Snowbridge Funding Proposal

The amount of proposed treasury spends are:

- Polkadot
  - 438,395 DOT
  - Beneficiary: `12UDxESUsqUZi5R5MpovTZLpAWZXPVWHJQkEprcT6MVdKh3A`
- Kusama
  - 25,016 KSM
  - Beneficiary: `Gbb7iGbd6Q7o1fGcT2Re4L6RXJ3U7A32itSLMjsUJzmq5LD`

Overview

Snowbridge is a fully trustless and decentralized bridge between Polkadot and Ethereum.

The proposal covers a request for two years and four months of runway for all operations for the Snowbridge team. Our bridge will launch on the Bridge Hub, a common-good parachain in development by Parity for Kusama and Polkadot.

It also includes a motivation for supporting and promoting Snowbridge, a long-term roadmap, governance, economic plans, and incentives for successful execution, launch and running of the project.

Resources

- Code: https://github.com/Snowfork/snowbridge
- Documentation: https://docs.snowbridge.network

Purpose

What is Snowbridge

Snowbridge is a set of libraries and services for trustless bridging between Ethereum and Polkadot.

Snowbridge brings real innovation to cross-chain interoperability, not just for Polkadot but for the broader blockchain ecosystem. It is the only Polkadot⟷Ethereum bridge that is fully decentralised and trustless. Many other Ethereum bridges exist. However, they all compromise in some way:

1. Some Ethereum bridges trade off trustlessness and decentralisation by relying on a set of trusted parties in a multisig, e.g, Chainbridge, Anyswap, Polygon and Terra. These bridges risk both being regulated away and involve massive counterparty risk for all users. They also completely degrade the trust and decentralisation of any assets that flow through them.
2. Some Ethereum bridges mitigate this counterparty risk by adding a secondary collateral, insurance or bond/slashing system to their multisig or optimistic design. In Axelar, LayerZero, Chainlink and Gravity Bridge, users are not insured, and although there may be slashing to disincentivize fraud and partial collusion, if a majority of signatories collude, then fraud cannot necessarily even be detected.
    a. These mechanisms make them more trustless, but trade off on capital efficiency, leading to higher hidden costs.
    b. They may depend on fraud proofs and have long confirmation times. This introduces a systematic risk if an attacker can censor them for longer than their optimistic confirmation window.
    c. They are collateral-constrained and arguably only able to secure as much value as their collateral allows.
3. Some Ethereum bridges are fully trustless with full on-chain light clients, but still use an optimistic design to reduce computational costs, e.g. NEAR Rainbow. This trades off latency and confirmation time, and also introduces the same systematic risk if an attacker can censor them for longer than their confirmation time.

Snowbridge aims to make no compromises and have minimal trade offs. It will be more trustless than bridges in category (1). It should likely be cheaper, faster and more trustless than bridges in category (2). It should be faster and more secure than bridges in category (3). At worst, the main trade off once fully deployed and completed is that it could be slightly more expensive than bridges in category (1) and (3).

Building and deploying Snowbridge may take longer than other bridges, but as we have all learned from the bridge hacks in 2022, the tortoise beats the hare.

Snowbridge is general purpose

Snowbridge is also general-purpose and bridges arbitrary state, rather than assets. It can connect Ethereum dApps to Polkadot and Kusama parachains, allowing for cross-chain messaging. The light-client based design also means that its trust model is independent of the assets it bridges. It can bridge any value of assets and scale up TVL without any major bottlenecks or barriers related to some underlying collateral or token value.

Risks to the Polkadot ecosystem from insecure bridges

There is high demand for Ethereum bridges across parachains, and some chains have already started introducing more centralised bridges as a stop-gap. However, without Snowbridge, these stop-gaps present multiple systemic risks to the Polkadot ecosystem.

Counterparty Risk

Existing bridges all use some kind of multisig, meaning that assets flowing across those bridges now have counterparty risk in those signatories. A hack or loss of keys could result in major asset losses to those substrate chains and their users and lead to wider sentiment issues for Polkadot as a whole. For example much like how there is now a sentiment around dApps running on Binance Chain being much more dangerous due to repeated hacks and low-quality projects.

Regulatory Risk

These multisigs also introduce regulatory risks onto the parachain teams that use them and the multisig participants. They could be regulated and so forced to shut down or

restrict access, with implications for the security and decentralisation of all assets that flow through those bridges and parachains.

Risk to Product-Market Fit

The biggest risk is actually not legal or trust related, but cuts into the core value proposition of Polkadot. Polkadot's value proposition is that it leases out high security, trustless and decentralised consensus to other chains.

The existing bridges degrade these trust and security properties of any parachains that use them, as most value that exists on those parachains will flow through their Ethereum bridge that is not secured by Polkadot.

If these existing bridges do remain secure and do not become impacted by regulations, while the market continues to accept their trust assumptions and design, then this undermines the whole purpose of Polkadot.

If the existing bridges remain successful, the parachains that use them will be effectively wasting their slot, gaining minimal additional security while paying for a Polkadot slot/lease and would become better off and more efficient if they eject from Polkadot to become a sovereign chain in future. There is a systematic risk to Polkadot if it does not influence the existing parachains and their users to care about the trust properties of their bridges.

New Opportunities for Polkadot

Polkadot secures any assets that flow through Snowbridge. As Snowbridge generates more interest and asset flow both into and out of the Polkadot ecosystem, it uses Polkadot's security and extends Polkadots security outwards.

Assets flowing into Polkadot

The biggest expected use case is asset flow from Ethereum into Polkadot's ecosystem, as people start to tap into the more secure, faster and cheaper protocols and parachains that live on Polkadot. The opportunity here is straightforward and easy to understand. More assets means greater user activity, increasing network effects and positive feedback loops.

Assets flowing out of Polkadot

The basic example of this is assets that originate on Polkadot (eg: Acala/Moonbeam assets) that flow to Ethereum and get used within Ethereum protocols. This basic use already extends Polkadot's security blanket outwards into the Ethereum ecosystem. As these assets become used in DeFi protocols or AMMs providing liquidity, the payoff that an attacker stands to gain by manipulating or controlling these assets increases. This implies that the effective cost of fraud for these assets needs to increase too in order to retain a balanced theoretical crypto-economic security.

Increasing the cost of fraud should directly lead to increased revenue for Polkadot in the long term. Of course, at the moment this balance is not that relevant in practice and so may be difficult to understand, so let's elaborate a bit further:

A more dynamic security marketplace

- Currently, Polkadot sells security under a fairly static model. A chain can buy a fixed-lease slot for a period of time. There is a slot auction, but once a slot is acquired, it gives the same kind of fixed term security based on turnkey slashing conditions and incentives to all chains. A particular chain is not able to configure its required slashing conditions and levels in a bespoke way. This means that all chains get the same kind of security and share it equally, irrespective of how much security they actually need.
- The above setup means that some chains are using their security more efficiently than others and getting a better deal for the cost they pay. Similarly, some chains are overpaying: A chain that has a smaller amount of assets at risk may only need to slash a smaller portion of Polkadot's stake to prevent fraud, and may in fact be better off moving to a cheaper chain like Kusama. Alternatively, it may want to specify a maximum amount of slashable stake that it reserves from the relay chain and get a better deal for reserving less stake. This kind of configurability is not possible at the moment as Polkadot's slashing conditions are the same across all chains.
- Parathreads will come out in time, which do make the market more dynamic in terms of how long/how often a chain purchases security, but longer term we can imagine that a dynamic market around slashing conditions and reserved stake could also become possible.
- Longer term as there are more chains selling security and more competitors, some metric like value-for-money-per-reserved-stake could become relevant for how and

where chains choose to buy security from, especially if layer-2/shared security style standardisation evolves to allow a more free, flexible framework-agnostic market. We're already starting to see this possibility today in new chains that are looking to sell security like Octopus Network and Interchain Security over IBC.

Imagine long term a dynamic market like this does exist, it should be more clear to see how Snowbridge's asset flow out of the Polkadot ecosystem will increase demand and eventually revenue for Polkadot's security.

History

Snowbridge originally started as a W3F grant project in early 2020. The design targeted a security model with minimally trusted actors and a stronger focus on cryptographic proofs and data structures. It completed the initial grant with a working bridge in September 2021, however given dependencies on new features in Polkadot (BEEFY) has been delayed in our ability to launch.

Since then, the team has continued to run independently and continued to maintain and update the existing codebase, scale up with new developers, and make improvements with new functionality to the bridge, including shipping a new architecture to support post-merge Ethereum.

Economics

Our common-good bridge will act as a permissionless hub for cross-chain communication between Polkadot parachains and Ethereum.

In the long-term, the bridge aims to be self-sustaining by generating revenue from usage of the bridge.

The motivation for a common-good bridge also aligns with our motivation to allow the bridge to operate cheaply with as minimal overhead as needed and avoid rent-seeking unless needed, ideally making resources available to everyone fairly as a public good.

Costs

This section covers costs that the bridge and its users will need to cover in order for the bridge to function. Specifically, these are costs that cannot be directly controlled by on-

chain components, as they are charged by outside parties and services.

Operational costs

These are costs that are essential and required to be covered in order for the bridge to remain operational and secure. If for whatever reason these costs cannot be covered, and nobody is willing to pay for them, the bridge will not be sustainable. These are costs that should be shared and covered as a common good.

- **Real-world costs:** This includes all the costs associated with off-chain activities, including running the bridge, infrastructure, maintenance, development, support and all the kinds of things needed to operate a complex system and run a real-world team to do so. It also includes potential requirements for incentives and upside for all entities involved in this. This cost will need to be covered by long term treasury funding, and is detailed later in this document as the core funding request for this proposal.
- **BEEFY relay:** This is the cost for keeping the BEEFY light clients on the Ethereum side of the bridge updated with the latest BEEFY state on Polkadot. This is a flexible cost, as the frequency of updates can be tuned to meet the desired price–performance ratio. This cost is not part of this proposal, and an additional funding proposal closer to launch time should be expected.
- **Ethereum header relay**: This is the cost for keeping Ethereum light clients on the Polkadot side up to date with the latest beacon and execution headers from Ethereum.

Individual Usage Costs

These are costs that an individual user of the bridge may incur as part of their usage of the bridge. These costs can be paid per-user/per-parachain, or on a case by case basis, or on demand as needed.

- **Basic Channel:** With the basic channel, every user has their own message delivery lane, and so cost can be charged and covered independently by individual users or parachains themselves.
- **Incentivized Channel:** This is the cost for submitting a message on-chain and paying the fees imposed by our incentivized channel. This cost can be covered on a

case by case basis, per user/per parachain and does not need to be covered globally, as described above.

Revenue

The service that the bridge will be providing is cross-chain messaging. Charging fees for this service will be the primary source of revenue.

We aim for the bridge to ideally only charge users based on market demand. It will initially aim to operate freely with funding from the treasury, but as demand grows, become self-sustaining.

Cross-chain message fees

These are fees that can be charged for sending cross-chain messages. They will likely be priced on resource usage and message size.

We have considered a fee that is based on the actual contents of a message, for example, charging a basis-points/percentage fee of the value when fungible assets are transferred, but this is unlikely to be effective given that the bridge is designed to support arbitrary message transfer and arbitrary applications, so sticking to resource-based fees is likely best

Parachain transaction fees

The bridge is based on a hub model, where all messages between Polkadot and Ethereum will flow through the bridge parachain. This means that transaction fees for including transactions into the Parachain can also be a source of revenue.

XCM fees

The bridge will communicate with other parachains via HRMP and require XCM messages as part of usage.

Pricing model

Basic Channel

Users or teams must independently relay their messages with the software we provide at their own expense. This model offers flexibility for advanced integrators who, for example, may wish to subsidise the activity of their users.

The channel will impose a small usage fee to prevent spam attacks.

Incentivized Channel

The pricing model will be on pay as you go basis, with each message incurring an upfront fee. This could be priced as a fixed fee, updated infrequently, first come first serve, or could be priced via a typical fee market model.

Users will be charged a fee in wrapped Ether for sending messages to Ethereum. In the opposite direction, users will be charged a fee in wrapped DOT or KSM.

Governance

Overview

As a trustless bridge, we need our governance mechanisms to be appropriately decentralised, with checks and balances.

Since we have on-chain components on both Polkadot and Ethereum, we also need a form of cross-chain governance.

Polkadot Governance and Upgrades

As a common-good bridge, we will rely on the governance of Polkadot itself. Specifically this means the Gov2 decentralised governance system that is being deployed to Kusama and Polkadot.

Compared to Gov1, this will allow for greater governance participation by both ordinary users and domain experts in the Polkadot fellowship.

Ethereum Governance and Upgrades

Our bridge has a significant number of contracts on the Ethereum side, and these contracts need to be able to evolve along with the parachain side.

As a prime example, Polkadot and BEEFY consensus algorithms will change, and so we need to make sure our smart contracts support these changes over time.

In general, the design for our upgradable smart contracts is quite simple, relying on versioning of immutable contracts. This contrasts with the popular but complicated

proxy upgrade pattern, which has many drawbacks.

Smart contract upgrades and configuration changes will be triggered by governance on Polkadot, through the use of cross-chain messaging secured by the bridge itself. There are implications if governance messages cannot be delivered to Ethereum for any reason. For this reason, we considering various fallback options.

Bridge Hub

Our bridge will launch on the Bridge Hub, a common-good parachain that is being developed by Parity for Kusama and Polkadot.

This choice helps reduce the operational load on our team, so we can focus on bridging technology rather than network operations.

Launch Plan

We will deploy first to Kusama, followed by Polkadot. The deployments will be independent. Both deployments will bridge to Ethereum mainnet. There are currently no plans to bridge to other Ethereum networks.

Upon launch, the bridge will support bidirectional transfers of Ether, ERC20 tokens, DOT and KSM. A client library will also be provided to allow third-party teams to build their frontends around the bridge.

The launch will be followed by future upgrades that implement more of the features requested by the community. These features are described in the roadmap section.

Rococo

We already have the bridge deployed to the Rococo testnet, bridging to Goerli, the main test network for Ethereum. Our main use for Rococo is for testing our light clients and XCM integrations.

While development continues, we expect the bridge to break or be reset fairly often.

Kusama

Even though Polkadot is the end goal, we see Kusama as a very important stepping stone for our bridge, where we can exercise it with real users and assets, but within

certain limits.

By the time we deploy on Kusama, our full security model and security audits will be in place. However, there will have been minimal testing with real world assets and scenarios. So we envision the following operating model:

- There will initially be strict limits on the TVL locked into the bridge. As confidence in the bridge grows, this limit will be progressively increased.
- There will be some level of insurance against an exploit, funded via an extra liquidity proposal.
- White-hat hackers will be incentivised to exploit the bridge via bug bounty programs

Polkadot

We want our bridge to bake on Kusama for at least three months before deploying on Polkadot.

As with Kusama, the maximum-allowed TVL will start off low, and then increase over the year, following a similar launch process to Kusama.

Once our Polkadot bridge is live and stable, we may consider deprecating the Kusama bridge and replacing it with a Kusama⟷Polkadot⟷Ethereum bridge, but this is a decision that can be made longer term in the future.

Roadmap

Overview

This section covers the long term roadmap of the project, broken down into milestones, each of which is roughly 6 months in duration. While we have a big list of features we'd like to develop, we also invite the community to share their own ideas. That's why we've only listed 12-18 months worth of improvements and features.

The order and content of our milestones is by no means final, and we expect shifts to occur. However, launching on Kusama and Polkadot is a priority, and all proposed feature development needs to fit into that schedule.

These are the estimated dates for launching the bridge. Note there is at least a 3-month gap between launching on Kusama and Polkadot.

1. April 2023: Deployment of bridge on Kusama
2. July 2023: Deployment of bridge on Polkadot

These dates are intended to be *flexible*. There are many various internal and external factors that could influence delivery:

- Our delivery progress on technical milestones
- The deployment and activation of the following items by Parity:
  - BEEFY
  - BridgeHub
  - Gov2
  - XCMv3 and Statemint upgrades
- Scheduling of security audits & pentesting

Milestone M1

This milestone lists projects for the remainder of 2022 and early 2023.

Use XCMv3 for base layer messaging protocol

The goal is to extend XCMv3 to Ethereum and use it as the default cross-chain messaging protocol.

Mint wrapped assets on Statemint

Statemint should be the reserve chain for all wrapped assets bridged over from Ethereum.

Governance on Ethereum

We need to be able to govern changes to the Ethereum side of the bridge. This is important for controlling upgrades to Ethereum contracts. For example, BEEFY will evolve over time, and so we duly need to upgrade our BEEFY light client in tandem.

Upgradable Smart Contracts on Ethereum

This needs to be fully implemented before we can go live. Our upgrade design is quite simple. Smart contracts will remain immutable. Contracts can be updated to refer to

new versions of contracts they depend on.

Client Library

Provide a Typescript library for interfacing with the bridge.

Milestone M2

Limiter

After surveying many bridge and defi hacks it has become increasingly apparent that some kind of limiter would enhance the security of the bridge. It would provide defence in depth, in case our proof-based security model is subverted for any reason. This limiter could be implemented as either a dynamic circuit breaker on withdrawals of collateral, or more simply as a maximum limit on the TVL locked into the bridge.

Security Audits

The Snowbridge codebase has previously undergone 2 security audits in 2021 for fulfilment of its initial W3F grant. Our codebase has evolved considerably since then, and so those audits are obsolete.

As such, we plan to secure new audits for our code before deploying onto Kusama. After the initial deployment, we also plan to hold regular audits, especially for major ongoing protocol-level changes.

Production Infrastructure

For our testnet, we currently deploy our parachain nodes, ethereum nodes, and off-chain services using our own infrastructure platform, built using AWS EC2, Hashicorp Nomad, Consul and various other cloud-native tooling. This stack is working well for us, but as Parity is building out shared infrastructure and tooling for common-good chains, we'll likely want to migrate over to their solution.

Launch on Kusama

The launch will be phased in over a course of several weeks:

1. Deploy pallets onto Bridge Hub parachain
2. Activate Ethereum→Parachain bridge with strict TVL limits

3. Activate Parachain→Ethereum bridge with strict TVL limits
4. Remove TVL limits after an appropriate amount of time

Milestone M3

Unlock General-Purpose Messaging

Enable any third-party parachain to communicate with arbitrary smart contracts on Ethereum using `Xcm::Transact`

Launch on Polkadot

The launch will be phased in over a course of several weeks:

1. Deploy pallets onto Bridge Hub parachain
2. Activate Ethereum→Parachain bridge with strict TVL limits
3. Activate Parachain→Ethereum bridge with strict TVL limits
4. Remove TVL limits after an appropriate amount of time

Bridge Statemint assets to Ethereum

Any fungible asset homed on Statemint could be bridged over to Ethereum.

NFT Support

Support for NFT transfers between Statemint and Ethereum

Ongoing Maintenance and Support

Besides for specific milestone deliverables, working in the Polkadot ecosystem on a parachain demands a heavy workload for maintenance and operational support.

As a light-client powered bridge, we need to ensure our system is compatible with evolving consensus models in both Polkadot and Ethereum.

Team

Aidan Musnitzky and Vincent Geddes have been leading the bridge team. We have prepared some biographies for more information on our current team.

Aidan Musnitzky

Aidan is the founder of Snowfork and supports various projects at Snowfork, including supporting and advising the Snowbridge team. Aidan has a background in a range of areas. A long time back, he worked on distributed systems at Amazon Web Services building out functionality for EC2. He's spent the last decade consulting on a wide range of projects, including other Blockchain and Cryptocurrency projects and helped bootstrap various crypto startups and advises an early-stage fund in the space.

Aidan started Snowfork a few years ago and has scaled it up to 20+ engineers across various teams and works on various different projects at Snowfork. Aidan played a primary role in the initial development of Snowbridge during 2020/2021 as an engineer and architect, and now supports the team, advising on technical and strategic leadership on an ongoing basis.

Vincent Geddes

Vincent is the technical lead for Snowbridge and has been with the project for over two years. Previously, Vincent had stints at Oracle and Amazon Web Services. In both roles, he specialised in virtualisation hypervisors, cloud infrastructure, and monitoring.

As an early AWS EC2 team member, Vincent co-developed the first generation of CPU-burstable instance types, among other projects. At Oracle, Vincent helped integrate the Xen hypervisor in the compute service of Oracle Cloud (first generation). He later led maintenance and feature development for that aspect of the Compute service.

In the distant past, he dabbled with compiler and runtime development for languages such as Smalltalk and Scheme.

Alistair Singh

Alistair has been a member of the Snowfork team for one year, working on Snowbridge's XCM implementation as well as onboarding Snowbridge onto Rococo. He completed a Bachelors in Computer Science degree and currently resides in the City of Cape Town. With 13 years of experience developing software in the traditional FinTech spaces, such as insurance and online casino industries.

He was previously employed at Amazon AWS as part of EC2's Control Plane team, where he obtained experience building and maintaining critical systems at scale. In the

computing field, he is passionate about databases, simulations, game development, programming language design, and most recently, blockchain technology.

Clara van Staden

Clara is a backend engineer with 9 years of experience in commercial software. After completing a B.IT degree (graduating top of her class) at the University of Pretoria in South Africa, she joined Globetom to work on many different projects for mainly telecommunications clients. She represented Globetom at the TM Forum, a global telecommunications standard's body and won several awards for her contributions.

Thereafter she joined Over, a distributed startup building a visual communication app. Clara was responsible for building APIs to enable serving content (fonts, project metadata, images) for the web and mobile apps, using Go. Over was acquired by GoDaddy in 2020.

In 2022, Clara joined Snowfork to work on Snowbridge. She is responsible for the work required for the Ethereum upgrade. Over the last year, she has implemented a beacon light client to track the Beacon chain consensus.

David Dunn

I'm an obligate tinkerer: fiddling with workflows, tools & languages is a favourite pastime of mine. I've worked at fintech companies for a few years and joined Snowbridge to change things up by working with blockchains & the Rust programming language. So far so good! Having fully remote work on an open source project is also fantastic.

My current task is to allow multiple accounts to send messages over our basic (non-incentivized) channel. This enables anyone to run their own relayer to forward their messages, which is a key part of the bridge being trustless. Nobody should have to trust that someone will run a relayer (whether for an incentive or not) to get their messages across the bridge.

Retrospective

The project has been self-funded since September 2021, when we completed our last grant deliverable for the W3F. This deliverable was to ship a working end to end trustless Ethereum bridge based on a Proof of Work light client and an old, now

deprecated version of BEEFY. Since then we continued to evolve the project, and have completed and embarked on many projects listed further below.

Overall, the core technical focus over the last year has been on the following:

1. Supporting Ethereum PoS Consensus, and deprecating our Ethereum PoW light client.
2. Tracking upstream BEEFY development as it evolves to its final production ready form.
3. Reworking and refining our core bridging protocols and pallets
4. Maintaining a testnet on Rococo.

Another priority has been building up our team, and developing enough in-house expertise to execute on new features with greater velocity. Our project requires solid experience in both Polkadot and Ethereum, and so onboarding and growth has involved many months of ramp up time for new developers who have joined us.

Completed or ongoing projects

Light Client for Ethereum Proof-of-Stake Consensus

Now that Ethereum and its testnets have been merged, we can no longer use our PoW light client (which we developed back in 2020). As such we have developed a new light client, tracking the Beacon chain's PoS consensus.

This development has involved close collaboration with the Ethereum consensus community, as we are one of the few teams developing light clients for the Beacon chain.

The PoS light client is working and operational on our Rococo testnet. That said, we expect a few more months of refinement, testing, fuzz-testing, and auditing before we can consider it ready for production workloads.

See the design for a high-level overview. The light client pallet lives in our codebase here. The off-chain relayer component can be browsed here.

BEEFY Light Client Development

The BEEFY protocol has continued to evolve and improve since we completed our W3F grant deliverables. We have followed closely, keeping our light client up to date, and

collaborating with BEEFY developers to troubleshoot issues and test new changes in the protocol.

Our BEEFY light client and related off-chain services have been totally rewritten since the initial versions delivered to W3F. The code is more readable, secure, and robust.

Current development efforts are focused on:

- Compatibility with the new RANDAO randomness source in post-merge Ethereum.
- Optimizing gas usage

Pull requests

Testnet Operations

For a short while, we maintained our own private relaychain and parachain testnet, which bridged to the Ethereum Ropsten network. Upon joining the Substrate Builders programme in early 2022, we migrated to the official Rococo testnet, where we help exercise BEEFY.

Our system also requires many offchain services such as message relayers, as well as nodes for Ethereum.

As part of the Substrate Builders programme, our team has gained a lot of experience operating a parachain on Rococo. Like upgrades, storage migrations, dealing with block production issues, and so on.

Everything is hosted on AWS EC2. HashiCorp Nomad and Consul are used for service orchestration and discovery. Traefik is used for load balancing, SSL termination, etc. There is a lot of complexity here and so in future we'd really like to migrate to whatever infrastructure is being used to host other common-good parachains and adjunct services.

Assets V2

As we gained experience with Substrate and XCM we realised our initial approach to representing Ethereum-native assets on our parachain was deficient, limiting, or would cause more problems down the line.

- Replaced our custom homebrew assets pallet with the upstream pallet-assets from Substrate

- Ethereum-native assets represented using 128-bits instead of 256-bits for better compatibility with XCM.

Pull Requests: #562, #9742

XCM Auto-forwarding

This is a feature which allows Ethereum users to transfer assets on Ethereum directly to third-party parachains, initiated by a single Ethereum transaction.

Without this feature, users would first have to bridge Ethereum assets to our parachain, and then issue a separate transaction with XCM instructions to transfer the wrapped assets to the final destination parachain.

Pull Requests: #533, #654, #556, #563

Permissionless Basic Channel

Our basic channel (See Technical Design) was previously permissioned in the sense that only privileged users may use it to send messages over the bridge.

We changed its design to make it permissionless. This was a fairly complicated feature, as it involved adding another layer of merkle proofs in our bridging protocol for the Parachain→Ethereum direction.

Pull Requests: #637, #679

Contributions to Go-Substrate-RPC-Client

GSRPC is the main Golang client for Substrate, built and maintained by Centrifuge. As one of the main consumers of this library since 2020, we have contributed significant resources towards keeping it up to date as Substrate evolves.

Since Sep 2021, we have contributed the following: #249, #259

Contributions to Substrate

Besides helping to test the BEEFY protocol, we also added a new feature to the FRAME assets pallet, to help support use cases beyond Statemint: #9742

Smart Contract Versioning

This is ongoing design and implementation work to support upgradability of our smart contracts.

Pull Request: #714, #706, #697

Other work

Besides new features, we have also invested a lot of resources in maintenance and iterative improvements, including:

1. Improvements to core bridging protocol: #631
2. Updating parachain with new versions of Polkadot/Substrate/Cumulus: #534, #591, #710.
3. Update pallets to FRAME 2.0 macros: #527
4. Reorganise Javascript/Typescript projects: #717

There are many other smaller improvement and maintenance tasks. See our repository for a full commit history of work since September 2021.

Funding Motivation

This funding proposal and plan revolves around a central goal: Maintaining and incentivizing a high-performance engineering team that can produce great value for the Polkadot ecosystem with a longer-term runway of two or more years.

Most parachain teams today that do this are funded under a traditional VC-backed model with a token and incentives that may make it challenging to align with a common-good parachain approach.

The VC model effectively creates teams with a stable, secure long-term runway, security and flexibility in spending, and generous incentives for upside in the project's success. Running a project related to bridging and interoperability is a complex task that requires significant resources and incentives.

Most interoperability projects in the blockchain ecosystem have required runways in the tens of millions of dollars, in addition to the high potential upside with valuations on the order of hundreds of millions of dollars.

Snowbridge decided against seeking external funding and has been bootstrapped beyond our initial grant for over a year. This choice allows us to maintain optionality in our direction and maintain the potential for alignment as a common good.

This funding proposal requests the Polkadot treasury to support major public good projects and parachain teams through similar dynamics to VC-funded projects. We're hopeful that this can succeed and that our project can also play a part in growing a more robust culture around funding high-impact public goods that need a long-term runway and strong incentives.

Funding Structure

The funding and resources required and requested for this project can be broken down as follows:

1. **Runway funding:** General-purpose funding for the team, covering costs across all areas, including salaries, infrastructure, software services, travel, conferences; and business functions as accounting, tax, payroll, legal and recruitment.
2. **Incentives funding:** Funding for the team to provide incentives for successful execution, running and success of the bridge project and to give the team upside in the success of the project and its impact on the Polkadot ecosystem.
3. **Funding for audits and bug bounties:** Funding for at least two audits from highly reputable firms for both an initial audit and ongoing audit and security support as needed.
4. **Funding for insurance:** We'll likely want some insurance coverage for the bridge in the event of loss due to a bug. Insurance may not scale long term, as eventually we hope the bridge's security will stand sufficient on its own, but initially it will be valuable to get from the treasury to add a safety net for users.
5. **Operational funding for light clients:** As detailed in Operational Costs, our light clients have operating costs that need to be covered.
6. **Liquidity bootstrap for wrapped assets:** We will want to get Ethereum liquidity into Polkadot's ecosystem, as well as some DOT liquidity into Ethereum's ecosystem.

The funding request in this proposal covers only the runway funding in (1).

Runway Funding

Snowfork is requesting **$3,060,000** runway funding in total to cover the period from 1 Sept 2021 to 30 Dec 2023 (28 months).

1. **$1,218,166** will apply to the period from 1 Sept 2021 to 30 Dec 2022 (16 months)
2. **$1,841,834** will apply to the period from 1 Jan 2023 to 30 Dec 2023 (12 months)

The team expects to maintain complete autonomous control over its runway and how to spend it, so the total amount is requested upfront.

Compared to the requested amount in our previously circulated proposal draft, we have revised our budget downwards. The requested funds will be stretched to cover an extra four months of runway. This is in recognition of the recent downturn in the crypto market in mid-2022, and the need to operate more frugally.

Retroactive funding

The retroactive numbers are based on actual investment already made into the project over the last year, broken down as follows:

Item	Details	Amount
Engineering Team	This was initially 3 core contributors with 2-3 additional part time contractors in 2021, but has ramped up to currently 5 core contributors across dev and management	$942,300
Supporting Staff	Costs from supporting Snowfork staff and services, including HR, Accounting Services, Tax Services, Recruiting Services and Referrals	$134,500
Infrastructure	System infrastructure costs, including costs like AWS, Tenderly, Alchemy, ElasticSearch, Infura and a few other hosting services Every dev has their own EC2 instance for development, as our development environment does not work well on laptops.	$84,916

Item	Details	Amount
Software Services	Software services used by the team, including costs like Google Workspaces, Slack, Discord, Github, Linear, Lever, Quickbooks, Notion and a few other software services	$16,760
Travel, Team Events, Conferences	Costs related to travel, team events, coworking and conferences	$22,000
Hardware	Hardware costs, primarily laptops for staff	$8,500
Admin, Legal, Insurance	Fees and payments related to administrative costs, payroll, legal and insurance related fees	$7,150
Total		**$1,218,166**

The above numbers are more heavily weighted towards recent months as the team has scaled up and currently runs at around $85,000 per month. Additionally, the project leads have been working for significantly below market rates.

We give a detailed accounting of the work done over the last year in the retrospective section of our proposal.

Future Runway

For upcoming year we're requesting funding to support market-competitive pay for the entire team. We also expect to spend more on the following:

- 1-2 additional developers
- Travel costs for attending both Polkadot and Ethereum events

The runway funds are therefore aimed to cover a team of 7 as well as support staff for admin, payroll, recruitment, and so on.

We are also including a 10% buffer, in case the price of DOT falls significantly in the voting and enactment period for this proposal.

We expect to submit a similar proposal for runway funding in a year. However, if the team does not utilise the additional buffer of funds requested, nor scale up as quickly as expected, then those funds may spillover and allow us to delay that runway proposal.

Incentives Funding

With a runway in place for team expenses, there is still the need to ensure that incentives are in place so that the team has a sense of long-term ownership and a part in the upside related to the project's success.

We're requesting funding to be allocated for this, covering incentive bonuses for:

- Succeeding at shipping and launching the milestones outlined in our roadmap
- Overseeing successful operation and maintenance of the bridge, including being part of governance.
- Successful long-term stewardship for operation and security of the bridge
- Research & development of future next-gen improvements or evolutions of the bridge

This will consist of several incentive triggers, each with a DOT reward that triggers based on certain conditions. Rewards based on engineering milestones are expected to vest over 2 years, and rewards based on measured success and impact on the Polkadot ecosystem are expected to vest immediately.

We feel a total of $10,000,000 in exposure to DOT, measured based on the price of DOT at time of the follow up incentive funding proposal, is fair if the project is highly successful and makes a measurable impact on the Polkadot ecosystem, with the majority of exposure being weighted to success and impact triggers rather than engineering milestone triggers.

This will be structured as:

- $1,875,000 in long term, vested DOT exposure as a reward for engineering milestone completion and successfully shipping and launching the bridge on both Kusama and Polkadot
- $8,125,000 in long term DOT payouts over 24 months based on successful operation and usage of the bridge and its impact on parachains in the ecosystem

Payout Trigger	**Amount (will be measured in DOT and KSM @ the Subscan EMA7 exchange rates at time of submission of follow up proposal)**
P1 - Milestone M1 and related tasks fully completed and reviewed	$375,000, in DOT vesting over 2 years

P2 - Milestone M2 and related tasks fully completed and reviewed, including live Kusama launch	$562,500, in DOT vesting over 2 years
P3 - Milestone M3 and related tasks fully completed and reviewed, including live Polkadot launch	$937,500 in DOT vesting over 2 years
P4 - Bridge is live with successful operation on Kusama for 3 months and at least 3 parachains integrated and bridging to Ethereum	$625,000 in KSM paid out on trigger
P5 - Bridge is live with successful operation on Polkadot for 3 months and at least 3 parachains integrated and bridging to Ethereum	$937,500 in DOT
P6 - Continued successful operation on Polkadot from a period of 3 months after launch to 24 months after launch, with at least 6 parachains integrated and bridging in assets	$312,500 DOT paid out monthly on trigger for 21 months
Total	**$10,000,000**

For all triggers related to successful operation and parachain usage, if for any reason there is a break, delay or security issue or loss of funds from the bridge, that trigger will be paused.

The trigger will then only resume if the bridge resumes in operation successfully and usage and sentiment of the bridge from parachains continues.

Evaluation of milestones and payments

Our milestone deliverables will need to be reviewed, and then funds disbursed accordingly using a *vested.Transfer* call. To structure this process, we anticipate a governance collective being formed from various stakeholders (Parity, W3F, parachain teams, community members, etc). Snowfork will obviously have no representation on this body.

The collective will:

1. Review the scope of the milestones and any requests to change scope
2. Review the milestone deliverables
3. Vote on the whether to mark the milestone as completed satisfactorily
4. Execute the *vested.Transfer* call, transferring funds from the treasury to accounts under Snowfork's control.

For this to work, the review collective should have control over the incentive funds. Given that the collectives functionality is not yet live, we propose to defer payment of the incentive funds until then. Once the collectives functionality is live, the incentive funds should be transferred to an account controlled by the Review collective. If the collectives functionality is not live, or not suitable for use by the time of the first milestone, then voting should be coordinated offchain and the current Polkadot council should execute the *vested.Transfer* on behalf of the offchain collective.

The collective will be subordinate to Polkadot governance. This is a remedy in the case that the collective becomes inactive or if any counterparty wishes to dispute an issue.

Additionally, given that the Polkadot ecosystem involves evolving technologies, we will still need to be able to adapt to changes and maintain an agile development workflow as part of our roadmap. In practice, this means being able to make change requests to planned roadmap items and milestone evaluation criteria if the space changes in unexpected ways. This same review collective will be responsible for evaluating and accepting requests to change the roadmap and milestone deliverables.

Funding for audits

We'd like to get independent audits from two different auditing firms. This includes a full initial audit of all aspects of the protocol and all on-chain code on Polkadot and Ethereum. This should also lead to an ongoing relationship with an updated audit every few months as any changes are shipped.

We have not engaged with or gotten a quote from auditors yet, but we expect this to cost in the realm of $300,000 to $500,000 per auditor.

Given this, we're requesting $1,000,000 to be allocated for initial audits, although this can be adjusted in more detail when we have concrete quotes.

Remaining funding requests

Funds for insurance, light client operations, and liquidity bootstrap will likely be requested in follow up proposals closer to the launch time.

For the operational costs of the light clients we expect a figure of anywhere between $200,000–$1,000,000 per year, as detailed in Operational Costs.

Source of funds

Given that the eventual launch will be primarily focused on Polkadot, we expect the majority of this proposal to be covered by the the Polkadot treasury, however it does make sense for some portion to be covered by the Kusama treasury given that the technology will be deployed to and benefit Kusama as well.

We propose for the split to be as follows:

- The runway funding should be split with 20% covered by Kusama and 80% covered by Polkadot.
- The incentive funding should be split with the Kusama-specific incentive payouts being covered by Kusama and the remainder being covered by Polkadot.

Summary of Funding Request for this proposal

USD EMA7 prices at 2022-11-21T14:41:00 UTC+2 by Subscan

Token	Amount	USD Price (EMA7)	USD Value
DOT	438,395.42	5.584	$2,448,000
KSM	25,016.35	24.464	$612,000

DOT beneficiary address:

`12UDxESUsqUZi5R5MpovTZLpAWZXPVWHJQkEprcT6MVdKh3A`

KSM beneficiary address:

`Gbb7iGbd6Q7o1fGcT2Re4L6RXJ3U7A32itSLMjsUJzmq5LD`

Future expectations (not part of this proposal)

- Audit funding: **$1,000,000**
- Operational costs for light clients: **$200,000–$1,000,000** per year
- Incentive funding
  - **$1,875,000** allocated across successful completion of milestone work and launch of the bridge on Kusama and Polkadot, vesting over 2 years from completion and launch
  - **$8,125,000** allocated for success and impact of the bridge for a 2-year period post launch of the bridge