Concero Cross-Chain Messaging V2: A Dual-Layer Security Framework for Trustless Cross-Chain Communication

Oleg Kron[1], Andy Bohutsky[1], Nikita Gruzdev[1], Phuc Le[1]

[1]Concero Labs

21 April 2025 **(v1.0)**

Abstract

Concero Messaging V2 presents a decentralised framework for trustless cross-chain communication, combining cryptographic verification with economic security mechanisms. Our protocol eliminates centralised trust assumptions through a dual-layer security architecture: a decentralised compute layer using Chainlink Functions to generate cryptographic proofs of message validity, and a self-regulating economic layer leveraging Symbiotic's restaking infrastructure to enforce operator accountability. Cryptographic proofs ensure message integrity through multi-node verification, while economic incentives align participant behavior through stake-weighted rewards and automated slashing for malicious actors. This design prevents single points of failure while maintaining constant-time transaction confirmation without centralised coordination. Its modular design allows seamless integration with emerging decentralised verification protocols, supporting flexible security configurations tailored to application needs.

The trustless architecture decouples message propagation from validation, allowing any participant to relay transactions while ensuring cryptographic proof verification comes before transaction release. As a result, Concero Messaging V2 establishes a foundation for secure cross-chain applications without centralised intermediaries. This dual-layer approach establishes a new standard for blockchain interoperability, demonstrating that hybrid security models can deliver both scalability and strong trust guarantees, and paving the way for the next generation of cross-chain applications.

Contents

1 Introduction

Blockchain technology has revolutionised the way digital information is recorded and transferred, spawning entire ecosystems where decentralisation and trustless interactions are paramount [9]. However, as blockchain adoption increases, the diversity of networks, each with its own consensus mechanism and data model, has led to a fragmentation that poses significant challenges for inter-chain communication. Cross-chain messaging—vital for bridging isolated blockchain silos—faces substantial hurdles in achieving both security and scalability while remaining truly decentralised and trustless [11].

The problem of cross-chain messaging lies in reconciling the need for rapid, efficient communication between heterogeneous networks with the strict security guarantees demanded by financial and application-layer protocols. Traditional approaches to chain interoperability have primarily relied on either pure cryptographic techniques or economic security models. Pure cryptographic methods offer robust data integrity through cryptographic proofs and consensus-driven validation, yet they often incur high computational and infrastructural costs, making them less viable for large-scale, real-time applications. On the other hand, purely economic security systems leverage incentive-driven mechanisms such as staking and slashing to curb malicious behavior, but these models can be susceptible to centralisation risks and typically require significant capital backing to function effectively [10].

The current landscape of blockchain interoperability is typified by disparate solutions that often trade off security for speed, or vice versa [11]. Many existing protocols suffer from limitations imposed by the scalability versus security dilemma, where designs optimised for one attribute accidentally compromise another [7]. For example, protocols that depend solely on cryptographic verification tend to struggle with scalability due to the excessive computational resources required for multi-node verification. Conversely, systems that overly depend on economic incentives may experience delays associated with capital lock-up requirements, grace periods for slashing, or vulnerability to coordinated attacks by economically powerful actors. In contrast, the modular design of Concero Messaging V2 allows for the decoupling of message propagation from value settlement. This separation not only streamlines operational efficiency but also permits independent optimisation of the messaging and security layers, thereby achieving both fast transaction confirmation and high security without compromising decentralisation. The modularity of our design further supports adaptability: as emerging decentralised verification protocols come to the fore, the framework can seamlessly integrate these innovations without significant restructuring [12].

Concero Messaging V2 addresses these intertwined issues by adopting a hybrid, dual-layer security framework that synthesises the strengths of both paradigms. At its core, our design utilises a decentralised compute layer—employing Chainlink Functions—to generate cryptographic proofs that unequivocally attest to the validity and integrity of cross-chain messages. This cryptographic layer is complemented by a self-regulating economic security layer, which leverages Symbiotic's restaking infrastructure to enforce strict operator accountability through stake-weighted incentives and automated slashing mechanisms. By integrating these two layers, the protocol ensures that even if one mechanism faces temporary weaknesses, the overall system remains robust and resistant to compromise.

A key principle of this hybrid architecture is decentralisation. Rather than relying on a single point of trust or control, Concero Messaging V2 decentralises both validation and

incentive distribution through the use of dynamically managed operator cohorts. These cohorts are designed to prevent any single entity from gaining disproportionate influence over message verification, thereby reducing the risk of relayer centralisation. Each operator within a cohort participates in a two-phase consensus process that begins with the cryptographic verification of messages, followed by an economic validation that ensures operators are financially motivated to act in the system's best interest. In doing so, the framework eliminates centralised trust assumptions and distributes responsibilities evenly across a wide network of nodes, thereby enhancing the overall resilience and trustlessness of the protocol.

Furthermore, the dual-layer security architecture of our protocol addresses critical challenges inherent in existing cross-chain messaging systems. The cryptographic layer ensures that every message is verified through redundant, multi-node consensus, making it computationally infeasible for an adversary to forge or tamper with data without detection. Simultaneously, the economic security layer provides real-time financial incentives to all participants, ensuring that any deviation from honest behaviour is immediately disincentivised through automated slashing mechanisms. This combined mechanism establishes a balanced and self-correcting environment in which the cost of malicious behaviour far exceeds potential gains, thereby fostering a truly trustless ecosystem.

In summary, Concero Messaging V2 represents a significant advancement in cross-chain communication by resolving long-standing tensions between scalability, security, and decentralisation. By merging cryptographic verification with a self-enforcing economic security model, the protocol not only overcomes the inherent limitations of single-approach systems but also lays the foundation for a new era of trustless, decentralised interoperability. This introduction sets the stage for a detailed exploration of the technical architecture, security mechanisms, economic models, and future enhancements that together enable Concero Messaging V2 to address the critical needs of a rapidly evolving multi-chain ecosystem, and accelerate the future of chain unification.

2 Technical Architecture

2.1 System Components

The architectural framework of Concero Messaging V2 is modular and designed to harmonise both cryptographic and economic security mechanisms (Figure. 1). At the heart of the system are the ConceroRouter contracts, which manage and direct the flow of cross-chain messages between disparate blockchain networks. These contracts are complemented by Chainlink Functions, a decentralised compute layer that generates verifiable cryptographic proofs to ensure message integrity. Reinforcing this cryptographic assurance, the Symbiotic contracts implement a robust economic security layer by managing staking, restaking, and automated slashing to hold operators accountable. Symbiotic Relayer nodes, operating off-chain, facilitate the efficient propagation of messages while maintaining decentralisation and redundancy. This cohesive assembly of components promotes a trustless, resilient, and scalable cross-chain communication framework.

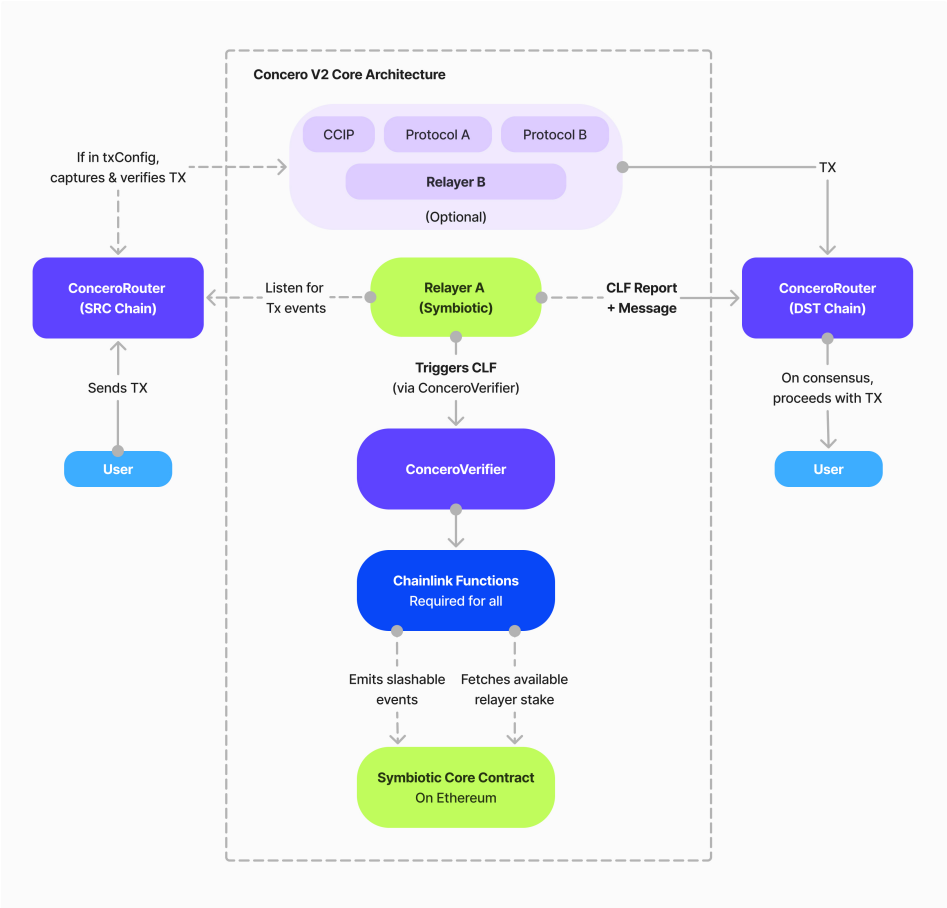

Figure 1: Concero Messaging V2 Architecture. It employs a multi-layered architecture that integrates four key components: ConceroRouter contracts that handle cross-chain message routing and verification, Chainlink Functions for decentralised computation and validation, Symbiotic contracts for economic security, and relayer nodes for efficient message transmission between blockchain networks.

ConceroRouter Contracts ConceroRouter contracts constitute the primary interface on every blockchain network supported by Concero Messaging V2, serving as the single entry point for all end-user interactions with the protocol. These contracts are tasked with several core functions essential to the secure and efficient operation of the system. Firstly, upon receiving an incoming message from an end user, the ConceroRouter contract emits a corresponding event. This event acts as a trigger for off-chain relayer nodes, which pick it up and process the message in line with its specific transaction configuration.

Subsequently, the ConceroRouter contract undertakes the verification of incoming messages. Depending on the message configuration, this verification may involve reaching a consensus among authorised verifying networks. Alternatively, a Chainlink Functions report may be used as the single source of truth, ensuring that the message has been duly recorded on the source chain using cryptographic proofs. Once decoded and verified, the ConceroRouter contract on the destination chain then releases the outbound message.

Chainlink Functions Chainlink Functions is a serverless developer platform that enables smart contracts to access off-chain data and perform custom computations in a decentralised, trust-minimised manner [12, 4]. It works by allowing developers to send requests containing JavaScript code from their smart contracts to a Decentralised Oracle Network (DON) [12, 13]. Each node in the DON independently executes the code in a serverless environment, fetching data from APIs and performing calculations as specified [12]. The DON then uses the Chainlink Offchain Reporting (OCR) protocol to aggregate the results from all nodes, reaching a consensus on the final output [2]. This aggregated result is then sent back to the requesting smart contract via a callback function, where it can be used for further on-chain operations [2, 3].

Thanks to this advanced architecture, Concero V2 employs Chainlink Functions as its trust-minimised decentralised compute infrastructure to facilitate essential cross-chain verification operations. Its primary function is to verify transaction presence on source chains. This verification process follows a systematic workflow: when computation results are finalised, the DON nodes form a consensus-based report which is individually signed by each node operator of the DON, making the data in the report verifiable and tamper-proof. Inside the report, there is a list of allowed operators which the ConceroRouter can receive messages from, eliminating the need for a regularly updated list of operators, as it can directly take the operator information from the report itself, which cannot be tampered with. This cryptographically secured report is transmitted back to the initiating contract. The report then undergoes a specific routing process, where Relayer A captures the verification data and forwards it to the ConceroRouter on the destination chain.

This computation layer operates through a carefully structured process, where computational requests originate from ConceroVerifier. ConceroVerifier is deployed on the master network, currently Arbitrum One (subject to change depending on the needs of the protocol). The actual computation executes across four independent nodes within the DON, ensuring decentralised verification of cross-chain transactions.

ConceroVerifier serves as the central governance and security hub for the protocol's verification operations. Beyond initiating computational requests, it manages crucial protocol functions, including operator registration and stake tracking. Through this contract, the protocol can maintain a registry of authorised operators, track their delegated stake amounts, and enforce compliance with network rules through potential slashing actions when necessary.

The integration of Chainlink Functions into Concero V2's architecture establishes a reliable verification mechanism that bridges the gap between source and destination chains. By leveraging the decentralised nature of the DON and its four-node computation model, the system maintains high security standards while enabling efficient cross-chain communication.

Symbiotic Contracts Symbiotic is an innovative shared security protocol designed to provide flexible and permissionless restaking for decentralised networks [6, 8]. It functions as a thin coordination layer that allows network developers to have complete control over their restaking implementation and operator set [6]. The protocol works by enabling users to deposit their assets into vaults, which are managed by curators who control stake allocation and delegate to qualified operators running network infrastructure [5]. These operators can then opt into networks and utilise the delegated collateral for validation, supporting network operations and earning rewards that are distributed back to the users [6]. Symbiotic's modular architecture supports various assets as collateral and allows

networks to independently manage their restaking mechanisms, choose operators, and set specific rules for rewards and slashing [14, 1]. This flexibility, combined with its immutable core contracts, creates a secure, efficient, and scalable ecosystem for shared security across multiple blockchain networks and decentralised applications [14, 1].

In Concero V2, Symbiotic contracts form the economic security foundation, ensuring the integrity of network operations. These contracts implement a comprehensive system for monitoring operator behaviour and enforcing protocol compliance through economic incentives and penalties. The primary objective is to maintain network security by creating financial stakes that align operator interests with protocol requirements.

The implementation of Symbiotic contracts follows a cost-efficient architecture, with core contracts deployed on the Ethereum network. This design minimises state changes to reduce operational costs while maintaining robust security measures. Since the Symbiotic restaking contracts are deployed on Ethereum, the on-chain Concero V2 interactions with Symbiotic are reduced exclusively to slashing requests, making the integration as cost-efficient as possible and leaving zero cost footprint on the protocol during normal operations. During standard operations, the system primarily performs state reads to verify operator credentials and stake requirements. These verification processes confirm two essential aspects: the operator's registration status and the adequacy of their delegated stake for performing specific actions.

The protocol's economic security model operates through a state management system that activates only during critical events. State modifications occur exclusively during slashable events, when the protocol must penalise malicious or non-compliant behaviour. This selective approach to state changes significantly reduces gas costs while maintaining the protocol's ability to enforce security measures effectively. By limiting state modifications to essential security operations, the system achieves an optimal balance between operational efficiency and robust security enforcement.

Symbiotic Relayer Nodes Concero V2 implements a dual-relayer architecture that combines mandatory and optional relayer nodes to facilitate cross-chain communication. This system comprises two distinct types of relayers, each serving specific functions within the protocol's message transmission framework.

The primary component, Relayer A, serves as the mandatory infrastructure element essential for Concero V2's core operations. This relayer performs three critical functions in the message transmission process. First, it monitors and captures events from ConceroRouter contracts. Second, it initiates confirmation processes through the ConceroVerifier, which operates on the master chain to generate verification reports. Third, it maintains continuous surveillance of the ConceroVerifier for new report emissions, processing these reports through decoding operations before transmitting them to the appropriate destination chain ConceroRouter contracts.

Complementing the primary relayer, Relayer B operates as an optional component that enhances the protocol's consensus mechanisms. This secondary relayer captures events from source chains and facilitates their transmission to destination chains, working in conjunction with Chainlink Functions reports and other network validations. The optional nature of Relayer B provides developers with flexibility in implementing additional security measures based on their specific requirements and risk assessments, and allows developers to freely create different use cases.

2.2 Message Types and Transaction Flow

Concero V2 handles two distinct message types through a streamlined dual-layer system. Relayer A transmits messages to the master chain and delivers verification reports to destination ConceroRouters. Chainlink Functions then acts as the verification layer, examining source chain transactions and generating cryptographically secure reports.

This architecture provides efficient message transmission with robust security validation across all supported chains. Additional security layers can be implemented based on specific application requirements.

Message Type	Focus	Additional Relayer Requirements
Non-value bearing messages	Speed, Costs	None
Value-bearing messages	Security, Speed, Costs	Additional Relayer B recommended

Table 1: Message Types and Transaction Flow

2.2.1 Non-value bearing messages

Non-value bearing messages in Concero V2 are designed to prioritise transaction speed and cost efficiency. Since these messages do not involve asset transfers, they require minimal verification overhead, enabling rapid cross-chain communication while maintaining essential security measures.

The message processing workflow follows a systematic sequence that ensures reliable message transmission (Figure. 2). Initially, an end-user initiates the process by sending a message to the source chain router contract. Upon message reception, Relayer A detects the event emission from the source chain router contract. The relayer then forwards this message to the Master Chain to obtain verification through Chainlink Functions.

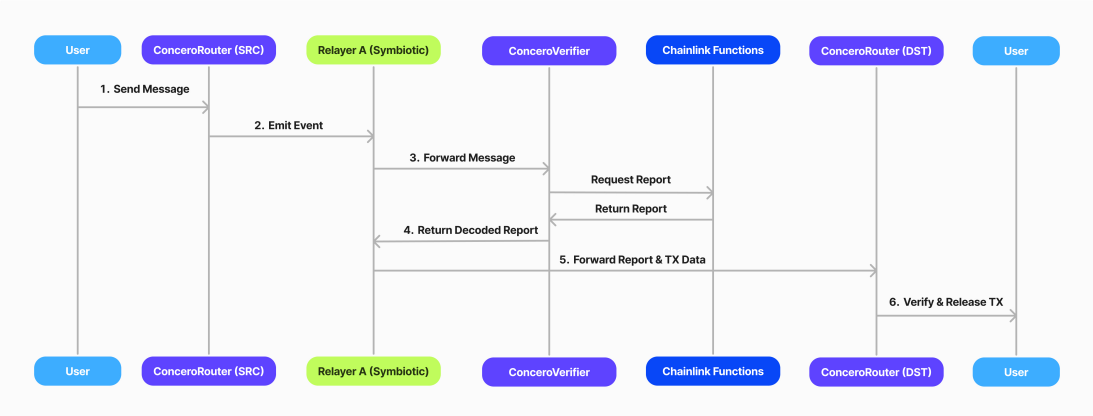

Figure 2: Non-Value Bearing Message Flow in Concero V2

After processing the message, Chainlink Functions generates a verification report which is returned to the Chainlink Functions-enabled Master Chain. Relayer A captures and decodes this report, subsequently transmitting both the report and transaction data to the destination chain router contract. The final verification occurs at the destination

chain router contract, which authenticates the report's origin from Chainlink Functions node operators and verifies its integrity. Upon successful verification, the contract releases the transaction, completing the message transmission process.

2.2.2 Value bearing messages

Value-bearing messages represent transactions where the protocol cannot definitively determine if value unlocking will occur at the integrator level. For these cases, Concero V2 recommends implementing an optional additional security layer through Relayer B verification, which operates in conjunction with the Chainlink Functions report to establish destination chain router consensus.

The transaction workflow follows a comprehensive seven-stage process that ensures complete verification and security (Figure. 3). Initially, the end-user initiates the process by transmitting a message to the source chain router contract. Upon receipt, the source chain router contract emits an event that triggers simultaneous responses from both Relayer A and Relayer B, initiating parallel verification paths.

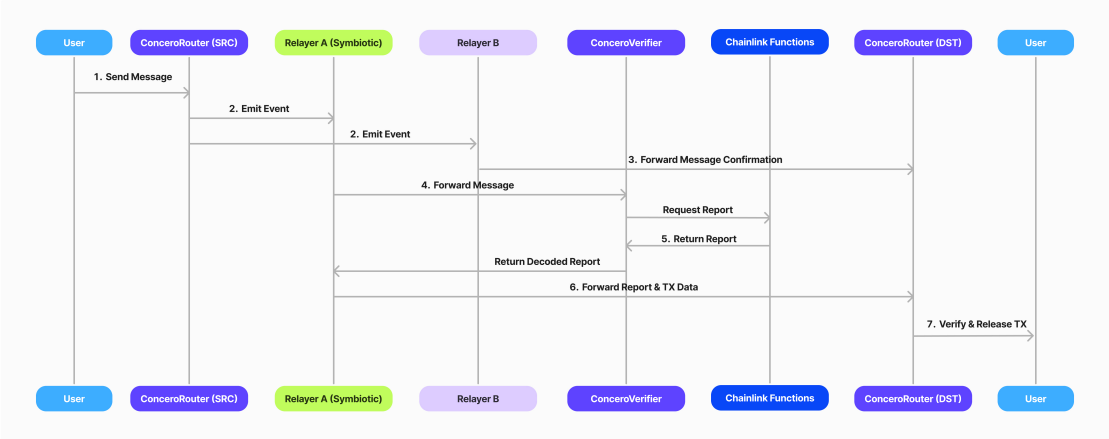

Figure 3: Value Bearing Message Flow in Concero V2

In the subsequent stage, Relayer B processes the event and forwards a message confirmation directly to the destination chain router. Concurrently, Relayer A transmits the message to the Chainlink Functions-enabled Master Chain to initiate the Chainlink Functions verification process. This dual-path approach ensures redundant verification while maintaining efficient processing times.

The Chainlink Functions system then processes the verification request and generates a comprehensive report, which is returned to the Chainlink Functions-enabled Master Chain. Relayer A monitors this chain, captures the returned report, and performs necessary decoding operations to extract the verification data. Following successful decoding, Relayer A forwards both the report and the associated transaction data to the destination chain router contract.

The final stage occurs at the destination chain router contract, where multiple verification steps ensure transaction integrity. The contract first verifies the report's authenticity by confirming its origin from authorised Chainlink Functions node operators. It then checks for any potential tampering by validating the report's cryptographic signatures.

The contract proceeds to confirm the receipt of all required confirmations, including those from Relayer B in value bearing message cases. Finally, after establishing consensus on the message validity, the contract releases the transaction, completing the cross-chain transfer process.

3 Dual-Layer Security Framework

Cross-chain interoperability solutions traditionally adopt either cryptographic security through verification mechanisms or economic security through stake-based incentives. Each approach presents distinct advantages and limitations. Concero V2 introduces an innovative dual-layer security framework that combines both approaches to create a robust and scalable cross-chain messaging system.

The framework integrates cryptographic security through Chainlink Functions with economic security facilitated by Symbiotic restaking protocol. This combination addresses the limitations of single-layer security models. While cryptographic security provides objective, verifiable proof of message validity, economic security ensures proper behaviour through financial incentives and penalties. The interaction between these layers creates a security synergy where economic incentives encourage efficient message transmission, while cryptographic proofs prevent unauthorised messages from being processed.

A significant innovation in this framework is the rapid challenge period for stake-based verification. Traditional economic security models require extended challenge periods of approximately seven days for dispute resolution. Concero V2 reduces this to approximately 20 seconds by using cryptographic proofs from Chainlink Functions to make immediate determinations about message validity. This improvement enhances capital efficiency for relayer nodes while maintaining security guarantees.

The framework provides flexibility through optional security configurations. While the cryptographic security layer serves as a mandatory foundation, developers can enable additional verification through multiple relayer networks based on their specific security requirements. This adaptability allows applications to optimise their security model based on the value and sensitivity of their cross-chain operations. The following sections examine the technical implementation of each security layer in detail.

3.1 Cryptographic Security Layer (Chainlink Functions)

The cryptographic security layer in Concero's architecture utilises Chainlink Functions as a decentralised compute network to verify cross-chain messages. This section examines the technical implementation and operational workflow of this critical component.

Core Architecture Chainlink Functions operates through a DON consisting of four independent nodes. When a computation request is initiated from a supported network, all four DON nodes execute identical code simultaneously. The system requires consensus from at least three out of four nodes to validate results, creating a robust verification mechanism.

Generation of Verifiable Reports The verifiable report generation process in Concero represents a critical component of the cryptographic security layer. This process creates tamper-proof evidence of transaction validity through a distributed consensus mechanism implemented via Chainlink's DON (Figure. 4).

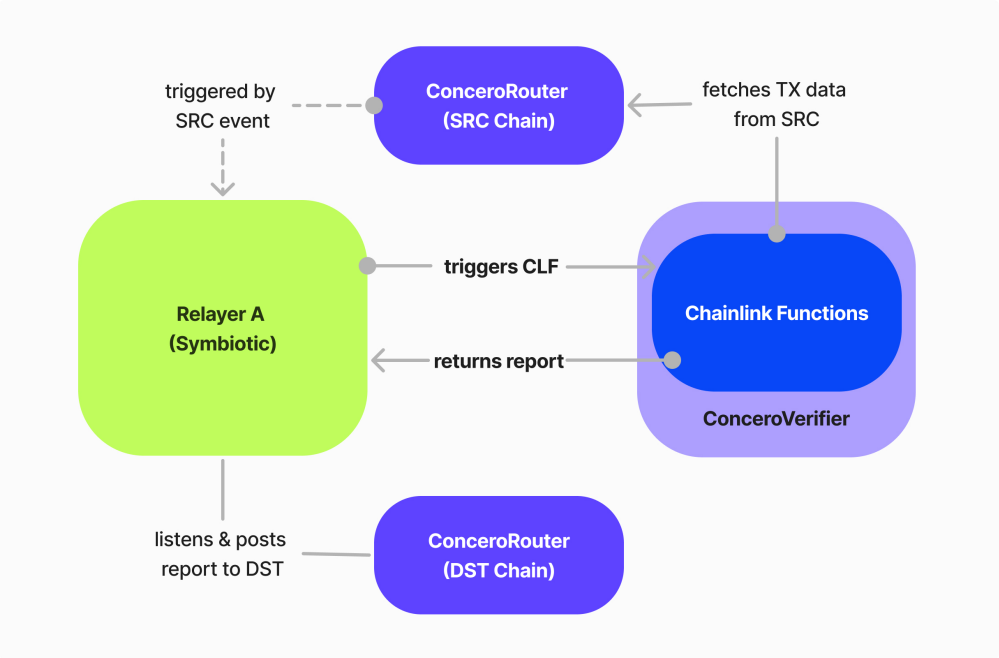

Figure 4: Chainlink Functions Verification Process

During runtime, Chainlink Functions executes a multi-step verification process across its DON nodes. Each node independently obtains event confirmations by querying transaction details using the provided block number, chain identification, and transaction hash. To enhance data reliability, the system implements provider randomisation, where each DON node queries different JSON RPC providers. This approach significantly reduces trust assumptions in the data collection phase by distributing queries across multiple independent data sources.

The consensus mechanism requires agreement from at least three out of four DON nodes to generate a valid report. When consensus is achieved, each participating node cryptographically signs the agreed-upon result. These signatures, combined with the consensus data, form a comprehensive report that is submitted to the destination chain by Relayer A. This report serves as a verifiable proof of the transaction's validity and includes both the consensus data and the cryptographic signatures from the participating nodes.

The verification process incorporates multiple layers of security checks. When the report reaches the destination chain's ConceroRouter, the system performs signature recovery to confirm that the signers match the authorised Chainlink DON nodes. This verification step ensures the report's authenticity by validating its origin. Additionally, the system verifies that the data represents a genuine consensus by confirming contributions from at least three separate DON nodes, each having independently collected confirmations from multiple randomised RPC providers.

The system's tamper resistance is achieved through hash verification. The destination chain validates that the report's hash sum matches its authorised signatures, ensuring

that the data remains unaltered during transmission.

3.2 Economic Security Layer (Symbiotic integration)

The economic security layer of Concero V2 is implemented through Symbiotic, a restaking protocol that creates a comprehensive system of incentives and penalties to ensure reliable operation of the network. This implementation establishes economic checks and balances that reward genuine operations while penalising malicious behaviour.

Core Infrastructure Symbiotic's core contracts are deployed on the Ethereum network, operating with minimal state changes to optimise cost efficiency. The system performs state changes exclusively during slashable events, while normal operations utilise only state reads. These reads verify two critical elements: operator registration status and sufficient delegated stake for operations. This architecture ensures that operators maintain adequate economic backing for their activities while minimising operational costs.

Node Operator Cohort System The implementation of a cohort-based system for relay operators represents a significant advancement in addressing the challenge of fee distribution inequality in cross-chain messaging protocols. This system introduces a deterministic and decentralised approach to operator organisation whilst maintaining operational reliability and equitable revenue distribution.

The core mechanism of cohort assignment operates through a mathematical conversion of operator addresses into cohort placements. When an operator registers with the protocol, their blockchain address undergoes conversion to an integer value, followed by a modulo operation against the total number of cohorts to determine their cohort assignment. This same principle applies to message routing, where each message's unique identifier undergoes a similar modulo operation to determine its designated cohort.

To maintain optimal security parameters, the system implements dynamic cohort sizing. The protocol initiates with a conservative configuration of two cohorts, each maintaining a minimum threshold of five operators. This structure evolves dynamically as the network expands, with the system automatically adjusting cohort parameters to balance security requirements with operational efficiency. The adjustment mechanism ensures that no cohort operates below the minimum operator threshold, thereby maintaining system redundancy and preventing single points of failure.

The system effectively addresses the common issue of performance centralisation in relay networks. Traditional systems often suffer from high-performance nodes capturing a disproportionate share of fees, leading to centralisation as operators with superior infrastructure dominate the network. The cohort system mitigates this through restricted competition within cohorts, ensuring that operators compete for fees only within their assigned cohort rather than across the entire network. This structure creates a more balanced economic environment where infrastructure investment provides diminishing returns beyond certain thresholds.

The implementation demonstrates particular effectiveness in maintaining system reliability through redundancy. For instance, if a cohort contains three operators and one experiences downtime, the remaining two can continue processing messages, ensuring uninterrupted service. The system's economic model incentivises operators to maintain high availability, as extended downtime results in missed fee opportunities and potential slashing penalties.

This architectural approach yields significant benefits for network decentralisation and operational stability. By preventing fee monopolisation and encouraging diverse operator participation, the system maintains robust decentralisation whilst ensuring reliable message delivery. The dynamic scaling capability enables the network to accommodate growth without compromising performance or security parameters.

The success of this system relies heavily on careful parameter management. The protocol must continuously monitor and adjust cohort depths and widths to maintain optimal performance. These adjustments occur through automated mechanisms that respond to network metrics, ensuring the system remains responsive to changing network conditions whilst maintaining security thresholds.

Reward Distribution System The reward mechanism operates through ConceroRouter contracts deployed across multiple chains. When transactions are successfully fulfilled, operators receive rewards through two primary channels. Relayer A collects rewards from both ConceroVerifier and ConceroRouter, while Relayer B receives rewards solely from ConceroRouter. This distributed reward structure incentivises consistent performance across the network while maintaining the protocol's cost efficiency.

Slashing Mechanism and Verification Concero V2 implements a targeted slashing mechanism focused on ensuring operator responsiveness and network reliability. By leveraging a carefully designed accountability framework, the system incentivises timely message fulfillment from designated operator cohorts. If a designated cohort fails to fulfill a time-sensitive message within the required timeframe, another operator can submit a report to the ConceroVerifier. Upon verification of the report's validity, the ConceroVerifier will issue a slashable report. When this report is relayed to the Symbiotic Ethereum contracts, it will result in the slashing of every operator within that specific cohort for their collective failure to respond in a timely manner. This approach ensures network reliability by incentivising consistent and prompt message fulfillment, while the inherent protocol design prevents tampered messages from being propagated to destination contracts, as they would automatically revert.

Challenge Period Innovation A significant advancement in Concero V2's economic model is its near-instant challenge period of 10 - 20 seconds, substantially improving upon traditional week-long challenge periods. This rapid verification process, enabled by Chainlink Functions, enhances capital efficiency for operators. The system allows operators to relay transactions worth up to their delegated stake amount within this brief window. For instance, an operator with 1 ETH delegated stake can process 1 ETH worth of transactions every 20 seconds, with the limit resetting after each challenge period concludes. This innovation significantly reduces barriers to entry while maintaining robust security guarantees.

This economic security implementation creates a self-sustaining ecosystem where operators are incentivised to maintain honest operation while facing substantial penalties for any deviation from protocol rules. The integration with Chainlink Functions for verification ensures rapid and accurate determination of slashing events, enabling efficient capital utilisation while maintaining system security.

4 Fee Structure

Concero V2 will implement a transparent and competitive fee structure designed to maintain economic sustainability while providing value to all participants in the ecosystem.

The messaging service will implement fixed fees based on message complexity and data size rather than percentage-based pricing. This approach will make costs predictable for developers implementing cross-chain communication. The exact messaging fee structure will be announced prior to mainnet launch, following comprehensive analysis of operational costs and market conditions.

For integrators building on top of Concero, the protocol will offer flexible fee options. Third-party applications can implement their own additional fees starting from 0%, creating revenue opportunities while maintaining competitive pricing for end-users. This model allows integrators to determine appropriate pricing based on their specific value addition and market positioning.

5 Technical Innovations and System Benefits of Concero V2

Concero V1, while innovative in its approach, operates within the confined intersection of CCIP and Chainlink Functions supported networks, currently spanning only five EVM chains: Ethereum, Polygon, Avalanche, Arbitrum, and Base. Recognising this constraint as a significant barrier to widespread blockchain integration, we developed Concero V2 to enable seamless communication between any blockchain networks. This advancement marks a pivotal shift from limited chain support to universal blockchain connectivity, addressing a fundamental need in the evolving blockchain ecosystem.

5.1 Cost and Integration Efficiency

Concero V2 delivers remarkable cost-efficiency for cross-chain integration, with integration costs reduced to zero dollars and implementation timeframes of approximately two hours. This pioneering efficiency stems from the protocol's innovative verification approach, which eliminates the need for expensive full node or light client implementations that burden traditional cross-chain solutions. Instead, Concero V2 employs a consensus-based RPC verification system where multiple independent providers must agree on transaction validity before message propagation occurs. This design allows Concero V2 to rapidly deploy cross-chain functionality with minimal engineering resources, dramatically reducing barriers to entry for cross-chain application development.

Future protocol iterations will enhance decentralisation through an advanced node discovery mechanism enabling direct communication with network nodes. This streamlined architecture, combining zero-dollar integration costs, rapid integration capabilities, and security through distributed consensus position, positions Concero V2 as an exceptionally compelling solution for cross-chain communication in today's fragmented blockchain landscape.

5.2 Unlimited Chain Support

Concero V2 achieves unlimited chain support through an innovative dual-layer security architecture. The protocol utilises relayer nodes, which are economically secured through

Symbiotic restaking, working in conjunction with Chainlink Functions' decentralised computation capabilities. This architectural approach eliminates the need for specific protocol support on participating chains, enabling Concero V2 to establish secure connections with any blockchain network. The system's design represents a significant advancement over traditional interoperability solutions that typically require dedicated infrastructure or protocol modifications for each supported chain.

5.3 Modularity

Concero V2's modular architecture introduces a flexible consensus mechanism for cross-chain message validation. The protocol implements a mandatory base layer consisting of Relayer A and Chainlink Functions, which provides fundamental security guarantees. Beyond this foundation, developers can incorporate additional validation layers through existing interoperability protocols, enabling customised consensus requirements for different transaction types.

This design allows precise control over the security-performance trade-off, where developers can strengthen security by enabling multiple validators, though this may increase transaction completion time and costs. For instance, a high-value transfer might warrant validation from multiple protocols, while a simple message could use the base layer for optimal speed.

This architectural approach ensures that Concero V2 can adapt to varying security requirements while maintaining operational efficiency across different use cases in cross-chain communication.

5.4 Enhanced Data Transmission Capacity

Concero V2 significantly expands cross-chain data transmission capabilities by removing protocol-imposed limitations on message size. While Concero V1 restricted message payloads to approximately 650 bytes, V2 allows messages to reach the maximum theoretical limits of the underlying blockchain networks. For EVM chains, this translates to a substantial increase to 1.875 MB per message, based on Ethereum's 30M block gas limit and the 16 gas units cost per non-zero calldata byte.

This enhancement enables the transmission of complex data structures and larger payloads across different blockchains, supporting more sophisticated cross-chain applications. The protocol's architecture now accommodates varying data capacity requirements across different blockchain ecosystems, with limits determined solely by the technical constraints of the participating networks rather than by Concero itself.

6 Risk Mitigation

Cross-chain communication protocols introduce unique security considerations that require robust risk mitigation strategies. Concero V2 implements a multi-layered approach to address these challenges effectively, combining cryptographic verification with economic incentives.

6.1 Relayer Node Risk Management

The decentralised nature of relayer networks introduces potential vulnerabilities that must be systematically addressed. When relayers serve as message carriers between blockchains, their integrity becomes paramount to system security. Concero V2 employs a dual-pronged approach to ensure relayer honesty.

First, the protocol implements an economic security model through the Symbiotic restaking protocol. This requires all operators to register with delegated stake before participating in the network. Should a relayer attempt to transmit fraudulent messages, this stake becomes subject to slashing penalties that exceed any potential gains from malicious behaviour. The economic disincentive renders attacks financially unviable, aligning relayer incentives with network security.

Second, and perhaps more importantly, Concero V2 never relies solely on relayers for message verification. The system employs what can be termed "dual verification," wherein Chainlink Functions serve as an independent cryptographic verification layer. For any message to be accepted on the destination chain, it must carry a valid report generated by Chainlink's DON, consisting of multiple independent node operators who reach consensus on the validity of the source chain event. This cryptographic verification ensures that even if relayers were compromised, they could not successfully transmit unauthorised messages.

6.2 Oracle Network Security

While Chainlink Functions provide critical security through their consensus mechanism, Concero V2 recognises the theoretical risk of oracle failure. In the unlikely scenario that the majority of Chainlink DON nodes were to produce an incorrect validation, the system provides an additional safeguard through its modular design.

The protocol allows developers to enable supplementary verification networks, such as Relayer B or other interoperability protocols. When these additional verification layers are activated, the destination chain requires consensus between multiple independent verification sources before releasing any messages. This ensures that even in the case of oracle network compromise, the cross-chain message would remain secure, as the conflicting reports would fail to achieve the required consensus threshold for message release.

6.3 Denial of Service Resilience

Operational continuity represents another important consideration for decentralised communication systems. The reliance on independent node operators creates potential vulnerability to service interruptions should insufficient nodes remain active. Concero V2 addresses this challenge through its economic model, which creates compelling incentives for operator participation.

The protocol implements a cohort-based fee distribution system that promotes equitable revenue sharing among operators, while simultaneously incentivising high-quality service provision. Newly supported chains present particular opportunities for operators to capture larger fee shares due to initially lower competition. This economic design ensures that the network maintains sufficient operator distribution and redundancy, even during scaling phases.

7 Use Cases and Applications

Concero V2 unlocks a wide range of use cases and applications, empowering developers and businesses to build innovative solutions. As the blockchain ecosystem continues to evolve, new possibilities will emerge, driving further adoption and innovation. With the protocol maturing over time, it will adapt to industry needs, enabling even more advanced and impactful applications. These are some of the use cases and applications that could be enabled by Concero V2:

7.1 Cross-Chain DeFi Composability

Concero V2 revolutionises DeFi by establishing seamless interoperability between blockchain networks, allowing for unprecedented composition of financial primitives across chains. With its robust trustless message passing, developers can build sophisticated multi-chain applications where:

- Users can collateralise assets on one chain (e.g., Ethereum) while accessing borrowing facilities on another (e.g., Arbitrum) within a single transaction flow
- Liquidity providers can deploy capital across multiple chains simultaneously and manage positions through a unified interface
- Cross-chain yield aggregators can automatically route capital to the highest-yielding opportunities across the entire blockchain ecosystem
- Flash loans can be initiated on one chain and utilised on another, with repayment occurring atomically within the same transaction

This unified liquidity environment significantly reduces capital fragmentation while enhancing capital efficiency throughout the DeFi ecosystem. By providing fast confirmation times, Concero V2 enables time-sensitive financial operations that were previously impossible in cross-chain environments.

7.2 NFT Interoperability and Metaverse Integration

The expanded data transmission capacity of Concero v2 (up to 1.875 MB per message) creates unprecedented opportunities for complex digital asset transfers across blockchain ecosystems. This facilitates:

- Seamless NFT migrations between chains while preserving complete metadata, ownership history, and associated rights
- Cross-chain NFT marketplaces where collections from multiple blockchains can be traded within a single interface
- Interoperable metaverse environments where digital identities, land parcels, and virtual items function consistently across different blockchain-based worlds
- Gaming guilds that operate scholarship programs across multiple blockchain games simultaneously

- Cross-chain NFT collateralisation, allowing users to leverage digital assets from one chain as collateral in DeFi protocols on another

Metaverse developers particularly benefit from Concero v2's ability to translate complex state changes between virtual environments, ensuring persistent digital identity and asset ownership across the fragmented metaverse landscape.

7.3 Cross-Chain Governance and DAO Coordination

Concero v2's trustless architecture provides a secure foundation for sophisticated governance mechanisms spanning multiple blockchains:

- Multi-chain DAOs can implement unified voting systems where governance tokens on different chains contribute proportionally to decision-making
- Governance proposals can trigger synchronised execution of smart contracts across multiple chains
- Treasury management can be coordinated across diverse blockchain assets without requiring centralised control
- Delegation of voting power can occur cross-chain, enabling more flexible governance participation
- Risk parameters for cross-chain protocols can be adjusted holistically based on system-wide metrics

The protocol's economic security layer provides cryptographic guarantees that governance decisions are faithfully transmitted and executed across all participating chains, enhancing trust in cross-chain governance systems.

7.4 Omnichain dApp Development

Concero v2 empowers developers to build truly chain-agnostic applications with consistent functionality across the entire blockchain ecosystem:

- A single codebase can be deployed across multiple chains with state synchronisation handled automatically by Concero's messaging protocol
- User interactions on any supported chain can trigger coordinated updates across the entire application state space
- Applications can leverage the unique strengths of different blockchains while presenting a unified experience to users
- Chain-specific optimisations can be implemented without fragmenting the overall application architecture
- Dynamic load balancing can distribute application processing across chains based on congestion, gas costs, or other efficiency metrics

By abstracting away the complexities of cross-chain communication, Concero v2 dramatically reduces development overhead while expanding potential user bases to include participants from any supported blockchain.

7.5 Enterprise Blockchain Integration

Concero v2's modular security architecture provides the reliability and auditability required for regulated industry applications:

- Organisations can implement secure data-sharing workflows between permissioned enterprise chains and public networks
- Supply chain logistics can be coordinated across industry-specific and public blockchains with cryptographic verification at each step
- Financial institutions can maintain compliance while participating in broader blockchain ecosystems
- Healthcare providers can securely share anonymised data across specialised medical chains and general-purpose networks
- Carbon credit markets can achieve global interoperability while maintaining rigorous verification standards

The protocol's customisable verification requirements allow enterprises to implement precisely the level of security needed for their specific regulatory environment and risk profile.

7.6 Interchain Identity and Reputation Systems

Concero v2 facilitates the development of unified identity frameworks that function consistently across blockchain boundaries:

- Verifiable credentials can be issued on one chain and presented on another with cryptographic proof of validity
- Reputation scores derived from activity on multiple chains can inform access decisions throughout the ecosystem
- KYC/AML verifications performed on one chain can be securely transmitted to other networks without revealing sensitive data
- Social graphs and relationship networks can extend across chain boundaries
- Decentralised identifiers (DIDs) can be resolved across multiple chains with consistent results

These systems enhance security throughout the blockchain ecosystem by providing more comprehensive identity context for access decisions while preserving user privacy and autonomy.

7.7 Interchain Account Abstraction

Concero v2 transforms user experience by enabling true account abstraction across multiple blockchains:

- Users can control assets on multiple chains through a single interface, with ownership verification handled seamlessly
- Smart contract wallets can coordinate operations across multiple chains with consistent security policies
- Social recovery mechanisms can function across chain boundaries, improving resilience
- Gas fees on destination chains can be abstracted away, allowing users to pay for cross-chain transactions in their preferred token
- Transaction batching across chains reduces overall costs and improves efficiency

This capability dramatically simplifies blockchain interaction for end users while enhancing security through consistent cross-chain authentication and authorisation mechanisms.

7.8 Cross-Chain MEV Protection

By leveraging its fast transaction confirmation and Chainlink proof verification, Concero v2 provides robust protection against cross-chain MEV exploitation:

- Users can execute trades atomically across multiple DEXs on different chains, preventing front-running through simultaneous settlement
- Private transaction pools can coordinate across chains to protect sensitive transactions
- Time-locked transactions can be synchronised across multiple chains to prevent information leakage
- Complex arbitrage strategies can be executed atomically to prevent partial execution risks
- MEV auction mechanisms can be extended across chain boundaries, creating more comprehensive protection

These protections ensure fair execution across the entire blockchain ecosystem, protecting users from sophisticated cross-chain extraction techniques that would otherwise compromise transaction integrity.

8 Future Enhancements

8.1 Expanded Blockchain Support

Non-EVM Chain Integration Concero V2's next evolution will prioritise comprehensive integration with non-EVM blockchain ecosystems, establishing truly universal cross-chain messaging capabilities.

This expansion would begin with incorporating Solana's high-throughput architecture by developing specialised adapters that translate between Solana's account model and Ethereum's UTXO structure while preserving Concero's security guarantees. The integration will extend to the Cosmos ecosystem by implementing compatibility with the Inter-Blockchain Communication (IBC) protocol, allowing Concero to serve as a bridge between IBC-enabled chains and the broader blockchain landscape. Additionally, establishing connections with Polkadot's parachain ecosystem through XCMP adaptors would enable secure message passing to this growing network of specialised blockchains.

To maintain Concero's security standards across these diverse protocols, the implementation will require custom verification modules for each blockchain family that account for their unique consensus mechanisms and data structures.

Layer 2 Optimisation For Layer 2 solutions, Concero will develop optimised verification methods tailored to the distinct architectures of zkRollups and Optimistic Rollups, leveraging their native verification mechanisms to reduce overhead while maintaining security. This would involve creating specialised proof validation for zkRollups that integrates zkProofs directly into Concero's verification layer, while implementing fraud-proof monitoring systems for Optimistic Rollups that align with their challenge-response security model.

Such comprehensive blockchain support would position Concero as a universal interoperability layer capable of facilitating seamless communication between any blockchain networks regardless of their underlying architecture or consensus mechanisms.

8.2 Performance Optimisations

Latency Reduction Strategies Concero V2 will implement several techniques to achieve sub-five-second transaction completion times. The protocol will process cryptographic operations in parallel rather than sequentially, allowing signature verifications to happen simultaneously. We will introduce predictive mechanisms that prepare destination chains while source chain confirmations are still processing, effectively overlapping operations that currently happen one after another.

For frequently traveled routes, dedicated relayer cohorts will be established with optimised connections. A verification cache will store recent proofs to avoid repeating calculations for similar transactions. Priority lanes will allow urgent transactions to be processed faster, while optimistic verification will conditionally approve low-risk messages pending final confirmation. These improvements will bring transaction times closer to network propagation limits.

Bandwidth Optimisation As message capacity expands to 1.875 MB, bandwidth efficiency becomes crucial. The protocol will use adaptive compression that selects the best method based on data type, whether it's smart contract code, NFT information, or

numerical data. For repetitive data, only the changes from standard templates will be transmitted rather than complete messages. Large messages will be intelligently broken into optimal fragments to maximise throughput. Chains that frequently exchange similar messages will establish shared dictionaries where reference codes replace repeated data transmission.

For non-urgent large data transfers, content hashes will be transmitted with actual content retrieved only when needed. These optimisations will reduce costs for data-heavy applications while enabling new use cases requiring substantial cross-chain information exchange.

Batch Processing Implementation To improve efficiency when handling multiple messages simultaneously, Concero V2 might group similar destination-bound messages for unified verification. Multiple message hashes will be organised into Merkle trees, allowing many messages to be verified through a single root hash check. For high-volume situations, a single compact proof will validate numerous messages at once. The system will automatically adjust batch sizes based on current gas prices, network conditions, and message urgency. By analysing dependencies between messages, the protocol will order batched transactions optimally to avoid unnecessary waiting. On destination chains, batched messages will execute in parallel while maintaining proper ordering.

These improvements will significantly reduce per-message costs while increasing network capacity for applications requiring frequent cross-chain communication.

Gas Optimisation Concero V2 will implement gas optimisation strategies to reduce transaction costs across all supported chains. The protocol will encode frequent parameters into compact bit-packed formats, minimising the on-chain footprint of cross-chain messages. An adaptive gas estimator will predict the minimum viable gas required based on historical data and current network conditions, preventing transaction failures and overpayment. The system will reuse deployed code through proxy patterns and shared libraries, reducing contract interaction costs.

Gas-intensive computations will move off-chain where possible, with only result verification occurring on-chain. Router contracts will optimise storage through variable packing and ephemeral storage for temporary values. Transaction simulations will pre-calculate gas requirements, enabling precise allocation without wasting resources.

These optimisations will reduce cross-chain transaction costs by approximately 30-40% compared to current implementations, improving economic efficiency for applications requiring frequent cross-chain interactions.

8.3 Developer Experience Improvements

SDK Enhancements Concero V2 will develop comprehensive multi-language Software Development Kits to reduce integration complexity and accelerate adoption. We will create fully-featured libraries for JavaScript/TypeScript, Python, Rust, Go, and Java, maintaining consistent APIs across all implementations. These SDKs will include high-level primitives that simplify complex cross-chain operations, while providing middleware hooks for custom processing and validation.

Additional features will include automatic chain detection, cross-network gas estimation, and optimal path routing. The libraries will implement robust error handling with diagnostic information and retry logic with exponential backoff. Extensive documentation

and seamless integration with popular web3 frameworks will help developers implement cross-chain functionality in hours rather than weeks.

Simulation Environment Concero V2 will establish a simulation framework enabling developers to test cross-chain applications before production deployment. This environment will create a multi-chain sandbox that replicates all supported blockchains in a controlled setting where developers can simulate interactions without network costs. Time controls will allow testing under various network conditions, including accelerated block production and delayed messages.

For automated testing, the system will generate thousands of randomised test cases covering edge conditions like reorganisations and network congestion. Integration with testing frameworks like Hardhat, Foundry, and Brownie will let developers write cross-chain tests using familiar tools. Transaction tracing will visualize the complete lifecycle of cross-chain messages, while deterministic replay will help debug complex issues by reproducing specific interactions exactly.

Visual Monitoring Tools Concero V2 will develop intuitive monitoring dashboards providing real-time visibility into cross-chain message status and network health. The platform will include a message explorer tracking every transaction through its complete lifecycle, displaying detailed timing analytics for verification latencies, relayer performance, and total finality time. Network health monitoring will show real-time analytics on cohort performance, success rates, gas consumption, and economic security metrics. Customisable alerts will notify operators of anomalous conditions such as delayed messages or verification failures.

For enterprise users, comprehensive analytics with exportable reports will support business intelligence needs. API access will enable integration with existing DevOps monitoring infrastructure. These tools will enhance operator efficiency, improve issue response times, and provide developers with critical insights into application performance.

9 Tokenomics

At the momement, there is no final decision on the tokenomics, Concero team is currently evaluating the tokenomics and will make a decision based on the feedback from the community and the needs of the protocol.

10 Conclusion

Concero Messaging V2 represents a significant advancement in cross-chain interoperability, delivering a trustless communication framework that effectively resolves long-standing tensions between security, scalability, and decentralisation. The protocol's dual-layer security architecture—combining cryptographic verification through Chainlink Functions with economic accountability via Symbiotic's restaking infrastructure—establishes a robust foundation for secure cross-chain communication without centralised intermediaries. This innovative hybrid approach overcomes the inherent limitations of single-approach systems, providing stronger security guarantees than pure economic models while maintaining greater efficiency than purely cryptographic solutions.

The protocol's architecture introduces several innovative approaches to blockchain interoperability. Its modular design decouples message propagation from validation, enabling trustless verification while maintaining quick finality times. The cohort-based relayer system ensures equitable fee distribution, preventing centralisation while incentivising consistent performance. Meanwhile, the protocol's capacity for unlimited chain support—extending beyond EVM-compatible networks to potentially any blockchain—creates unprecedented opportunities for true cross-chain composability.

Additionally, Concero V2 is engineered for affordability and rapid adoption, enabling integration with new blockchains and projects in a matter of hours and at virtually zero cost. This unprecedented ease of deployment ensures that any network—regardless of size or resources—can leverage Concero to overcome cross-chain barriers and unlock seamless interoperability.

As blockchain technology continues to evolve towards a multichain future, Concero V2 establishes a critical foundation for secure, efficient, and truly decentralised communication between heterogeneous networks. By eliminating centralised trust assumptions while maintaining high performance, the protocol enables a new era of blockchain composability where applications can seamlessly leverage the unique strengths of different networks. This advancement not only resolves current interoperability challenges but also creates the infrastructure necessary for the next generation of blockchain innovation—a future where chain boundaries become transparent to users and developers alike, unlocking the full potential of a unified blockchain ecosystem.

Acknowledgements

We would like to thank Chainlink Labs for their valuable support and insightful feedback on the protocol architecture. We also extend our gratitude to the Symbiotic team for their guidance in developing the economic security layer of the protocol.

Author Contributions

O.K. and A.B. designed the architecture of Concero V2. O.K. wrote the first draft of the technical article. O.K., A.B., and N.G. reviewed and edited the whitepaper. P.L. learned the technical concepts from O.K. and A.B., compiled the information, prepared the figures, and wrote the complete whitepaper.

References

[1] Symbiotic crypto: Modular restaking for enhanced security, oct 2024.

[2] Chainlink documentation, 2025.

[3] Chainlink documentation: Architecture, 2025.

[4] Connect the world's apis to web3 with chainlink functions, 2025.

[5] Symbiotic - documentation, 2025.

[6] Symbiotic: Leading permissionless protocol for shared security, 2025.

[7] I. L. O. Bolgurtseva. Scalability and interoperability in blockchain. *Serokell*, sep 2024.

[8] Everstake Team. Symbiotic: a cornerstone for the future of shared security. *Everstake*, jan 2025.

[9] A. Gromyko et al. Blockchain technology and its implications. *OxJournal*, 2025.

[10] S. Kejriwal. Understanding blockchain interoperability. *Coin Bureau*, jan 2025.

[11] B. Lim. Cross-chain messaging: potential and challenges in web3. *Web3Auth Blog*, dec 2024.

[12] R. Mbogni. Modular blockchain: the future of scalable architecture. *HeLa*, nov 2024.

[13] C. Nightingale. Off-chain data and computation with chainlink functions. *Thirdweb*, mar 2023.

[14] Zhao. What is symbiotic and how it is changing the restaking wars. *Coingecko*, jul 2024.