APOLLO CAPITAL

RESEARCH REPORT

ChainFlip Research Report

Author: Matthew Harcourt

1.0 INTRODUCTION

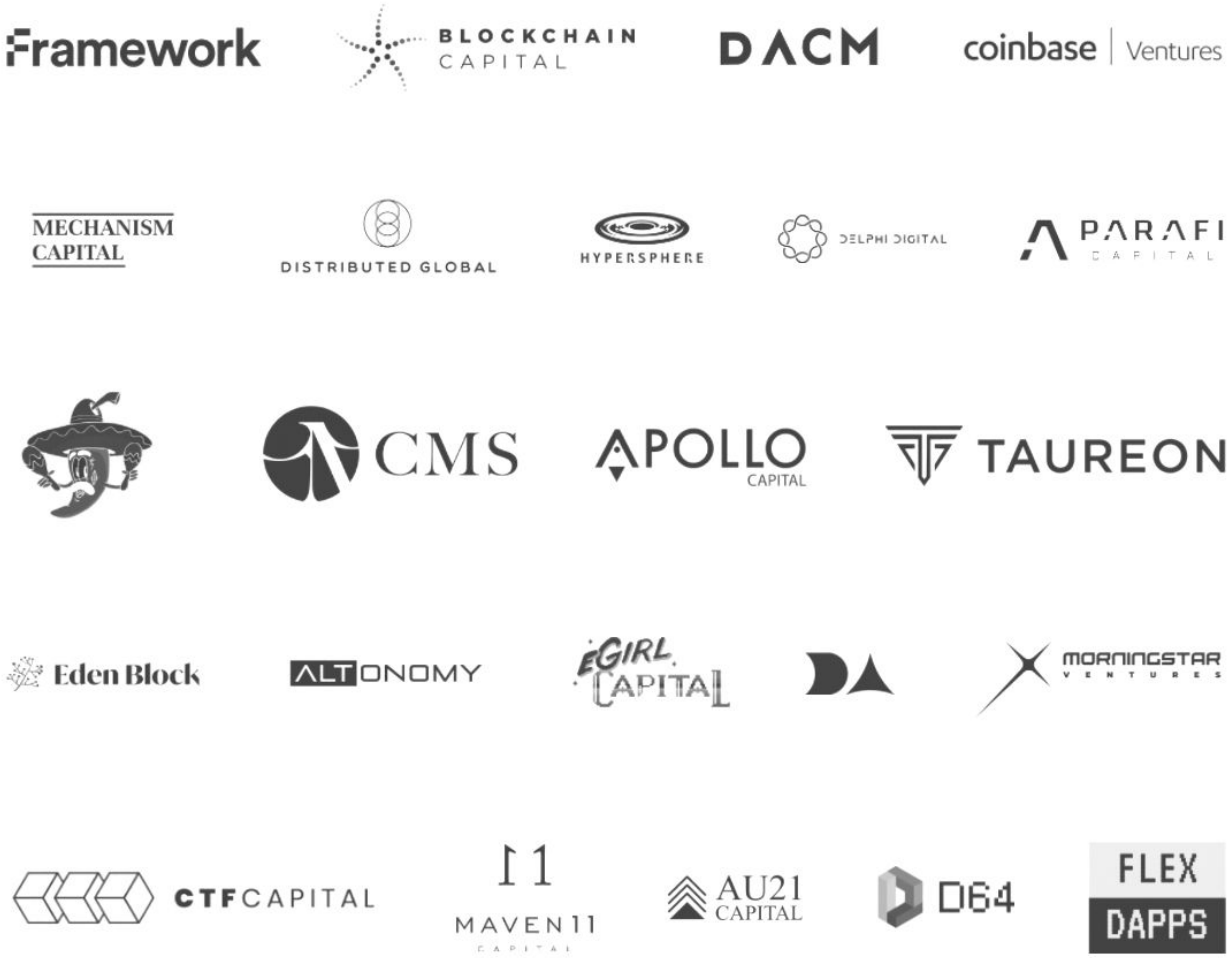
Over the past year, it has become increasingly obvious that the future of blockchain and Decentralised Finance (DeFi) will be a multichain one. Many regular DeFi users find themselves constantly 'bridging' between the various Layer 1 protocols in an attempt to move capital into more profitable yield farms and test out innovative new protocols. However, the current leading interoperability solutions are highly complex and hard to understand for the vast majority of DeFi users. Their level of security, trustlessness, and reliability is highly variable and hard to assess without a deep understanding of the underlying technology powering them. The interoperability sector is young and in high demand, this creates an exciting opportunity for projects to create leading innovations.

Chainflip is a decentralised and trustless protocol that enables cross-chain swaps between different blockchains. Chainflip removes the need for wrapped tokens and synthetic counterparties by facilitating swaps between native assets on their native blockchains. The Chainflip protocol uses a 'State Chain' to coordinate a decentralised network of nodes; these validators use threshold encryption to create a single Vault for each supported blockchain. These Vaults are jointly owned and operated by the Validators and are used to create liquidity pools, allowing users to swap their assets in a Uniswap-like fashion directly on Layer 1.

While Chainflip is not without notable competition in this burgeoning sector, their careful development process, established team and extremely impressive list of backers has the project positioned to become a cornerstone of DeFi infrastructure. After recently speaking with Chainflip Founder and CEO, Simon Harman, the investment team at Apollo Capital have an even higher level of confidence in the team's ability to execute the high ambitions of the protocol.

As an early investor in Chainflip, we eagerly await the mainnet launch of the protocol in early 2022.

Backed by



Chainflip is planning to launch an incentivised testnet named ‘Soundcheck’ on the 15th of December in an attempt to engage potential mainnet node operators, battle test the network, and reward community participation.

This testnet will be followed by three mainnet releases; Sandstorm, Ibiza, and Berghain. Simon Harman and the team have their sights set on March 2022 for a full mainnet and FLIP token launch.

2.0 Drivers of the Multichain Future

There are a number of key drivers underpinning the movement towards the multichain future that Chainflip will take advantage of. Exploring these drivers can give an understanding of the potential market size for the Chainflip protocol.

2.1 Scalability Issues

One of the key trade-offs in the design of a blockchain is between speed and security. Bitcoin is currently the most secure blockchain in the world, but is unable to support a significant number of transactions due to scalability issues. Bitcoin's ability to only facilitate 7 transactions per second (TPS) is miniscule when compared to Visa's average of 1,700 TPS. Ethereum is another great example of a highly secure blockchain that has experienced scalability issues, resulting in the cost of transacting on the blockchain to increase exponentially over 2020/2021.

On the other end of the scalability spectrum, Solana is a high-performance blockchain that boasts 50,000+ TPS. However, Solana has experienced two major outages in the past 12 months with the most recent outage lasting 17 hours in September 2021. Both Bitcoin and Solana are key blockchains that have bright futures, but they are currently not capable of single-handedly facilitating mass adoption of crypto assets.

2.2 Chain Specialisation

Bitcoin, Solana, and various Layer 1 protocols all serve vital functions in the development and adoption of crypto assets. In its current form, BTC serves as a 'Store of Value' that is not designed to be actively transacted (on the main chain), while Solana is an experimental DeFi hub where retail users are not priced-out due to gas fees like they are on Ethereum. The rise of Ethereum Virtual Machine (EVM) compatible chains like Polygon, Avalanche, and Binance Smart Chain has also opened the door for quality Ethereum-based projects like Aave and Curve Finance to reach retail users through multi-chain deployment of their smart contracts.

Terra (LUNA) is another example of a differentiated chain that is creating a unique value for the market. Throughout 2021, Terra's native algorithmic stablecoin, USD Terra (UST), has increased in market capitalisation from $181 million to $8.65 billion. This stablecoin exists on multiple blockchains and is widely praised for its ability to withstand market volatility better than centralised alternatives like USDC and USDT.

2.3 Technological Advancement

The crypto asset and blockchain industry has always evolved quickly, and this rapid pace of development means that blockchains can now interact and communicate with each other in a more secure, trustless, and efficient fashion. An early example of technological advancement introducing new possibilities to the crypto asset market is Ren's 'wrapped' assets such as renBTC. renBTC allows the value of BTC to be represented on the Ethereum blockchain. Since launching in June 2020 renBTC has wrapped US$750 million worth of BTC. renBTC enables BTC to participate in Ethereum DeFi and is a pioneer of the current blockchain interoperability space.

Beyond these drivers, the rise of decentralised exchanges throughout 2020 and 2021 indicates a strong desire from users to transact in a decentralised, permissionless and non-custodial manner.

3.0 HOW DO CROSS CHAIN SWAPS WORK?

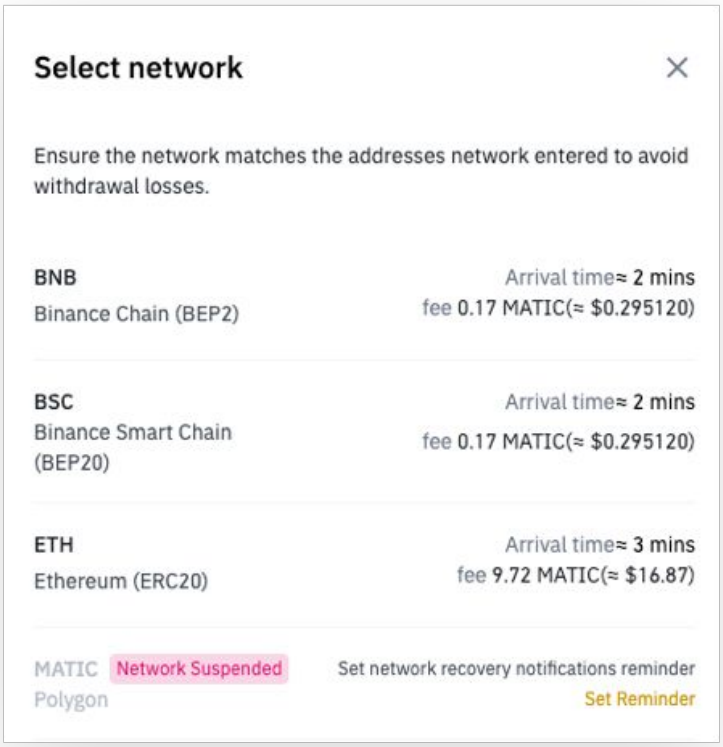
The easiest way for a crypto investor to swap between crypto assets on different blockchains is currently through a centralised exchange. Understanding how centralised exchanges enable 'cross chain swaps' can help to understand how Chainflip will improve this process.

3.1 Centralised Exchange 'Cross-Chain Swaps'

Centralised exchanges control wallets on various blockchains from which users can deposit and withdraw their funds. These wallets are custodied by the exchange, meaning that users ultimately do not have direct control or ownership over their funds.

Exchanges utilise their own in-house security and development teams to maintain control and security over these wallets. Exchanges can be vulnerable to hacks and also have the power to prevent a user from withdrawing assets to their desired location.

For example, it is not uncommon for Binance to suspend withdrawals of an asset to its native chain and instead only allow withdrawals to the Binance Smart Chain, as seen below. It is also important to point out that centralised exchanges require users to provide their personal details when completing 'Know Your Customer' (KYC) compliance procedures. These compliance procedures can take weeks to fully complete, especially for corporate entities.



Once crypto assets have been deposited into the custodied wallets of the centralised exchange, users can interact with the exchange's order book and matching engine in order to execute orders. When an order is executed, there is no on-chain transaction and no actual movement of the assets that are being traded. Instead, the centralised exchange shifts what they owe the users on each side of the trade, retain full custody of both assets and charge their fee. This process is internally managed, non-transparent and ripe for disruption from decentralised alternatives like Chainflip.

The rise of Uniswap and other DEXs demonstrates a strong appetite from the market to transact in a decentralised, permissionless, and non-custodial manner. For the spot trading of assets native to the blockchain, DEXs provide a superior user experience to centralised exchanges.

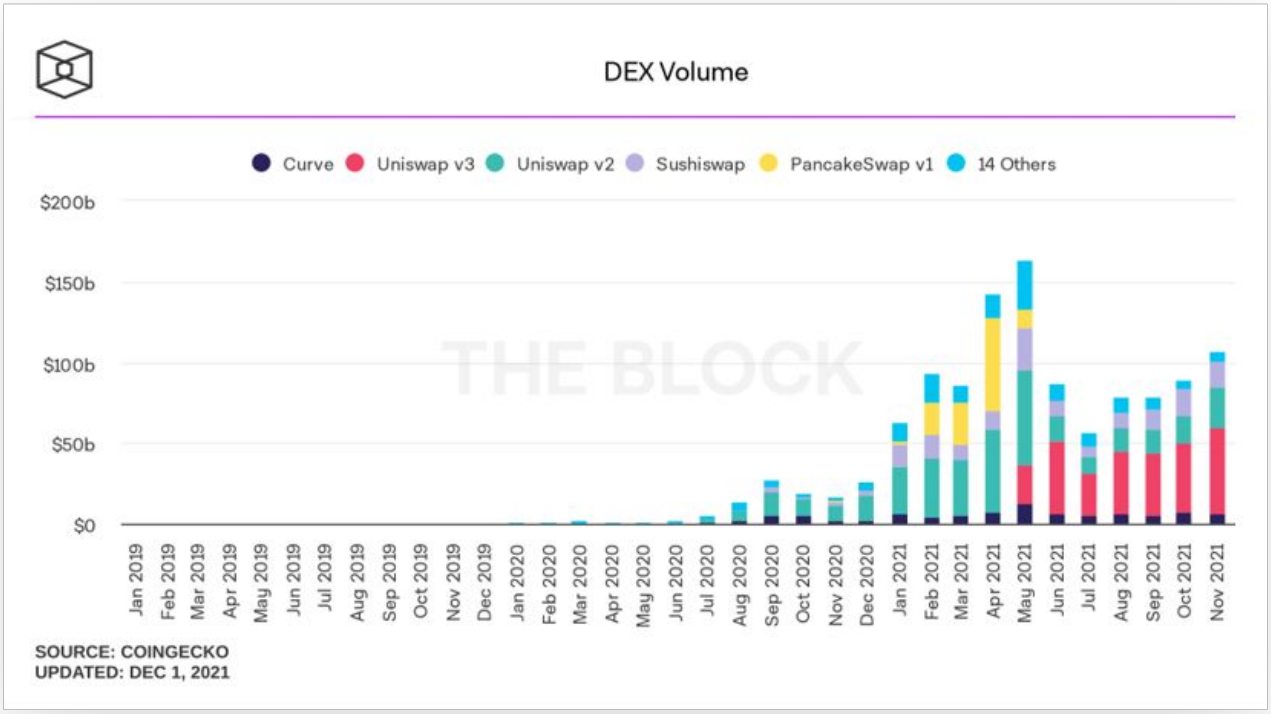
Decentralised Exchanges:

- Do not require account creation & KYC compliance
    - Users do not give away their data to trusted parties
- Are instantly accessible
- Enable users to retain complete custody of assets
- Enable permissionless market creation
- Can be more liquid than CEXs, especially for long tail assets

3.2 Chainflip Cross Chain Swaps

Unlike centralised exchanges, the Chainflip protocol does not take custody of users' funds. Instead, the protocols network 'control' the wallets that hold the assets in the Automated Market Makers (AMM) liquidity pools. These wallets are known as 'Vaults' and are controlled by a decentralised network of nodes/validators coordinated by the 'State Chain'. This network of nodes utilises threshold encryption to jointly own and operate the private keys of the protocol wallets in a trustless manner. Transactions in and out of these Vaults can only be sent if a given threshold of Validators sign a transaction, this ensures that liquidity provider funds cannot be controlled by a single entity or group.

Instead of using a centralised order book and matching engine, Chainflip will utilise the AMM model to enable trading. AMM's lower the barriers to entry for liquidity providers by making it extremely easy for users to provide liquidity and start earning fees. Providing liquidity to an AMM is incredibly easy when compared to the complex strategies that traditional market makers must implement on order book exchanges. In addition to this, users do not need to give away their personal identity and retain full custody over their crypto assets throughout the entire process.

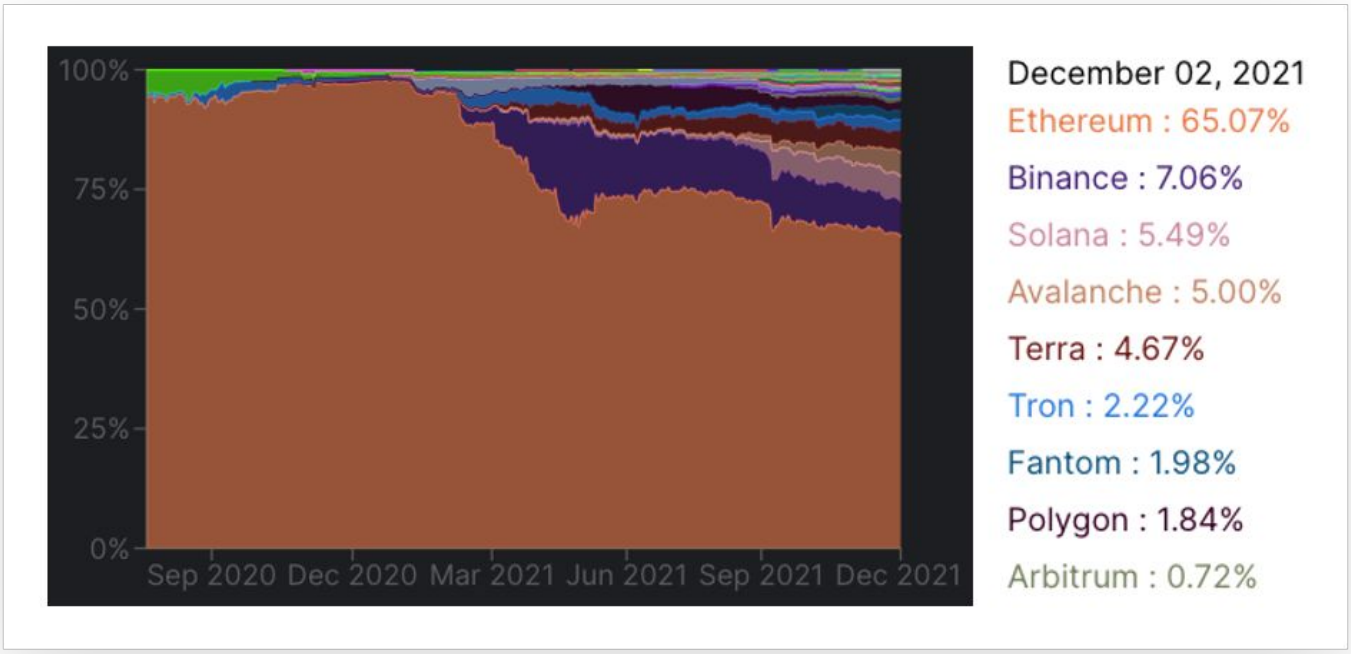


Decentralised exchange volumes increased significantly throughout 2020 and 2021, signaling strong product-market fit and a sustainable business model (The Block).

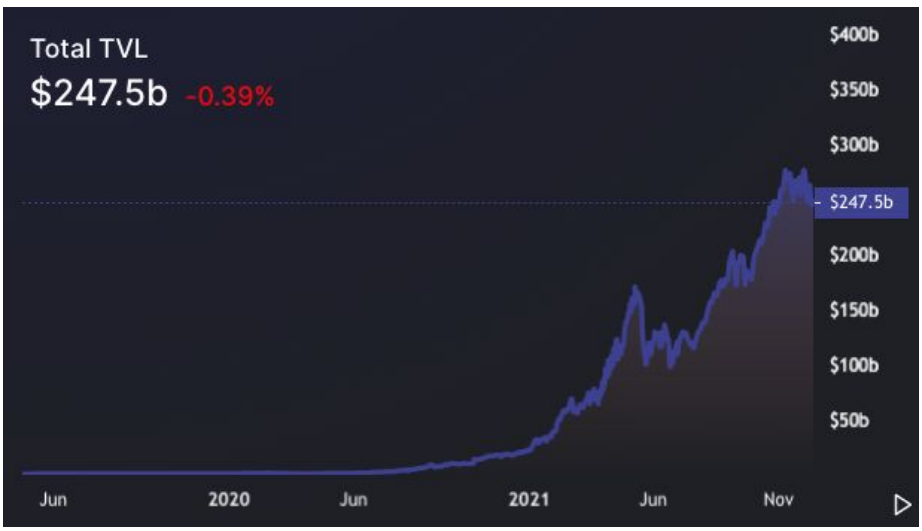
3.3 Non-Ethereum DeFi Growth

As shown in the charts below, DeFi activity on non-Ethereum blockchains has increased rapidly throughout 2021. This growth is highly likely to continue into the future, even if Ethereum is able to successfully implement both Layer 1 and Layer 2 scaling solutions. This continued increase in DeFi activity on competing chains strengthens Chainflips underlying value proposition as a protocol that enables cross-chain interoperability and swaps.

Share of Total DeFi Total Value Locked (TVL) by Blockchain



Cumulative TVL in DeFi



4.0 Competitive Environment

4.1 THORChain

Chainflip's most prominent competitor is THORChain (RUNE), which was an early mover in cross-chain-swaps. RUNE boasts a circulating market capitalisation of US$1.86 billion (fully diluted US$3.13 billion) and has been trading since July 2019. THORChain has fostered one of the most loyal followings in DeFi through a high level of community engagement, retail-focused marketing, and by using their first-mover advantage to full effect.

In early 2021, THORChain was on the verge of becoming a core part of DeFi infrastructure by finally allowing users to conduct cross-chain swaps in a permissionless and decentralised manner. With the notable crypto fund Multicoin Capital publicly disclosing a large position, RUNE rocketed to a market capitalisation just short of US$5 billion in May 2021. Although this incredible price action was amplified by the overwhelming speculation in the broader crypto asset market, it shows a clear desire from the market for protocols with cross-chain capabilities.

Unfortunately, THORChain suffered multiple exploits in July 2021, resulting in a loss of US$13 million in users' funds. Analysis by leading DeFi exploit journalist rekt.news suggests that these exploits were caused by a lack of oversight by the THORChain developers, and may have been easily preventable. These exploits have resulted in a loss of trust from DeFi users and creates an opportunity for competitors.

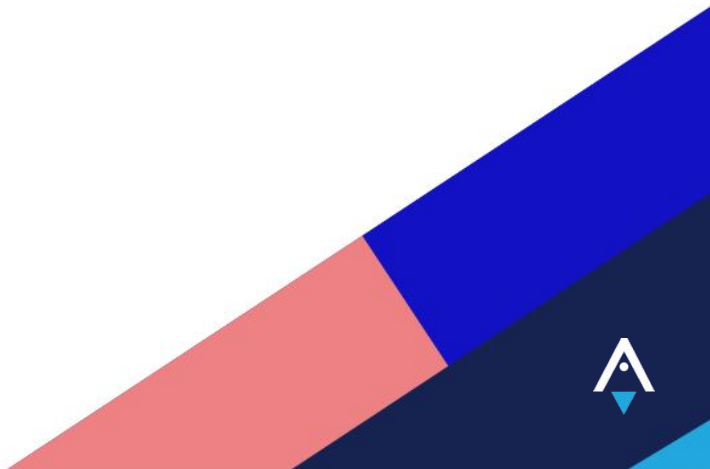
Users can access the smart contracts of THORChain through multiple front ends with the premier front end being THORSwap. THORSwap's token, THOR, current trades at a market capitalisation of US$24.5 million (fully diluted US$551 million). The THORChain protocol has accumulated a TVL of US$185 million across 6 chains.

4.2 AnySwap Protocol

The Anyswap bridge has recently emerged as a significant competitor in the cross-chain interoperability sector of DeFi. The protocol currently supports 10 chains, 1039 tokens, and has US$4.55 billion in Total Value Locked (TVL). The protocol gains TVL by 'wrapping assets' from one blockchain onto another. Anyswap has been quick to add support for the smaller EVM compatible blockchains and has established itself as one of the go-to bridges for Avalanche, Arbitrum, Fantom, and Binance Smart Chain. These chains represent almost 15% of the TVL in DeFi applications. The ANY token trades at a market capitalisation of US$240.9 million (fully diluted US$1.4 billion).

The Anyswap network is maintained in a 'decentralised' way through 35 nodes that control the private key holding all of the deposited assets. Similar to Chainflip, the network ensures that no single entity or group can gain access to these funds using threshold encryption. However, there are concerns surrounding the level of centralisation associated with the protocol due to the small network of nodes and lack of documentation for node operators. By comparison, Chainflip will have 150 nodes and detailed documentation. Node documentation is important to the decentralisation of a protocol as it allows anyone from around the world to participate in the network.

Anyswap has certainly benefited from the DeFi community's "deposit first, ask questions later" approach. In many circumstances, the potential returns associated with using these new and potentially risky protocols far outweigh the risks, and we are yet to see a large-scale exploit on a protocol like Anyswap. Anyswap enables cross-chain interoperability through locking assets on the origin chain and minting the equivalent on the destination chain; these newly minted assets hold their value as they are fully backed on the origin chain. Users who yield farm with these 'wrapped' assets bear the risk of the underlying security mechanism failing for as long as they hold the assets. Chainflip users will not interact with any wrapped assets as swaps will be between native assets on their native blockchains. Once a trade is executed and confirmed, a user will bear no additional or hidden risks.



5.0 Tokenomics

Chainflip's founder, Simon Harman, has produced a series of in-depth blog posts that document the Chainflip token's economics. The blog posts will act as future reference for further debates, discussions and analysis of the FLIP token. While all parts of the Chainflip protocol are designed by multiple team members, tokenomics is one of Simon's favourite aspects of the protocol and these blog posts showcase his knowledge and thinking in the area.

'Cryptoeconomics' Series:

- Part 1: Uncapped Supply:
  Outlines Chainflips infinite supply model as well as the plan to buy-and-burn FLIP tokens using protocol trading fees.
- Part 2: Validator Auction Theory:
  Outlines the validator auction system that will be used to determine which validators uphold the network over a given period of time.
- Part 3: Swapping Logic:
  Details the improvements that Chainflip intends to make on the current Automated Market Maker (AMM) model.
- Part 4: Incentive Design:
  Outlines Chainflip's incentive scheme that is designed to capture value for FLIP token holders, reward validators sensibly, and attract 'sticky liquidity'.
- Part 5: Economic Security (Yet to be released).

We believe that Simon's approach to tokenomics gives Chainflip and the FLIP token a competitive advantage over its competition. According to Simon himself, significant value is set to accrue to the FLIP token if the team are able to achieve their TVL and volume goals.

6.0 Team

Simon Harman (Founder & CEO)

Simon first began his crypto journey purchasing Bitcoin back in 2015. Upon graduating from RMIT University with a Bachelor of Arts in 2017, he became heavily involved in the Australian Blockchain community and joined the Blockchain Centre. Having a strong interest in digital privacy and anonymity, he conceived Oxen (formally named Loki). This private network allows users to transact and communicate privately and anonymously over the internet. The project was designed to empower users to build applications, including messaging services, online marketplaces, and social media platforms. Today, Session (a fully anonymous encrypted messaging service) and Lokinet (a cutting-edge low-latency onion router) utilise the Oxen Service Node network to safeguard user privacy and anonymity.

Simon's track record in creating a successful and highly technical protocol makes him well qualified to lead a talented team of around 20 individuals in creating Chainflip.

Below are the highlights of the workings he has contributed to;

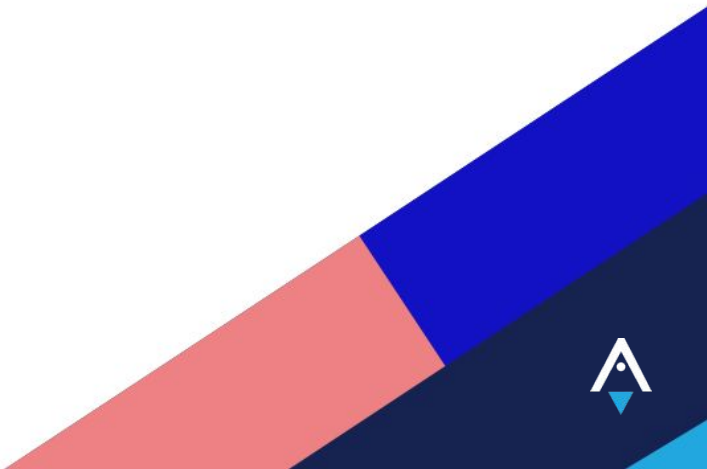
- 2020 - Chainflip Whitepaper - Core protocol design of the Chainflip system.
- 2020 - LRC-7 - an analysis of Blockswap's economic implications for Loki and recommendations to address them.
- 2020 - LRC-3 - the second analysis of the Loki network's economic scheme in light of Proof of Stake.
- 2019 - Session Whitepaper - Our secure messaging app's primary design document.
- 2018 - Loki Cryptoeconomics - a preliminary design for Service Nodes.
- 2018 - Loki Whitepaper - The founding document for the Loki Project.

Tom Nash (CTO)

Tom Nash completed a Bachelor of Science and Computer Software Engineering degree at Lancaster University in 2014. After graduating, he began working as a developer by joining a small web development company. From 2016, he worked in Melbourne at several software start-ups as a Blockchain Developer and Blockchain Consultant, focusing on smart contract development and building decentralised applications and blockchain software architecture.

At the beginning of 2019, he co-founded “Flex Dapps” - a leading Australian blockchain development firm specialising in an array of Web 3.0 services such as front-end development, smart contract development, smart contract audits, and tokenomics strategies. Flex Dapps also contribute and invest in a variety of Australian early-stage crypto projects, Chainflip, prePo, Maple Finance and mStable to name a few.

As CTO, Tom manages a group of 11 software engineers with a range of specifications, primarily Rust developers. At the end of every month, Tom provides a valuable update on the development goals and progress of the engineering team.



7.0 Conclusion

Chainflip has a unique opportunity to pioneer a new primitive within DeFi by becoming the first decentralised cross-chain swap protocol to gain significant TVL, volume and adoption. The ability for users to be able to trustlessly complete cross-chain swaps in a permissionless and non custodial manner will be a vital piece of blockchain infrastructure.

Interoperability is an important and quickly growing sector within the crypto asset market and there will be no shortage of competition. However, we are confident that the Chainflip protocol will be the leading solution within the cross-chain swap market.

The user interface and front end design of the Chainflip protocol is still in development but Simon is confident that his CTO is building one of the best front ends in DeFi. The team realises the importance of making the protocol simple and usable for the average DeFi user, something their competition is not doing an outstanding job of.

To keep up with the major developments of the Chainflip protocol, make sure to follow their Twitter, subscribe to their Blog and visit their Website to sign up for their newsletter and join their Discord.

Chainflip Whitepaper
Chainflip Litepaper