CHAINFLIP

Lightpaper 2.0

Produced by
CHAINFLIP LABS

INTRODUCTION

- Vitalik Buterin

@vitalikbuterin

March 25th, 2020

> “We should put resources toward a proper (trustless, serverless, maximally Uniswap-like UX) ETH ←→ BTC decentralized exchange. It’s embarrassing that we still can’t easily move between the two largest crypto ecosystems trustlessly.”

Low friction cross-chain exchange has been an elusive dream of the crypto community for years, and we’ve been talking as if a true solution to the problem is always just around the corner. In 2016, Atomic swaps were allegedly going to solve all the problems. Very few bothered to ask if that even made sense, let alone whether it solved trustless cross-chain swaps in a way that would result in a usable product.

Uniswap in recent years has reaffirmed the community’s desire to use low friction services to exchange crypto, but Ethereum and its projects make up only a fraction of the overall market value and trading volume in the industry. Ongoing scaling challenges have brought about a multichain paradigm, and most users are forced to use centralised solutions to bridge between ecosystems.

There are lots of projects claiming to solve this problem. Upon closer inspection however, the proposed user experiences on offer don’t line up with expectations. To capture any decent amount of liquidity and volume, a solution to this problem must offer a better user experience than centralised offerings. A solution must support standard layer 1 transactions across multiple arbitrary blockchains with no special software, no wrapped tokens, no accounts or registration, no collateral requirements, and no unnecessary complexity. A big ask.

The original Shapeshift demonstrated demand for frictionless swaps. Uniswap replicated the experience across a small subset of crypto assets. Chainflip is the multichain evolution we have all been waiting for.

HIGH LEVEL CHAINFLIP FACTS

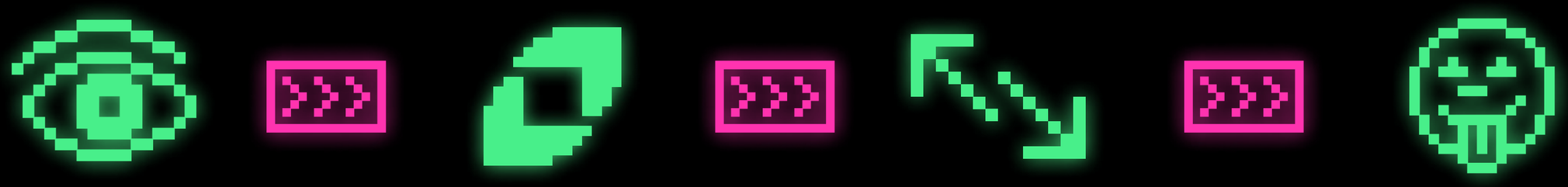
- **NO WRAPPED TOKENS**
  Cross-chain AMM that supports native blockchain assets
- **NO ADOPTION BARRIERS**
  No special software or wallets required by users
- **NOT IMPACTED BY SCALABILITY ISSUES ON OTHER BLOCKCHAINS**
  Built on a standalone Substrate based proof of stake blockchain
- **FAIR TOKEN MODEL**
  FLIP token bought and burned with every swap for protocol value capture
- **DEFI & MULTI-CHAIN READY**
  FLIP token offered as ERC20 token initially, but can be represented on other chains
- **NATIVE BTC, ETH, DOT, ETC.**
  Chainflip Validators track all swaps and liquidity on the Chainflip state chain, and use MPC and threshold encryption to jointly hold funds on multiple external blockchains

OVERVIEW

Chainflip is a decentralised protocol that supports the direct cross-chain exchange of cryptocurrencies without a trusted intermediary.

With Chainflip, you get the same permissionless experience as Uniswap, but without the limitation of being stuck on the Ethereum blockchain. You can swap ETH directly for BTC, or XTZ for DOT. There is no need to put your trust into wrapped tokens or suffer from the host of user experience issues with current offerings.

Chainflip maintains its own Substrate-based proof of stake blockchain, called the State Chain. The multichain nature of Chainflip means that it can support any generic decentralised transaction network, provided it meets minimum security guarantees. All balances, swaps, and events are tracked on the Chainflip State Chain, meaning users will only pay transaction fees for the blockchains they interact with. For example, a user sending BTC and receiving DOT will only pay one transaction fee in BTC on the way in, and one transaction fee in DOT on the way out. You don’t have to pay ETH gas fees if you’re not sending or receiving any ETH-based assets.



Using the FLIP token as collateral, Validators construct joint wallets on each supported blockchain. These wallets are secured through threshold encryption, multi-party computation, game theory, and the protocol's consensus rules.

Every time swaps are processed by the system, FLIP is automatically bought and burned, paying for the emissions required to fund Validators and provide liquidity incentives.

For the average user, it's simply a case of swapping your digital assets for another native token. No staking, no collateral, no wrapping, no special wallets. Users don't need to buy FLIP directly to use the system. Users only need a browser and a destination address. Just swapping. No adoption barriers. Send and receive. Layer 1. It really is that good.

THE PROBLEM

Currently nothing exists that facilitates low-friction cross-chain swaps as a fully decentralised protocol. Swapping tokens should be a simple process - you should be able to choose the assets to be swapped, plug in the destination address for the receiving chain, and have a deposit address generated for you. Using this address, you should be able to send funds no matter the wallet you have, and then simply receive the other asset on the other chain.

Current and proposed protocols alike fall short of this optimal experience. Wrapped tokens, necessitating specific wallets and pre-deposits, collateral requirements and needing a user account are just some of the issues. Digital asset swapping should be simple and sovereign, and right now, it is not.

Shapeshift was popular because it was the optimal cross-chain experience. Fast and permissionless. As a result, it collected a huge amount of volume despite the fact that it was quite expensive for users. Once the central entity behind the product was required to follow KYC/AML guidelines it lost all utility, as the barriers to entry removed the main advantages of the platform. Fees were high, users no longer saved extra time compared to more liquid options, and it could no longer be natively integrated into wallets and other services that made switching crypto so simple.

Other projects have bold claims, but behind the marketing jargon they lack true cross chain swapping functionality, or are at least built in such a way that very few will use them.

Layer 2 solutions and atomic swaps do not solve this problem. Any solution that requires you to store extra collateral on chain in order to conduct a swap or a centralised broker has missed the point entirely. People want to be able to liquidate their whole position in one quick step. Unless users are performing fewer steps overall than they would on a centralised exchange, the chances of a DEX being widely adopted are low. Users should not be expected to move their funds to a new special wallet or platform before they can interact with the system.

THE SOLUTION

CHAINFLIP

Put simply, Chainflip connects chains in the same way that centralised exchanges connect chains: the platform deploys a bunch of wallets on a bunch of chains which users can deposit to in order to use the platform.

However, rather than having a centralised pool of assets, the protocol works through a decentralised network of nodes.By using a few different types of threshold encryption schemes, the Chainflip Validators can create a single joint wallet for each supported chain.

The State Chain then acts as the coordinator, making sure that everything is as it should be and allowing assets to be moved around the protocol. We then create Liquidity Pools, which let users swap their assets in a simple and intuitive way directly on layer 1.

That's a very high level description, but if you want to delve deeper and read about how the thing actually works, then go to https://chainflip.io to read the full whitepaper.

That said, we'll walk you through the basic components which allow us to facilitate truly decentralised cross chain swaps; Vaults, Validators, the State Chain, Quoters and Liquidity Pools.

Vaults

The Vaults are wallets that are jointly owned and operated by the Validators. To create these Vaults, Validators participate in a setup process where new nodes are deterministically chosen to serve in the next active Vault. These nodes construct a threshold signature wallet from which transactions can only be sent if a given threshold of Validators sign a transaction. The schemes used to generate the Vaults do not require a trusted dealer or the revelation of keys during the signing process. Vaults use different types of threshold encryption depending on the type of blockchain. Some use MPC, some use simpler Ed25519 threshold schemes, and some use threshold encryption embedded within smart contracts.

Validators

Validators are bonded nodes which perform an extended set of operations when compared to a typical blockchain node. These nodes compete for a limited set of Validator slots, earn rewards from the block reward, and maintain the State Chain for Chainflip. They are required to have access to (or run their own) clients for every blockchain containing supported assets. Chainflip Validators perform similar functions to Validators in other blockchain networks, but carry more responsibilities due to their obligations to monitor and interact with external blockchains through their shared keys.

State Chain

Built using Substrate, the State Chains a standalone blockchain which acts as Chainflip's coordination mechanism. It contains all of the data pertaining to Vault contents, as well as the ruleset for how to deal with transactions once they enter the Chainflip Vaults, how to manage liquidity and swaps, and how the Validators come to consensus on when and where to send an outgoing transaction on another blockchain. In that sense, the rules for the AMM are written into the very fabric of the blockchain.

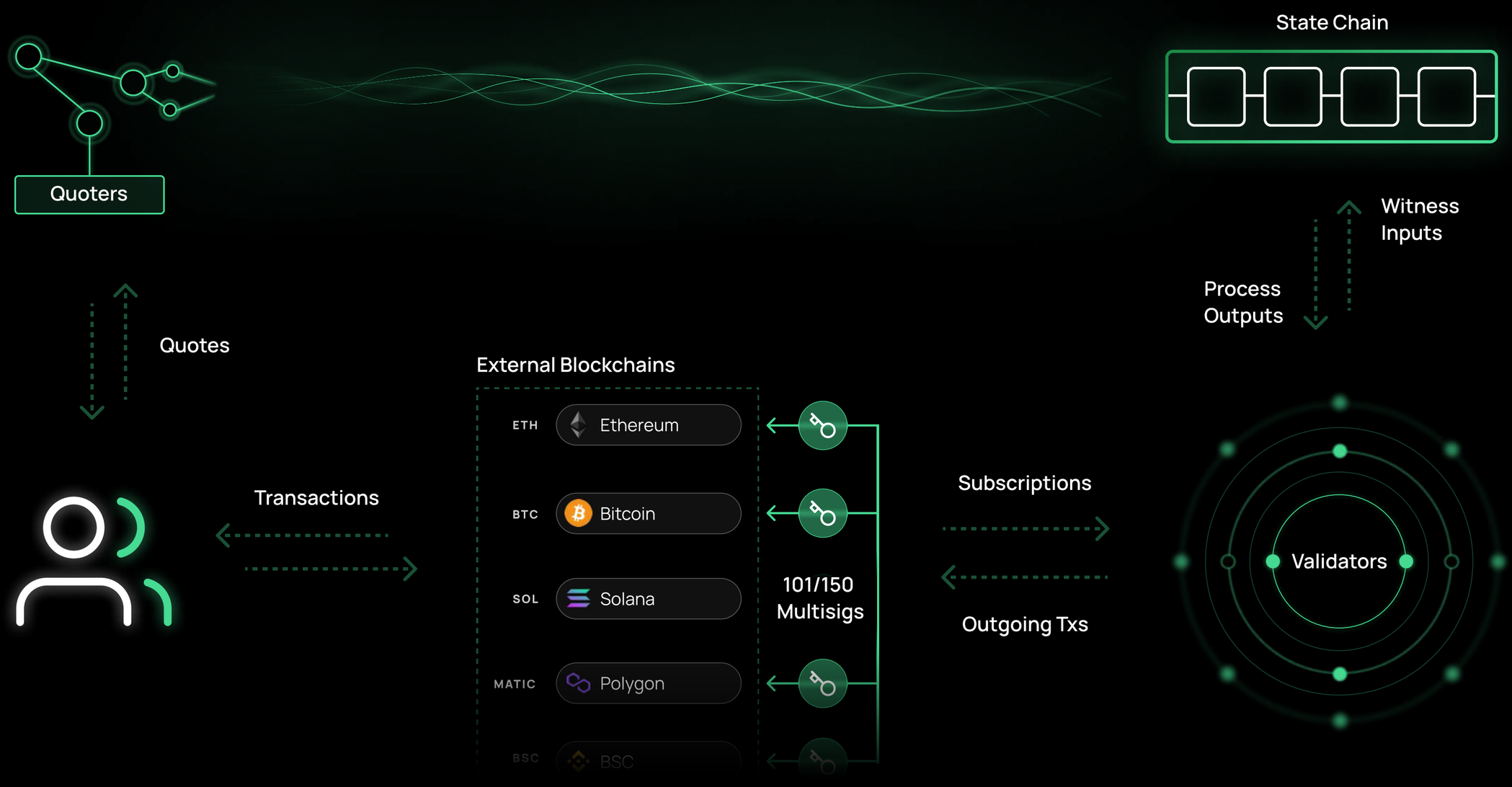
Quoters

Quoters are the interface between the user and the State Chain. A Quoter's main function is to insert Quotes into the State Chain on behalf of a user. Quotes contain swap details such as input and output addresses, and optional additional instructions such as slippage limits, return addresses, and timeout rules. Quotes are also used to telegraph the addition of liquidity to Liquidity Pools. Quoters allow users to interact with the system without any special software on their own device.

Liquidity Pools

Liquidity Pools are simply defined as reserved portions of two Vaults. For example, a BTC/USDC Liquidity Pool would have a reserved portion in each of the Bitcoin and USDC Vaults. Each blockchain only requires one Vault, but the contents of each Vault may be split among multiple Liquidity Pools virtually. Liquidity Providers add liquidity to these pools in order to earn fees when people trade across the pool in the same way that LPs interact with Uniswap.

THE CHAINFLIP PROTOCOL



In conclusion, Chainflip will solve many issues that are bugbears of the DeFi community. You will be able to swap cryptocurrencies cross-chain in a completely trustless manner. All you need is an internet connection, web browser and a destination address.

DeFi is no longer an Ethereum-only playground; more and more projects are looking to other chains to build their projects on. Allowing users to access these cryptocurrencies without a trusted intermediary is an absolute necessity if we are to build a truly decentralised ecosystem that is accessible, user friendly, and better than the centralised offerings currently available.

Chainflip is more than a cross-chain DEX.The infrastructure which makes this possible can be repurposed to replicate a whole suite of DeFi products in a cross-chain context. With simple APIs and integration capabilities, Chainflip is poised to become a cornerstone of DeFi infrastructure.

If you want to learn more then head over to https://chainflip.io where you can download our whitepaper.

Sign up to the mailing list on our website and be the first to hear about project updates and the launch.

@chainflip