The ArbitrumDAO is one of the best examples of decentralized, permissionless and autonomous governance being applied at scale.

As the DAO continues to grow, it uses a polycentric governance approach, where each of its approved initiatives (e.g. ARDC, ADPC, Delegate Incentive Programme, LTIPP, STIP, etc.) has unique governance structures and operational procedures. It is common for these initiatives to have a multi-signature wallet (multi-sig) committee responsible for managing and dispersing DAO-approved funds, following the terms agreed by the DAO via on-chain governance, as well as with the Arbitrum Foundation.

The DAO recently approved the Multi-Sig Support Service (MSS), so there will likely be greater standardization and streamlined multi-sig operations going forward. Accordingly, the Arbitrum Foundation would like to share some 'Multi-Sig Best Practices' based on its observations of the existing DAO-related multi-sigs. It is recommended that DAO-related multi-sigs, including the MSS, follow the guidelines and processes outlined below to adhere to high operational security (OpSec) standards.

Signer Best Practices

1. Use Secure Hardware:

Maintain at least two hardware wallets with the same seed phrase. These hardware wallets should be exclusively dedicated to DAO-related multi-sig transactions.

1. Dedicated Devices:

Utilize a separate, dedicated laptop or device solely for signing transactions.

1. Unique Signer Addresses (Keys):

Use a unique signer address (key) for each DAO-related multi-sig wallet. Avoid reusing addresses (keys) across different DAO-related multi-sig wallets. Each unique signer address (key) can be generated from the same wallet (i.e. using the same seed phrase). All signer addresses must be shared with the Arbitrum Foundation to pass compliance.

1. Unique Payment Address:

If you receive compensation for performing multi-sig signer duties, use a separate address from your signer address(es) to receive payments. All payment addresses must be shared with the Arbitrum Foundation to pass compliance.

1. Transaction Simulation:

Always simulate transactions using Tenderly (available on Safe) to ensure the transaction performs as intended before signing.

1. Verify Information:

Double-check all relevant sources of truth, such as the on-chain Tally proposal, before signing any transaction. If in doubt, do reach out to the DAO Relations team at the Arbitrum Foundation (@raam and @cliffton.eth), and to fellow signers, to ensure that all details about the queued payment(s) are accurate as per the on-chain Tally proposal and agreement terms.

1. Exercise Caution and Seek Assistance:

If you are unsure about a transaction, do not sign. Raise any concerns with fellow signers immediately. If you encounter any technical issues, promptly ask for help.

1. Bookmark Essential Links:

Bookmark links to DAO-related multi-sig wallets or rely on pre-established, trusted sources. Avoid clicking on links provided by external parties.

1. Availability Notification:

Inform fellow signers at least 24 hours in advance if you expect to be unavailable or unable to sign transactions for any period.

1. Report Key Issues:

Notify other signers and the Arbitrum Foundation via email immediately if you lose access to your signing keys or suspect they have been compromised.

Setting Up a Multi-Sig Wallet

1. Initial Communication:

All signers should exchange email communications and share a signed message from the key to be installed. The message should include:

- Ethereum account address: “[signer address]"
- A statement identifying the signer and the multi-sig wallet they are joining: “[Message: I am X and I am joining the Y multi-sig]"
- Signature hash: ”[signature]"
- Key Authentication:

Conduct 1-to-1 and group calls among signers to authenticate the signing key with the owner. Do not rely solely on Telegram for key authentication.

1. Clawback of Funds:

As the ultimate owner of its funds, the ArbitrumDAO should be able to clawback funds from any of its multi-sigs by executing a respective Tally proposal - which can be enabled if multi-sigs are set up using the Zodiac Governor Module, for example.

Adhering to Terms and Conditions

1. Review Proposals Carefully:

Always review the respective on-chain Tally proposal before disbursing any funds, as they are the source of truth for payment schedules, payment caps, recipients, and other important details. If you have doubts, please reach out to the DAO Relations team at the Arbitrum Foundation.

1. Follow Agreements:

Abide by the terms and conditions of any agreements made with the Arbitrum Foundation. For example, only sign transactions to distribute funds which (a) have been approved by the ARB Community per the Tally proposals, (b) have satisfied appropriate compliance measures (such as know-your-customer checks) and documentation (as applicable) as confirmed by Foundation and (c) comply with the ArbitrumDAO Constitution.

1. Conflict Resolution:

If there is a conflict among proposals regarding fund disbursement, contact the Arbitrum Foundation for guidance.

1. Compliance Confirmation:

Never disburse funds without receiving confirmation from the Arbitrum Foundation that all compliance and necessary background work have been completed.

1. Recipient Detail Changes:

If a recipient needs to update any details (e.g. the address for receiving funds), they must contact the Arbitrum Foundation to restart the compliance process before any payments can be made.

Communication Protocol

1. Telegram Group:

Establish a Telegram group that includes all signers and members from the Arbitrum Foundation’s DAO Relations team.

1. Multi-channel Communication:

Do not rely solely on Telegram. Regularly speak with fellow signers through calls to ensure clear communication.

1. Transaction Request Template:

When requesting signatures, use a consistent template. This could either be through a bot (e.g. Onchain Den) or a manual template that includes:

- Nonce
- Payment details
- Amount
- Compliance status

- Multi-sig wallet name (avoid using links)
- Transparent Queuing:

For greater transparency, the person queuing the transaction can record a Loom video of the process and share it with the other signers.

1. Record Keeping:

Maintain a shared record of payments made (e.g. on Google Sheets) with version history that tracks:

- Recipient name
- Recipient address
- Payment amount
- Compliance completion status
- Recipient address confirmation
- Transaction Confirmation:

Signers should confirm on their Telegram group when they have signed or executed a transaction.

1. Periodic Reporting:

Publish transaction summaries on the DAO forum at regular intervals (e.g. monthly) to maintain transparency.

Notification Process Between Arbitrum Foundation and Signers

1. KYC Completion:

‘Recipient A’ completes KYC with the Arbitrum Foundation.

1. Notification:

The Arbitrum Foundation informs ‘Multi-Sig A’ via email that ‘Recipient A’ is eligible for payment.

1. Acknowledgement:

‘Multi-Sig A’ acknowledges the update with the Arbitrum Foundation.

1. Address Verification:

‘Multi-Sig A’ verifies with ‘Recipient A’ that they control the KYC-approved address by requesting an on-chain signature, and sharing this proof over email.

1. Transaction Queuing:

‘Multi-Sig A’ queues the transaction (or batch of transactions) and shares the details with other signers using a transaction form template, Onchain Den bot, Google Sheet, and/or Loom video.

1. Signer Communication:

Signers coordinate and confirm when they have signed the transaction.

1. Execution Notification:

Once the transaction is executed, ‘Multi-Sig A’ communicates this update to the Foundation and the DAO via the forum.

Key Terms:

- Multi-signature (multi-sig) wallet:

Wallet that requires multiple private key signatures to execute transactions.

- Signer:

Member of a multi-sig wallet

- Hardware wallet:

Physical device (often resembling a USB pen), that securely stores private keys, offline.

- Seed phrase:

Sequence of random words that stores the data required to access or recover private keys

- Signer address:

The public address (an ENS or a randomly generated string of numbers and letters), like an email address, of a member of a multi-sig wallet

- (Private) key:

Randomly generated string of letters and numbers, like a password, that allows a respective signer to sign and execute transactions

- Payment address:

Address of a member of a multi-sig wallet used to receive compensation

- Recipient:

A DAO stakeholder who receives funding from a DAO-related multi-sig