Loom Network

Lightpaper

Building an **ecosystem of blockchains** to sustain the next generation of **DeFi** protocols, **NFT**s, and high-performance multi-chain dapps.

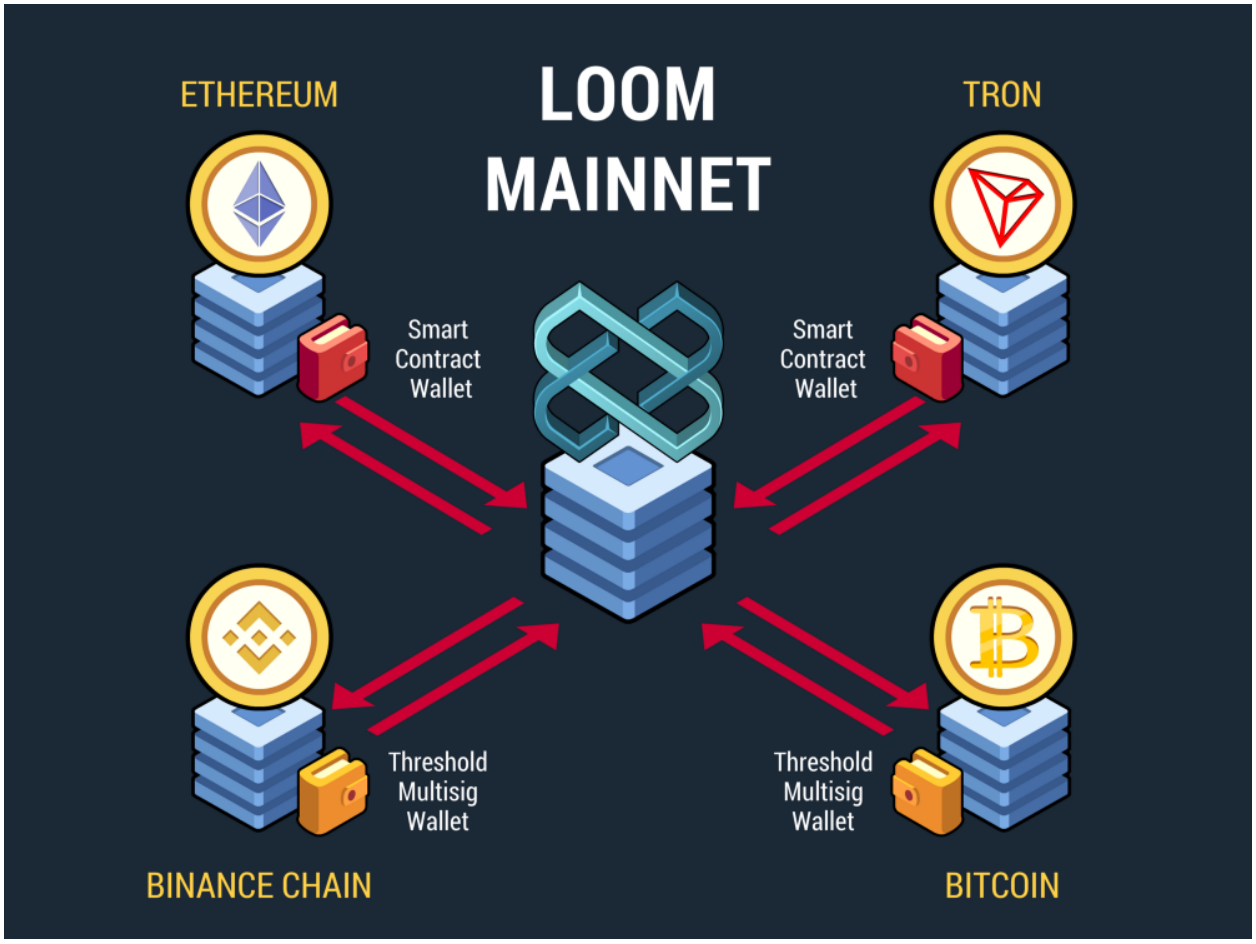
---

https://loomx.io

Table of Contents

Introduction

For the foreseeable future no one blockchain will be able to scale to run every conceivable dapp, and today all practical scaling solutions rely on offloading compute and storage to other more specialized chains. This was true three years ago when we launched our **Basechain** network, and it's still true today. **Ethereum** might still be the undisputed king of smart contract capable blockchain networks, but the high transaction fees are forcing developers to look at newer smart contract capable networks like **Binance Smart Chain** and **L2 scaling solutions** based on **zkRollup** and **Optimistic Rollup**.



Loom Network's mainnet Basechain is a central piece in an ecosystem of blockchains, with the LOOM token acting as a medium of exchange between all members of the ecosystem. Ethereum's growing pains present a unique opportunity for Loom Network to expand its reach, as developers look for more affordable and accessible networks for their dapps.

Key Advantages

Production Ready

There's no need to wait for some distant scaling solution. Loom Network's **Basechain is live in production** — so developers can launch new dapps and start on-boarding users immediately.

Frictionless UX

Loom blockchains process **transactions at lightning speeds and at low cost**, making it much cheaper to deploy dapps, and much easier to quickly on-board users.

Fast & Scalable

Loom Network's Basechain runs on **Delegated Proof of Stake (DPoS)** and is optimized for the fast confirmation times and **high-transaction throughput** necessary for real-world dapps.

Top-Notch Security

Basechain is a DPoS blockchain with validators located all around the world. The chain has also been **audited by Trail of Bits** — a renowned information security company specializing in blockchain audits.

Future Proof

Loom Network is **continually building integrations** with the most populous networks to ensure developers can build dapps that reach the widest audience, instead of being siloed within a single network.

Technology

From its inception Loom Network aimed to provide a **scaling solution** for Ethereum dapp developers. Three years ago the most practical way to do so was to build an Ethereum sidechain secured by multiple distributed validators. To date, blockchains built using the Loom protocol have proved to be **performant and secure**, but the reliance on a consensus of validators to secure the chain has resulted in a lot of wasted CPU cycles, storage, and bandwidth. This wastage is an unavoidable artifact of distributed consensus because every validator has to run their own machines that all perform exactly the same computations when processing transactions.

Thanks to the extensive research work that's been done into scaling Ethereum in recent years, we believe it's time for a radical shift in our blockchain tech, rather than just incremental improvements. Our engineering team has been keeping an eye on **practical applications of zero knowledge proofs**, and the development of **zkRollup** based projects like **zkSync** by **Matter Labs**, and **LoopRing**. We believe that a new Loom protocol based on zkRollup is the best way to reduce the environmental impact of our blockchains, while at the same time improving both the performance and security of the Loom protocol.

zkLoom Protocol

In the zkRollup based Loom protocol (which we'll refer to as zkLoom from here on out) the validators accept transactions from clients, process those transactions, and then generate zero knowledge proofs (**zkSNARK**s) that are verified by a smart contract on Ethereum every time a new block is created on the Loom blockchain.

The zkLoom protocol architecture offers a number of advantages:

- **Forging** a zero knowledge proof is **practically impossible** so the smart contract on Ethereum effectively guarantees that every transaction in a block committed by the zkLoom protocol has been processed correctly. If a hostile validator attempts to commit a block with an invalid proof the smart contract on Ethereum will reject that block, so a malicious validator can't steal funds or cause an invalid state transition.
- **Funds** transferred by users from Ethereum to a zkLoom blockchain **can be recovered** even if all zkLoom validators go offline, or simply refuse to process transactions. This is made possible by safeguards built into the smart contract on Ethereum.
- Users no longer have to place their trust in validators, instead they can rely on the security guarantees provided by Ethereum. By **leveraging Ethereum for security** zkLoom blockchains can operate in a secure manner with only a few validators, which makes it much **easier to bootstrap** new blockchains, and to operate them at a **lower cost**.

The security of zkRollup protocols is ensured by cryptography rather than game theory, and today these protocols provide the most promising scaling solutions for Ethereum smart contract developers. A lot of investment is currently going into extending the practical applications of zkRollup, and we're keeping an eye out for any major breakthroughs by other startups in this field to ensure that the zkLoom protocol doesn't lag behind.

Loom SDK 3.0

The Loom SDK is over three years old now, and continues to be one of the most cutting edge, multi chain scaling solutions. The next major public release will include some very exciting features:

- zkRollup architecture and tooling
- Optimistic Rollup with liquidity providers
- Cross Chain Oracles, similar to Band Protocol and Chainlink
- Binance Smart Chain support

Our SDK allows developers to quickly spin up new Loom chains specialized for their applications. Since it's not really practical for each developer to maintain their own interconnections to other major blockchains Basechain will act as a single interconnection point for application specific Loom chains — enabling asset transfers to other major blockchains for a small fee.

LOOM Token

Utility

The LOOM token is used for staking, transaction fees, and bonding.

Staking

LOOM is a Proof-of-Stake token that is used to secure Loom Network's mainnet Basechain. Validators and delegators who stake their LOOM tokens collectively uphold the security of the network.

Validators earn LOOM as block rewards for performing various duties on the network (similar to the role of ETH on Ethereum), while individual LOOM holders can earn a portion of these rewards by delegating their tokens to validators.

Transaction Fees

Transaction fees serve two important purposes. They ensure that validators that run Basechain nodes can be fairly compensated for the running costs of their servers, and they help prevent spam transactions.

Bonding

Developers can spin up their own blockchains using the Loom SDK, and connect them to Basechain to take advantage of its interconnections with Ethereum, TRON, and Binance Smart Chain. To dissuade malicious behavior these standalone chains will have to bond LOOM tokens on Basechain before they can use its transfer gateways.

Multi Chain

The LOOM token is currently deployed on both Ethereum Mainnet as an ERC20 token, and on Binance Smart Chain as a BEP20 token. It can be easily transferred between Binance Smart Chain and Ethereum through the Binance Bridge. With the upcoming Binance Smart Chain integration Basechain will also allow users to deposit and withdraw LOOM on Binance Smart Chain.

The ERC20 and BEP20 versions of the token have largely the same utility. However, the BEP20 version has some distinct advantages. Since Binance Smart Chain transaction fees are much lower than Ethereum it's much cheaper to stake LOOM on Basechain from Binance Smart Chain. The BEP20 token can also be easily integrated into DeFi protocols deployed on Binance Smart Chain, like Pancake Swap, further improving liquidity.

Token Swap

The process of upgrading our Basechain network to the zkLoom protocol will require a number of steps. The old LOOM ERC20 token contract is not upgradable, so we are unable to implement the features necessary for the token to operate with the new zkRollup based architecture. Therefore we deployed a new LOOM ERC20 token contract to Ethereum mainnet on February 1st 2021, and we're now performing a token swap from the old LOOM ERC20 token to the new one.

The total supply of the new LOOM ERC20 token is still 1 billion, just like the old LOOM ERC20 token, and tokens are swapped at a 1:1 exchange rate.

The old LOOM ERC20 token can no longer be used for staking on Basechain, only the new LOOM ERC20 token can be staked.