SIP-15 Delay Migration and Upgrade the dApp

Summary

This proposal considers taking advantage of opportunities made possible by the Arbitrum migration, delaying the migration date by a further 6-8 weeks (from the date of this proposal), to integrate some major upgrades to the SlingShot dApp.

Author

winglash

Sponsors

k3nto
tabby7227

Type of proposal

Initiative proposal

Community incentives & rationale

Hey Slingers!

Another proposal for us all to consider and vote on. This proposal considers delaying the migration to Arbitrum for a further 6-8 weeks to enable Slingshot to build in some pretty epic upgrades to its tech stack.

As everyone across the community has been helping migrate to Arbitrum, a few contributors have identified the potential for some big improvements to UX moving forward.

The proposed upgrades would integrate seamless creation of non-custodial MPC wallets, one-click social logins, gas sponsorship, seamless transaction signing and instant bridging between Arbitrum and the SlingShot layer 3.

Ultimately, this would combine to create a unified, seamless UX for both web2 and web3 users, making interacting with SlingShot dApp feel like a web2 experience.

These upgrades would push out the migration date, by an estimated 6-8 weeks (from the date of this proposal), and would mandate changing how claiming of migrated tokens work, but these upgrades

are only realistically possible to integrate now, during the migration period.

Once everything is live again, it would not be possible to retroactively integrate this technology, as by then token locks would already be present on the new layer 3 chain.

Let's talk more about each of the upgrades.

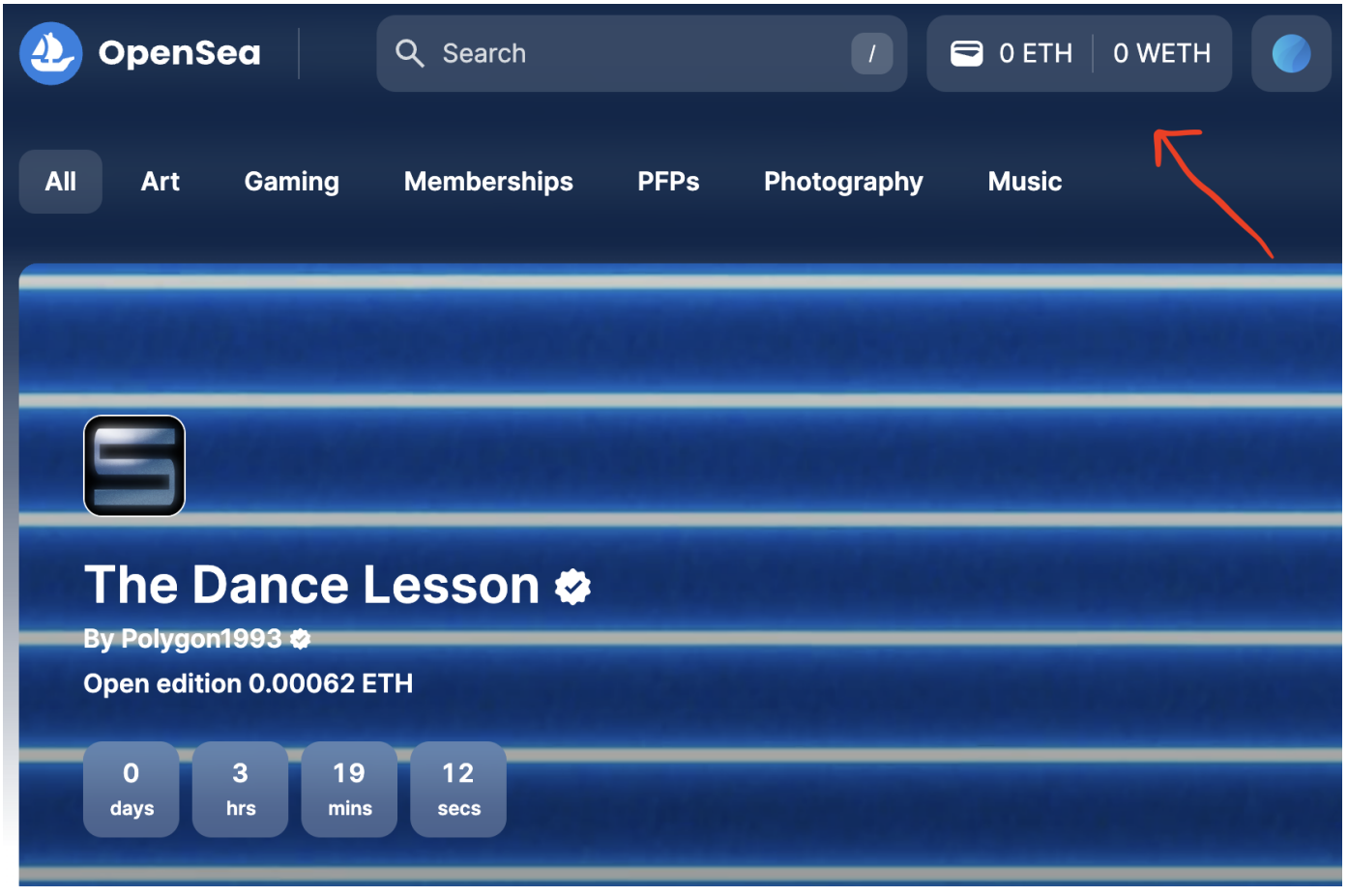
Non-custodial MPC Wallets

What is an MPC wallet?

Following in the footsteps of projects like OpenSea, Binance, Ronin Wallet (& others) SlingShot DAO could integrate the seamless creation of MPC wallets to users who sign into the dApp.

In simple terms, users would automatically create a self-custodial wallet when they sign in (i.e. via google login). This wallet would be natively integrated into the dApp UX.

(try logging in via an email to OpenSea for a good example).



Only the user can ever control the private keys to this wallet, so they would remain in control.

With this technology anyone who signs in to the dApp, will be able to interact with the dApp straight away with this wallet, without having to go through the complexities of using an external wallet or extensions like Metamask.

Using MPC wallets like this opens up some other opportunities too, such as

Gas sponsorship (the user no longer needs to pay gas to interact with the SlingShot dApp).
Unified user journey (one UX for both web2 and web3)
Seamless bridging (invisible bridging between Arbitrum and the SlingShot layer 3 chain).

Pros:

- Seamless user onboarding for web2 and web3 users alike.
- Future development efficiency as only 1x user flow needs to be designed and engineered.
- Seamless user journeys, such as invisible bridging, seamless bundled transactions and gas sponsorship.
- Ability to design the product and services for both web2 audiences and web3 audiences with one solution.

Cons:

- Everyone will need to use an MPC wallet.
- Increased cost to run MPC infrastructure.
- Inability to interact with SlingShot directly with a hardware wallet through the UI (see "changes to supported wallets" below).

Some popular providers of MPC wallet infrastructure are https://web3auth.io https://privy.io and https://turnkey.com

Gas Sponsorship

What is gas sponsorship?

SlingShot DAO would also be able to sponsor the gas fees of users, enabling gas free transactions within the SlingShot ecosystem. This can be achieved by pairing MPC wallets with smart accounts (ERC-4337).

At a technical level, this would mean every user who signs in to the SlingShot dApp would generate a self-custodial MPC wallet and then that wallet set up as an owner of an ERC-4337 compatible smart account.

In simple terms, this means that a user would not have to pay for gas to interact with the SlingShot dApp once they have been onboarded.

Gas Cost

The majority of transactions to sponsor would be on the SlingShot layer 3 chain, where $SLING is the native token used for gas. As the DAO is also running a sequencer on the layer 3 chain, a large proportion of the gas fees are effectively recovered by the DAO, meaningfully reducing the cost of sponsoring gas further.

However, care should be taken to ensure reasonable rate limits and other defenses are in place, to ensure that abusing gas sponsorship (i.e. by spamming transactions) does not become an easy target for malevolent actors.

Pros:

- Users can bridge tokens and use the SlingShot dApp without having to consider gas costs.
- Greatly simplifies UX and product design to focus solely on the dApp utility instead of blockchain technical requirements.
  Allows web2 audiences to engage without having to educate about gas.

Cons:

- Increased cost to sponsor gas fees (predominantly on Arbitrum).
- Increased complexity using ERC-4337 smart accounts.

Seamless Bridge

What is a seamless bridge?

This same approach could be used to simplify the bridging process, making it almost invisible to users.

By combining both MPC wallets and smart accounts, a user would be able to deposit tokens on Arbitrum, complete a sequence of clicks within the dApp, resulting in having quickly and seamlessly bridged tokens to the SlingShot Layer 3 chain.

Every transaction after the initial deposit on Arbitrum would not require the user to have any gas, and allows for a seamless bridging and dApp experience that would feel “invisible” to most users.

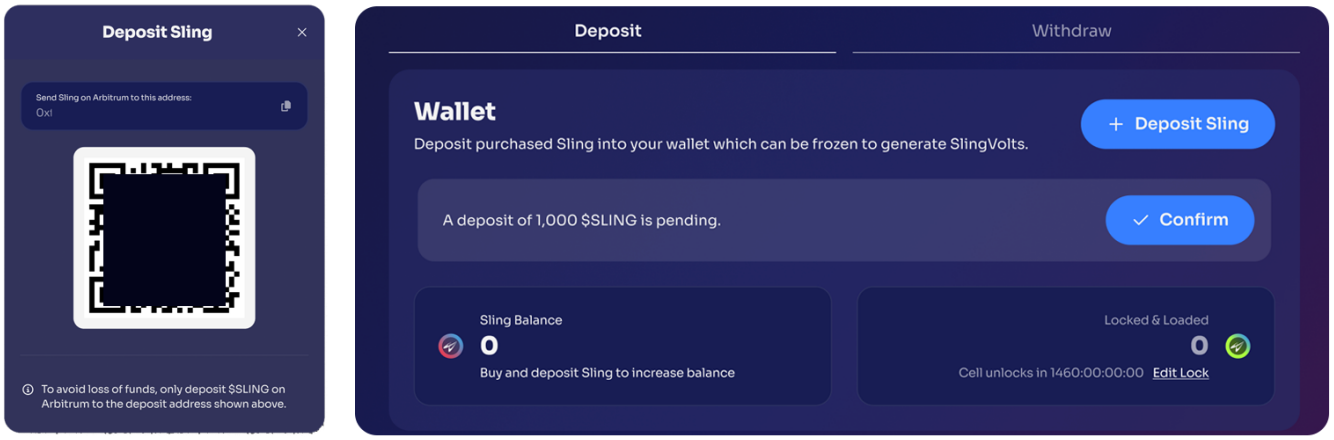
Technically this can be achieved by using MPC wallet providers with arbitrary support for EVM compatible chains and deterministically deploying the smart accounts (ERC-4337) to both Layer 2 and Layer 3 simultaneously, sponsoring the gas payments on both sides.

Security

An audit of the bridge infrastructure and deployment should be undertaken to minimize the risk to the DAO.

Concept

Below is a concept UI for a seamless bridge:



Clicking “confirm” would invisibly bridge the $SLING to the layer 3 chain with no gas fee for the user.

Gas Cost

Minimizing the friction of user onboarding is important but it's also important to understand the increased cost to the DAO of sponsoring bridge transactions and ensuring that denial of service attacks against SlingShot as the gas payer are not feasible.

Based on preliminary testing, it’s expected that each sponsored bridge transaction on Arbitrum would cost the DAO 0.00000115544 ETH (at current gas prices).
This scales as follows:

No. of TX -> Gas Cost
100,000 = 0.115544
250,000 = 0.28886
500,000 = 0.57772
750,000 = 0.86658
1,000,000 = 1.15544

As per the table above, at current gas estimates the DAO would be able to sponsor approximately 1,000,000 bridge transactions between Arbitrum and the SlingShot layer 3, for just over 1 ETH.

Once again, good care must be taken to ensure this does not become an easy target for malevolence. A combination of minimum deposits, rate limits and potentially fees taken in given directions should be explored and must be implemented to increase the cost of any such ill intent beyond feasibility.

Pros:

- Make bridging invisible to the user.
- Greatly simplifies the user journey and minimizes friction to onboarding.
- Instant bridge maximizes engagement and conversion of new members joining the DAO.
- An audit can be undertaken of the instant bridge infrastructure to better reduce the risk.

Cons:

- Risks with running an instant bridge, such as exploits and/or loss of keys.
- Cost of auditing the instant bridge infrastructure.
- DAO needs to actively maintain pools of tokens on both sides of the bridge.
- Users who bridge outside of the dApp would be outside of the dApp expected user journey.

Changes to the migration

To implement this technology, the migration to Arbitrum would need to be pushed out by an estimated 6-8 weeks. This would give the DAO a chance to re-work a lot of the dApp infrastructure, undertake audits and properly test the new integrations.

It would also mean some important changes to how the migration will work.

Previously, in SIP-13 (Migration to Arbitrum) the intention was to develop an automatic distribution mechanism on the Arbitrum chain. Users wouldn't have to do anything to claim their $SLING tokens, as they would be programmatically sent to the same addresses that had locked tokens on Polygon.

Unfortunately, this is fundamentally incompatible with transitioning to the use of MPC wallets in the SlingShot dApp.

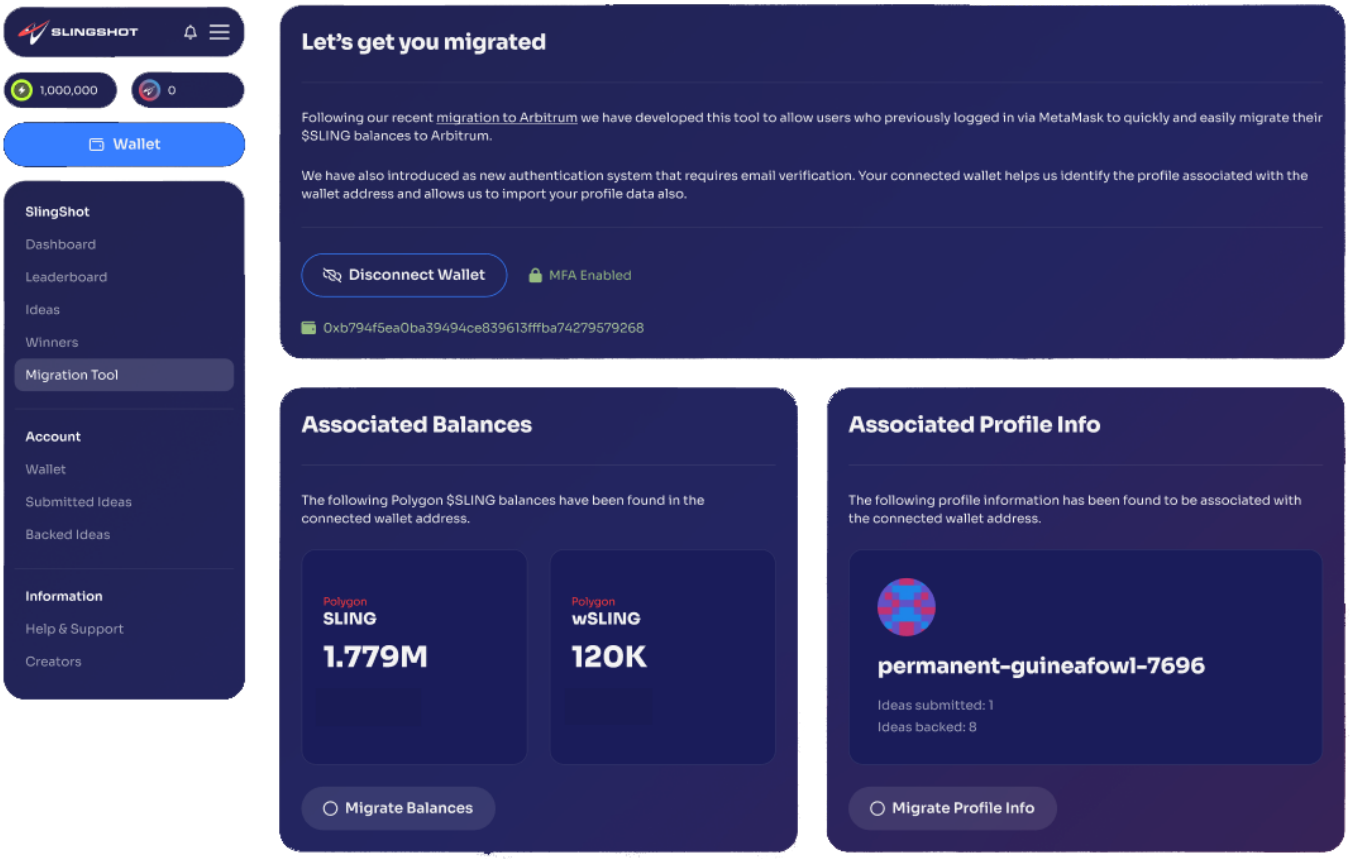
Instead, SlingShot would need to implement a more traditional 'claim' system.

Users who want to migrate their tokens over would have to:

1. Sign in to the SlingShot dApp (and generate an MPC wallet)
2. Connect their old wallet from Polygon
3. Confirm the migration of their locked $SLING to their new ERC-4337 wallet address.

In reality this is only a few extra steps and nice UI/UX can be built around it. But it is a departure from what was voted on in SIP-13, and so important that it is understood when considering this proposal.

Below is a concept UI for claiming from the migration:



Pros:

- This is a "once in a lifetime" opportunity that can only be done during this migration period.
- Can build a nice UX around migration claiming. See concept above.
  Cons:
- Migration will require active claiming by users, instead of being seamless as per SIP-13.
- Extra development to create a migration claim page.

Changes to supported wallets

Limited initial wallet support

It's important to note that this is a departure from the current approach where users can connect their wallets directly. With this new direction everyone must interact with the dApp with an MPC wallet as the signer of the ERC-4337 smart account.

In simple terms, users would no longer be able to use their hardware wallets directly with the SlingShot smart contracts through the UI.

Possibility to re-enable hardware wallet use in the future
Theoretically, it would be possible to allow a user to use their hardware wallet as the signer on the ERC-4337 smart account, so this limitation does not need to be permanent, but would be out of scope for this initial implementation.

This also means that users who lock tokens via this new direction are not necessarily stuck with using the MPC wallet as the signer. The token lock occurs at the ERC-4337 smart account, the signer of which can be changed.

This would theoretically allow for users to, in the future, change the signer to a hardware wallet without having to worry about having tokens locked already.

Risks

Risks if this proposal does not pass

- SlingShot DAO will have to develop two entirely separate user journeys forever going forward, one for web2 users and the other for web3 users that have locked tokens directly and are locked for up to 4 years.
- Developing two user journeys is resource intensive and will not be sustainable for the DAO in the years to come.
- Inability to currently solve seamless onboarding to L3 for web3 users.
- Friction onboarding to L3 threatens SlingShot DAOs ability to grow.

Risks if this proposal passes

- All users will need to use MPC wallets.
- It will no longer be possible to use a hardware wallet directly with the contracts through the UI.
- Increased cost for MPC wallet infrastructure and reliance on third party providers.

Key Terms

Self Custodial

Description: A self custodial wallet in the blockchain context is a type of digital wallet where the user has full control over their private keys and, consequently, their assets. This means the user is solely responsible for the security and management of their cryptocurrency holdings, as opposed to relying on a third-party custodian.

MPC Wallet

Description: A Multi-Party Computation (MPC) wallet is a type of digital wallet that enhances security by splitting the private key into multiple parts, held by different parties. This decentralized approach requires a consensus among the parties to authorize transactions or reconstruct keys, reducing the risk of a single point of failure or compromise.

Arbitrum

Description: Arbitrum is a layer 2 scaling solution for the Ethereum blockchain designed to improve transaction throughput and reduce fees. It uses optimistic rollup technology to process transactions off-chain while leveraging the security of the Ethereum mainnet, thereby enhancing scalability and performance.

L3

Description: In the blockchain ecosystem, L3 refers to the third layer of protocols built on top of layer 2 solutions (L2). These protocols aim to further enhance scalability, interoperability, and functionality, providing additional layers of abstraction and services to improve the overall experience.

ERC-4337

Description: ERC-4337 is a proposed Ethereum standard for account abstraction, allowing the separation of the wallet logic from the underlying account. This enables more flexible and user-friendly account management features, such as multisig wallets, social recovery mechanisms, and more advanced access control policies.

UI

Description: User Interface (UI) refers to the visual and interactive elements of a blockchain application that users interact with. A well-designed UI ensures that users can easily navigate and utilize the application's features, contributing to a better overall user experience.

UX

Description: User Experience (UX) encompasses the overall experience and satisfaction a user derives from interacting with an application. It includes aspects such as usability, accessibility, performance, and user satisfaction, aiming to create a seamless and intuitive interaction with the technology.

dApp

Description: A decentralized application (dApp) is a software application that runs on a blockchain network, rather than being hosted on centralized servers. dApps leverage smart contracts to operate in a decentralized manner, offering transparency, security, and resistance to censorship.

Bridge

Description: In blockchain, a bridge is a protocol that allows the transfer of assets and data between different blockchain networks. Bridges facilitate interoperability, enabling users to move tokens or information across separate blockchains, thus enhancing the interconnectedness of the blockchain ecosystem.

Specifications

Actions

- Defer the Arbitrum migration by an estimated 6-8 weeks to allow for further development.
- Integrate the seamless creation of MPC wallets at user sign in.
- Re-design the onboarding user journey to account for:
- MPC wallet creation.
- ERC-4337 smart account creation.
- Securing MPC wallet recovery before depositing.
- Depositing $SLING to MPC wallet.
- Claiming tokens from the migration.
- Seamless bridging to the SlingShot layer 3 chain.
- Gas sponsorship.
- Develop dApp to meet new designs.
- Audit the new integrations and bridging infrastructure.

Measurements of success and desirable outcomes

- All new technology developed and integrated within 6 weeks.
- Easy claiming of migration $SLING.
- Onboarding and bridging within a few clicks.
- Bridging between Arbitrum to layer 3 within a few seconds.

Impact on working groups

Predominantly design, engineering and governance efforts involved.

Impact on economics

- SlingShot DAO will need to seek good terms with an MPC wallet provider. *(https://privy.io , https://web3auth.io and https://turnkey.com are well known providers that can be referenced for pricing.)*
- The cost of the new integrations being independently audited.
- At the time of writing, estimated costs are around $4000 per month for 100,000 monthly active wallets, with discounts per MAW as volume increases.
- Estimated cost of approximately 1 ETH for every 1,000,000 bridge transactions sponsored.