Polkadot Bridges RFP

Publication Date: August, 12, 2019

Introduction

The Web3 Foundation (W3F) supports technologies and applications that support the decentralised web, particularly those which utilise modern cryptographic methods to safeguard decentralisation to the benefit and for the stability of the Web 3 ecosystem. One of the principal projects being lead by the W3F is the development of the Polkadot network. Polkadot will empower blockchain networks to work together under the promise of shared security. The network will consist of many heterogeneous chains, known as parachains, which are a more general form of blockchain network with an arbitrary state transition function. Shared security is accomplished through the use of the relay chain which provides security to parachains and relays messages between them. The flexibility of this structure allows Polkadot to offer a broad range of functionality including smart contract and payment support as well as much more. The ability of parachains to exchange arbitrary messages increases both the scalability and the range of functionality offered by the network.

Bridges

Bridges are specialized parachains that allow communication to external blockchain networks such as Bitcoin or Ethereum, that are not secured by Polkadot's relay chain. In order to achieve the broadest notion of interoperability, it's crucial that bridges are constructed for as many different existing blockchain networks as possible.

Scope

The Web3 Foundation is interested in collaborating with teams interested in implementing bridges and has made grant funding available for this purpose. The foundation has not yet designed a specification for a bridge to any existing blockchain network but has developed a list of requirements for bridges that support trustless token transfers. Grant funding is available for the following bridge-related projects:

- Teams who wish to write a full specification and produce a minimal PoC
- Teams who wish to write both a full specification and a full implementation
- A joint application from two teams - one that wishes to write the specification and another team that wishes to do the implementation work

We welcome expressions of interest from teams who are interested in implementing a completed specification. However since we don't currently have a specification, we will not yet be able to award grant funding for this. Such expressions of interest will be used:

- If we choose to run a seperate RFP process solely for implementation teams once completed specification(s) have been produced

- To encourage collaboration by matching implementation teams with those writing a specification.

The Web3 Foundation would like to support bridge development with all major blockchain networks. However, the highest priorities for us at the moment are bridges to Bitcoin, Ethereum and Zcash.

It is expected that successful grant applicants will work very closely with the W3F during the project.

Functionality

Similar to the inter-parachain messaging functionality that Polkadot provides for connected parachains, the gold-standard of bridge functionality is to provide the ability for arbitrary messages to be passed from the external blockchain to Polkadot (and vice-versa) in a trustless manner. Ultimately, this is the level of functionality that the Web3 Foundation wishes to have in its bridges with external chains. However, we believe that the design of bridges with level of functionality is a hard problem.

At a minimum, we would like the bridge to support trustless token transfers from the external blockchain to Polkadot and also provide the ability for those assets to be transferred back from Polkadot to the external blockchain. Based on the XClaim framework, W3F researchers have considered a potential approach to this problem for PoW chains such as BTC and ETH (1.x) which is elaborated upon in this document. This document by no means represents a complete specification and many details have not yet been determined. Submitted bridge specifications are free to use this approach or an alternative one.

Candidates are free to submit applications for bridge designs that offer more functionality than trustless token transfers. However, they must support this functionality at a minimum.

Requirements

The following requirements are for a bridge design that only supports trustless token transfers from the external blockchain to Polkadot and also provides the ability for those assets to be transferred back from Polkadot to the external blockchain. This is the minimum functionality required in any bridge design. Applicants submitting more general bridge designs must ensure these requirements are met where applicable. However, they will also need to develop a more general set of requirements suitable to the functionality that they provide.

It should also be noted that these requirements are based on the W3F researchers’s approach to bridge design and may need to be modified if the applicant submits an alternative design.

- **Safety**
  - Where possible, the bridge should only admit finalized transactions from external blockchains and from the Polkadot relay chain. For blockchains that

lack deterministic finalization such as PoW chains, transactions should only be admitted by the bridge where there is a negligible probability that they will be reversed.

-
  - In the event of a 51% attack on the external blockchain (but not on the bridge parachain):
    - It is impossible to prevent double spending on the external blockchain. However, it should not be possible to manufacture assets on the bridge parachain where the equivalent asset was not collateralized on the external blockchain.
    - It should be possible for bridge actors to detect attacks and respond by delaying finality of manufactured bridge assets or by suspending transactions completely until the issue is resolved.
  - In the event of an attack on the Polkadot relay chain finality (but not on the external blockchain)
    - It is impossible to prevent double spending. However, it should not be possible to redeem bridge assets to the external blockchain where such an asset never existed in the Polkadot network.
    - It should be possible for bridge actors to detect attacks and respond by delaying finality of the redeemed bridge assets or by suspending transactions completely until the issue is resolved.
  - In the event of an attack on the bridge protocol (e.g. 51 % attack on the bridge relayers):
    - As long as a single honest relayer exists, the attack should only have the potential to halt the bridge operation (i.e. harm liveness) but not have the potential to harm safety.
- **Liveness**
  - Every user should able to obtain bridge assets as long as an equivalent amount of assets have been collateralized on the external blockchain.
- **Consistency**
  - The bridge is only able to issue assets on Polkadot if the equivalent value of the assets have been collateralized on the external blockchain.
- **Redeemability**

    - Every user that owns bridge assets on Polkadot should be able to redeem them for the equivalent value of the asset that has been collateralized on the external blockchain.

- **Auditability**
    - The correctness of the bridge operations should be completely auditable and everyone should be able to detect failures.

- **Scalability**
    - The bridge protocol should be scalable and avoid having components that limit scalability.

Deliverables

For the specification, the chosen team will produce the following:

- A description of the functionality and requirements of their bridge design.
- A full written specification of the bridge design. The specification should be detailed enough such that a competent team could implement the bridge.
- A security analysis to explain how the specification corresponds to the stated requirements.

For the implementation, the chosen team will team will produce the following:

- A fully working software implementation of the bridge specification
    - Our acceptance tests should mostly consist of sending messages and/or value through the bridge while preserving trust model constraints.
- Complete documentation
- A demonstration that security was considered throughout the entire project lifecycle and evidence that the implementation has no known security flaws.
- Software should be licensed using Apache 2.0 (preferred) or the GNU GPL v3 license.

It is expected that the chosen team(s) work closely with the W3F during both the writing of the specification and the implementation.

How to apply

To apply for this grant we require that you submit an application form at [Link].

The following information is required in order to be eligible for consideration:

- An indication of whether you are interested in writing the specification with the PoC or both writing and implementing a full specification.
- Official name of project, names of applicant and core developers.

- Details of entity, if any, e.g. legal structure (GmbH, Foundation, LLC) and legal domicile.
- List all previous projects and activity the team and/or its members have worked on in the areas of blockchain or distributed systems.
  - Please include brief descriptions.
- Provide evidence of previous experience.
  - Links to all code repositories, LinkedIn, team website, relevant papers, etc..
- Describe your team's long-term plan and intention after the grant has been awarded.
  - Will your team continue to support the specification and/or software post-grant?
  - Will your team continue to work on the future components of Polkadot?
    - For example: by producing additional bridge specifications or by launching a bridge parachain
- Estimated timeline for development.
  - Include descriptions of each milestone as well as the estimated completion time and required funding for each milestone.
- Indicate the amount of funding required and include a total overall budget that supports this figure.
- For applicants applying to build a specification, please include the following additional items:
  - A description of the proposed functionality of the bridge design
  - An outline of the proposed specification
  - An outline of the bridge requirements if they differ from the Requirements section above.

The Web3 Foundation will evaluate all applications and selectively follow-up to engage in further discussion.

Selection Criteria

The selection of the team(s) is based on the received proposals as evaluated by the W3F. The foundation may contact third parties to request references or request additional information from the applicant.

The following criteria will be taken into account when selecting the team(s). It is expected that proposals will include all necessary information to evaluate the criteria below. When experience is asked for, this applies to both the team as a whole as well as the individual members of the team.

General Criteria:

- Experience with distributed systems and cryptography
- Experience with the Rust programming language
- Any planned usage of subcontractors or other external assistance
- Expected timeline
- All-in cost

Criteria for the team writing the specification:

- Experience in bridge design
- Assessment of the proposed requirements and specification

Criteria for the team writing the implementation:

- Experience in implementing bridges

Process and Timelines

The following table provides a high-level outline of the anticipated process from submitting a proposal to commencement, all the way to project completion. **We anticipate leaving applications open for 3-4 weeks** following publication of this document.

Week	Milestone
0	Issuance of the RFP document
1	Pre-bid calls
3	Submission of proposals by project teams
	Selection of preferred team(s) by the Foundation
	Commencement of project development Development will be separated into predetermined milestones as indicated in the proposal
	Project team to provide an overview of their progress to the Foundation upon completion of each predetermined milestone
	The Foundation reviews each milestone for accuracy and completeness.
	Funding transferred subject to Web3 Foundation review of accuracy and completeness

Resources

Teams may find the following resources useful:

- The Polkadot Wiki
- The W3F Research website

- XClaim’s paper on which the W3F’s bridge design is based
- XClaim’s’ paper on cryptocurrency deposits
- A document by the W3F outlining one approach to bridge design