Trustless Currency Protocol

Whitepaper

v0.5

Abstract

The novel promise of Decentralized Finance is a trustless and permissionless financial system entirely different from the centralized power structures in place today. A maximally decentralized, broadly distributed lending protocol with solid fundamentals is a step in the right direction.

Existing collateralized stablecoin protocols rely on centralized governance for prices, collateral, and interest rate updates. These entities rely on weekly governance votes to adjust interest rates and do not distribute the protocol token broadly to those that make the network valuable: the community.

---

1. Introduction

The Trustless Currency Protocol allows users to lock Eth and mint a token of stable value called Hue. The TCP token acts as a temporary voting token and backs Hue if the Eth collateralization mechanism fails. The TCP protocol is unique:

- Does not require a continuous price feed
- Uses Uniswap V3 instant TWAPs for prices
- Allows for negative interest rates
- Automatically adjusts interest rates
- Distributes most of TCP automatically to the community
- Enforces automatic lock times on governance
- Indexes all keeper data trustlessly on-chain
- Accepts only Eth as collateral
- Tokenizes all debt positions
- Uses extensive code comments and sensible labels

2. Borrowing

2.1 Eth only Collateral
Eth is the only collateral type accepted by the Trustless Currency Protocol.

2.2 Tokenized Debt Positions
All debt positions are tokenized as an NFT. An NFT makes it possible to transfer a position to another address, lock ownership of a debt position into other protocols, bundle many positions into a new financial product, allow another protocol to manage a position's collateralization or anything else the defi ecosystem imagines.

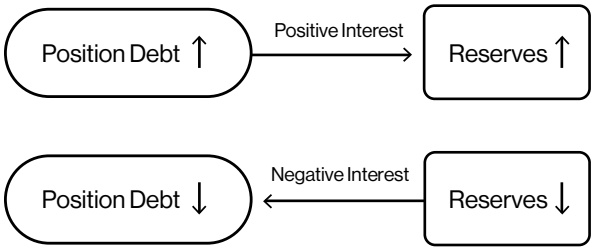
2.3 Incentivized Borrowing
Locking liquidity and borrowing Hue are incentivized with a portion of TCP inflation proportional to their contribution to total debt.

3. Lending

Anyone can stake Hue into the protocol and earn a portion of the positive interest charged to borrowers. Staking Hue provides immediate value for Hue before integration into other protocols: it gains interest.

4. Peg Stability

In order to maintain a 1 Hue = 1 Dollar peg, TCP charges a variable interest rate on borrowers. The interest rate can be positive, negative, or zero. If the interest rate is positive, the debt of each position increases over time. If the interest rate is negative, the debt of each position decreases over time. Proceeds from positive interest are stored as reserves; negative interest is paid out of reserves. If reserves are depleted, interest rates are floored at zero.

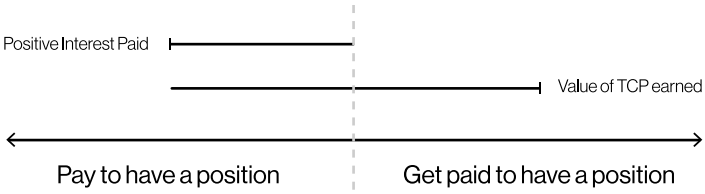


4.1 Interest Rates
At regular intervals, the interest rate update function can be called by anyone. If Hue has been trading above the peg, the interest rate is reduced. The incentive increases to borrow Hue, increasing supply, decreasing the price. If Hue has been trading below the peg, the interest rate is increased. The incentive increases to pay back Hue loans, decreasing supply, and increasing the price.

4.2 Interest Rate Controller
A simple interest rate controller maintains the interest rate. If Hue is off the peg by a certain threshold, then for every increment above or below the peg the interest rate is changed by one step, up to a maximum number of steps on each update.

Because the interest rate algorithm is predictable, changes to the interest rate can be front-run before an update is made, further enforcing the peg.

4.3 Virtually Negative Interest Rates
Borrowers of Hue accrue TCP. If the value of TCP accrued outweighs positive interest charged borrowers receive negative interest rates without eating into reserves.



5. Reserves

Proceeds from positive interest are stored as reserves. Conversely, negative interest and undercollateralized debt are paid from reserves.

5.1 Deficit Auctions
Anyone can create deficit auctions if reserves are below a threshold of total debt. Deficit auctions sell a decreasing amount of newly minted TCP to buy a fixed amount of Hue.

5.2 Surplus Auctions
Anyone can create surplus auctions if reserves are above a threshold of total debt. Surplus auctions sell a fixed amount of Hue to buy an increasing amount of TCP to be burned, causing positive interest to indirectly accrue to TCP by decreasing supply.

6. Liquidations

If a position falls below the collateralization threshold, it can be liquidated by anyone. A portion of the value from the position is paid to the keeper that discovers the undercollateralized position, placing the debt into the pooled liquidation account. Some value is paid to the keeper that provides capital to pay off the liquidation account.

6.1 Discovering Undercollateralized Positions
A keeper specifies the positions they believe to be undercollateralized. The protocol confirms these positions are undercollateralized by pulling a price from the Uniswap V3 price oracle. Each undercollateralized position is liquidated by removing its debt and adding it to the liquidation position. A fee on the liquidated debt is paid in the collateral currency (Eth) to the liquidator. Next, collateral equal in value to the position debt plus a penalty is added to the liquidation account. Any remaining collateral stays in the position.

6.2 Liquidating Undercollateralized Debt
Anyone can pay off the debt from the liquidation position and retrieve an equal portion of the collateral in the liquidation account. There is no price required for this operation. For example, if a keeper pays off half of the debt in the liquidation account, they get half of the collateral.

6.3 Maintaining Liquidation Incentives
If the liquidation position has less value in collateral than debt, anyone can trigger the protocol to pull a price to confirm this. Hue is then removed from reserves to pay off the excess debt.

6.4 Liquidation Reward Limits
Liquidation rewards are limited to a percentage of system debt. This limit is reset at regular time intervals. This puts a cap on the total value that can be extracted by manipulating the collateral price. This is achieved with minimal effect on the ability to liquidate undercollateralized positions, as the reward

for liquidating is a small portion of the size of the position.

6.5 Position Index

A gas-optimized index of all debt positions by collateralization is maintained. This means that a keeper needs only the current state of the chain to liquidate undercollateralized positions. This eliminates trust in any centralized parties to provide correct indexed data and dramatically simplifies the keeper algorithm.

7. Price Oracles

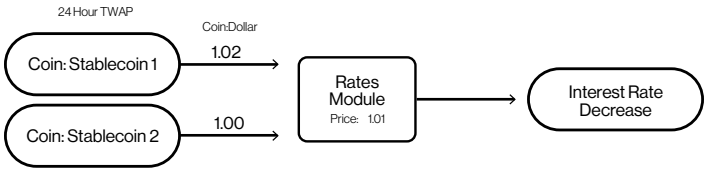
TCP uses Uniswap V3 for price data. Instant Uniswap TWAPs are used for confirming that a position is adequately collateralized. Longer Uniswap V3 TWAPs are used to track the price of Hue relative to the Dollar. Prices for collateral are pulled from a Hue:Eth pool called the “collateral pool”. Prices for Hue relative to the Dollar are pulled from one or more pools of Hue paired with another stablecoin, called the “reference pools”.

7.1 Incentivized Price Liquidity

In order to ensure that the Uniswap V3 TWAP is cost-prohibitive to manipulate, adding liquidity to the relevant pools is incentivized with a portion of TCP inflation. Users must lock this liquidity into the pools through the protocol to be eligible.

7.2 Peg Price

The reference pools are Hue tokens paired with other stablecoins that track the US Dollar. The median price of these pools determines the price of Hue relative to the Dollar. This price is used in the interest rate controller described in section 4.2.



Because the US Dollar is a centralized asset, any token pegged to the US Dollar must have a point of centralization. TCP’s centralization is isolated to only the Hue price reference pools. Governance can add or remove reference tokens unless it has decided to forgo that ability. In addition, the protocol can handle all but one of the reference assets failing.

8. Pool Liquidity

Uniswap V3 is a leap forward in AMM technology. In Uniswap V2, liquidity positions were tokenized as an ERC20 token. In Uniswap V3, liquidity is locked within a user-defined price range allowing liquidity to be highly concentrated. However, this also means that Uniswap V3 positions are no longer fungible.

In TCP, users can provide liquidity around the current price for the collateral and reference pools. Out-of-range liquidity is disallowed. The protocol takes in tokens from the user and creates a tokenized position through the Uniswap V3 NonfungiblePositionManager, and stores the resulting NFT within the protocol. Users are rewarded with a portion of TCP inflation in proportion to the share of total virtual liquidity they have provided.

8.1 Liquidity Position Incentives

Users can take a given number of real tokens and provide them to the incentivized pools on a narrow or broad range. If provided on a narrow range, the virtual liquidity is greater; if provided on a broad range, the virtual liquidity is less. The real liquidity provided remains the same.

Because the protocol incentivizes virtual liquidity and not real liquidity, it is in a liquidity provider’s best interest to provide liquidity along as narrow of a range as possible. However, the protocol also has no use for liquidity that is not in range. In order to balance these incentives out of range positions can be liquidated.

8.2 Liquidity Position Liquidations

A keeper specifies a pool and which liquidity positions they believe are out of range. The protocol calculates an instant TWAP for the pool to confirm out-of-range positions. Each confirmed position is removed, and the real tokens received back from the pool are sent back to the position owner, with a liquidation penalty removed for the keeper.

This balances the incentive to provide liquidity along a tight price range for increased virtual liquidity with providing liquidity along a broad enough range to remain useful to the protocol.

8.3 Increased Peg Stability

Because Hue is a stablecoin, liquidity providers for the reference pools could be expected to provide liquidity along a tight range of 1 Hue = 1 Dollar.

Because narrow liquidity ranges can increase virtual liquidity by multiple orders of magnitude, Hue will move more slowly away from the peg than if that liquidity had been provided along the entire range of possible prices for Hue, as would be the case in Uniswap V2.

8.4 Liquidity Position Index

A gas-optimized index of all liquidity positions by price range is updated whenever a new liquidity position is created. A liquidity position keeper needs only the chain's current state to find out-of-range positions. This eliminates trust in any centralized parties to provide correct indexed data and dramatically simplifies the keeper algorithm.

9. One-to-One Minting

For a limited time, anyone can lock reference tokens (Dollar pegged stablecoins) for an equal amount of newly minted Hue. Hue can be redeemed one-to-one for these locked tokens if they are available. This keeps Hue on peg through early turbulence while strictly timeboxing this mechanism on chain due to its direct reliance on potentially centralized assets.

10. Shutdown

The protocol can be shut down instantly by staking more than a quarter of the protocol tokens or by governance vote. If the protocol shuts down, a price is discovered for the Dollar relative to Eth. Anyone can then retrieve Eth for Hue from any position at this rate, position owners can retrieve their collateral, and anyone can retrieve their Uniswap liquidity position.

10.1 Price Discovery

A shutdown price oracle is specified at launch. After the protocol is shut down, users can stake TCP to indicate that they do not trust the shutdown price oracle. If more than a threshold of TCP is staked before a deadline, the shutdown price oracle can be removed. TCP governance must then specify a new price oracle before a price can be confirmed.

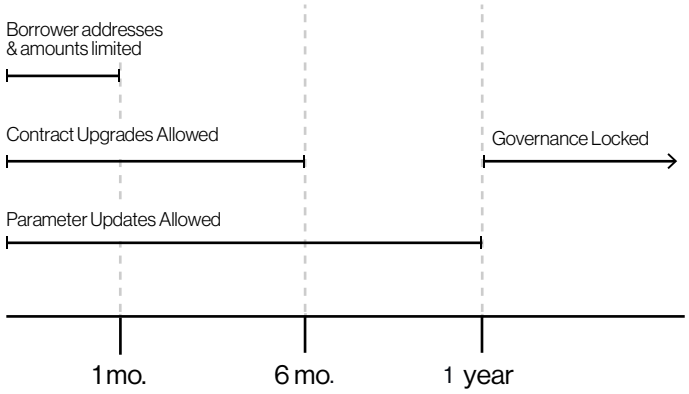
This mechanism seeks to give governance control over the shutdown price without the delay from voting on a price. By the time a price is voted on and committed to the protocol, it is stale.

10.2 Upgrade

After shutdown, by governance vote, the protocol is upgraded by allowing another contract to mint TCP.

11. Launch Schedule

TCP uses a multi-phase launch schedule. This schedule aims to progressively decentralize while also ensuring Hue stays on peg during early turbulence. Unlike the vast majority of centralized protocols, TCP enforces this launch schedule automatically on chain. There is no trust involved in enforcing the decentralization schedule. Some deadlines can be delayed, but only by decentralized governance, for fixed increments, and up to a maximum number of times.



Phase 0

There are no inflation rewards, and the timelock is controlled by a multisig since there are no TCP tokens to vote with. The one-to-one minting mechanism above is active.

Phase 1 - Genesis

TCP Inflation rewards start, and TCP governance controls the timelock. Users are limited to borrowing a low, fixed number of Hue, and providing a low, fixed number of Hue of real liquidity to each incentivized pool.

Capital limits are enforced by signatures that are pre-generated for each ethereum address that sent any transaction in the year leading up to launch. Users must provide this signature in order to borrow or provide liquidity during the genesis phase. This ensures that all early users of TCP are on the same playing field regardless of amassed capital. All can earn an equitable portion of TCP during genesis.

The genesis phase also allows time for the community to get familiar with the protocol mechanics and for keepers to set up bots, all while the total value in the protocol is relatively low.

During this phase TCP inflation is elevated. A target of 20% of the first four years of TCP inflation is allocated during Genesis. The Genesis phase lasts for 3 weeks.

Phase 2 - Bootstrap
Capital limits are lifted. The Bootstrap phase lasts 2 months, with the option to extend by one month one time.

Phase 3 - Finalize Contracts
One-to-one minting is disabled. This is the last phase contracts are upgradable. The Finalize Contracts phase lasts 4 months and can be extended by one month up to three times.

Phase 4 - Finalize Parameters
The last phase that most parameters can be updated. Shutting down and upgrading the protocol and updating the settlement price provider are always allowed. Setting the interest rate step and adding or removing reference pools are always allowed if the ability to change them has not been explicitly removed by governance.

The Finalize Parameters phase lasts 6 months, and can be extended by one month up to three times.

Phase 5 - Trustless
Full governance is in place since phase 1, one-to-one minting is disabled since phase 3, contract upgrades are disabled since phase 4, parameter changes are severely limited, TCP tokens are broadly distributed, and Uniswap V3 is used for all prices. Trustless Currency Protocol has inexorably decentralized 12-15 months after launch.

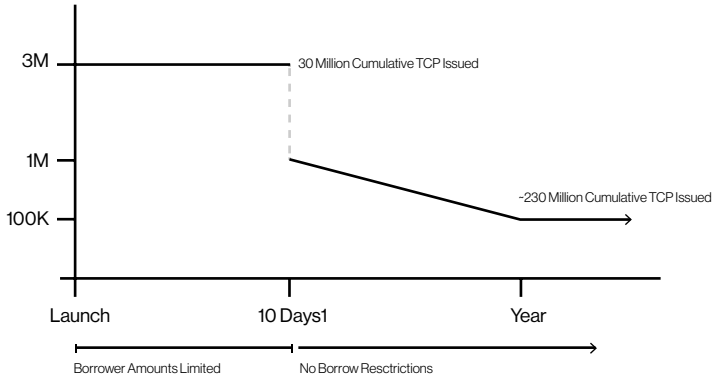
12. Valueless

TCP has no inherent value and will not even exist in an accessible form until the genesis launch phase meaning no TCP can be bought or sold before launch.

13. TCP Liquidity Incentive

A TCP:Eth pool, called the “protocol pool,” is incentivized alongside the collateral and reference pools. The protocol pool is intended to create extra liquidity for those wishing to participate in TCP governance and is not used for prices.

14. TCP Inflation Schedule



TCP inflation will be elevated during genesis and will decrease smoothly from the end of genesis until one year later. Afterwards TCP will inflate at a low, constant amount per day. A perpetual low inflation rate is necessary to maintain liquidity incentives.

15. TCP Allocation

15.1 Community Allocation
80% of the first four years of TCP inflation is distributed directly to the community through clearly defined on-chain incentives to borrow and provide liquidity, both of which are essential for the system’s proper functioning.

15.2 Bug Bounty Allocation
5% of TCP is held by the Trustless Foundation specifically to run a bug bounty program, incentivizing finding and disclosing bugs with a portion of the protocol. No additional tokens are held by the foundation.

15.3 Creator Allocation
The creators of TCP will be minted 15% of TCP. 10% of these tokens will be locked on chain for one year, 20% for two years, 30% for three years, and 40% for four years. This will allow the protocol creators to continue to be involved in the TCP community.

16. Conclusion

We have shown that Trustless Currency Protocol is a maximally decentralized, broadly distributed lending protocol. There is no longer a need to trust banks, governments, or centralized actors. TCP hands back control of decentralized lending to the community.