Nephrite: A Confidential Stablecoin

The Nephrite Team

1st July 2022

Abstract

Nephrite is a censorship-resistant, non-custodial, and governance-less confidential stablecoin on the Beam blockchain, pegged to an external asset and overcollateralized by BEAM. Here is why we believe the world needs it.

Bitcoin is not enough

Bitcoin is a significant step in the evolution of money, but it is not money. There are at least two reasons why bitcoin can't become money: volatility and privacy.

Bitcoin has a perfectly inelastic supply which, along with frequent demand shocks, causes high volatility in its price. This volatility is a good feature for speculators but not regular money users. Since its creation, bitcoin has shown eye-popping performance and become a part of corporative treasuries, but this success stops it from becoming money. No one will use an asset as a means of payment if this asset could appreciate. Everyone will hold it and use something else for their everyday purchases. Gresham's law says that bad money drives out good, but in the case of bitcoin, an asset is just too good to become money.

Bitcoin is pseudonymous, but the whole history of bitcoin transactions is recorded forever in a public database. Today there are paid services allowing one to identify bitcoin and other cryptocurrency holders and track their transaction history. Spying on crypto whales is just the tip of the iceberg. Throughout the history of money, cash has had a transaction privacy feature - this is a core feature of money. Bitcoin is digital, but it is not cash. Even central bankers admit that cash transactions respect our fundamental right to have our privacy, data, and identity protected in financial matters. It is not about shady deals. It is about economic efficiency and human rights.

The issues are apparent, and partial solutions already exist.

Partial solutions

Generally, those two issues of bitcoin are solved separately. Stablecoins become a solution to bitcoin volatility, and privacy coins solve its pseudonymity issues.

Of course, only decentralized stablecoins are in line with the bitcoin philosophy. Decentralization, in this case, means censorship resistance, non-custodial design, and an absence of a single entity controlling a stablecoin.

Censorship resistance is non-excludability - every network participant has equal rights to issue, transfer, and, if applicable, redeem a stablecoin, and no one can ban them from doing this. Non-custodial design refers to non-seizability - a private key owner is the only person who controls a respective stablecoin balance, and, if applicable, collateral that backs this coin. DAOs are usually considered as a way of a single controlling entity elimination. In fact, this is not always

true. If a DAO is controlled by governance token holders, then a single entity could control the DAO by accumulating the majority of the tokens. The only way of making a stablecoin truly decentralized is non-upgradeability - stablecoin smart contracts are immutable, i.e. non-upgradeable by any entity.

Privacy coins fix bitcoin pseudonymity issues using different techniques. Amongst them are built-in mixers, ring signatures, stealth addresses, and zero-knowledge proofs, to name a few.

To sum up, we have stablecoins that are not confidential and privacy coins that are not stable. A ridiculous situation when you can't have both at once. Why not combine stability and privacy in one cryptocurrency? Here is where confidential stablecoins come into play.

Choosing stablecoin design

The only working confidential stablecoin we are aware of is xUSD by Haven. This stablecoin utilizes Terra's UST design and, given the recent UST collapse, this approach doesn't look sufficiently safe. Silk is a project of a confidential stablecoin on Secret Network, trying to overcome UST design flaws by using additional reserves for the peg support. UST also had such reserves, but these enormous reserves didn't help save UST from a death spiral. Banknote redeemability as an automatic stabilization mechanism proved its efficiency back in the days of the gold standard, but the collateral printer is not.

The last but not least confidential coin which we should mention is ZeroStableCoin. Its design is brilliant but infeasible until the discovery of quantum interpersonal DeFi-agnostic computing.

We believe that the only way of building a robust decentralized stablecoin is overcollateralization. DAI by Maker is the most successful and battle-tested decentralized stablecoin, but it has flaws. It has a too complicated design, charges loan interest, is not redeemable, and is not truly decentralized in terms of collateral and governance. Good decentralized stablecoin should have opposite characteristics. LUSD by Liquity is such a stablecoin. DAI and LUSD are compared in Table 1.

Table 1. DAI and LUSD comparison

Criterion	DAI	LUSD
Immutable	No	Yes
Decentralized collateral only	No	Yes
Redeemable	No	Yes
Simple design	No	Yes
Interest-free borrowing	No	Yes

These are the reasons why the Nephrite team has chosen Liquity as a reference stablecoin design.

Choosing privacy technology

As long as Nephrite is an overcollateralized stablecoin working on smart contracts - it needs a privacy coin network that supports smart contracts.

We already mentioned that the only non-native confidential stablecoin project we know is building their coin on Secret Network. The two questionable points with this type of network are trusted execution environments and PoS consensus. We prefer old-fashioned and battle-tested PoW, closer to bitcoin. Beam is such a network.

Beam utilizes Mimblewimble, an elegant privacy-preserving solution, together with modified Dandelion (a node IP obfuscation protocol). This is the only confidential PoW chain that supports smart contracts and doesn't require third-party frontends to interact with its Dapps. A stablecoin created on Beam via the Confidential Assets feature can have the same level of privacy as its native token BEAM. These are the reasons why the Nephrite team has chosen Beam as a confidential smart contract platform.

We have chosen a reference stablecoin design and a confidential smart-contract platform - it's time for Nephrite!

Nephrite: combining stability and privacy

Nephrite uses the base Liquity design, and if one doesn't feel familiar with this concept - Official Liquity Documentation is the best place to fill this gap. Nevertheless, Nephrite is not just a copycat of Liquity on Beam. There are several differences between these stablecoins, presented in Table 2 and elaborated in the respective paragraphs below.

Table 2. Nephrite and Liquity comparison

Criterion	Nephrite	Liquity
Liquidations		
Liquidator's Reward	10 NPH	50 LUSD + 0,5% of the debt in ETH
Liquidation order	From the weakest trove only	Arbitrary
Recovery mode		
Stability pool	Withdrawals are paused	Withdrawals are not paused
Frontends		
Frontend entity	Each Beam desktop wallet is a frontend	Need for frontends provided by independent economically incentivized entities
Collateral		
Collateral token	BEAM	ETH
Oracles		
Main oracle	BeamX Network Oracle	Chainlink
Fallback oracle	Phase 1: maintained by the Nephrite team. Phase 2: a decentralized oracle network.	Tellor
Secondary token		
Utility	BEAMX (governance token of BeamX DAO)[1]	LQTY (pure profit-sharing token of Liquity)

[1] BEAMX is not a secondary token of Nephrite by default. We elaborate on this point in the respective paragraph below.

Criterion	Nephrite	Liquity
Liquidations		
Liquidator's Reward	10 NPH	50 LUSD + 0,5% of the debt in ETH
Liquidation order	From the weakest trove only	Arbitrary
Recovery mode		
Stability pool	Withdrawals are paused	Withdrawals are not paused
Frontends		
Frontend entity	Each Beam desktop wallet is a frontend	Need for frontends provided by independent economically incentivized entities
Collateral		
Collateral token	BEAM	ETH
Oracles		
Main oracle	BeamX Network Oracle	Chainlink
Fallback oracle	Phase 1: maintained by the Nephrite team. Phase 2: a decentralized oracle network.	Tellor
Privacy		
Stablecoin	Confidential	Pseudonymous
Secondary token	Confidential	Pseudonymous
Collateral	Confidential	Pseudonymous

Let's take a closer look at these differences.

Liquidations

Beam is a way cheaper smart contract platform than Ethereum, so $10 worth of a stablecoin is quite enough for liquidation initiator compensation, and there is no need for charging an additional 0,5% liquidation fee.

A more significant improvement is that Nephrite allows liquidations only in strict order - from the weakest trove to the strongest one. This feature guarantees that liquidators will not liquidate only the most lucrative troves leaving smaller and weaker troves without liquidation.

Recovery mode

The Stability pool could serve as a source of liquidity during times of increased demand for a stablecoin. But during the Recovery mode, it should fulfill its core function - to be a source of stablecoin liquidity for liquidations. Nephrite pauses withdrawals from the Stability pool during the Recovery mode (when the system's Total collateral ratio is below 150%). This ensures that the Stability pool depositors will not game the system, collecting rewards during the Regular mode, and runaway once the system switch to the Recovery mode.

Frontends

Liquity functioning requires the participation of economically incentivized frontend operators that provide UI for interaction with Liquity smart contracts. Beam works in another way - every

desktop wallet is an independent frontend. Thanks to that, Nephrite increases its censorship resistance and security, and doesn't need to pay third-party services for the UI - all rewards go solely to the Stability pool depositors.

Collateral

Both Nephrite and Liquity are single-collateral stablecoins, but Nephrite uses BEAM instead of ETH. BEAM is more volatile than ETH, but its volatility is relatively the same as other low-cap privacy coins. Table 3 allows comparing their price volatility as of 15 June 2022.

Table 3. Price volatility of ETH, ARRR, BEAM, DERO, FIRO, SCRT, XHV

Coin	Standard deviation of log returns				Worst daily drawdown			
	Since Beam lauch	Last 365 days	Last 180 days	Last 90 days	Since Beam lauch	Last 365 days	Last 180 days	Last 90 days
ETH	4.89%	4.38%	4.21%	4.30%	-43.05%	-17.12%	-17.12%	-17.12%
ARRR	11.19%	6.84%	6.62%	6.41%	-43.05%	-29.43%	-29.43%	-29.43%
BEAM	8.52%	6.84%	6.02%	6.83%	-54.45%	-36.05%	-36.05%	-36.05%
DERO	7.93%	7.42%	6.95%	6.55%	-43.20%	-22.78%	-22.78%	-22.78%
FIRO	6.72%	6.04%	5.98%	6.48%	-41.71%	-34.51%	-34.51%	-34.51%
SCRT	8.37%	7.58%	6.76%	6.11%	-33.06%	-25.75%	-23.23%	-23.23%
XHV	9.58%	10.32%	10.83%	12.17%	-52.95%	-41.40%	-34.90%	-34.90%

To retain Liquity's capital-efficient approach, Nephrite sets the same Minimum Collateral Ratio of 110%. It is up to Nephrite users to choose their desired collateral ratio, balancing their capital efficiency and liquidation risk preferences. Nevertheless, the Nephrite team strongly encourages its users to follow the vast majority of Liquity's and MakerDAO's users in maintaining their collateral ratio equal to or above 200%.

Oracles

Liquity uses Chainlink as its primary oracle and Tellor as a fallback oracle (there is a detailed table describing Liquity oracle logic). The LUNA case has shown that the Chainlink price feeds could be unreliable during the market turmoils, and no one should neglect a fallback oracle.

Nephrite also utilizes a two-oracle approach but uses other oracles. The main oracle is BeamX Network Oracle provided by Beam Foundation as a public good, and a fallback one is an oracle maintained by the Nephrite team. Eventually, the fallback oracle would be connected to a decentralized oracle network resilient to LUNA-sudden-drop-like issues.

Secondary token

Liquity's secondary token, LQTY, is not a governance token - its only utility is to be a pure profit-sharing token. An immutable decentralized application like Liquity doesn't need a governance token, but its pure profit-sharing token could be treated as unregistered security by authorities.

Nephrite plans to distribute collected fees amongst BEAMX holders via BeamX DAO regular revenue distribution procedure. BeamX DAO distributes its revenue as a reward for the DAO management, so these rewards are not passive income. Only the BEAMX holders who vote on all the current proposals are eligible for the DAO rewards.

BeamX DAO will not get Nephrite's fees for free. Nephrite's proposal to BeamX DAO is to allocate a share of BEAMX from its Liquity Mining fund to reward Nephrite's Stability Pool depositors. No investors and team allocation - only the Stability Pool depositor rewards. A respective merging proposal will be published on the Beam governance forum before the Nephrite launch on the mainnet.

Only 33.3% of LQTY total supply will be distributed amongst the Stability pool depositors and frontend operators for 35 months. Nephrite aims to get 6% of BEAMX total supply and distribute these tokens to its Stability Pool depositors for 24 months.

Yes, the eventual share of the Nephrite Stability Pool depositors in the collected fees will be five times less than the Liquity ones. But, in exchange, they get a right to participate in the BeamX DAO governance and an additional source of revenue from the growing number of Dapps launched by this DAO. Besides that, Nephrite gets access to BeamX DAO development, liquidity mining, and promotion resources.

Privacy

Liquity is launched on Ethereum, a pseudonymous smart contract platform. Its collateral, stablecoin, and secondary token are pseudonymous. Nephrite will be launched on Beam, a confidential smart contract platform. Its collateral is BEAM, a privacy coin, its stablecoin, and its secondary token are Confidential Assets that have the same level of privacy as BEAM.

Roadmap

To ensure a smooth and secure transition to immutable mode, Nephrite will go through three phases: Test mode, Limited upgradeable mode, and Immutable mode.

Q3 2022:
- Nephrite Manifesto publication
- Nephrite Dapp launch on Dappnet (Phase 0: Test mode)
- Publishing a security audit

Q4 2022:
- The Merge Proposal submission
- Nephrite Dapp launch on mainnet (Phase 1: Limited upgradeable mode)
- Stability Pool Liquidity Mining launch

Q1 2023:
- Nephrite Dapp final upgrade (Phase 2: Immutable mode)
- BEAMX/NPH Liquidity Mining Proposal submission
- BEAMX/NPH Liquidity Mining launch

* * *

The Nephrite team will communicate with the community only via two channels: Twitter and Beam Forum. Keep calm and stay private.