# Trustless Currency Protocol v1.2

## Abstract

Blockchain technology is widespread today for one simple reason. **It enables anyone, anywhere, to move value without trusting one another.** Blockchain networks are valuable *because* they are decentralized, *because* they give every individual control over their own value, and *because* each actor does not need to trust anyone else. Otherwise they would not exist: there would be nothing that separates blockchain technology from existing power structures. The perceived value of this decentralization can be seen in the growing market capitalization of countless decentralized finance and other cryptocurrency projects.

However, decentralized finance builders have lost sight of these truths. Creators and VCs hoard a majority network stake and seem to take every opportunity to introduce centralized power structures and control. The irony is not only does this trivialize the incredibly hard work done before them to create trustless blockchains, it erodes the value of the network they create by limiting the opportunity for participation and control by those that make the protocol valuable.

The Trustless Currency Protocol (TCP) shows that it is in fact possible to build a truly decentralized lending protocol that prioritizes trustlessness and community ownership above all else. This is not only the right thing to do for the decentralized future of blockchain; ensuring that the users that support TCP also own TCP is the best chance it has at success.

## Introduction

The Trustless Currency Protocol enables users to lock Eth collateral and borrow a token called Hue. Hue's target price is the median price of a basket of assets. The TCP token backs Hue if the Eth collateralization mechanism fails and is used to coordinate protocol changes for up to one year after launch. The TCP protocol is maximally trustless because it:

- **Distributes 65% of protocol ownership to the community**
- **Does not distribute ownership to venture capital firms**
- **Accepts only Eth as collateral**
- **Enforces automatic, hardcoded lock times on protocol changes**
- **Enforces long-term governance minimization**
- **Provides instant liquidations**
- **Uses Uniswap V3 instant TWAPs for trustless prices**
- **Automatically adjusts interest rates**
- **Enables negative interest rates**
- **Indexes all keeper data trustlessly on-chain**
- **Incentivizes decentralized user interfaces**
- **Uses extensive code comments and sensible labels.**

# 1. Equitable Distribution

## 1.1 Community Focused Distribution

Setting aside inflation due to deficit auctions (section 4.3.2) and voting rewards (section 1.1.3), TCP will allocate **100 million** tokens: 65m to the community and 35m to the Foundation.

#### 1.1.1 65m Community Distribution

TCP distributes 65m tokens to the community that makes TCP valuable. 30m are distributed to community members through incentives to borrow and provide liquidity, both essential for the system's proper functioning. 15m are distributed during genesis to liquidity providers. 20m are distributed to the first community members: those that have worked to imagine, build, and launch TCP. They are therefore able to continue to participate in the TCP community.

#### 1.1.2 35m Foundation Allocation

TCP will distribute 35m tokens to the Foundation. It will use them for whatever purpose the TCP community decides and can not vote using these tokens.

#### 1.1.3 Participation Allocation

TCP will increase the TCP token supply by 0.5% for each community proposal and distribute the new tokens to those who vote. This means that TCP is only owned by community members that work to make it successful. Those who own TCP but do not work to improve the protocol can expect their proportional ownership to dissolve.

#### 1.1.4 Perpetual Foundation Allocation

Whenever the supply of TCP increases due to liquidity mining or voting rewards, the supply of TCP is increased an additional 20% and added to the foundation's allocation. This means that the Foundation will always be able to support TCP.

## 1.2 Broad Community Distribution

#### 1.2.1 Equitable Genesis Distribution

TCP distributes genesis tokens to users that support the vision of TCP over the long term instead of defi users that are rich, encouraging a broad community to be involved.

Anyone who creates a position during genesis will be equally rewarded. TCP distributes 15m tokens to genesis participants without regard to relative wealth. TCP accomplishes this by distributing an equal portion of tokens to each participant address, regardless of how much value they have added beyond a low minimum value. Mechanisms are in place to prevent spamming.

#### 1.2.2 Distribution to Liquidity Providers

After genesis, TCP will automatically distribute 75,000 TCP tokens per day, decreasing by 0.25% each day, to anyone who creates a debt position or provides liquidity to the Uniswap pools. Just like with Bitcoin, the total number of tokens distributed by this mechanism converges. TCP will distribute at most 30 million TCP tokens by this logic given infinite time, and the number of TCP issued per day halves smoothly approximately every nine months.

## 1.3 Token Lockups

#### 1.3.1 Long Term Incentive Alignment

All tokens listed above besides the foundation tokens are distributed according to a strict lockup schedule that is automatically enforced on-chain. This aligns long term incentives helping to transform early interest and momentum into long term network health.

# 2. Strict Decentralization

## 2.1 On-Chain Decentralization Schedule

TCP strictly enforces a decentralization schedule on-chain. This hard-coded logic is in stark contrast to other protocols that make the users who create value wait for those holding centralized control to give up power when they feel like it. The schedule has four phases:

**› Phase 0 - Genesis:**

The protocol is fully functional, and borrowers and liquidity providers earn genesis rewards. The Foundation controls protocol changes since there are no TCP tokens for community members to vote with in circulation.

**› Phase 1 - Finalize Contracts:**

The community controls the protocol changes, although the Foundation can cancel malicious proposals. Phase one is the last phase contracts are upgradable. This phase lasts 1.5 years and can be extended by the community for two months up to three times.

**› Phase 2 - Finalize Parameters:**

The Foundation can no longer cancel proposals. Phase 2 is the last phase that the community can update most parameters. TCP always allows shutting down and upgrading the protocol, and updating the settlement price provider (section 5.1). TCP additionally allows setting the interest rate step (section 4.2.3), adding or removing reference pools (section 4.1), and approving or disapproving of UIs (section 2.2.2) if the community has not explicitly removed the ability to update each. Phase 2 lasts 1.5 years beyond phase 1 and can be extended by one month up to three times.

**› Phase 3 - Trustless:**

TCP has disabled contract upgrades since phase 1 and has severely limited parameter changes since phase 2. TCP has broadly distributed the network and uses Uniswap V3 for prices. Trustless Currency Protocol has automatically and completely decentralized 3-4 years after genesis.

## 2.2 Decentralized User Interfaces

Trustless Currency Protocol promises maximum decentralization. User interfaces are no exception. Those that host UIs can earn TCP inflation for doing so.

#### 2.2.1 Registering an Interface

User interface providers must first register their UI, providing a kickback portion, kickback destination, and IPFS hash of the interface. The kickback portion is limited to 25%. Users can compare the relative cost of using each UI to minimize the TCP inflation they must share. When the user accrues TCP inflation, TCP distributes some of those tokens to the interface hoster. Interface hosters must provide an ID for the user interface along with the transaction.

#### 2.2.2 Approving Interfaces

Each interface hoster must provide an IPFS hash for an immutable interface. The community can register approval or disapproval of specific registered interfaces indicating to users which interfaces the community has reviewed and deemed trustworthy or not. Users could also use a non-IPFS based interface and then know that the kickback cost for doing so is at most 25%, although this is riskier as it is impossible to indicate those interfaces are trustworthy as they can be changed at any moment.

#### 2.2.3 Avoiding Interface Costs

A user can interact directly with the blockchain to avoid sharing rewards. They could also host and use their own interface. If users have already used an interface to manage a position, they can call a function directly on TCP to stop sharing rewards.

# 3. Providing Liquidity

## 3.1 Borrowing

#### 3.1.1 Decentralized Collateral: Eth only

The Trustless Currency Protocol only accepts Eth as collateral for borrowing Hue. By using only the native currency of the ethereum blockchain, TCP eliminates the risk that a government or centralized actor could use its power over a collateral token to destroy the protocol.

#### 3.1.2 Incentivized Borrowing

Anyone can create a debt position. The protocol incentivizes debt positions by giving their owner a portion of TCP inflation proportional to the position's debt, ensuring that TCP is owned by those that make it valuable.

#### 3.1.3 Tokenized Debt Positions

TCP tokenizes debt positions as non-fungible tokens (NFT), allowing Defi builders to create any number of financial products using TCP debt positions as the underlying economic primitive.

## 3.2 Lending

Anyone can stake Hue into the protocol and earn a portion of the positive interest charged to borrowers. TCP provides an immediate use case for Hue: it gains interest.

## 3.3 Liquidating Undercollateralized Positions

Anyone can instantly liquidate a position if it is undercollateralized. TCP pays a fee from the position's collateral to the keeper that discovers the undercollateralized position. TCP pays an additional fee to the keeper that pays off the undercollateralized debt.

#### 3.3.1 Discovering Undercollateralized Positions

A keeper specifies a batch of positions that they believe to be undercollateralized. TCP confirms that these positions are undercollateralized by pulling a time-weighted average price (TWAP) from the Hue:Eth pool. TCP pays a fee on the liquidated debt in the collateral currency (Eth) to the keeper. Next, TCP adds collateral of equal value to the position debt plus an additional penalty to the liquidation account. TCP leaves any remaining collateral in the position.

#### 3.3.2 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.

#### 3.3.3 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. TCP removes Hue from reserves to pay off the excess debt. If there are insufficient reserves, anyone can direct TCP to run deficit auctions to raise reserves.

#### 3.3.4 Limiting Liquidation Rewards

TCP limits liquidation rewards to a percentage of system debt and resets this limit at regular time intervals, capping the total value that an attacker could extract by manipulating the collateral price. TCP achieves this 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.

#### 3.3.5 Indexing Positions

TCP maintains a gas-optimized index of all debt positions by collateralization. A keeper only needs the chain's current state to liquidate undercollateralized positions, eliminating trust in any centralized parties to provide indexed data and dramatically simplifying the keeper algorithm.

## 3.4 Capital Efficiency through Instant Liquidations

Due to the instantaneous nature of the liquidation mechanism, the community can move the minimum collateralization ratio to below the 150% value set at launch. If the value of Eth decreases quickly, keepers can liquidate positions instantly instead of waiting until they are further undercollateralized. This reduces the need for a large buffer of extra collateral in each position, making TCP more capital efficient.

## 3.5. Providing Uniswap Liquidity

Uniswap V3 is a leap forward in AMM technology. Uniswap V3 allows users to provide liquidity within a narrow price range, allowing liquidity to be highly concentrated. TCP uses Uniswap V3, providing instant prices that are more difficult to manipulate, deeper liquidity, and a more stable peg.

TCP enables users to provide liquidity around the current price for any pool the community decides to incentivize. TCP pulls in tokens from the user and creates a liquidity position that is tokenized as an ERC20. This is accomplished using a trustless protocol specializing in optimally allocating Uniswap V3 liquidity and tokenizing the positions. TCP rewards users with an amount of TCP inflation proportional to the share of liquidity they have provided.

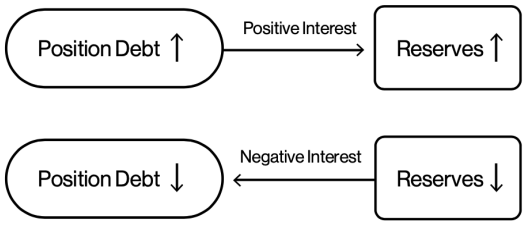
# 4. Automatic Peg Maintenance

## 4.1. Determining Peg Price

TCP calculates long Uniswap V3 TWAPs on pools pairing Eth with the price reference assets to determine whether Hue is on-peg. It does so by medianizing the reference values and comparing them to the Hue:Eth price to determine if Hue is on-peg. The community can vote to add or remove reference assets until deciding to forgo that ability.

## 4.2. Stabilizing Hue Value

To maintain the target value for Hue, TCP charges a variable interest rate on debt. 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. TCP stores positive interest as reserves and pays negative out of reserves. If reserves are depleted, TCP floors interest rates at zero.




#### 4.2.1 Adjusting the Interest Rate

Anyone can direct TCP to update the interest rate at regular intervals. If Hue has been trading above the peg, TCP reduces the interest rate. This increases the incentive to borrow – which increases Hue supply and decreases the price. If Hue has been trading below the peg, TCP increases the interest rate. This increases the incentive to pay back debt – which decreases Hue supply and increases the price.

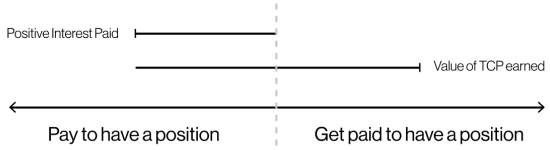
#### 4.2.2 Calculating the Interest Rate

TCP sets the interest rate using a simple interest rate controller. If Hue is off the target value by a threshold, then every increment above or below the peg TCP changes the interest rate by one step up to a maximum number of steps on each update.

Because the interest rate algorithm is simple and predictable, users can front-run interest rate changes, further enforcing the peg.

#### 4.2.3 Virtually Negative Interest Rate

Borrowers of Hue receive TCP. If the value of TCP accrued outweighs positive interest charged, borrowers receive negative interest rates without eating into reserves.




## 4.3 Negative Interest Rates Create Peg Resilience

Other lending protocols on Ethereum defi have proven unable to maintain the peg after a token's value has slipped above the peg. Negative interest rates allow TCP to pay borrowers, if necessary, to create more debt and restore the peg in this scenario.

## 4.4. Maintaining Reserves

Users can trigger TCP to run auctions to keep reserves within a target portion of total debt.

#### 4.4.1 Accruing value to TCP

The auction mechanism allows positive interest to accrue to the TCP token so that it can act as a collateral of last resort in the event of a rapid decrease in the value of the primary collateral: Eth.

#### 4.4.2 Starting Deficit Auctions

Anyone can direct TCP to create deficit auctions if reserves are below a threshold of total debt. This could happen due to persistent negative interest rates or a cascade of liquidations of undercollateralized positions. Deficit auctions sell a decreasing amount of newly minted TCP to buy a fixed amount of Hue.

#### 4.4.3 Starting Surplus Auctions

Anyone can direct TCP to create surplus auctions if reserves have accrued above a threshold of total debt. Surplus auctions sell a fixed amount of Hue to buy an increasing amount of TCP to be burned.

# 5. Shutdown and Upgrade

Users can shut down TCP instantly by staking more than 20% of all TCP. The community can also shut down TCP by a normal vote. If the community shuts down the protocol, TCP determines a price target for Hue relative to Eth. Anyone can then retrieve Eth for Hue at this rate. Additionally, position owners can retrieve their collateral in excess of debt. Anyone can retrieve their Uniswap liquidity position.


## 5.1 Discovering a Shutdown Price

TCP is launched with a shutdown price oracle set. After the community shuts down the protocol, users can stake TCP to indicate that they do not trust the shutdown price oracle. If users stake more than 10% of TCP before a deadline, TCP removes the shutdown price oracle. The TCP community must then specify a new price oracle before TCP can confirm a new price.

This mechanism gives the community control over the shutdown price without delay from voting on a price. A price is stale by the time it could be determined, voted on, and committed to the protocol.

## 5.2 Upgrading TCP

After shutdown, the community can upgrade the protocol. A TCP upgrade allows another contract to mint TCP. The community formed around the Trustless Currency Protocol can therefore immediately support the new version of the protocol.

# Conclusion

The Trustless Currency Protocol is a maximally decentralized, broadly distributed lending protocol. Each mechanism is reimagined from the ground up to be maximally trustless and to create community ownership. There is no longer a need to trust banks, governments, or centralized actors. TCP hands back control of decentralized lending to the community – restoring DeFi to its original vision of a truly trustless and permissionless financial system.