POLYBRIDGE: A Crosschain Bridge For Heterogeneous Blockchains

Yue Li
Peking University
Beijing, China
liyue_cs@pku.edu.cn

Han Liu
Tsinghua University
Beijing, China
liuhan0518@gmail.com

Yuan Tan
PolyNetwork
Shanghai, China
tanyuan666@gmail.com

***Abstract*—While the Bitcoin and Ethereum are still leading the world of permissionless blockchains, we are increasingly seeing a multipolar ecosystem where new blockchains keep emerging instead of migrating to the two big players. As a result, it is highly desired to enable multiple blockchains to *interoperate*, *e.g.*, move assets from one blockchain to the other. The crosschain bridge service, as a solution to the blockchain interoperability problem, has been offered by a wide range of service providers. However, the existing bridges either rely on centralised notaries or require complicated preparations, therefore are far from sufficient in practice. In this demo proposal, we highlight the `Poly Bridge` for heterogeneous blockchains to interoperate with cryptocurrencies. In specific, `Poly Bridge` is based on an underlying `Poly Chain` and a pair of relays to confirm crosschain transactions and form consensus among relevant parties. More importantly, `Poly Bridge` delivers extensibility to flexibly interface to blockchains with different consensus models and atomicity as well in a way that a sequence of crosschain operations are either all confirmed or all rejected. `Poly Bridge` is now available as a web application to support crosschain requests with over 200 types of cryptocurrencies on 18 blockchains.**

I. INTRODUCTION

The past decade has been witnessing the rapid growth of blockchains and cryptocurrencies. While the Bitcoin [1]and Ethereum [2] are still leading the market, we are increasingly seeing a multipolar ecosystem where new blockchains keep emerging instead of migrating to the two big players. As a result, it is more desired than ever to enable two potentially different blockchains to interoperate, *i.e.*, allow one blockchain to operate data and assets on the other in a systematic way. The most obvious use case for such interoperation is to "move" cryptocurrency from a source blockchain to a destination for the purpose of joining a specific decentralized application, *e.g.*, a DeFi protocol.

State of the art. Crosschain bridges [3]–[6] are designed to address such demands and have been offered by a wide range of blockchain service providers. Popular realisations of crosschain bridges commonly fall into four categories, *i.e.*, notary, threshold signature, hash time lock and relay chain. Specifically, the notary scheme refers to a centralised solution which implements the interoperation by a deciding entity, *e.g.*, centralized exchanges. While the notary is able to deliver fast response, it introduces potential risks due to the high level of centralisation. Threshold signature is an instantiation of multiparty computation which generates and manages private keys in a distributed manner. In that case, the real private key to sign transactions is never revealed to the public. However, the scheme is hard to implement and extend due to the inclusion of many cryptographic primitives. Hash time lock sets hash locks for both sides and validate the transaction if both locks are unlocked in an expected timing order. Participants are required to stay online to complete the checks.

The `Poly Bridge`. We highlight the `Poly Bridge` crosschain bridge for heterogeneous blockchains in this demo proposal. As an instantiation of relay chain. `Poly Bridge` is based on the `Poly Chain` and a pair of relays to enable interoperation from a source chain to the destination chain. Compared to existing bridges, `Poly Bridge` introduces the fundamental optimization to support heterogeneous blockchains in an extensible way that no modifications are required on the participating blockchains or `Poly Chain` itself. The core functionalities of `Poly Bridge` are summarized as below.

– **Extension.** Developers are allowed to extend `Poly Bridge` with new blockchains. The extension requires implementing a corresponding relay and a smart contract to validate the block header of the new blockchain.
– **Interoperation.** Users of `Poly Bridge` can move their cryptocurrencies back and forth between two supported blockchains. The interoperation is a click-button process without complicated configuration. The assets involved are guaranteed to be consistent across all blockchains even if a specific step fails in the process.

II. SYSTEM DESIGN

This section describes the design of `Poly Bridge` in detail. As shown in Figure 1, `Poly Bridge` consists with five modules: `Poly Bridge Application` provides the crosschain service for users; `Chain A` and `Chain B` are supported blockchains in `Poly Bridge Application`; `Poly Chain` is a cross-chain coordinator, which deliveries crosschain transactions between supported blockchains; `Relayer` are a set of nodes that monitor supported blockchains and transfer crosschain requirments and block headers to target blockchains (*e.g.*, `Poly Chain` or `Chain B`). Note that all participant blockchains are deployed with two specific contracts: *Header Sync Contract* and *Cross-Chain Manager Contract*. The former maintains valid block headers of other blockchains so as

978-1-6654-9538-7/22/$31.00 ©2022 IEEE

to verify the inclusion of transactions in those blockchains. Specifically, supported blockchains (*e.g.*, `Chain A` and `Chain B`) synchronize block headers of `Poly Chain`, and `Poly Chain` synchronizes block headers of all supported blockchains. The `Cross-Chain Manager Contract` is responsible for initiating crosschain requests and validating crosschain transactions from other blockchains.

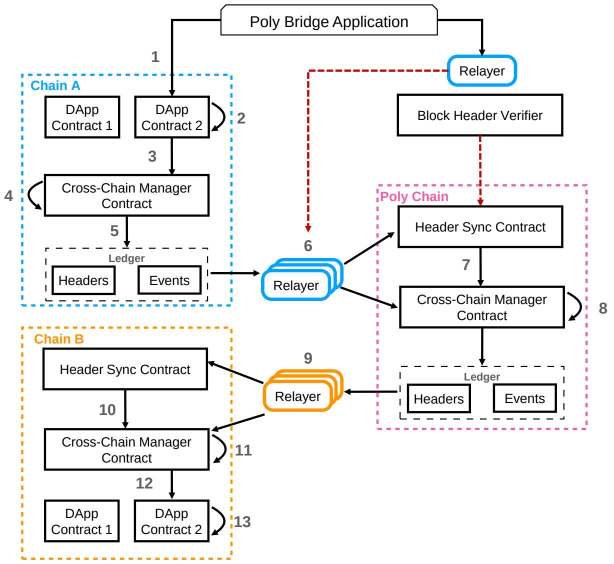


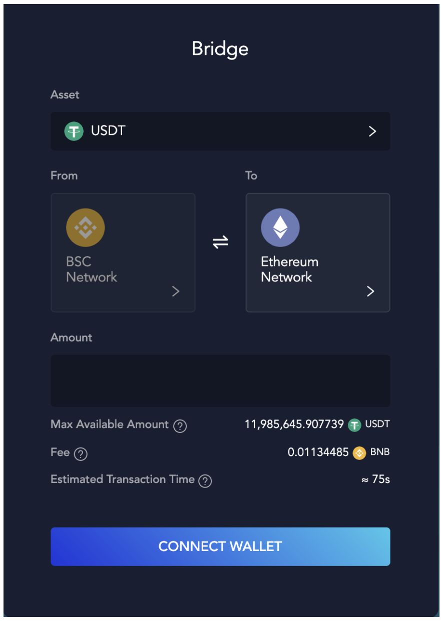
Fig. 1: The architecture design of `Poly Bridge`.

The lifecycle of a crosschain transaction in `Poly Bridge` is as follows: The user of Poly Bridge Application initiates a crosschain transaction T thats invokes DApp contract 2 ① ; `Chain A` performs a transaction T_A (part of transaction T) by executing the function of DApp contract 2 ② and invoking the Cross-Chain Manager Contract ③ ; The Cross-Chain Manager Contract analyzes the crosschain request ④ and logs critical informations M, such as, the target blockchain `Chain B` ⑤ ; The relayer then retrieves the log and transfers M, the hash of T_A, the merkle proof of T_A to the `Poly Chain` by invoking the Cross-Chain Manager Contract on `Poly Chain` ⑥ . The Cross-Chain Manager Contract finds the block header of `Chain A` ⑦ , verifies the inclusion of T_A ⑧ and logs the crosschain information M if T_A is verified, which is denoted as T_P. The relayer then sends M, the hash of T_P, and the merkle proof of T_P to the target blockchain, *i.e.*, `Chain B` by calling the Cross-Chain Manager Contract on `Chain B` ⑨ ; The Cross-Chain Manager Contract invokes the DApp Contract 2 with the information M after proving the inclusion of T_p in `poly chain`, which is denoted as T_B (⑩ - ⑬). Note that a rollback operation is triggered once any transaction fails during the above process.

Besides, `Poly Bridge` can dynamically extend supported blockchains by deploying new relayers and adding new Block Header Verifiers to the Header Sync Contract of `poly chain`.

III. Demonstration Description

The `Poly Bridge` is currently a web application and available at `https://bridge.poly.network` to support over 200 types of cryptocurrencies on 18 heterogeneous blockchains. Figure 2 shows a screenshot of `Poly Bridge`. We plan to demonstrate with the following use cases.



Bridge

Asset

USDT

From

To

BSC Network

⇌

Ethereum Network

Amount

Max Available Amount 11,985,645.907739 USDT

Fee 0.01134485 BNB

Estimated Transaction Time ≈ 75s

CONNECT WALLET

Fig. 2: The web service of `Poly Bridge`.

Use Case A: Extend `Poly Bridge` with a new blockchain. We plan to run a live demo to show the process with `Poly Bridge` to support a new blockchain, which runs a different consensus model than the existing list. Specifically, we will describe the implementations of the relay and block header verifier with pre-defined programming interfaces.

Use Case B: Move `USDT` from Binance to Ethereum. THe crosschain process starts from a user specifying the interoperation, *i.e.*, choose USDT from asset, select the from and to blockchains and input the amount of cryptocurrencies he or she would like to move. The user is supposed to review the validity of the information and cost of the transaction before he or she confirms it. `Poly Bridge` will indicate the status of the transaction once it has been confirmed.

References

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

[2] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, 2014.

[3] M. Zavershynskyi, "Eth-near rainbow bridge," https://near.org/blog/eth-near-rainbow-bridge/, 2020.

[4] T. Baneth, "Waterloo: a decentralized practical bridge between eos and ethereum by kyber network," https://blog.kyber.network/, 2019.

[5] R. Lan, G. Upadhyaya, S. Tse, and M. Zamani, "Horizon: A gas-efficient, trustless bridge for cross-chain transactions," *arXiv preprint arXiv:2101.06000*, 2021.

[6] D. Stone, "Trustless, privacy-preserving blockchain bridges," *arXiv preprint arXiv:2102.04660*, 2021.