A decentralized, over-collateralized, Bitcoin backed stablecoin on the Internet Computer

Elliptic Labs

April 26, 2023

Abstract

The Elliptic protocol is an innovative decentralized and over-collateralized stablecoin platform that aims to provide a stablecoin pegged to the US dollar on the Internet Computer. The protocol allows users to exchange ckBTC into stable assets, providing a stable value in US dollars represented as eUSD. As one of the founding pillars of Decentralized Finance (DeFi), stablecoins play a crucial role in the ecosystem. The Elliptic protocol aims to be at the forefront of innovation by leveraging the cutting-edge technology of the Internet Computer. With its innovative approach, the Elliptic protocol is poised to become the first decentralized stablecoin backed with native Bitcoin in the blockchain space.

Contents

1 Introduction

Decentralize Finance (DeFi) is growing on the Internet Computer (IC) blockchain. Stablecoins are the foundation bricks of decentralized finance, providing stability and support to the rapidly growing industry. Existing stablecoins all have their pros and cons :

- Centralized stablecoins (USDT, USDC, BUSD), which are the most prominent in terms of market capitalization, all have in common: the need to rely on a central authority and the lack of transparency. Relying on a third party always presents the risk that this authority may abuse its influence. Those stablecoins are not the most interesting technically, the legal framework represents a big part of the work. An advantage is that such stablecoins have a low chance of being in liquidity crises if well-managed. One issue is that you cannot verify or audit how those protocols use their reserves.
- Decentralized stablecoin doesn't rely on the centralized party. The Maker Protocol, also known as the Multi-Collateral Dai (MCD) System is a protocol that allows users to exchange volatile assets like Bitcoin for DAI stablecoin. It can appear complex for regular users to create and maintain vaults, and to understand the stability fee and all the liquidation risks.
- Attempts to create even more capital-efficient stablecoins, which operate by being under-collateralized, have not been successful. Many have experienced liquidity crises or even worse, a bank run (e.g. Iron Finance's Titan Token Falls [1]).

The Elliptic protocol doesn't require relying on a third party to ensure stability. It takes its roots from successful stablecoins designs, including the robustness of protocols like Angle [2]. All the stablecoins cited above are not available on the Internet Computer (IC) Blockchain. Hence the introduction of the Elliptic protocol proposes an innovative way of providing a decentralized stablecoin to the IC. The Elliptic protocol, among the first on the IC, will allow its users to swap their volatile assets into eUSD at the current exchange rate.

The Elliptic protocol articulates three groups of users. Users looking for stability, users that are willing to take the volatility of the first group, and users looking to collect ELP tokens to get the fees collected by the protocol. Those three groups, by living together form a virtuous ecosystem, allowing the protocol to remain over-collateralized in a capital-efficient manner. All the logic of the protocol will be implemented on the IC, an ecosystem too often looked by that is more powerful than most of the other projects.

This whitepaper aims to present the mechanisms of the Elliptic protocol and give a glimpse of what the protocol will be.

2 Stability seekers

This section presents the basic definitions and operations of the protocol.

2.1 Defining ckBTC

Chain-key Bitcoin (ckBTC) is an ICRC-1-compliant [4] token that is backed 1:1 by bitcoin held 100% on chain. It is a Bitcoin twin living on the Internet Computer thanks to tECDSA [3] cryptography.

2.2 Minting and Burning eUSD

A user seeking stability can exchange their assets for eUSD at the current exchange rate. He sends his whitelisted collateral to the protocol, he receives eUSD in exchange.
Example: A user deposit 1 ckBTC at a current price of 1000$, and he will receive in exchange 995 eUSD: 1000$ minus a minting fee of 0.5%.

If a user wants to exchange his eUSD for the selected collateral. He sends eUSD to the protocol, he will then receive an amount in the selected collateral at the current exchange rate.
Example: A user withdraws 1000 eUSD, the current Bitcoin price is still 1000$ per BTC, the protocol burns the eUSD and transfers 0.995 ckBTC to the user, 1 ckBTC minus the 0.5% fee which represents 0.005 ckBTC.

The fees collected by minting and burning operations are used to reward liquidity providers and ensure that the protocol is always over-collateralized.

2.3 Transacting eUSD

Users can then transfer eUSD as an ICRC-1 token [4] on the IC. A fee is collected on each transaction to prevent DoS and reward liquidity providers. This fee is variable and depends on the vitality of the protocol. The more over-collateralized the protocol is, the less the fee is, and vice versa.

To keep its value stable eUSD needs to always be over-collateralized to allow users to claim back assets at any time. How the Elliptic protocol tackles this challenge will be presented in the following section by presenting two new groups of protocol users: Risk Mitigators and Collateral Supporters.

2.4 Peg Mechanisms

Being able to maintain a peg to the US dollar for a stablecoin is crucial for trust. On any market, price stability is guaranteed by bots and arbitragers. Indeed, if the price of eUSD goes below 1$ on any exchange. Arbitrageurs are able to buy the eUSD on the exchange and swap it for ckBTC at the current Bitcoin market price, hence making a profit. They can repeat until eUSD price goes back to 1$. And it works the other way around too. If eUSD goes above 1$, they can buy ckBTC, swap it for eUSD, and sell eUSD on the exchange. They just need to repeat until the peg is recovered. The Elliptic protocol offers arbitrage opportunities from which anyone can profit.

3 Covered Leverage

The Elliptic protocol provides a decentralized covered leveraged position for taking a long position on whitelisted assets. Unlike centralized exchanges that offer leverage trading, Elliptic allows users to trade without the need for a central exchange, which is especially valuable following the recent FTX incident. The idea is that the protocol is selling volatility to users seeking leverage. For each token that the protocol owns, an option can be taken. Each leveraged position is backed 1:1 with assets locked in the protocol.

3.1 Leverage

The leverage of a long-position buyer can be calculated using the following formula. In the following definitions 'c' represents the covered amount of assets brought by users seeking stability, and 'm' represents the collateral margin amount brought by the user looking for leverage.

$$leverage = \frac{m+c}{m} \tag{1}$$

Example: c = 10 ckBTC are locked in the protocol. A leverager can then bring up to 10 ckBTC for their position. A leverager brings m = 5 ckBTC, according to equation (7), will have a 3x leverage on his ckBTC.

3.2 Return On Investment

The claimable amount of assets by the buyer of the long position at any time is defined on 2.

$$ROI = m + c \cdot \left(1 - \frac{\text{initial price}}{\text{current price}}\right) \tag{2}$$

Example: Let's continue the previous example. The leverager entered an initial price of 1 ckBTC = 5 $. Now, the price of ckBTC is 8 $. The user is entitled to claim 8.75 ckBTC to the protocol if he wants to close his position.

3.3 Liquidation Risk

The long taker can be liquidated if the price of the asset he is covering goes below or at a price defined in 3, the protocol will liquidate the position. In the following equation, 'p' represents the price of a given asset.

$$p_{liquidation} = \frac{m}{c+m} \cdot p_{initial} \tag{3}$$

Example: Using the numbers of the previous example, his position would be liquidated at 3.33 $ per ckBTC.

3.4 Imbalances

If all of the assets exchanged for eUSD were covered by long-takers, the protocol would always be collateralized. It would be a perfect place for people looking for stability and for people seeking to take the volatility of the first group's assets.
Unfortunately, it is not possible to guarantee such a property. We need to introduce a new group: collateral supporters. This group will be the buffer for temporary imbalances between offer and demand. They will keep stability in the protocol when the leverage offers are not fully covered.

4 Liquidity Provider

4.1 Definition

Contrary to stable seekers, liquidity providers do not seek stability, they want to earn the DAO token: ELP. Owning ELP entitles you to a share of the fees collected by the protocol, everything is explained in section 5. Collateral supporters are providing liquidity to the protocol, which ensures that the protocol will always be over-collateralized. They are not seeking stability but for yield on their assets. The liquidity amount provided by liquidity providers is noted as 'l'.

4.2 Collateral Ratio

The collateral ratio is simply defined as follows. The collateral ratio is noted as 'CR'.

$$M = \sum_{i}^{leveragers} m_i \tag{4}$$

$$C = \sum_{i}^{stable\ seekers} c_i \tag{5}$$

$$L = \sum_{i}^{liquidity\ providers} l_i \tag{6}$$

$$CR = \frac{(M+C+L) \cdot p_{current}}{eusd_{circulating}} \tag{7}$$

Example: 1 ckBTC has been converted into 20000 eUSD. BTC price is now 18000$. The protocol is now under-collateralized, the collateral ratio is 90%. BTC price is now 22000$, the protocol becomes over-collateralized and the collateral ratio is now 110%.

4.3 Risk

Being a liquidity provider to the Elliptic protocol comes with great rewards but you also have to understand the risks. You might not be able to fully get back the liquidity you provided. If the collateral ratio (CR) of the protocol falls below 120% you will only be able to get a part of the provided liquidity. The amount that you can get back is predictable and defined as follow. Note that, as long as the collateral ratio stays above 120%, you can claim at any time your provided liquidity.

$$claimable\ liquidity = provided\ liquidity \cdot f(CR) \tag{8}$$

$$f(CR) = \begin{cases} \frac{10}{12} \cdot CR & \text{if } CR \leq 120\% \\ 1 & \text{if } CR > 120\% \end{cases} \tag{9}$$

4.4 Incentive

By providing liquidity to the protocol, the collateral supporters help to make the protocol over-collateralized at any point in time. They are rewarded with ELP tokens, which give them a chance to collect a share of the fees collected by the protocol. Once the Ethereum integration is here or when DeFi on the IC becomes more robust, the protocol will be able to earn a yield on the controlled assets by lending assets to protocols like Compound [12] or Aave [11] on Ethereum or any other protocol voted by the governance. These rewards will be distributed to collateral supporters, offering an exciting yield as they will earn a yield on their assets plus the assets provided by the stable seekers.

5 Governance of the Elliptic Protocol

5.1 Decentralized Autonomous Organization

To understand how the Elliptic protocol will be decentralized, it is first needed to define what is a DAO. A decentralized Autonomous Organization [8] (DAO), is a decentralized organization that operates an entity. It works through smart contracts (or canisters on the IC) executed on the blockchain, allowing for autonomous decision-making and management without intermediaries or central authority. The rules and operations of a DAO are governed by its code, and decisions are made through voting by its members, who hold a certain amount of stacked ELP. The transparency, security, and immutability of blockchain technology ensure the integrity and accountability of a DAO.

5.2 Service Nervous System

DAO roots its strength in decentralization and usage. To reach decentralization there will be an initial launch of the ELP token on the Service Nervous System [7] (SNS). The SNS is a system that allows many parties to jointly control an entity. The Elliptic DAO that controls the Elliptic protocol, will be able to propose changes to the protocol that will be voted on by the ELP holders. In order to have voting power you will need to stake your ELP in a neuron (in the same manner it is done in the Network Nervous System [13] on the IC). The more voting power you have the more influence you have on a proposal voting.

5.3 Voting Power

By locking tokens in a neuron, you will be able to vote on proposals made by the DAO. A neuron will generate a yield proportionate to the number of locked tokens. The biggest default of this kind of DAO control is that if it's poorly implemented it leaves room for hostile take-over using loans and flash loans on synchronous blockchains like ethereum. Here this kind of take-over is not possible, you need to lock your tokens in order to vote, the longer your tokens are locked the higher the maturity of your neuron will be and the higher your voting power will be. The following formula describes how voting power is distributed:

$$voting\ power = (ELP\ stacked + ELP\ yield\ stacked) \cdot dissolve\ delay \cdot age\ bonus \tag{10}$$

5.4 Reward distribution

The Elliptic has five ways of generating rewards. It can be from transaction fees on the eUSD ledger, from the fees collected for minting and burning eUSD, from the fees collected on leverage positions, from the fees collected on liquidity positions, or from the potential yield generated on collaterals. Rewards generated from the protocol can either be distributed to the ELP stakers or used to over-collateralize the protocol in case the collateral ratio is under the 120% threshold.

6 Implementation details

6.1 Emergency response

In case of an emergency, like a flash crash of the crypto markets that could lead to an under-collateralization of the protocol, the Ellipse protocol can switch to an emergency mode. List of actionable items to reach over-collateralization:

- **Freeze Asset Claiming:** The DAO can choose to temporarily halt the claiming of assets to allow the protocol to recover.
- **eUSD transfer fee:** Increase the transfer fee of the ICRC-1 token to reduce the claimable supply.

- **Fee Increase:** Increase the fees used for minting and burning eUSD.
- **Cheaper Stablecoin Burning:** Governance can utilize the bonding curve to reduce the cost of burning stablecoins, allowing the protocol to re-collateralize itself.
- **Leverage taker fee decrease:** The fee used for leverage taker can be reduced to incentive newcomers. Rewards in the form of governance tokens could also be used.

In case of collateral settlement, a preferred treatment will be given to governance token (ELP tokens) holders.

6.2 A multi-chain protocol

The IC allows integration directly with the Bitcoin network [10], allowing canisters on the IC to receive, hold, and send Bitcoin, all directly with transactions on the Bitcoin network. Canisters can act exactly like regular users holding Bitcoin on the Bitcoin network. A user could deposit native Bitcoin (on the Bitcoin chain) to the protocol and receive eUSD, all without any centralized entity, thanks to the Elliptic protocol.

The capabilities of the IC blockchain are truly unique. Using HTTPS calls [6] in combination with Threshold ECDSA [3], the IC is capable of signing Ethereum transactions and fetching the state of the Ethereum blockchain. The development of direct Ethereum integration 6.2 is the next item on the Dfinity Foundation's agenda. Having direct Ethereum integration will allow the protocol to use assets on the Ethereum chain as natively as with the Bitcoin chain and the IC chain. The protocol could also generate yield using Ethereum protocols like Yearn Finance [9], and the DAO could vote to earn interest on the assets owned by the protocol and hence generate a new income stream for ELP owners. Users will have the option to choose the output chain for their swaps between Ethereum, Internet Computer, and any ECDSA-compatible chain.

The IC's use of tECDSA [3] makes it a powerful technology in the blockchain space, and in a multi-chain future, the IC is well-positioned to be the binder of the DeFi space as a whole. The combination of the Elliptic protocol and the IC is limitless, and users will be able to deposit assets from any chain and receive eUSD on the chain of their choice.

6.3 Oracles

The IC is a blockchain with unique capabilities compared to other popular chains. It does not rely on external oracles to make HTTPS calls to web2 services, as smart contracts on the IC can access off-chain data directly using HTTPS outcalls [6]. The reliability of the HTTPS outcalls made by smart contracts is ensured as multiple nodes of a subnet make the calls and reach a consensus on the accessed information, aggregating data from different exchanges such as Binance, Coinbase, KuCoin, Okx, GateIo, and Mexc. The protocol will rely on the exchange rate canister [14] to fetch the prices of assets and always select the lowest price for an asset between all the prices fetched.

6.4 Fees

The Elliptic protocol takes a one-time fee for each action available by the protocol. The fees can be decomposed as follow, the collateral ratio is noted CR. The collected fees are distributed to the ELP owners and can be used to have the collateral ration above 120%.

$$fees = base\ fee + f(CR) \tag{11}$$

$$f(CR) = \begin{cases} 2.5\% & \text{if } CR \leq 80\% \\ 0\% & \text{if } CR > 120\% \\ 2.5 \cdot \frac{120-CR}{40}\% & \text{if } 80\% < CR \leq 120\% \end{cases} \tag{12}$$

The varying part of the fee is predictable as it's a saturating piecewise linear function, saturating at 120% of the collateral ratio. f(CR) sole purpose is to maintain the protocol over-collateralized.

6.5 A cash-out scenario

Initial Price	$p_{initial}$
Current Price	$p_{current}$
User Collateral	c
Liquidity Provided	l
Leveragers Margin	m
Collateral Supporters Rewards	r

When the stable holders want to cash out, the amount due to them is defined as follows:

$$c \cdot \left(\frac{p_{initial}}{p_{current}} \right) \tag{13}$$

When the group of leverage position takers wants to cash out, the amount due to them is defined as follows:

$$m + c \cdot \left(1 - \frac{p_{initial}}{p_{current}} \right) \tag{14}$$

After the two first group claimed their assets, the protocol is left with:

$$l + r + (c - m) \left(1 - \frac{p_{initial}}{p_{current}} \right) \tag{15}$$

When c equals m, as defined in 16, all the collateral supporters can be reimbursed. The protocol must insure that at any point in time M $\leq$ C.

$$(C - M) \to 0 \text{ as } M \to C \tag{16}$$

If the protocol verifies M = C and stable holders cash out their eUSD. We now have m greater than C. The protocol will have to close some leverage position in order to come back to a state where M $\leq$ C.

The protocol will have an acceptance range until it starts closing position of 95%.

7 Summary

- Elliptic is a protocol that allows the creation of a truly decentralized stablecoin in a capital-efficient manner.
- At any time, full convertibility of eUSD at a 1:1 rate with assets owned by the protocol.
- The protocol is sustainable and self-sufficient, it allows three groups of users to benefit from the protocol: the stable seekers, the leveragers, and the collateral supporters.

8 Bibliography

[1] Iron Finance's Titan Token Falls to Near Zero in DeFi Panic Selling: https://www.coindesk.com/markets/2021/06/17/iron-finances-titan-token-falls-to-near-zero-in-defi-panic-selling/

[2] Angle Protocol Whitepaper: https://docs.angle.money/overview/whitepapers

[3] Threshold ECDSA: https://internetcomputer.org/docs/current/developer-docs/integrations/t-ecdsa/

[4] ICRC-1 Standard: https://github.com/dfinity/ICRC-1/blob/main/standards/ICRC-1/README.md

[5] Exchange rate canister forum discussion: https://forum.dfinity.org/t/new-exchange-rate-mechanism/14543

[6] HTTPS outcalls: https://wiki.internetcomputer.org/wiki/HTTPS_outcalls

[7] Service Nervous System: https://internetcomputer.org/docs/current/tokenomics/sns/sns-intro-tokens/

[8] A Next-Generation Smart Contract and Decentralized Application Platform by Ethereum Foundation (2014)

[9] Yearn Finance: https://docs.yearn.finance/

[10] Bitcoin Integration: https://internetcomputer.org/docs/current/developer-docs/integrations/bitcoin/

[11] Aave Protocol whitepaper: https://github.com/aave/protocol-v2/raw/master/aave-v2-whitepaper.pdf

[12] Compound whitepaper: https://compound.finance/documents/Compound.Whitepaper.pdf

[13] Network Nervous System: https://internetcomputer.org/docs/current/tokenomics/nns/nns-intro

[14] Exchange Rate Canister: https://wiki.internetcomputer.org/wiki/Exchange_rate_canister