Telegraph cross-chain protocol

black zero, Ahmed Ali

January 2025

Abstract

This paper introduces Telegraph, a novel cross-chain communication protocol designed to facilitate seamless interaction between smart contracts across multiple blockchains. The key features of Telegraph include:

- A decentralized network of validator nodes that control multi-signature smart contracts called ”Ports” on supported blockchains.
- An accessible and affordable solution for developers to integrate cross-chain functionality with minimal code.
- Integration with the Bittensor blockchain, enabling AI inference capabilities directly from smart contracts.
- Continuous collection of DeFi price data and competitive training of price prediction AI models within the Telegraph subnet.

Telegraph aims to democratize cross-chain communication while leveraging AI capabilities, positioning itself as a pivotal player in the evolving blockchain ecosystem.

1 Introduction

Telegraph is a blockchain messaging protocol that aims to make cross-chain communication for smart contracts across multiple blockchains both easily accessible and affordable. Current blockchain messaging protocol node networks keep their systems behind registrations and approvals, which in turn stifles innovation. With Telegraph, developers will finally have a cross-chain messaging protocol that they can integrate into their project with a few lines of code. No registration required.

The Telegraph messaging protocol itself is an off-chain set of validator nodes that share control over multiple multi-signature smart contracts known as ”ports.” These ports act as relay points on each supported chain and always require a threshold of nodes to supply their signature to approve a transaction. Using this method, each node is able to retain privacy with control over their own private keys while being able to sign the messages off-chain. This means that only one final transaction has to be sent to the destination blockchain, rather than one transaction from each node.

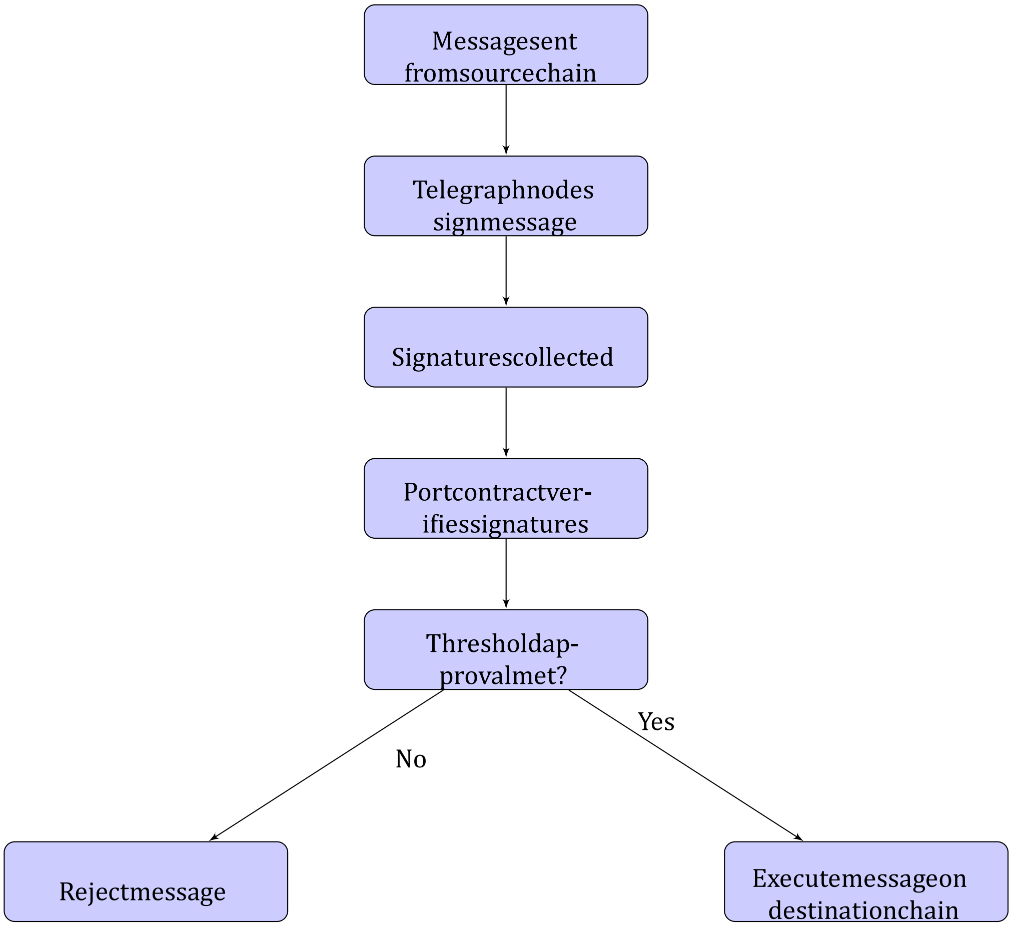
As an ecosystem, Telegraph nodes will be rewarded with a percentage from the fee of each successfully transmitted message. This reward is provided in the form of Bittensor's wTAO. These rewards will incentivize node operators to continue their maintenance and support for the Telegraph ecosystem.

Telegraph is integrated with the Bittensor blockchain, enhancing its functionality by providing access to AI inference directly from smart contracts. This integration not only empowers developers to leverage advanced AI capabilities but also creates a marketplace of models within the Telegraph subnet on the Bittensor network. Telegraph nodes will continuously collect DeFi price data from all supported chains, using this data to train new price prediction AI models. Miners in the Telegraph subnet will then compete to train superior price predictor models, earning rewards for their contributions. This synergy between crosschain communication and AI model training positions Telegraph as a pivotal player in the blockchain ecosystem, driving innovation and creating new revenue streams for other subnets on the Bittensor network.

2 Protocol Architecture

2.1 Smart Contracts (Ports)

Telegraph's smart contracts, known as Ports, are designed to be simple and userfriendly, making them accessible even to inexperienced developers. These Ports serve as the relay points on each supported blockchain, facilitating seamless cross-chain communication for smart contracts. By integrating Telegraph into their projects, developers can easily achieve cross-chain functionality with just a few lines of code, eliminating the need for complex setups and extensive blockchain knowledge.


Messagesent fromsourcechain
Telegraphnodes signmessage
Signaturescollected
Portcontractver-ifiessignatures
Thresholdap-provalmet?
No
Yes
Rejectmessage
Executemessageon destinationchain

2.1.1 Port Functionality

Each Port is a multi-signature smart contract that requires a threshold of Node signatures to approve a transaction. This multi-signature approach ensures the security and integrity of cross-chain messages. When a message is sent through the Telegraph network, it undergoes a verification process that leverages address retrieval from signatures signed by the nodes. This process uses the ecrecover function, a cryptographic method that retrieves the address associated with the signature, verifying the authenticity of the message.

2.1.2 Verification Mechanism

The verification mechanism works as follows:

1. **Message Detection and Signing**: Lead Nodes detect the message and sign it using their private keys.

2. **Signature Collection**: Nodes send their signatures to each other.

3. **Merkle Tree Creation**: Lead Nodes create a Merkle tree from the collected signatures once a threshold is reached.

4. **Submission to Port**: The Nodes submit the signed message in a predetermined manner, including the Merkle root, to the Port contract.

5. **Address Retrieval and Verification**: The Port contract uses the ecrecover function to retrieve the addresses from the Node signatures, ensuring they match the registered Node addresses.

6. **Threshold Approval**: Once the required threshold of valid Node signatures is met, and the Merkle root is verified, the message is approved for execution on the destination chain.

2.1.3 Rewards

Telegraph incentivizes its nodes directly on the destination chain where the Port is located. Upon successful message transmission and approval, Bittensor's wTAO distributed to the signing nodes. This decentralized reward mechanism ensures that all nodes are fairly compensated for their efforts over time.

2.2 Telegraph Validator Nodes

Telegraph Validator nodes form the backbone of the network's decentralized cross-chain communication protocol. The system employs a one-tier architecture consisting of nodes, implementing a robust mechanism for message validation, Byzantine Fault Tolerance (BFT), and network governance.

2.2.1 Node Hierarchy and Roles

The Telegraph network employs a hierarchical node structure to optimize performance and security. Nodes function as primary validators and coordinators, maintaining a cryptographically secured registry of other subscribed nodes. This registry includes public keys and subscription statuses, enabling efficient verification of incoming signatures. Nodes implement advanced signature aggregation algorithms and Merkle tree construction protocols, interfacing directly with Port smart contracts across various blockchains.

2.2.2 Subscription Mechanism

The subscription process for nodes involves a series of cryptographic operations. Initially, a node generates a registration message containing its public key, desired subscription duration, and a digital signature of this data using its private key. This message, accompanied by the requisite subscription fee, is transmitted to the port contract on the Ethereum network.

Upon receipt of the payment, other nodes within the network will then deliberate offchain and vote on the approval of the new entrant. If denied, the entrant will receive a full refund. If approved, the new node's information is added to the list of authorized signers in the contract and stored within the offchain database of each node.

2.2.3 Message Validation Process

The message validation process in the Telegraph network involves several cryptographic and distributed systems concepts:

Message Detection - Nodes implement event listeners for supported blockchain networks. These listeners employ efficient polling mechanisms or websocket connections to detect cross-chain message events. Upon detection, nodes extract the message data and prepare it for signing.

Signature Generation - Nodes employ the Elliptic Curve Digital Signature Algorithm (ECDSA) to sign messages. The resulting signature includes a timestamp to mitigate replay attacks, enhancing the network's resilience against temporal vulnerabilities.

Signature Collection and Aggregation - Nodes transmit their signatures to subscribed nodes via secure communication channels.

Merkle Tree Construction - Upon reaching a predefined threshold of node signatures, each node initiates Merkle tree construction. This process employs a cryptographic hash function such as SHA-256 or Keccak-256. Leaf nodes are created by hashing individual signatures, while internal nodes are constructed through concatenation and hashing of child node values. The resulting Merkle root serves as a compact representation of the included signatures.

Merkle Proof Generation - For each included signature, nodes generate a Merkle proof consisting of the sibling hashes along the path from the leaf to the root. These proofs, stored alongside the Merkle root, enable efficient verification of individual signatures without requiring the entire set of signatures.

Node Submission - The node whose turn it is in the signing order creates a submission package encompassing the original message, Merkle root, it's signature on both, and a bitmap indicating included node signatures from other nodes. This package is broadcast to other nodes and submitted to the relevant Port smart contract using blockchain-specific transaction protocols.

Verification Process - Receiving nodes and the Port contract perform multistage verification. This includes validating the signing node's signature, verifying the Merkle root against a threshold of known node public keys, and checking individual Merkle proofs for a randomly selected subset of included signatures. The Port contract mandates signatures from a quorum of authorized nodes before executing any cross-chain actions, ensuring consensus across the network.

2.2.4 Byzantine Fault Tolerance and Governance

The Telegraph network implements a robust Byzantine Fault Tolerance mechanism coupled with a decentralized governance model:

Fault Detection - Nodes continuously monitor the network for anomalies, including invalid Merkle roots or proofs, signature repetitions, and signatures from unauthorized or expired nodes. This monitoring utilizes advanced anomaly detection algorithms to identify potential Byzantine behavior.

Vote of No Confidence Upon detecting a fault, a node initiates a vote of no confidence by creating a cryptographically signed fault report. This report is broadcast to other nodes and a designated governance smart contract, triggering a network-wide alert.

Manual Review Process The governance contract emits an event notifying all node owners of the pending vote. Node owners then retrieve the fault report and supporting evidence through decentralized storage protocols. A predefined review period of 24 or more hours allows for thorough examination of the presented evidence.

Voting Mechanism Votes are submitted as signed messages to the governance contract.

Node Removal Upon reaching the required supermajority, the governance contract executes a series of actions: it removes the implicated node's public key from the list of authorized validators, emits a network-wide event signaling all participants to update their node lists, and potentially slashes the stake of the removed node if a staking mechanism is implemented.

This comprehensive system leverages advanced cryptographic primitives, efficient data structures, and smart contract capabilities to ensure high security, scalability, and Byzantine Fault Tolerance in the Telegraph network. The synthesis of automated fault detection mechanisms with manual governance processes facilitates rapid response to potential issues while safeguarding against false positives and malicious attacks on network integrity.

3 Integration with Bittensor Blockchain

The integration of Telegraph with the Bittensor blockchain enhances the protocol's functionality by providing access to AI inference directly from smart contracts. This connection allows developers to leverage advanced AI capabilities, creating a seamless and powerful combination of cross-chain communication and AI-driven insights.

3.1 Integrating Bittensor Subnets.

- **Selection Process**: Subnets interested in integrating with Telegraph Protocol must provide their API specifications.
- **Bittensor Subnet Registration**: Upon successful integration, subnets are registered in the marketplace, making them available for inference requests from Telegraph nodes. Each subnet Telegraph may support will be registered under separate specific subnet IDs. These IDs will act as a public ”phone-book” that anyone can use to quickly interact with participating subnets.

3.2 Handling Inference Requests

1. **Inference Codes**: When a request is sent in for inference, it is expected to be accompanied by a relevant inference code in order for the Telegraph nodes to know the which subnet the request needs.
2. **Payment Mechanism**: Once a subnet is selected, the payment for the inference service is processed. wTAO will be used as the payment for these requests.

4 Conclusion

The Telegraph cross-chain protocol delivers a robust solution for enabling seamless and secure cross-chain communication for smart contracts across multiple blockchains. Its core architecture leverages off-chain validator nodes and multisignature smart contracts (Ports), ensuring transaction integrity and validator privacy. This decentralized approach reduces complexity and facilitates easier integration for developers, democratizing access to cross-chain functionality.

Telegraph's integration with the Bittensor blockchain enhances its offerings by incorporating AI inference directly into smart contracts. This synergy allows for real-time AI-driven insights and creates a dynamic marketplace for AI models within the Telegraph subnet. The continuous collection of DeFi price data and the competitive environment for training price prediction models further enrich the protocol's capabilities, providing valuable tools for financial applications.

The use of wTAO of Bittensor ensures fair and transparent token distribution, aligning with the principles of decentralization

Telegraph addresses key challenges in blockchain interoperability with a userfriendly, secure, and efficient protocol. Its integration with AI capabilities and a fair token economy positions it as a transformative player in the blockchain space, driving innovation and fostering new opportunities across interconnected blockchain networks.