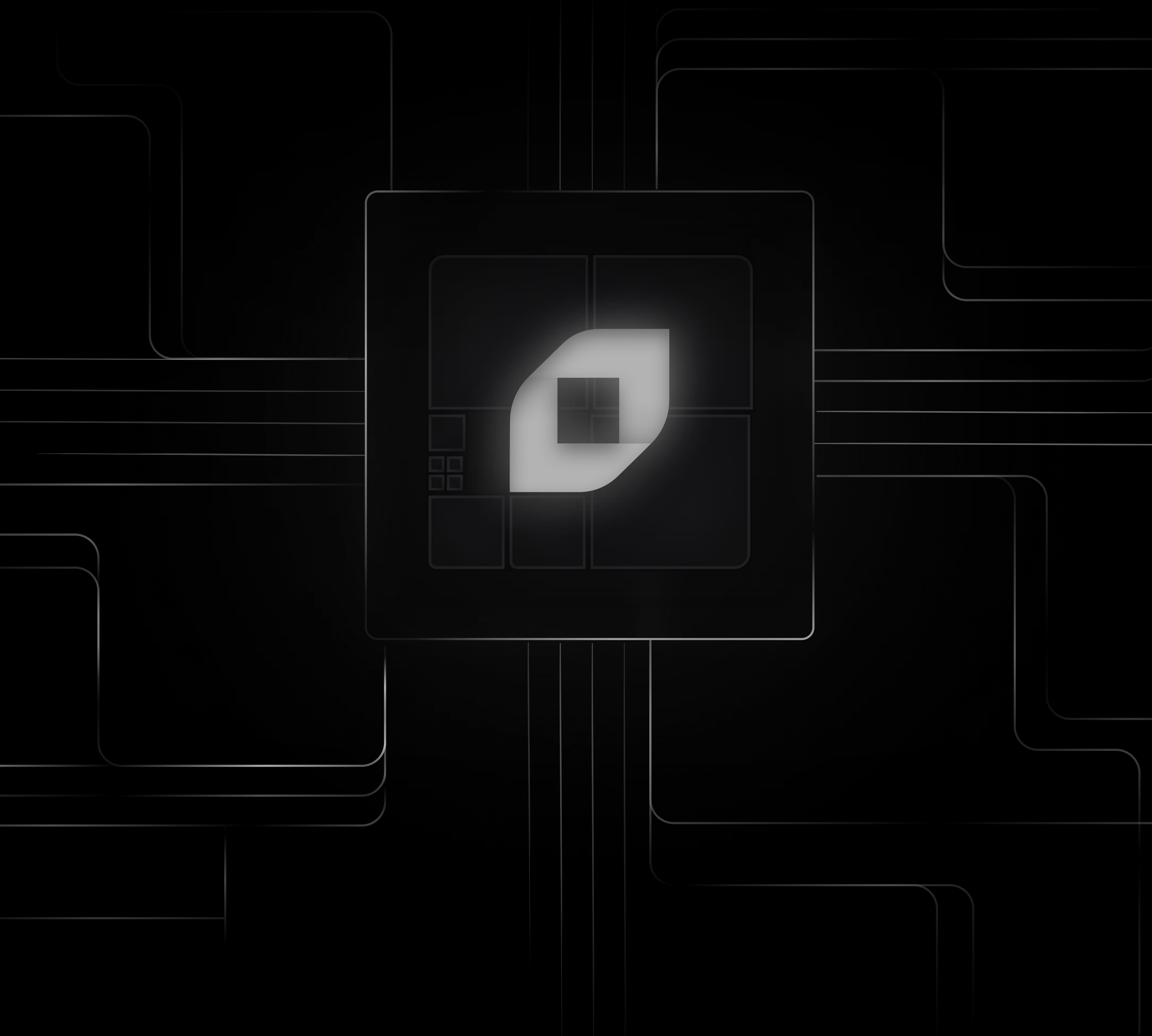
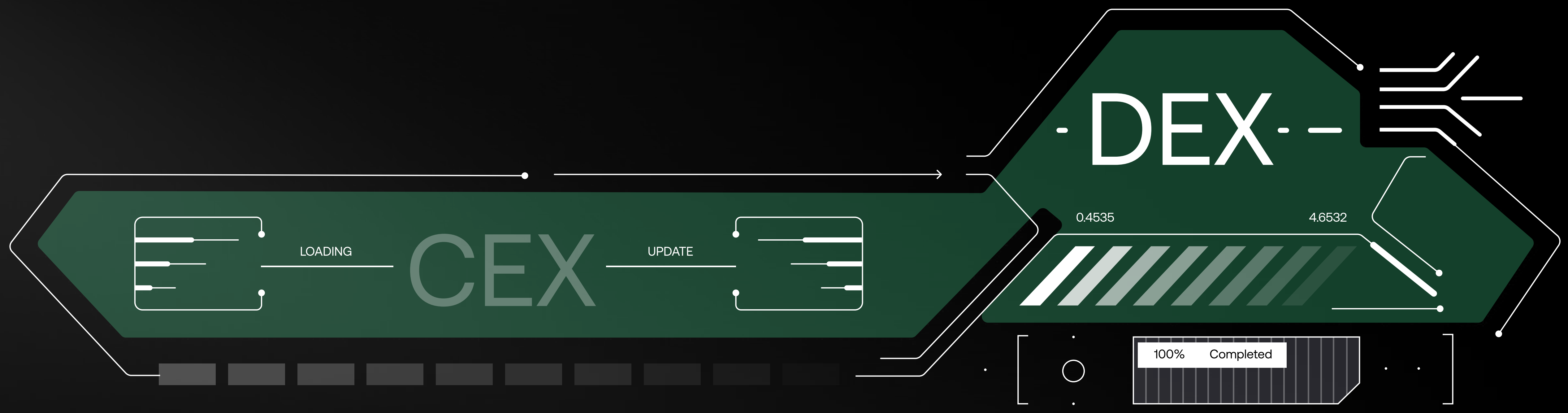


CHAINFLIP

Lightpaper v5.0

June 10th, 2023



Our mission is to displace the centralised exchange.

Introduction

For over a decade, the primary method of transferring value between blockchains has been the centralised exchange. This reality has limited composability between ecosystems and has made it difficult for new blockchains to be readily adopted by increasingly large Web3 userbases. Despite this, the vast majority of Web3 users rely on non-custodial wallets to perform even the simplest functions with DeFi, NFTs, DAOs, and a myriad of other applications.

Engineering a generalised solution to the cross-chain problem has been under discussion as far back as 2012. A decade later, and centralised exchanges still have a firm grip on the market share, but on-chain solutions have been making significant progress.

Whilst it is clear that there is huge interest within the cross-chain sector, and that on-chain trading is more important than ever considering recent events, no protocol has yet achieved widespread adoption to the extent of Uniswap in spite of the fact that the addressable market is much bigger than swapping just ERC-20 tokens alone.

Lately, interest has focused on cross-chain messaging, but this simple approach alone isn’t optimised to address the biggest and most valuable markets - they are and have always been the major spot markets. The fact that it’s been nearly impossible to swap 100k USDC for native BTC in one step with less than 3%(!!) slippage to this point is a joke.

Our mission is to attempt to displace the centralised exchange and become the go-to on-chain trading facility across the Web3 ecosystem, and ultimately enable unprecedented composability for builders needing cross-chain support.

What is Chainflip?

Chainflip is a cross-chain decentralised exchange, coordinated through its own application-specific blockchain. It is designed to have amazing pricing, support for both native BTC, EVM & substrate networks, and many other chain types. It also features cross-chain messaging support to maximise composability with current and future solutions to maximise asset coverage for users.

We are not building yet another bridge. Chainflip takes the best of all current cross-chain solutions and makes further optimisations not presently available to any of them. The protocol enables Chainflip to leverage existing on and off-chain spot markets to provide a truly game-changing experience to users.

Conceptual Overview

Centralised exchanges are the most successful model thus far for cross-chain value transfers, but can be simply described as just servers with wallets. Users send assets to the wallets on the server, the server then registers that balance to their account, and the user can then place trades on the server. Once they're done and want to withdraw assets, the server will send funds from the same wallets it runs.

This simple model is generic: it can support any chain, any transaction type, and gas fees are cheap because it's just a simple transfer. All trading logic is done off-chain in a purpose-designed trading system.

Chainflip, rather than trying to avoid this model entirely, instead builds on it. We ditch the monolithic system controlled by one entity and replace it with the decentralised Chainflip network of 150 validators, acting collectively to create giant Threshold Signature Scheme-based wallets (also known as TSS or MPC) and process trades using a unique Just-In-Time Automated Market Maker (JIT AMM) protocol. Anyone can join or leave the validator network without permission, and those participating in the network receive rewards for processing trades, settling assets, and securing the network. This unique design means that Chainflip can support any arbitrary digital asset type, and offers a simple user experience for permissionless asset swapping with extremely competitive pricing.

This differentiates Chainflip from other cross-chain products. Many offerings in the market today rely on bridging and messaging or other approaches, and they often come with a range of problems, including:

- Liquidity fragmentation
- Unfavourable pricing and high transaction fees
- Over-reliance on incentives
- Suboptimal capital efficiency and user experience
- Alarming degrees of centralisation
- High exposure to security risks for users

However, it's important to recognise that some solutions do offer benefits to counter some of these tradeoffs. In fact, Chainflip leverages cross-chain messaging technologies in harmony with the core protocol to maximise composability, allowing users the freedom to create swaps across many chains and protocols while using Chainflip for part of their trade. The overall result is a solution that champions security, efficiency, and true decentralisation, but also gives users the freedom to build routes flexibly and cheaply.

The network is made possible through the $FLIP token, a native ERC20 token that is used as collateral for the Validator network and as a utility token for all network participants.

Protocol Goals

Generalised Cross-Chain Capability

Provide users with a permissionless method to swap assets between arbitrary chains and networks (L1, L2, EVM, Non-EVM, Substrate, Cosmos SDK, Custom Appchains, Bitcoin, etc) without introducing new wrapped assets, liquidity fragmentation, excessive confirmation times, or leaving users with tail risk.

Decentralisation

Maintain credible decentralisation, audited open-source software, and transparent network operation from the very beginning.

Useful Product

Offer extremely good swap rates and minimise slippage to make the protocol competitive with centralised exchanges, in addition to a simple and intuitive user experience with great asset coverage, even if this means routing swaps through other great protocols like Uniswap.

Composability

Engineer the protocol such that it can be easily utilised by wallets, aggregators, and other products to bring their users greater functionality, who in turn become users of the protocol by proxy. As we will beat other protocols on price through the JIT AMM in the high-volume pairs we will offer, Chainflip will be very effective on the aggregation market, made easier by tools like the Chainflip SDK.

Inter-Protocol Compatibility

Enable compatibility with existing cross-chain messaging protocols, allowing Chainflip to easily become a part of any existing cross-chain projects, but offering better pricing and access to assets that others simply can not (non-EVM & non-smart-Contact chains)

Security

Maintain high-security standards with rigorous code policy, thorough external audits, extensive monitoring software, layered defences and failsafes within and around the core protocol, web properties, and network, and other mitigating measures such as bug bounties and penetration testing programs.

Sustained Value Capture

The protocol should be self-sustaining if enough users want to use the product without artificial incentives. The protocol should feed value from fees into the $FLIP token itself to distribute it to token holders and offset any incentives offered.

Features & Benefits

150 Main Validators

A credibly decentralised network needs a sufficiently large validator set in order to meet the goals of redundancy, security, and censorship resistance. 150 validators sign for every vault in the primary Chainflip design, meaning economic security is always shared and is simpler than other cross-chain vault management designs.

Scalable Signing Algorithm

Even with 150 validators, the use of Schnorr signatures and a novel application and implementation of the FROST signing scheme will allow the Chainflip validators to support dozens of assets and many parallel signing ceremonies without excessive hardware costs for validators.

Novel & Unique JIT AMM Design

The Chainflip JIT AMM is purpose-designed with the challenges of cross-chain in mind. It will simultaneously minimise slippage while offering users accurate pricing and out-competing other AMM designs in its class for high-liquidity pairs. This is achieved by allowing LPs to fully leverage just-in-time market-making strategies on all inbound trades.

Extreme Capital Efficiency

The JIT AMM design offers a system that minimises reliance on incentive-funded inefficient liquidity deployment. Instead, Chainflip can facilitate very large trades with minimal slippage, acting as a decentralised liquidity aggregation system across all on and off-chain markets. Chainflip behaves more like an open, transparent, and decentralised OTC service. The protocol should beat every other cross-chain service on price in most cases.

Polished user experience

Where connecting to Metamask isn’t an option, through clever additions to the architecture, Chainflip can facilitate a wallet-agnostic swapping experience, eliminating the need for complex wallet integrations and UI work to use Chainflip or to integrate it into other apps. We hope that users will come to the Chainflip AMM simply because it is a joy to use.

Extensive token economics design

Rigorous token design and well-modelled value capture mechanism. Fees are collected in $USDC and are used to buy the $FLIP token automatically from the AMM. If there is enough volume, $FLIP, even with incentives, is capable of being a deflationary asset.

First Principles design and unique codebase

Chainflip has been designed from the ground up and shares no core code with any other existing cross-chain protocol, with the exception of the Substrate blockchain framework. Every aspect of the design has considered reducing complexity, increasing redundancy, and reducing the risks of failure.

About the Team

Chainflip was founded by Simon Harman in 2020 as an independent project from within the Oxen Foundation, creators of https://getsession.org. Through private fundraising, Chainflip Labs has established itself as a team of 30+ engineers, designers, quants, and analysts located in several offices in Berlin, Dublin, and Melbourne. With backing from the level-headed Framework Ventures, Blockchain Capital, Pantera Capital, Coinbase Ventures, and dozens more, the team is well-equipped to tackle the cross-chain sector with experience & conviction.

Chainflip is a unique protocol with a specific vision for capitalising on the largest market in the industry — spot trading. To read more about how we are tackling this problem, you can head to https://docs.chainflip.io and check out the full set of concept documentation, or read the full whitepaper at https://chainflip.io — it's a good read!

Join us on Discord or follow us on Twitter at @Chainflip

Discord ↗

Get involved with our community Discord server. Ask technological questions or just hang out.

Twitter ↗

Follow @chainflip for the latest news and updates across the system.

Telegram ↗

Become a part of our active Telegram channel and receive announcement for all things Chainflip

Blog ↗

Want to read our latest updates? Head on over to our blog.