Submitted by: The Arbitrum Foundation

Category: Constitutional, Software Upgrade

# Abstract

This Constitutional AIP proposes upgrading both Arbitrum One and Arbitrum Nova's Rollup Contracts to use Arbitrum BOLD: a new dispute resolution protocol that is designed to replace the existing and currently deployed Arbitrum protocol. BOLD delivers two critical improvements:

- Unlocks permissionless validation for Arbitrum chains,
- Enhances the security of Arbitrum chains by mitigating the risk ofdelay attacks.

BOLD accomplishes this feat by ensuring that any single honest party can always successfully defend against malicious claims to an Arbitrum chain's state. BOLD represents the next step on the journey to having the Arbitrum technology stack being recognized as a Stage 2 Ethereum rollup. The implementation of BOLD will be thoroughly tested to ensure both its effectiveness and safety. The testing plan includes:

- A comprehensive audit by Trail of Bits,
- Deployment of the protocol to public testnets for at least 8 weeks,
- A public audit program,
- Publication of mathematical safety proofs and formal specifications.

This proposal requests the ArbitrumDAO to approve an upgrade to the onchain smart contracts and to support the deployment of a new challenger manager contract on Ethereum. If the upgrade is approved, then validators on Arbitrum One and Arbitrum Nova can use the Nitro software to participate in BOLD.

Additionally, all Arbitrum Orbit chains may choose to adopt BOLD to reap the security benefits of this new dispute resolution protocol as soon as the upgrade is generally available. BOLD, like the current Arbitrum dispute resolution protocol, makes use of WebAssembly (WASM) technology and can seamlessly support Arbitrum Stylus, should the ArbitrumDAO adopt Stylus.

# Motivation

The ArbitrumDAO should consider approving this AIP as BOLD delivers critical security and decentralization improvements for Arbitrum One and Arbitrum Nova that benefit all Arbitrum users, Arbitrum node operators, dApps on Arbitrum, and Arbitrum bridges. These benefits can be extended to any Orbit chain that wishes to adopt BOLD.

More specifically, this new dispute resolution protocol brings the following benefits to Arbitrum chains:

- Permissionless validation
- Today, the critical role of being a validator for Arbitrum One and Nova is currently restricted to a permissioned set of validators in order to prevent delay attacks on the current rollup protocol - a class of attacks where actors can delay confirmations if they are willing to sacrifice their stakes. However, since BOLD mitigates the risks of delay attacks using a different mechanism (enforcing a fixed upper time bound on dispute resolution), reliance on a permissioned set of validators is no longer necessary. Therefore, passing this AIP and implementing BOLD to secure Arbitrum One and Nova effectively enables permissionless validation, marking a key milestone for Arbitrum chains to be recognized as Stage 2 Rollups, as part of Arbitrum's journey to full decentralization.
- Fixed delay time for assertion confirmation
- The current rollup protocol for Arbitrum chains has a ~6.4 day challenge period during which validators can dispute claims about the chain's state. These claims about the chain's state are called "assertions". While assertions are confirmable after 1 challenge period, malicious actors can open many challenges to delay confirming these assertions in a type of attack known as a delay attack. BOLD guarantees that all assertions, if there is a dispute using the validating bridge contract, will be confirmed within a fixed time window of 2 challenge periods (~6.4 days each), 1 day grace period for the security council to intervene, and a small delta for computing challenges.
- Security Council Safety-First Approach
- There is a set of contracts on Ethereum known as the OneStepProver contracts. These contracts are used to declare a winner in a challenge by producing the correct L2 state given the single step of WASM execution being disputed. As mentioned above, a 1 day "grace period" (also called the "challenge grace period") exists at the end of a dispute for the Security Council to intervene if there are any severe bugs in the OneStepProver contracts. The grace period is configurable by the ArbitrumDAO and initially set to 1 day.

# Rationale

Enabling permissionless validation has been a long term goal of Arbitrum on theprogressive journey towards decentralization.

BOLD mitigates the risk of delay attacks on Optimistic Rollups by ensuring challenges can be resolved within a fixed time period so long as there is an honest party involved. This particular change unlocks permissionless validation, enabling any well-resourced honest party or parties to defend and protect Arbitrum from malicious actors. All Arbitrum nodes are like watchtowers - honest validators by default and are able to catch fraudulent claims, and act if so desired.

More specifically, this AIP for bringing BOLD to Arbitrum chains is:

- Ethereum-aligned:

Arbitrum, with BOLD validation, will continue to rely on Ethereum for transaction data and the arbitration of disputes. Additionally, in line with Ethereum's commitment to being open to everyone, Arbitrum will become more decentralized and trustless since participation to secure the network (i.e. validation) will be entirely permissionless and open to everyone who wishes to participate.

- Sustainable:

The BOLD protocol is a long-term dispute resolution protocol to secure Arbitrum chains. Additionally, there are already future investments and research expected following the initial launch, to ensure BOLD and its security guarantees evolve alongside the Arbitrum protocol, technology, and community.

- Secure:

The BOLD protocol is an intentional and strict improvement to the security model of Arbitrum chains. Arbitrum rollup chains, with BOLD validation, will continue to rely on Ethereum for data availability of transaction data and the arbitration of disputes.

- Socially inclusive:

Should this AIP be adopted, permissionless validation using BOLD will allow any entity, individual, or team in the community to participate constructively in securing Arbitrum. Validation is not restricted to a single address, as BOLD considers all entities that are proposing honest claims to be part of the same team. Where one honest validator may fall off, another one can take up its same responsibility.

- Technically inclusive:

The BOLD protocol specification is publicly available on Github here. The technology is permitted for use by anyone (i.e. permissionless) for the sole purpose of operating and developing an [Arbitrum Nitro Instantiation.

](https://docs.arbitrum.foundation/assets/files/Arbitrum%20Expansion%20Program%20Jan182024-4f08b0c2cb476a55dc153380fa3e64b0.pdf)

- User-focused:

If this AIP is adopted, both users and dApp project developers on Arbitrum One and Nova alike will not need to take any additional action to reap the benefits of BOLD. BOLD will be working silently "under the hood" to ensure safe withdrawals and secure, permissionless validation.

- Neutral and open:

BOLD has been and will continue to be "built in the public", in line with how Orbit and Stylus are being developed. This AIP is made in good faith to be neutral, transparent, factual, and open for anyone in the community to critique and inspect.

# Implementation, Formal Specification, and Safety Proofs

The following link, BOLD Implementation Deep Dive, explains how BOLD is implemented and how it works at a high level. To read about the formal specification and mathematical safety proofs for the protocol, check out the official BOLD whitepaper.

# Overview of BOLD's Economics and Spam Prevention

This section describes the bonding mechanism behind Arbitrum BOLD at a high level. The following link, Economics of Disputes in Arbitrum BOLD, offers greater details on the rationale behind the proposed bond sizes, why bonds are important, and how to think about their magnitude in the context of designing a dispute resolution protocol.

Based on feedback, we wanted to clarify the various roles and expectations for those participating in bold validation -

By default, all Arbitrum nodes are validators that will track the progress of the chain to verify assertions being posted to the parent chain to flag if an invalid assertion is observed. Running this type of validator is permissionless today and does not require any bond. Running a validator in this mode is also known as a “watchtower” node.

BOLD lets validators permissionlessly become proposers and challengers if they want to. The role of a proposer is required to help progress the chain which requires bonding ETH, proposing and then posting state assertions to the parent chain. This bond is known as an “assertion bond”. The chain only needs 1 proposer to make progress. Therefore, most validators can watch the chain and independently verify assertions without being a proposer.

In the unhappy case where there is a dispute about a proposed state assertion, BOLD lets anyone permissionlessly put up a bond of ETH to open challenges in the defense of Arbitrum (in their capacity as a challenger to invalid state assertions). This bond is known as a “challenge bond”.

Given that participation in BOLD is permissionless, we recommend that the size of bonds required to participate be high enough to disincentivize malicious actors from attacking Arbitrum One and Nova and to mitigate against spam (that would otherwise delay confirmations up to approximately 1 challenge period). High bonding values do not harm decentralization because (1) trustless bonding (or staking) pools can be deployed permissionlessly to open challenges and post assertions, and (2) any number of honest parties of unknown identities can emerge to bond their funds to the correct assertion and participate in the defense of Arbitrum at any time within a challenge. As with the current dispute resolution protocol, there are no protocol level incentives for parties who opt in to participate in validating Arbitrum One and Nova with BOLD.

While both of these bonds can be any ERC20 token and be set to any size, this proposal recommends the use of the WETH ERC20 token & the following bond sizes:

- Assertion bonds:

1500 ETH - required from validators to bond their funds to an assertion in the eventual hopes of having that assertion be confirmed by the rollup protocol. This is a one-time bond required to be able to start posting assertions. This bond can be withdrawn once a validator’s assertion is confirmed and can alternatively be put together via a trustless bonding pool.

- Challenge-bonds, per level:

3600/1000/100/10 ETH - required from validators to open challenges against an assertion observed on Ethereum, for each level. Note that “level” corresponds to the level of granularity at which the interactive dissection game gets played over, starting at the block level, moving on to a range of WASM execution steps, and then finally to the level of a single step of execution. These values were chosen to achieve a ratio of malicious-to-honest costs of 10:1. These bonds can be refunded at the end of a challenge and can also alternatively be put together by the community using a trustless bonding pool.

The following link, Economics of Disputes in Arbitrum BOLD, covers the rationale behind the design and recommended values above in greater detail. Note that the ArbitrumDAO can change these values and the type of asset used for the bonds via a governance proposal.

BOLD makes permissionless validation possible for Arbitrum rollup chains and marks a major step towardsfull decentralization. This significant milestone also lays the groundwork for productive discussions about future economic incentives for those participating in the protocol since anyone can participate.

### Reimbursements and penalties

Once all of a validator’s proposed top-level assertions are confirmed, a validator can withdraw their full assertion bond. Other costs spent by the honest parties to defend Arbitrum, such as the L1 gas costs and the challenge bonds, are refundable following confirmation of all sub-challenges. The mechanism of reimbursement for challenge bonds will be finalized and shared as an update to this post at a later date. L1 gas costs will be reimbursed by the Arbitrum Foundation using an procedure that will be published at a later date. All costs spent by malicious actors, including the assertion bond, are confiscated and sent to the ArbitrumDAO treasury. The ArbitrumDAO will therefore have full discretion over what to do with the funds confiscated from a malicious actor. This includes, but is not limited to:

- Using the funds to refund L1 gas costs to honest parties,
- Rewarding or reimbursing the honest parties with some, or all, of the confiscated funds,
- Burning some, or all, of the confiscated funds, or
- Keep some, or all, of the confiscated funds within the ArbitrumDAO Treasury

Note that honest parties are not automatically rewarded with the funds confiscated from malicious actors, so as to avoid creating a situation where honest parties wastefully compete to be the first one to make each honest move in the interactive fraud proof game.

## Technical risks

Some of the technical risks of the BOLD upgrade include:

- Issues preventing liveness of challenges due to smart contract bugs in the new contracts. For instance, no honest validator able to make a move when it should be able to;
- Safety issues where a malicious party is able to game the system and win due to logic errors in smart contracts;
- Logic bugs in the assertion smart contracts that could affect assertion confirmation and posting, which could delay withdrawals until it is fixed; and
- Bugs in bonding logic in the smart contracts that could lead to loss of funds due to logic errors in the Arbitrum Rollup and challenge manager smart contracts.

Risks that remain the same between the current Arbitrum Rollup protocol and BOLD

- Bugs in the one step proof logic: BOLD does not change how one step proofs work for Arbitrum chains.

## Timeline and steps to implement BOLD for Arbitrum One and Nova

Below is a list of initiatives to ensure the new BOLD dispute resolution protocol is ready to be reviewed and ready to be voted on by the ArbitrumDAO for adoption in Arbitrum One and Arbitrum Nova. Feedback from the community and any findings from testing will be collected and used to inform decisions and evolve BOLD along the way.

1. Deployment of a public testnet with BOLD validators for a minimum of 4 weeks, meant to ensure BOLD gets tested against conditions closer to what would be seen on mainnet (e.g. complexity of txns, traffic volume, larger and diverse validator sets, L1 testnet with real usage, etc).
2. a. Please check out this guide on how to deploy a BOLD validator on the testnet to begin testing out permissionless validation using Arbitrum technology!
3. The submission of the AIP in the format of a forum post. [This post]
4. Audit of the protocol's implementation by Trail of Bits.
5. Hosting of a governance call to talk about BOLD to answer questions from the community about BOLD and this AIP.
6. A formal temperature check proposal to activate BOLD on Arbitrum's Sepolia for a minimum of 4 weeks. be made via a snapshot vote, as per Phase 1 in the The Lifecycle of an Arbitrum Improvement Proposal
7. Kick-start a public audit program.
8. Finalize pre-mainnet requirements, including:
9. a. Publication of BOLD migration documentation for existing validators;
10. b. Deployment of a monitoring stack to view on-going challenges on an Arbitrum chain; and
11. c. Publication of a formal procedure for The Arbitrum Foundation to handle L1 gas costs reimbursements for honest parties.
12. Formal AIP gets submitted to Tally. A call-for-voting will be made, as per Phase 2 in The Lifecycle of an Arbitrum Improvement Proposal.
13. Should the formal on-chain proposal pass, BOLD will activate on Arbitrum One and Nova following Phase 7 of the Lifecycle of an Arbitrum Improvement Proposal flow.

BOLD is now deployed on a permissionless public testnet as of April 15, 2024 that settles to Ethereum Sepolia. Should the corresponding governance proposals pass, the target timelines for BOLD to get activated on Arbitrum Sepolia is late Spring 2024 and then eventually Arbitrum One and Nova sometime in Summer 2024. These dates are tentative targets that will depend on a number of factors, including the governance vote outcomes, audit findings, and feedback from the ArbitrumDAO community.

## Overall Cost

There is no cost for this proposal to the ArbitrumDAO as Offchain Labs, Inc. will incur all engineering and audit costs to complete the implementation of BOLD and get this new dispute resolution protocol into a mainnet-ready state. Engineering efforts to prepare BOLD for mainnet, as documented in the Steps to Implement section above will be owned by Offchain Labs, Inc. Currently, future development work for BOLD is expected to also be undertaken by Offchain Labs, Inc.

## References

- BOLD whitepaper, containing both the formal specification and mathematical safety proofs.
- BOLD Implementation Deep Dive
- BOLD Economics Deep Dive
- Implementation on Github: https://github.com/OffchainLabs/bold
- Guide on how to run a BOLD validator on testnet:GitHub - OffchainLabs/bold-validator-starter-kit: Starter kit repo for running Arbitrum BOLD validators
- BOLD Gentle Introduction documentation
- Announcement blog for BOLD
- Solutions to delay attacks on Optimistic Rollups, a blog that highlights a core motivation behind BOLD's development: https://medium.com/offchainlabs/solutions-to-delay-attacks-on-rollups-434f9d05a07a

## Where to Learn More about BOLD?

- There will be a governance call about BOLD and permissionless validation, and this event is available on the ArbitrumDAO Governance Community Calendar.
- Date & Time: Thursday, 25 April, 16:00 - 16:45 UTC
- Link to join: https://meet.google.com/mmv-zfps-duz
- Date & Time: Thursday, 25 April, 16:00 - 16:45 UTC
- Link to join: https://meet.google.com/mmv-zfps-duz
- Tune in to the AMA on 'Uncovering BOLD & Permissionless Validation' on April 18, at 11:30 ET: https://twitter.com/OffchainLabs/status/1780643417522901337