



PROTON
BLOCKCHAIN

Whitepaper v2.0

JUNE 2022
WWW.PROTON.ORG

Abstract

In this whitepaper we introduce the Proton Blockchain, a fast scalable, layer one blockchain that can run decentralized applications and make free and instantaneous payments. At its core, Proton Blockchain is designed to communicate with banks, payment processors and traditional fiat gateways through Proton Signing Request (PSR). Additionally, Proton makes use of decentralized identity with human readable names, NFTs, token wrapping, a decentralized stablecoin index (XMD), defi lending, trading and governance.



Table of contents

1. Introduction

2. Mission and Vision

2.1 Commitment to helping developers and businesses build on Proton Blockchain

3. Proton Blockchain Overview

3.1 Decentralized Network

3.2 dPoS Consensus Mechanism

3.3 Resources on Proton Blockchain

3.4 Decentralized Identities (DeID)

3.5 Universal @names on Proton Blockchain

3.6 Transactions per second

3.7 Block production on Proton Blockchain

3.8 Block Producers

3.9 Decentralized, Independent Governance Model

3.10 Proton Consortium structure

3.11 Proton Signing Request (PSR)

4. XPR Token Info

5. Token Distribution

5.1 Token Inflation

5.2 Token Deflation

6. Token Utility

6.1 Short Staking

6.2 Long Staking

6.3 Yield Farming on Proton Swap

6.4 Proton Resources

6.5 NFT Minting

7. Proton Ecosystem

7.1 Proton Blockchain

7.2 WebAuth.com

7.3 Proton Swap

7.4 Proton NFT Market

7.5 Yield Farming

7.6 Proton Loan

7.7 Proton DAO Dashboard

7.8 Proton DEX

8. History

8.1 Origin of Proton Blockchain

8.2 Roadmap and Milestones

8.3 Commitment to Security

9. More Information and Resources

1. Introduction

Proton Blockchain is a layer one public blockchain and smart contract platform designed for both consumer and enterprise, built on delegated proof-of-stake forked from EOSIO. It is a highly resource-efficient chain that allows for scaling into thousands of transactions per second while providing extremely low latency.

Built around a decentralized identity protocol and financial settlements layer, Proton provides an alternative to traditional payment systems like ACH and SWIFT or Visa and Mastercard, through an innovative resource model.

2. Mission and Vision

Proton Blockchain was created to bridge the gap between traditional finance (TradFi) and decentralized finance (DeFi), creating a way for blockchains to communicate directly with the fiat payment messaging layer. Furthermore, Proton Blockchain was designed in such a way that banks and fintechs can pay for resource fees (versus their customers), while simultaneously having the capability to apply for resource grants from the Proton Consortium through the Worker Proposal System (WPS) for resources grants for wallet services.



2.1 Commitment to helping developers and businesses build on Proton Blockchain

The main language to build on Proton is C++; with over 6 million developers around the world, it's in the top five most popular languages and is a perfect choice for a growing blockchain environment. Proton additionally introduces WASM through [AssemblyScript](#), an extension of TypeScript to integrate with the existing web ecosystem. To encourage the continued progress of the Proton blockchain, and support developers who are actively building with Proton, we have released our Open SDK along with [documentation](#). Our Open SDK consists of the [Proton Web SDK](#), [ProtonSwift](#) (iOS), [ProtonKotlin](#) (Android) and the Proton API. Additionally, we created [demo dApps](#), running on the Proton blockchain with source code.

3. Proton Blockchain Overview

In the section below we cover specifics about the Proton Blockchain, how blocks are produced, how Block Producers operate, the scalability of the chain, and a deeper look at the consensus mechanism, delegated proof-of-stake (dPoS).

3. Decentralized Network

The Proton Blockchain is fully decentralized. The potential for adversarial attacks such as double spends, chain splits, and 51% attacks are mitigated through the use of the Delegated Proof of Stake (dPoS) consensus mechanism, which relies on Block Producers (BPs) and stakers to uphold the network constitution. The Proton Blockchain is permissionless and supportive of the FOSS movement. Our open-source documentation can be found on GitHub [here](#).



3.2 dPoS Consensus Mechanism

Proton Blockchain utilizes a decentralized consensus mechanism called Delegated Proof of Stake (dPoS). This mechanism balances performance with decentralization by relying on a minimized set of active Block Producers voted on by stakers of the native network asset, XPR.

Network users who hold and stake Proton (XPR) may select block producers to validate blocks through a continuous approval voting system. This ensures a balance between the network architecture providers and the democratic base of users who vote on their chosen providers (elected representatives).

3.3 Resources on Proton Blockchain

For most end users, using resources on Proton Blockchain should be a relatively foreign concept. For developers however, this is a different situation. Proton was designed with the web2 mentality that various wallets and services will pay for those fees for the end user or charge them in the form of services. Proton resources bought in XPR are burned as a deflationary mechanism to the circulating supply. Developers can start building for free on Proton, then add a resource plan to go live; each plan unlocks additional features. View [resource plans here](#).



3.4 Decentralized Identities (DeID)

Proton Blockchain integrates an optional KYC (Know Your Customer) decentralized identity protocol, with the capability to attach offline data-stores with attested data on-chain, without exposing personally identifying information for consumers or businesses. Users can establish their identities once, link funding sources, and authenticate rapidly into any platform without worrying about their information becoming compromised.

3.5 Universal @names on Proton Blockchain

The Proton Blockchain creates a unique human readable namespace of up to twelve characters, that can integrate into any payment app or platform. These names resemble what you would expect with a typical screen name or email address such as @irina or @marshall.xpr. Through the utilization of human-readable names, Proton Blockchain makes a more human web3 experience.

3.6 Transactions per second

The Proton Blockchain can process over 4,000 transactions per second (TPS) without having chain-splitting issues during stress tests. Currently, Proton and EOSIO are one of the fastest performant blockchains in the world. Settlement takes approximately 180 seconds, and can potentially be sped up through various means to eventually reach sub-second finality.



3.7 Block production on Proton Blockchain

The Proton Blockchain enables blocks to be produced at exactly every 0.5 seconds, with only one Block Producer authorized to produce a block at any given point in time. Blocks are produced in rounds of 126 (6 blocks each, multiplied by 21 producers). At the start of each round, 21 unique Block Producers are chosen by the preference of votes cast by token holders. The selected Block Producers are scheduled in an order agreed upon by 15 or more Block Producers.

3.8 Block Producers

The Block Producers are the heart of the Proton ecosystem. Block Producers are independent organizations that run the open-source Proton software to record and validate the transactions of the Proton Blockchain into immutable blocks. There are 21 active Block Producers which produce a new block every 0.5 seconds, with an additional 24 Block Producers on standby at any given moment. A 2/3 + 1 consensus of Block Producers is needed to write a transaction into the blockchain with 3-minute finality, during which time the transactions in the produced blocks are verified by the other active producers in rotation. Elections are conducted every few minutes where standby producers can become active producers based on their token weighted voting. The Block Producer ranking is public and can be viewed on the [Protonscan](#) block explorer.



3.8 Block Producers

The primary job of a Block Producer is to allocate computational resources to validate transactions. However, they also play additional roles in the ecosystem. For example, Block Producers ran the open-source price oracle for the Proton Long Staking experiment, continuously to provide tools and services to dApps, users, and developers, store the Proton Blockchain history and make it accessible via API to wallets and applications. Block Producers also serve as local resources to developers and users in their respective communities.

While any Proton Blockchain account can register as a Block Producer, gaining the ability to function as one is a careful process. In order to gain permissions for election, Block Producers must meet the minimum criteria set by the Proton Consortium, which includes running API, P2P, and Producer nodes with 99.99% uptime and participating in the Proton Testnet.



3.9 Decentralized, Independent Governance Model

Proton Blockchain uses a decentralized governance model that is broken down into three portions: stakers, Block Producers, and Consortium members. Stakers elect Block Producers by staking their coins and voting for their top four choices of Block Producers. Through this process, mining is weighted and those with the most votes earn the most XPR when actively producing. To actively produce blocks, a Block Producer must be within the top twenty one voted producers. Standards set by the Proton Consortium for accepting a new Block Producer are high, a majority vote of consortium members is needed to pre-approve any new Block Producers. Each Block Producer must meet minimum technical standards and must have a verified identity for their person and business. The consortium monitors all Block Producers, verifies that performance meets minimum thresholds, and in the case of non-compliance can terminate Block Producers. This system ensures that proper vetting takes place each and every time a Block Producer wants to join our network.



3.10 Proton Consortium Structure

The Proton Consortium consists of 5 independent members, that are also Block Producers, but it is not a requirement to be one. The Consortium members are voted in by a unanimous vote by current Consortium members. Similarly, they can be voted out.

The consortium serves a vital role for the network; by advising on the direction of the codebase and core protocols, setting the block rewards, resource pricing, and selecting worker proposal grants. All members of the consortium have an equal vote, serve for a term of 2 years, and nominate their replacements.

Consortium members oversee the Worker Proposal System (WPS) and actively distribute grants for the community to build open-source tools, protocols, core Proton functions, and core code commits to EOSIO.

To learn more about Proton Blockchain's independent decentralized governance system, visit our [governance page](#). See the bylaws [here](#).



3.11 Proton Signing Request

Proton Signing Request (PSR) is a secure method of signing a transaction or message. Similar to WalletConnect, Proton Signing Request is built to be highly responsive and capable of operating in any browser without additional software. From accepting a cryptocurrency swap, to into a dApp on Proton, PSR allows you to control what applications can and cannot interact with you and your funds.

Cryptocurrency platforms use a version of a signing request to authorize transactions; in most cases, this takes the form of Google's two-factor authentication (2FA) or another third-party multi-factor authentication (MFA). What makes PSR stand out from basic OTP is that it is immune to phishing attacks when utilizing decentralized identity. Furthermore, the deletion of individual access keys is simple when using Web Authentication and Proton.



4. XPR Token

XPR is the native cryptocurrency of the Proton Blockchain.

Token name: Proton

Token ticker: XPR

Consensus mechanism: Delegated Proof of Stake (DPoS)

Initial total supply: 10,000,000,000 XPR

Current supply: The current supply can be monitored in real time on the [Proton block explorer](#).

Max supply: ∞ (4% inflation per year that can be adjusted by BP vote)



5. Token Distribution

XPR is the native cryptocurrency of the Proton Blockchain.

Initial Distribution: 10B XPR

Airdrops: 151M XPR. On Monday, March 30th 2020, 1 PM GMT, a snapshot occurred that recorded all of the balances in the MTL and LNX ecosystems. An airdrop followed immediately after to all MTL (66M XPR) and LNX (85M total over 5 airdrops) token holders.

Venture: 100M XPR was granted to early investors in the core developer.

Founder and employee grant: 1.1B XPR was set aside for founder and employee grants with a 12 month vesting period.

Development: 8.65B was allocated to support development.



5.1 Token Inflation

To ensure that the Proton Blockchain remains secure in the future, it is essential to keep rewarding block producers to validate blocks, as well as all stakers, after all of the initial 10 billion XPR are put into circulation.

Block Producers are awarded block rewards for the work that they do for the network. Additionally, individuals who provide staking services for the Proton network are awarded as well. The block reward is set at 4% per annum, awarded on a 1/365 ratio, daily.

The reward is split as follows:

1% split amongst block producers

1% to all accounts that stake and vote for block producers

1% to the governing consortium

1% to yield farming

Additional XPR can come into circulation through long staking contracts, the last long staking payout will occur July 28 2022.



5.2 Token Deflation

Proton Blockchain Resources bought by businesses/developers in XPR will be burned as a deflationary mechanism. You can view the resource plans available [here](#) to get an understanding of how much could be burned in the future.

For every NFT minted, 10% of the XPR used is burned, with the other 90% becoming locked into the Atomic Assets smart contract. If the original NFT is erased (burned), the remaining 90% of the XPR will be returned to the creator. This places deflationary pressure on the Proton blockchain and represents a way for XPR to permanently leave the ecosystem.

Additionally, 0.1% of all fees generated from Proton Swap are burned, creating another pathway for XPR to permanently leave the ecosystem.

Token burns occur at the end of each quarter. What has been burned to date, can be tracked here: <https://www.protonscan.io/account/token.burn>



6. XPR Utility

Proton token has four forms of utility on-chain, using XPR to pay for resources (CPU, NET, RAM), staking, voting for block producers, and on-chain governance.

6.1 Short Staking

Short Staking allows users to participate directly in the Proton Blockchain ecosystem by voting for Block Producers. Users who stake their XPR in supported wallets will choose four Block Producers. After 24 hours, users who have staked their XPR and voted for block producers will receive a proportion of the block rewards for that period, based on a variable APR and the amount of XPR that they have staked.

The APR is a function of the percent of tokens on-chain; when the on-chain supply increases, so does the APR. The variable APR can be seen in Proton Blockchain supported wallets or block explorers. Staking rewards can be transferred, used in dApps, swapped for other tokens, or re-staked. Un-staking XPR takes 24 hours to complete.

6.2 Long Staking

Long staking was an experimental form of staking intended to showcase Proton's smart contract capabilities. Though no longer active, long staking allowed users to lock their XPR into a smart contract that was tied to the performance of Bitcoin. This allowed users to gain price exposure to two different assets at once; the longer the staking contract you chose (e.g., 90 days versus 365 days), the higher your potential yield. You can read more about long staking and how it worked [here](#).



6.3 Yield Farming

As described in greater detail later in this document, Yield Farming on Proton Swap allows users to stake XPR and another Proton-wrapped token in a liquidity pool. Doing so will earn the user Liquidity Pool (LP) tokens, which can then be staked in the associated farms for a variable APY.

The interest you receive on LP Tokens, which represent the liquidity you provided, is known as yield, and the process of earning interest on LP Tokens is known as yield farming. When you provide liquidity for the USDC/XPR liquidity pool for example, you will farm a yield in XPR.

LP tokens can be un-staked at any time, allowing you to regain those original tokens back in your Proton account.

6.4 Proton Resources

Proton Blockchain offers varying resource plans for businesses/developers, thus creating demand, that can allocate increased transaction per second, storage space, and more depending on the plan used. An overview of the resources and plans available can be found here.

6.5 NFT minting

NFT minting uses XPR in the Proton ecosystem. Although XUSDC is used for all transactions on Proton Market, that XUSDC is being automatically converted into XPR in the background for use in our ecosystem. This XPR is used to mint all NFTs on Proton Market. NFT minting through Proton Market is described in greater detail later in this document.



7. Proton Ecosystem

Users of Proton Blockchain will not necessarily interact with all of the different components separately, as the goal is to blend their usage seamlessly into one user experience. However, all parts of the Proton ecosystem can be used on their own; for developers, this allows the ability to have the flexibility and modularity of Proton in terms of what they need to fit their product.

7.1 Proton Blockchain

Proton Blockchain is the decentralized ledger to which all transactions and account data is stored. It is permissionless and decentralized. Anyone can access it from anywhere, anytime, in the world without any credentials required to create an account, submit a transaction or deploy a smart contract.

7.2 WebAuth.com (Proton Wallet and DeID Authentication Platform)

WebAuth.com is designed to be the next generation of the Proton wallet, offering all of the features of a traditional wallet, while integrating the latest standards in Web Authentication (WebAuthn)



WebAuth.com is a new industry standard for device authentication, turning essentially any device into a hardware wallet, with decentralized identity management, payment processing, and cryptocurrency transactions for Web 3.0, built to support the Proton Blockchain. With WebAuth.com, users can approve transactions, make crypto payments, link their decentralized identity, verify/add/remove access for all logins, and reject impersonation attempts through the use of a smartphone – similar to how Google Authenticator and other popular 2FA platforms operate without the weakness of one-time passwords.

WebAuth.com app functionalities:

- Multi-account support. Simply log in with your key or seed phrase, no email or password is required.
- Buy, sell, swap, send, and receive cryptocurrency. With a built-in exchanges tab, it's also easier than ever to send crypto to exchanges that support the available mainnet cryptocurrencies.
- Stake cryptocurrency. Staking Proton (XPR) takes just a few clicks, with the APR shown clearly.
- Multi-network support. Some of the most popular blockchains in existence are supported on the WebAuth app, including Proton, ERC20, BEP20, and Stellar.
- NFT Viewer. View your NFTs simply and quickly flip from coin and token assets.

In a world where passwords can be stolen, and devices can be lost, your accounts should be secured with no less than your own biometric information – something that can never be lost or stolen.



7.3 Proton Swap

Proton Swap is a decentralized Automated Market Maker (AMM) exchange that allows users to instantly swap Proton-based tokens. Users can convert Ethereum-based (ERC20) tokens to Proton-based (xTokens and Proton assets) tokens and vice versa. For example, using Proton Swap, a user can swap XBTC for XUSDT, or convert ETH to XETH before trading it for XPR.

This allows seamless transactions between blockchains due to the speed and flexibility of the Proton Blockchain. The more liquidity that exists between the pair of tokens being swapped, the lower the slippage will be.

7.4 Proton NFT Market

Powered by the Proton blockchain, Proton Market allows NFTs to be bought and sold for fees as low as just a few cents – a radical change from the gas fees ranging from \$50 to \$200 paid on competing NFT marketplaces. Additionally, because the Proton blockchain is one of the fastest in the world, the NFTs you purchase arrive in your account instantaneously.

As a brief refresher, NFTs – or non-fungible tokens – are a type of blockchain technology that allows authenticity and ownership to be proven for digital assets. NFTs can be used for things like digital art, collectible merchandise, event tickets, and even identifying documents. While the idea for NFTs has existed for a few years, they have only exploded into the mainstream consciousness in recent months.



Currently, all NFT prices on Proton Market are listed in Proton-wrapped USDC (XUSDC), meaning price calculations are simple and straightforward in US dollars. With Proton Market being open source, you can fork it and get up and running quickly. This avoids sending your visitors to another platform to purchase your NFTs, eliminating the potential for losing visitors and lowering the barriers. Have merchandise you'd like to sell? Want to offer exclusive images, videos, or audio files to your fans? Sell them an NFT of your creations and ensure they feel more connected to you than ever before.

Visit our [GitHub](#) to get all of the information you need to integrate Proton Market on your own website.

7.5 Yield Farming

As DeFi matures, new ways to put your money to work become available. Although liquidity pools have been quite popular in recent years, the high gas fees associated with adding funds to liquidity pools have been discouraging. On Proton, with zero gas fees and instant transactions, there are fewer barriers to becoming a liquidity provider.

In addition to providing liquidity on protonswap.com/pools and earning a portion of the transaction fees, **yield farming** is now available for the USDC/XPR and the LOAN/XPR liquidity pools on protonswap.com/farms. Liquidity Pool (LP) Tokens, earned by providing liquidity to the USDC/XPR or LOAN/XPR liquidity pools, can be staked on protonswap.com/farms for a **variable APY**. They can also be unstaked at any time.

By leveraging the speed, flexibility, and low-cost of the Proton Blockchain, participating in the growing DeFi yield farming movement is now easier for cryptocurrency users of all backgrounds. Additionally, with more incentivized liquidity pools expected to come online in the coming months, the potential use cases for XPR will continue to increase as well.



7.6 Proton Loan

Proton Loan is a new decentralized lending market built on the Proton blockchain. Utilizing the cross-chain capabilities of Proton wrapped xTokens, Proton Loan opens up a new possibility for borrowing and lending against multiple blockchains that were not previously accessible on Ethereum or other blockchain protocols.

As always, because this is built on the Proton blockchain, **there are no gas fees for Proton Loan.**

By using a system of smart contracts powered by the Proton blockchain, users can request and fulfill loans using cryptocurrency without the need for a central mediator and without regard for the parent blockchain protocol of the requested asset.

Proton Loan is a non-custodial decentralized lending protocol consisting of two parties:

- **Depositors** who lend tokens to a market
- **Borrowers** who borrow the lent tokens from a market and pay interest to the depositors in return

As one does not know the parties who engage as borrowers, it is impossible to accurately assess a borrower's default risk. This risk is accounted for by requiring all loans to be **over-collateralized**. To learn more about collateral, visit the [Documentation](#) for Proton Loan.



Proton Loan features variable interest rates that react based upon utilization ratio. The Proton Loan protocol was designed to adjust to supply and demand, meaning that the interest rates will increase as more liquidity is borrowed, and decrease as more liquidity becomes available. In this way, Proton Loan's responsive interest rates empowers borrowers and lenders to seek out the interest rates that best suit their investment strategies and risk tolerances.

The native token of the Proton Loan ecosystem is LOAN, which is used to reward both borrowers and lenders for using the platform, and govern the platform. Read more on Proton Loan governance here. <https://docs.protonloan.com/fundamentals/governance>

7.7 Proton DAO Dashboard

Proton Blockchain has a forthcoming unique Governance DAO Dashboard template which any decentralized autonomous organization can fork and openly use to manage their DAO on Proton. This open source dashboard can be used for its members to make and vote on proposals which can then be implemented within the DAO. This can be combined with decentralized identity to avoid negative plutocratic elements that can weigh down some other existing token-only based voting systems.

7.8 Proton DEX

Proton Blockchain has a forthcoming decentralized exchange (DEX) that allows for spot limit and market orders, with plans to expand trading functionality with more advanced options into the future.



8. History

8.1 Origins of Proton

Proton Blockchain was developed by Metallicus as part of a vision of making cryptocurrency more accessible to everyday consumers. Through Proton, we have built a compliant, consumer friendly platform for peer to peer payments, and developed an app-focused blockchain that is developer-friendly.

8.2 Roadmap and Milestones

Our roadmap and achieved milestones are continuously updated on our roadmap page: <https://www.proton.org/roadmap>. The public-facing roadmap that can be viewed on our website is non-exhaustive, but provides a helpful overview of our vision for the immediate future of the Proton Blockchain and ecosystem. Notable upcoming milestones include Fiat Transaction Integrations, which we expect will expand the ability for more people to interact with the Proton Blockchain.

8.3 Commitment to security

Throughout the development of the Proton Blockchain, we have sought input from external security experts to ensure that the safety of Proton is robust and above the industry norm. Proton has completed a voluntary external security assessment by Kudelski Security, a company that had previously done work for customers like Crypto.com and Binance.

Additionally, we had the Proton Swap and Yield Farming systems audited by PeckShield, an industry-leading blockchain security company. We also had the Proton LOAN staking system audited by Blockmancer, and we intend to continue to have various parts of the Proton ecosystem audited by external security experts in order to better secure our users and their funds.

Our commitment to the security of the Proton Blockchain is ongoing and ever-increasing. We recognize that a blockchain ecosystem is only as good as its safety, which is why we are constantly searching for new ways to improve the soundness of Proton.



8. More information and resources

Proton Website: <https://www.proton.org>

Proton Blog: <https://blog.protonchain.com>

Proton Governance: <https://www.proton.org/governance>

Proton Whitepaper: <https://www.proton.org/proton-white-paper-en.pdf>

Proton Wallet: <https://www.proton.org/wallet>

Proton Github: <https://github.com/ProtonProtocol/>

Token Trackers & Block Explorers

Coinmarketcap: <https://coinmarketcap.com/currencies/proton/>

Coingecko: <https://www.coingecko.com/en/coins/proton>

Block explorer (Proton Mainnet): <https://protonscan.io/>

Block Explorer (ERC-20): <https://etherscan.io/token/0xd7efb00d12c2c13131fd319336fdf952525da2af>

Social Media

Twitter: <https://twitter.com/protonxpr/>

Facebook: <https://www.facebook.com/protonxpr/>

Instagram: <https://www.instagram.com/protonxpr/>

Reddit: <https://www.reddit.com/r/ProtonChain/>

Telegram: <https://t.me/protonxpr/>

Telegram announcement channel: <https://t.me/xprannouncements>

