`, an array of `BatchRequest`, to the Router chain. Note that destination chain based batching can be of two types:

a) single-chain batching, wherein all transactions in a batch need to be executed on the same destination chain, and

b) multi-chain batching, wherein batches within the `BatchRequests` array can span multiple destination chains.

Single-chain Batching

In the case of single-chain batching, the `BatchRequests` array contains a single `BatchRequest` that contains all the cross-chain transactions to be executed on the same destination chain. In this case, transactions are, by default, executed in the order in which they are specified. The Router chain will create an `OutgoingBatchTx` for the `BatchRequest`, which eventually gets signed by orchestrators and broadcasted to the Gateway contract by a relayer. The `BatchRequest` will consist of an array of `ContractCalls` - an object consisting of `DestinationContractAddress` and `Payload`.

Multi-chain Batching

In multi-chain batching, the `BatchRequests` array consists of multiple `BatchRequest` arrays, each of which has to be executed on separate destination chains. Multi-chain batching can further be divided into two categories:

1) Ordered multi-chain batching: All batches need to be executed in sequential order.

2) Unordered multi-chain batching: Batches can be executed in any order.

For the latter, the relayer will broadcast all the batches in a `BatchRequests` array simultaneously to the respective destination chains. All the transactions within each batch will be executed sequentially as per the single-chain batching mechanism. For the former, however, applications will have to enforce it using the bridge contract on the Router chain -

Step 1: The bridge contract submits the first batch request to the Router chain.

Step 2: Router chain sends the batch request to the designated destination chain.

Step 3: The bridge contract receives an acknowledgment for its request.

Step 4: Upon receiving the ack, the bridge contract submits the next batch request to the Router chain. Steps 2, 3, and 4 can be repeated until all the batches are processed.

To make it easier for the bridge contract to handle acknowledgments, the Router chain will assign a `BatchNonce` whenever the bridge contract submits a `BatchRequests`. Eventually, when the bridge contract receives an ack, it can correlate the ack with the previously submitted request using the `BatchNonce`.

5.5 Batch Atomicity

Sygnal ensures atomic batch delivery, i.e., it ensures atomicity across multiple transactions in a batch to save users from the overhead of deploying wrapper contracts to handle multiple function requests. It is important to note that atomicity can only be ensured for batches submitted to a single destination. Whenever the Gateway contract on a chain receives a batch request, it verifies the signatures and executes all the contract calls in the batch. If any of the contract calls fail, the Gateway contract will revert, thereby ensuring atomicity.

If, in case, you want non-atomic execution of a batch's contract calls, you can deploy a proxy contract on the destination chain. In this case, the Gateway contract will execute the request via the proxy contract and errors arising in any of the contract calls will be handled on the proxy contract to ensure that the transaction doesn't get reverted and all the remaining calls are executed.

5.6 MetaMask Compatibility

Unlike most chains built using the Cosmos SDK, the Router chain will have full-fledged support for MetaMask, one of the most popular non-custodial crypto wallets. This means that users will be able to:

a) Add the Router chain to the list of networks on their MetaMask wallet.

b) Import their Router chain assets and balances to their MetaMask wallet.

c) Review transaction details, including tx data, gas price, and gas limit, and sign transactions directly from their MetaMask wallet while connected to the Router chain.

6 Future Work

6.1 Interoperability with Private Blockchains

Recent years have witnessed increased adoption of private blockchains across various sectors - e-commerce, healthcare, logistics, insurance, and financial services. The proliferation of private blockchains has been accompanied by growing concerns regarding their security. Due to the presence of fewer nodes, private blockchains can be more easily compromised compared to public blockchains. To mitigate this risk, we are planning to build a decentralized communication channel between public and private blockchains on top of the Router chain. Such a channel will allow private blockchains to commit their state proofs onto a public blockchain and thereby leverage the security guarantees of large public blockchains.

6.2 Providing Instant Finality for Transactions on Optimistic Blockchains

To solve for Ethereum's scalability constraints, various optimistic rollups have come to the fore. They seek to minimize transaction costs by batching various blocks of transactions before committing them on Ethereum. Once a batch gets committed on Ethereum, it must go through a challenge period before it can be considered valid. While this challenge period goes on, activities on the optimistic rollup can continue. However, if anyone generates and submits a valid fraud-proof during the challenge period, then the state of the entire optimistic rollup gets rolled back to the state that existed before the fraudulent batch was committed on Ethereum.

Since optimistic rollups, by design, do not have a way to achieve instant finality, there is always a theoretical possibility of transactions getting rolled back. This can be particularly problematic in cases where the optimistic rollup is part of a cross-chain transaction. Imagine a scenario wherein a user sends some funds from an optimistic rollup, Optimism, to another blockchain, Avalanche. Once the transaction is mined on Optimism, the bridge deducts funds from the user's wallet on Optimism and credits them to the user's wallet on Avalanche. Let us assume that after a few hours, someone found and proved that one of the transactions preceding this transaction was fraudulent. Now, Optimism will be rolled back to a state wherein the user's funds are not deducted on Optimism, but since Avalanche has not been rolled back - the user also has funds on Avalanche.

To solve the problem of instant finality for cross-chain contract calls, we will use the Router chain to provide the proof of validity of the rollup chain state committed to Ethereum. The validators of the Router chain will run a verifier of the Optimistic rollup chain. The verifier will construct the state root of the Optimistic rollup batch offline and compare it with the state root of the batch submitted to Ethereum. If the state root matches, the validators will submit an attestation to the Router chain with the batch state root. Once $\frac{2}{3} + 1$ majority of validators attest the state root, it's added to the Router chain state. Following this, an outbound transaction consisting of the attested state root gets relayed to the Gateway contract on Ethereum, thereby providing instant proof of validity. As the validators

have verified the state root already, it is guaranteed that a fraud-proof against the batch will not be created. The dApps on the Ethereum chain can query the Gateway contract for the attested state root and instantly proceed with the contract call rather than waiting for the challenge period.

6.3 Decoupling Validators and Orchestrators

In the future, Sygnal validators will be distinct entities from the Sygnal orchestrators. With this model, an orchestrator won't be required to act as a Sygnal validator, thereby loosening the technical requirements and allowing for greater participation. Sygnal orchestrators will be responsible for listening to events from third-party chains or specific contracts on third-party chains, validating these events, providing their signatures, and securely transmitting them to the Router chain. On the other hand, the primary role of Sygnal validators will involve proposing blocks and voting on them, ensuring the integrity and consensus of the Router chain.

6.4 Dual Mode Operation

In the future, we envision a dual-mode operation for Sygnal, allowing projects to choose between **Permissioned Mode** and **Permissionless Mode** based on their specific requirements.

- **Permissioned Mode:** To join Sygnal's interoperability network using this mode, projects will have to pass the Sygnal governance. However, once approved, they don't need to worry about a dedicated orchestrator set to listen to their transactions. By default, any validators operated by the internal team will run an orchestrator instance for all the chains integrated via the permissioned mode. Besides, Sygnal's validator set will also be highly incentivized to run an orchestrator instance for chains integrated via this mode. This approach ensures a high level of security, making it suitable for projects seeking enhanced reliability and protection.
- **Permissionless Mode:** To cater to more diverse and agile projects, permissionless mode enables blockchain projects to add their chain or application to Sygnal without the need to pass the governance poll. However, in return, they will be responsible for running their own orchestrators. This mode empowers projects with greater autonomy and quicker onboarding, ideal for experimental, niche, or rapidly evolving use cases.

6.5 Leveraging Shared Staking

Borrowing design principles from the EigenLayer model, in the future, we will allow participants to use the SGN token staked on the Router chain to act as an orchestrator for multiple chains. Much like a form of leverage, this approach allows participants to earn rewards across all the chains they support while sharing the responsibility for any malicious activity across those chains. In the event of malicious activity on any one chain, the stakeholder's tokens will be slashed across all the supported chains, thereby increasing accountability and security.

In the later stages of implementation, we envision expanding the staking options to include different native tokens. This will enable a broader range of participants and projects to engage with the Sygnal's ecosystem. However, we will implement a carefully designed governance process to maintain network integrity and avoid potential risks associated with the staking of random tokens. The governance mechanism will ensure that only reliable and credible native tokens can be used for staking, mitigating potential vulnerabilities while promoting inclusivity and diversity.

6.6 Automated Triggers/Scheduler-as-a-Service

One of the most critical features of the Router chain, once implemented, will be the inclusion of a scheduling service that will allow for the automatic execution of specified contract functions without the need for an external entity to trigger that event. To the best of our knowledge, no other blockchain provides an inbuilt service for the time-based or condition-based triggering of contract functions without needing a custom Web 2.0 service. Various use cases can be realized by leveraging this scheduler. For example, a bridge contract on the Router chain listening to external price feeds can trigger a buy/sell function if the price of the monitored token moves above or falls below a certain threshold.

6.7 Random Number Generator

In the past few years, randomness has proved to be a key ingredient in multiple Web 3.0 disciplines, ranging from Play-to-Earn games to forms of gambling like prediction markets. Given the intricate mathematics involved, a majority of these applications currently have to build their own randomness source from the ground up, leading to additional overhead. To solve this problem, Sygnal will ship with support for a Random Number Generator (RNG), which is cryptographically secure and can be easily integrated by any dApp on the Router chain. Since a True RNG cannot be established on a blockchain, we will devise a Pseudo RNG that will accept one or more initial values as input, perform mathematical operations on it, and produce pseudo-random determinism sequences as output.

7 Concluding Remarks

As it is with other domains, users are all-important in Web 3.0. As more and more blockchains come up, the user base gets fragmented across them. Even after much innovation in the blockchain interoperability space, cross-chain applications have been unable to make the most of their potential due to the issues plaguing the current crop of cross-chain solutions. Even though low latency, high security, and complete decentralization are necessary conditions in a cross-chain infrastructure, they are insufficient to combat the current problem. To get the most out of the current applications, what is needed, it seems, is an infrastructure that allows applications to apply custom bridging logic. Towards this end, in Sygnal, we are leveraging the Router chain - a Cosmos-based blockchain with an environment supporting the development and execution of CosmWasm smart contracts, as a hub-chain to provide a highly customizable cross-chain infrastructure. This new infrastructure will enable a new wave of dApps to take advantage of cross-chain composability.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`, Dec 2008. Accessed: 2022-08-01.

[2] Hashlock. `https://en.bitcoin.it/wiki/Hashlock`, 2015.

[3] Timelock. `https://en.bitcoin.it/wiki/Timelock`, 2016.

[4] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. A survey on blockchain interoperability: Past, present, and future trends. *arXiv preprint arXiv:2005.14282*, 2020.

[5] Alexei Zamyatin, Dominik Harz, Joshua Lind, Panayiotis Panayiotou, Arthur Gervais, and William Knottenbelt. Xclaim: Trustless, interoperable, cryptocurrency-backed assets. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 193–210, 2019.

[6] HashHub Research. Explaining the structure and types of blockchain bridges. `https://mirror.xyz/0x8Df126302a7EA75E7013Ec8Ad6bFaC14DD84a5fF/Cxa5L18eGjr8y08VkELx9m61-yl1-h-oTT2z7SjNhuo`, Feb 2022.

[7] Rick Delaney. Blockchain bridges explained — how crosschain messaging protocols work. `https://www.okx.com/academy/en/blockchain-bridges-explained-how-crosschain-messaging-protocols-work#Decentralized-or-trust-minimized-bridges`, Mar 2022.

[8] Dmitriy Berenzon. Blockchain bridges: Building networks of cryptonetworks. `https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8`, Sep 2021.

[9] Léonard LYS, Arthur Micoulet, and Maria Potop-Butucaru. R-SWAP: Relay based atomic cross-chain swap protocol. Research report, Sorbonne Université, April 2021.

[10] Chainsafe Systems. Ethermint Documentation. `https://docs.ethermint.zone/`. Accessed: 2023-05-08.

[11] Billy Rennekamp. Gravity Bridge. https://github.com/cosmos/gravity-bridge. Accessed: 2022-01-13.

[12] Interchain Foundation. Secure P2P. https://docs.tendermint.com/v0.33/tendermint-core/secure-p2p.html. Accessed: 2022-11-16.

[13] Daniel J Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 124–142. Springer, 2011.

[14] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1):36–63, 2001.

[15] Hyperlane Team. Sovereign Consensus. https://docs.hyperlane.xyz/docs/protocol/sovereign-consensus. Accessed: 2022-02-08.

Appendices

A Redelegation Mechanism for Failed Requests

When the Router chain tries to execute a request on the Router chain, the request may fail to execute on the middleware contract for various reasons. As the corresponding source chain action has already taken place, there should be a way to allow the applications to try and execute the failed request again. The Router chain has a redelegation mechanism to enable this functionality for failed requests. Anyone can trigger this mechanism by sending a `redelegate` transaction to the Router chain. However, unlike the standard execution flow, the middleware contract won't pay the fee for executing the stuck request. Instead, the sender of the `redelegate` transaction will have to pay the fee for executing the request on the middleware contract.

B Batched Cross-chain NFT Minting via the Sygnal Chain

Step 1: A user calls the NFT contract for a cross-chain mint and buy. The NFT contract takes the funds from the user's account and deposits them in the contract. The amount of funds to be taken is already set on the source contract based on the NFT minting price. The application contract then calls the `iSend()` function on the Sygnal Gateway contract with the relevant parameters.

Step 2: The Sygnal Gateway contract emits an event that is listened to by the orchestrators on the Router chain.

Step 3: After validating the event and deducting the fee for the incoming request, the Router chain passes the event to the application's Router chain bridge contract.

Step 4: Upon receiving the cross-chain mint and buy request, the bridge contract will store the request and increment the value of a counter by 1. Every time, after incrementing the counter, the bridge contract will check if it has received the required number of requests (say N). If not, it will do nothing further. If it has, the bridge contract will parse the payload of all the stored requests into a single payload with all the user addresses and generate an outgoing request for minting N NFTs on the destination chain.

Step 5: After the transaction initiated by the bridge contract is mined on the Router chain, the orchestrators verify the transaction's corresponding outgoing request.

Step 6: Once verified, a relayer picks the request and forwards it to the Gateway contract on the destination chain.

Step 7: The Gateway contract on the destination chain calls the NFT contract on the destination chain.

Step 8: The NFT contract on the destination chain mints the NFTs on the destination chain to all the user addresses specified in the payload.