pNetwork

Draft REV.5

pNetwork Litepaper

pNetwork litepaper

The pNetwork is a decentralized network of validators contributing to the verification of crypto asset switches across blockchains.

pTokens aims to be a decentralized open-source system facilitating cross-chain movement of assets.

As the cryptocurrencies industry continues to evolve, the development of alternative financial platforms is on the rise. A critical component for these to succeed is assets' liquidity, which in the decentralized scene is currently spread across multiple independent blockchain protocols.

The pTokens system bridges a variety of blockchains, powering the free movement of crypto liquidity. These bridges are operated by a network of validators, whose role is to verify the cross-chain asset switch and to guarantee the 1:1 peg with the underlying asset.

pTokens removes the need for a trusted intermediary by creating a crypto-economic incentive through a governance token.

The incentives mechanism is at the foundation of the pTokens system - the pNetwork Token (PNT) is leveraged to drive governance decisions, encourage community participation and adoption. While fueling validators' activities, the PNT token is a key element of the staking method at the basis of the network.

INDEX

Table of Content

How the pTokens system works

pTokens aims to be a decentralized open-source system facilitating secure cross-chain movement of assets.

Today, composability is possible and limited to the blockchain environment decentralized applications (dApps) are built on. As an example, most decentralized financial tools are being developed on top of the Ethereum network, making these dApps walled into it and limited to the liquidity of its native assets (ETH and ERC20-tokens). Similarly, crypto assets belonging to non-Ethereum platforms such as Bitcoin or EOS can only be managed using dApps built on top of their native blockchain, being unable to operate with existing Ethereum ones.

As the cryptocurrencies industry continues to evolve and the development of alternative financial platforms is on the rise, overcoming such limitations is an essential challenge.

At the basis of decentralized finance are two key elements - a common shared platform serving as a fertile ground where DeFi applications can flourish and assets that can be invested, collateralized and traded. As a direct consequence of the current blockchain silos, liquidity for decentralized financial applications is limited to the one locked within the ecosystem these are built on. Liquidity is largely spread across a large number of blockchain platforms and difficult to merge into a single pool. For this reason, it becomes essential to create solutions that allow effective cross-chain composability for decentralized applications to access any assets.

pTokens are designed to solve this very problem: they provide a general purpose, simple and secure foundation to make any token movement possible on any blockchain.

The potential of the decentralized financial market can be expressed as the size of the entire cryptocurrencies scene - a multi-Billion dollars market featuring over five thousand different crypto assets.

The pTokens system is aimed to expand even further the use and interaction of decentralized financial applications.

The pTokens bridges

The pTokens system is the enabler for unidirectional and bi-directional connections among a variety of blockchain networks. The navigation classification of these connections depends on the unique features of each blockchain protocol.
As an example, the Bitcoin blockchain model is currently not designed to natively support assets in the token format. Consequently, connections such as the one between Bitcoin and Ethereum are unidirectional. As a contrast, connections such as the one between Ethereum and EOS blockchains are bi-directional and crypto assets from either of the two can be moved into the other.

The pTokens bridge is a secure and transparent way for crypto assets to be moved cross-chain. A pTokens bridge can be built for each direction of a connection between two independent networks, for any asset to be moved into any blockchain.

The pTokens bridges power the peg-in and peg-out processes at the basis of the crypto assets switch from the native blockchain to the host blockchain. The former procedure happens whenever a crypto asset is locked within the native blockchain and transferred via a minting process of its tokenised form into the host blockchain. Opposite to it is the peg-out procedure, that happens whenever a pToken is burned within the host blockchain and released into the native blockchain.

A pToken identifies a token pegged one-to-one to a non-native cryptocurrency, whose issue and redeem is handled by a network of validators, each of these processing the asset switch within enclaves. As an example, a pToken on Ethereum is normally shaped as an Ethereum ERC-777 token pegged one-to-one to a non-Ethereum based cryptocurrency.

Three key elements are needed for a pTokens bridge to be set-up, namely:

- a full node for each blockchain being bridged
- secure enclaves running inside TEEs
- a network of validators that jointly cooperate to generate and manage the private key(s) used to orchestrate the peg-in and peg-out processes

More details on the inner workings of the pTokens bridges are available in the pTokens Litepaper.

The pNetwork

As the underlying architecture for pTokens, the pNetwork provides the foundation for a truly decentralized system, and is in fact, a realisation of its progressive decentralization aims.

The pTokens system will undergo a series of upgrades to achieve a fully decentralized network of validators, the pNetwork, where multiple operators (namely, validators) will ensure there is no single point of failure.

The pTokens system will continue to be underpinned by Trusted Execution Environments (TEE) that act as validators (nodes) in the network. These enclaves are encrypted hardware ensuring the integrity of the node, and guarantee a secure and fully auditable execution of all minting and redeeming processes.
In its initial iteration, the pTokens technology is backed by a single validator. A first upgrade of the pTokens system is aimed to introduce a network of validators that will cooperate in the automated verification of each peg-in and peg-out procedure.

The pNetwork will be launched as a permissioned network, that will then quickly evolve into a permissionless one. It is an open, public and independent network built upon Ethereum with an in-built governance system.

Validators are node operators having special signing capabilities - these are an essential component of the network as they validate the asset switch from one blockchain to another (peg-in and peg-out) in a secure and decentralized fashion. Validators can cooperate and perform the cross-chain movement of assets after they have all verified independently the external blockchains' conditions.

As a comparison, their role within the network is as essential to that of a miner within a proof of work blockchain. Whereas miners secure and verify transactions to secure the blockchain and its continuance, validators secure and verify the cross-chain movement of assets.

Anyone can be a validator and contribute in making the network effectively decentralized, withdrawing control from the development team. Economic upsides are given to validators as a reward for performing a fundamental role within the network. Peg-in and peg-out fees are paid to the network of validators for each cross-chain transfer and they are equally redistributed among validators.

The first pTokens upgrade will open the system to a set of known parties, who will operate on the network as validators. Ultimately, the pNetwork will reduce the control the development team has over the project.

Further upgrades aim to achieve full decentralization, making the pTokens system an open network which anyone can be part of. It's a permissionless network where a Multi-Party Computation (MPC) algorithm is jointly used by validators to reach consensus, power its computations and perform all peg-in and peg-out procedures.
This cryptographic algorithm allows a scalable number of parties in the network to run their computations collectively.

MPC is used to enable the distributed signing (via a threshold signature scheme) of peg-in and peg-out operations among the network validators. The use of Multi Party Computation enables the validators to cooperate and perform the cross-chain movement of assets after they have all verified independently the external blockchains' conditions.

Another fundamental feature of MPC is its ability to preserve certain security properties, even if some of the parties collude and maliciously attack the protocol.

The upgraded structure makes use of Trusted Execution Environments (TEEs) as an extra protection shield. A TEE is a secure sandbox that provides security features, guaranteeing the code and data loaded inside to be protected and remain confidential.

Multiple TEE techniques are employed to safeguard the generation and management of the key-pairs used by the pTokens bridges. This benefits the entire system by making it more expensive and impractical to attack - for example, the feasibility of sybil attacks is greatly limited thanks to the use of multiple TEEs (where different isolation techniques enforce the execution of the exact code the network has agreed on).

Ultimately, the pTokens peg-in and peg-out processes will be granted by a network of validators through the use of Multi Party Computation and where validators are operators of a multi Trusted Execution Environment setup.

The validators will cooperate to jointly trigger the issuance of pTokens or the release of the underlying asset (in the reverse process).

The introduction of an underlying network represents an improvement over the initial model as it strengthens the security of the pTokens’ bridges, while minimising various risks, as the network is supported by multiple parties.

The Decentralized Autonomous Organisation (DAO)

Upgrades of the pTokens system outlined in the previous section pave the way to a more decentralized and community-governed system.

In its initial phase, the pTokens bridges are governed and operated exclusively by the development team. This facilitates the set-up and speeds up the preliminary stages of the project. The pNetwork is a key element powering the switch to a more open system, where the governance of the pTokens bridges is passed over to the hands of the community.

The pNetwork is home to a Decentralized Autonomous Organisation (DAO) that governs the network itself, along with the pTokens bridges and their dynamics.

For the system to become truly decentralized, community participation is key. People can contribute to the success of the project by assuming an active role in it. Specifically, they can decide to operate a validating node or help shape its future by voting on pTokens improvement proposals via the pNetwork DAO.

The pNetwork DAO will be open for anyone to join and contribute to the developments of the pTokens system via a token-based voting mechanism.

Members of the DAO will initiate voting processes to influence the development and future of the pTokens system.

A series of Improvement Proposals (IPs) will be advanced by the development team on multiple pTokens related matters. DAO members will be called to vote and decide whether or not to approve the IPs. For example, members will be responsible for electing which pTokens bridges to develop and support next, deciding on the fee mechanism of the network and resolving any upgrade proposals.

Anyone can become a DAO member and contribute in making the network effectively decentralized, assuming an active role for the success of the project.

DAO members and validators within the network represent the keys to its decentralization, capturing the essence of these concepts pioneered by the Decentralized Financial movement.

Ecosystem overview and market opportunity

Liquidity is largely spread across a number of blockchain platforms and difficult to merge into a single pool. The pTokens system enables cross-chain composability effectively as it is an essential component for decentralized financial applications to be compatible with any crypto asset.

Alternative solutions have led the way to bridging the Bitcoin blockchain with the Ethereum one. The pTokens system positions itself as an automated, more decentralized and non blockchain-specific solution compared to the current market leader.

When compared to liquid solutions available on the market, the pTokens system is more appealing for market makers operating in the decentralized financial ecosystem as it grants cost-effective automated processes.

	WRAPPED BITCOIN (WBTC)	IMTOKEN (IMBTC)	PTOKENS (PBTC)
GOVERNANCE	Federation	Centralized	Decentralized
PEG-IN/OUT SPEED	Involves manual process (up to 48 hours)	Instant (after transaction finality)	Instant (after transaction finality)
PEG-IN/OUT COST	Low	Medium	Low

Alternative solutions, similarly-decentralized to pTokens, are in the workings. The pTokens system positions itself as a more flexible service when compared to these.

	KEEP NETWORK (TBTC)	REN PROJECT (RENBTC)	PTOKENS (PBTC)
GOVERNANCE	Bonded multi-federated peg	Decentralized system based on a custom MPC primitive (yet undisclosed) among its RenVMs	Decentralized system based on standard MPC primitive and multi-TEE setup
REACH	UTXO specific	Aimed for a multi-blockchain implementation	Multi-blockchain implementation
PEG-IN/OUT COST	High	Medium	Low
UNDERLYING TECHNOLOGY OF THE BRIDGES	Complex approach based on a multi-federated pegging mechanism	Complex approach based on multiple layers (including RenVM)	Purposely simple in its design (including a light client for each blockchain being bridged)
MACRO ECONOMICS	Close relation between the ETH price and the total value of assets that can be locked in the system	Close relation between Ren's system security and the value of the REN token staked into the network	Not limited in the amount of tokenised assets it can issue

pNetwork Token (PNT) and token economics

The pNetwork token (PNT) will be introduced to the system as a way to implement community-lead governance and as an incentive for actors within the network to perform their roles.

PNT token role within the system

The PNT token represents a key element of the system as it aligns incentives for all participants. In fact, PNT is leveraged internally by the pTokens system to enable operations for both validators and DAO members.

The flywheel effect is triggered by the need for validators and DAO members to hold and stake PNT tokens in order for them to perform their respective roles.

Prospective validators need to stake a minimum amount of PNT tokens (200K PNT), which is then used to show their commitment and serves as a bond. Such a role creates a potential economic benefit for validators, who are rewarded for their work with the peg-in and peg-out fees collected by the system. Should a validator operate maliciously, it is punished by the system by losing tokens at stake.

On the contrary, when operating remarkably, validators get back tokens at stake at the end of the validator's life cycle.

A network of validators contributes to a more stable and higher quality service, making the pTokens bridges more attractive for users. The pNetwork Token (PNT) is leveraged within the system as an incentive for all actors to participate in the decentralization of the system and in the verification of the cross-chain movement of assets.

The payment for the fees happens in terms of the asset users transfer cross-chain. As an example, while validating the tokenisation of Bitcoin on the Ethereum network, a peg-in fee will be collected by the system in Bitcoin and redistributed to validators. Such a model prevents the PNT token from being a burden for users adoption of pTokens, therefore incentivising usage of the system.

The utility of PNT is determined by its role within the ecosystem. It is an incentive for validators and a means for the community to actively participate in the pNetwork DAO's voting mechanism.

DAO members will be able to express their preferences in regards to a variety of Improvement Proposals by staking their PNT tokens within the Decentralized Autonomous Organisation and vote accordingly.

During the initial stages of the project, an additional economic incentive is introduced to the system to encourage active participation within the DAO.

While at stake, PNT tokens will mature an overall 63% interest over two years. Such interest is matured based on the tokens at stake, making rewards higher for those members who are more invested, and is distributed to members actively participating in DAO voting mechanisms.

The interest is split across the two-year period, granting a higher reward during the first year (42%) and transitioning to half that rate (21%) during the second year. Up to 28.35M PNT tokens are dedicated to this initiative, which are generated through an inflation mechanism that grows the initial approx. 60 Millions PNT supply proportionally to the tokens staked within the DAO and redistributes them to the community.

Active participation within the DAO leads to a more attractive pTokens system, growing the number of users for the pTokens bridges.

PNT token release schedule

Provable Things and Eidoo are sister companies whose teams work closely together to excel at the forefront of blockchain innovation.

Thanks to their complementary expertise and cohesive technologies, they are contributing to the development and growth of the decentralised financial industry. The pTokens project represents a new paradigm for the whole DeFi ecosystem. The effective and frictionless cross-chain movement of assets is helping to unlock liquidity in the market and push DeFi beyond its current boundaries.

In a collaborative decision, Eidoo’s native EDO token will be upgraded and effectively transformed into PNT so that it can be leveraged within the pNetwork ecosystem, playing a fundamental role in its maintenance. Such PNT tokens will be issued by the same legal entity that issued the EDO token (namely, Swiss-based Eidoo SAGL).

A one-to-one PNT airdrop will be received by all EDO holders at a specific point in time. In this way, the inherent value and potential of the EDO token will be effectively transferred to the PNT token.

The pNetwork Token (PNT) will be initially issued on the Ethereum network as an Ethereum ERC-777 token standard (backwards compatible with the ERC-20 standard).

PNT token circulating supply breakdown

The usage of an already-existing token contributes to a more distributed token allocation. From its very issuance, the PNT token will be in the hands of a large variety of different entities, therefore reducing the centralisation of the governance token of the project.

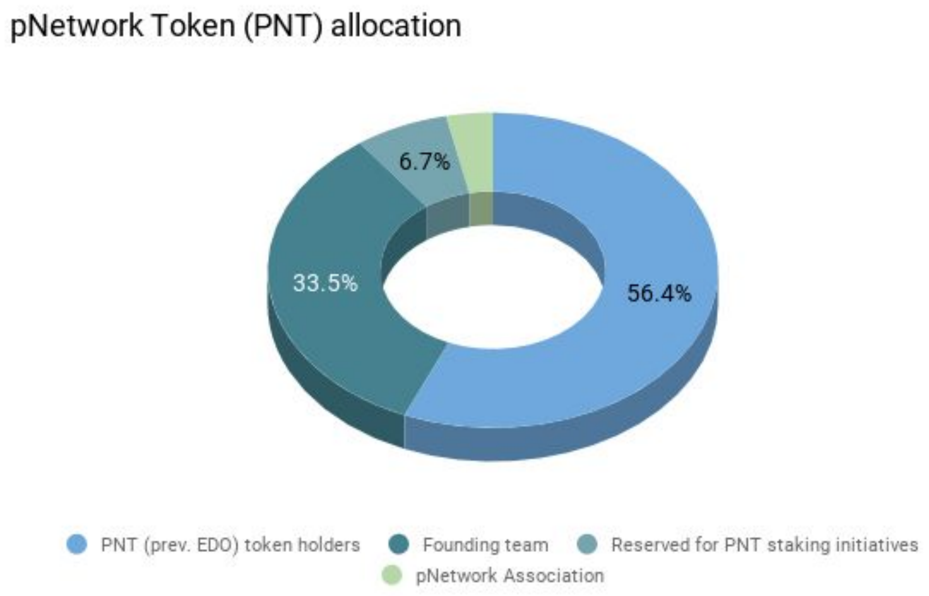
The circulating supply of the PNT token will be capped at 60 Millions tokens. The allocation of the circulating supply will be largely distributed as at the time of its issuance more than 50% of the PNT tokens will be held by thousands of different independent entities.

At the time of issuance, the PNT token will be allocated as follows:

PNT TOKEN DISTRIBUTION

PNT (previously EDO) token holders (over 7,000 independent addresses)	Approx. 33,650,000
Founding team	20,000,000
Reserved for PNT staking initiatives	4,000,000
pNetwork association	2,000,000

The majority of the PNT holdings (56.4%) will be distributed among over 7,000 Ethereum addresses. The remaining token holdings will be split among the founding team (33.5%), the pNetwork association and a PNT reserve dedicated to previously planned activities (more details below).



The pNetwork association is a Swiss-based entity dedicated to the promotion of the pNetwork and growth of the decentralized financial scene. An amount of PNT tokens will be given by the founding team to such an association for it to pursue its purpose.

The PNT reserve is a tokens reserve specifically dedicated to ongoing EDO-related staking initiatives (including the EidooCard staking programme).

The 60 Millions PNT tokens capping may increase over the course of the first two years to a hard cap of approx. 88 Millions PNT tokens. The inflation mechanism is closely related to the mechanics of the additional incentive introduced to the system to encourage active participation within the DAO during the first stages of the project.

Approximately 28.35 Millions newly generated tokens can be issued after the initial minting of the PNT token. In such a situation, the PNT token will be allocated as follows:

PNT TOKEN DISTRIBUTION

PNT (previously EDO) token holders (over 7,000 independent addresses)	Approx. 33,650,000
Founding team	20,000,000
Reserved for PNT staking initiatives	4,000,000
pNetwork association	2,000,000
Maximum inflation (introduced as an additional incentives mechanism for DAO stakers)	* 28,350,000

*The 28.35 Millions tokens will be gradually issued over the course of two years

Roadmap

The pTokens system is aimed to connect a variety of blockchain protocols, for any crypto asset to be moved cross-chain.

The first pTokens bridge (pBTC on ETH) had a successful mainnet launch on March 5th, 2020, with a number of integrations live, including industry-leading liquidity providers Kyber and Bancor Networks. Other platforms have performed seamless integrations so that peg-ins and peg-outs can be made straight from their interface. Examples include (but are not limited to) DMex and Eidoo.

Another pTokens bridge (pBTC on EOS) has been released to enable the connection of the Bitcoin and EOS networks. pTokens BTC has been adopted by the industry-leading Equilibrium framework as collateral for the EOSDT decentralized stablecoin.

Multiple pTokens bridges are already in the works and released on testnet. Examples include a pTokens bridge between Litecoin and Ethereum (pLTC on ETH) as well as the connection of the current two major DeFi networks, Ethereum and EOS (pEOS on ETH and pETH on EOS).

In the upcoming months, the following 3 steps will be implemented to introduce PNT to the system:

1. **PNT is issued on Ethereum.** The pNetwork Token (PNT) will initially be issued as an Ethereum token, following the ERC-777 token standard (backwards compatible with ERC20).
2. **The governance model (DAO) is introduced.** The pNetwork token (PNT) will be upgraded to a governance token to provide voting rights within the pNetwork DAO, which is introduced to the system along with the pNetwork itself. As the DAO will govern pTokens-related decisions, this will boost the decentralization of the system. Anyone holding PNT will be allowed access to the DAO and enabled voting via a staking mechanism.
3. **PNT staking for validators is enabled.** PNT can be staked within the DAO for validators to start operating.

The pTokens system is currently in Phase Zero. In its initial stages, the pTokens system is operated by a single validator.

The pTokens system will undergo a series of upgrades to achieve a fully decentralized network of validators, the pNetwork, where multiple operators (validators) will ensure there is no central point of failure.

Phase One

A first upgrade of the pTokens system (Phase One) is aimed to introduce a network of validators that will cooperate in the automated verification of each peg-in and peg-out procedure.

The pTokens system will continue to be underpinned by Trusted Execution Environments (TEE) who act as validators (nodes) in the network. These enclaves are encrypted hardware ensuring the integrity of the node, and guarantee a secure and fully auditable execution of all minting and redeeming processes.

The pNetwork will be launched as a permissioned network. The first pTokens upgrade will open the system to a set of known parties, who will operate on the network as validators.

With Eidoo being integrated from Day One, it is very convenient for its own users to access and use pTokens, such as pBTC. We expect this user base to drive its initial growth.

The pNetwork will not be a burden for pTokens users as they are not required to interact with it (unless they wish to). At the same time, it will create an incentive for a variety of actors to share efforts in making the governance of the pTokens bridges more decentralized.

The pNetwork is home to a Decentralized Autonomous Organisation (DAO) that governs the network itself, along with the pTokens bridges and their dynamics.

For the system to become truly decentralized, community participation is key. People can contribute to the success of the project by assuming an active role in it. Specifically, they can decide to operate a validating node or help shape its future by voting on pTokens improvement proposals via the pNetwork DAO.

The pNetwork DAO will be open for anyone to join and contribute to the developments of the pTokens system via a token-based voting mechanism.

Members of the DAO will initiate voting processes to influence the development and future of the pTokens system. A series of Improvement Proposals (IPs) will be advanced by the development team on multiple pTokens related matters. DAO members will be called to vote and decide whether or not to approve the IPs. For example, members will be responsible for electing which pTokens bridges to develop and support next, deciding on the fee mechanism of the network and resolving any upgrade proposals.

Phase Two

Further upgrades (Phase Two) aim to achieve full decentralization, making the pTokens system an open network which anyone can be part of. It’s a permissionless network where a Multi-Party Computation (MPC) algorithm is jointly used by validators to reach consensus, power its computations and perform all peg-in and peg-out procedures.

This cryptographic algorithm allows a scalable number of parties in the network to run their computations collectively. MPC is used to enable the distributed signing (via a threshold signature scheme) of peg-in and peg-out operations among the network validators. The use of Multi Party Computation enables the validators to cooperate and perform the cross-chain movement of assets after they have all verified independently the external blockchains' conditions.

The upgraded structure continues to make use of Trusted Execution Environments (TEEs) as an extra protection shield. A TEE is a secure sandbox that provides security features, guaranteeing the code and data loaded inside to be protected and remain confidential.

Multiple TEE techniques are employed to safeguard the generation and management of the key-pairs used by the pTokens bridges. This benefits the entire system by making it more secure - for example, sybil attacks are prevented thanks to the use of multiple TEEs (where different isolation techniques enforce the execution of the exact code the network has agreed on).

Ultimately, the pTokens peg-in and peg-out processes will be granted by a network of validators through the use of Multi Party Computation and where each validator is an operator of a machine running within a multi Trusted Execution Environment setup.

The validators will cooperate to jointly trigger the issuance of pTokens or the release of the underlying asset (in the reverse process).