Muon Network

Litepaper

last updated 10/07/2021

Decentralized cloud computing, cross-chain bridge interfacing and secure oracles for **gaming**, **DeFi** and **dApps**.

Muon Litepaper

Executive Summary

Muon is a decentralized Nodes as a service Network that enables running Web2 and Web3 applications, off-chain, on-chain, and cross-chain. The network acts as a base layer that bridges the division between blockchains, creating a fluid DeFi ecosystem. The Muon layer exists between blockchains, connecting different protocols and allowing them to talk to each other, ensuring blockchain interoperability.

Blockchains are great for storing valuable data securely, but connecting this data to other chains or sources is difficult. This is where Muon comes in: its elementary node layer allows external smart contracts to securely perform complex computations at zero gas cost through off-chain computation.

Muon will give partnering blockchain projects high-speed performance, by means of our "data-on-demand" principle, needed to become industry leaders in their respective fields. Using truly decentralized oracles and cross-chain bridges has never been as easy and secure.

Key features

Secure Subsequential Consensus

Muon's core consensus layer is a unique and completely new type of system which we've named Secure Subsequential Consensus. Through adaptive collateralization, the protocol can ensure fast execution times while simultaneously ensuring that node consensus **can** be reached.

Seamless scalability

The Muon network is not a chain, nor does it permanently store data, therefore, the network can scale horizontally with ease without any limits.

Decentralized Computation

With Muon, any Web3 app can run high-level, tamper-proof computations (Python, Java, C, C++, Rust, etc.) within its own Muon app container. Nodes running the same Application can gossip and even work together, forming a decentralized super-computer.

Customizable and cost-efficient

Nodes are not required to run all apps and are able to opt-in or -out of the program they'd like to run on their machine.

- Specialized nodes: nodes running a very specific app
- General nodes: nodes running (almost) all apps

Web3 developers can now shift between the trade-offs this configuration yields: security vs. speed.

Use-cases

Oracles and data feeds

Oracles provide reliable, trustworthy, immutable, and traceable data. When multiple sources, such as Muon nodes, verify an oracle's information to be true, a 'consensus' is formed on accurate data.

One of the first oracles built on Muon is a stock price oracle called Pythia. It provides prices to DEUS Finance for 50,000+ stocks near instantaneously. It does this by leveraging Muon's node-based infrastructure, and combines it with a unique collateral structure, thus providing integrity and speed.

Bridges

Muon creates bridges between all blockchains. Any type of data can be bridged cross-chain with Muon. Currently, two types of bridges are designed and being implemented: Permissionless Bridges and DEUS Bridges.

Permissionless Bridges

Muon permissionless bridges follow the same logical steps as any other bridge, e.g. what steps need to be undertaken to successfully bridge data & assets. Muon's core difference is the way signatures are being handled and how consensus is reached:

- The user transfers tokens to a designated contract on Chain A.
- Muon contract locks those tokens on Chain A via a transaction. To prevent errors, the tokens are marked with a unique ID. Locked tokens back up the permissionless transaction and as such, tokens remain on the original chain and nothing can ever be lost.
- The user informs Muon nodes about the transaction sent on Chain A.
- All Muon nodes sign confirmations of the transaction.
- The Client fetches said signatures and puts them into a smart contract.
- Smart contracts check Muon signatures on Chain B.
- If the signatures are valid, the user can now claim his tokens with another transaction on chain B.

A key element of permissionless bridges is that users need to create the tools, such as liquidity pools and exchanges, on the new chain themselves, as opposed to the DEUS bridges below which include the liquidity pools by default. The admins simply create/fill the liquidity pools, the actual bridging is permissionless.

DEUS bridges

- Tokens on chain B are deployed by admins.
- Admins control the list of tokens, while the rest of the functions are permissionless.
- DEUS bridge is also a Muon permissionless bridge but it has all the liquidity pools and exchanges on the other side by default.
- An implementation of the DEUS bridge can be found on the DEUS Github.

Merged dApps

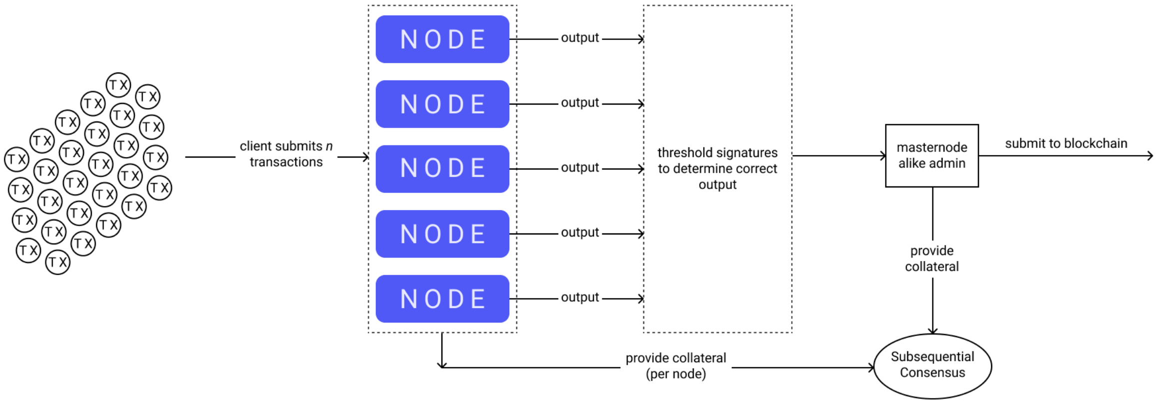
The Muon network facilitates the exchange of data across all dApps regardless of their programming language or any chain they transact on.

Artificial Intelligence

Muon nodes support running high-level apps in a decentralized manner and pushing their final data onto blockchains. For instance, AI can assist YEARN finance to determine the best yield opportunities or to create liquidity-providing strategies for Uniswap V3 alike market makers.

Merged Transactions

Similar to Bitcoin's lightning network or other roll-up technologies, Muon is able to merge small transactions and push data to blockchains periodically or upon request. This enables low-cost, fast exchange and payment solutions that are decentralized and secure.



Muon Technology

Node network

Muon nodes can have one or several roles. These roles include:

- signing and pushing data to the blockchain
- Observing data and placing disputes

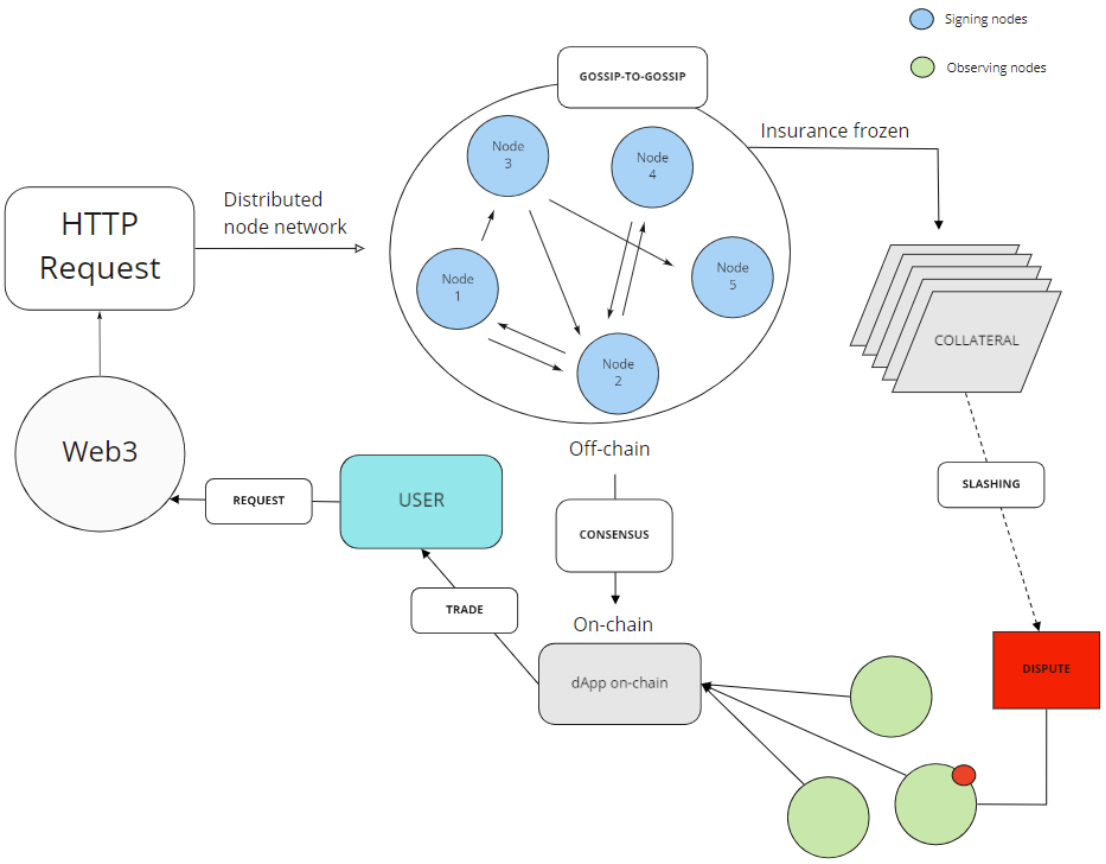
Muon nodes use gossip-to-gossip as the communication method on a protocol level. A user's request initiates the process in the first node, whereby it prepares the data, signs it, and propagates it to the other nodes. The data is processed by a number of nodes (configured by the application) and these nodes are chosen on a cryptographically secure random basis.

Every dApp can customize its class depending on its requirements. **Customization is applicable in the following ways:**

The number of required subsequent signatures from nodes in order to execute transactions

- The number of required non-disputed verifications
- The amount of collateral insurance required to execute transactions
- The request input/output and its computation
- The allowance of custom programs and scripts
- The deployed consensus algorithm
- Implemented shards

Once an HTTP request is received, the Muon network will internally verify the data that the oracle has signed and it will freeze the node's locked collateral in case of any disputes. If consensus on the data is reached then the stake of the node is unlocked and can be used to support incoming requests. The stake is only partially locked relative to the quantity of the required collateral.



Running a Node

Users can play an active role in the Muon node network by operating their own nodes. They are incentivized to do so through a rewards system. Nodes provide collateral as insurance for the data that they are signing as well as provide the infrastructure that makes it possible for heavy computational work to be processed on the Muon network. The computation is done off-chain, on the nodes themselves, with the data then pushed on-chain.

Because Muon is highly configurable and dApps can specify a wide array of requirements, there is no specific hardware needed to operate a Muon node. In order for a node to qualify in taking on requests from *all* dApps on the Muon network, it needs to provide a robust hardware solution with enough computational power to meet the most demanding needs.

Subsequential Consensus

The secret to Muon's impressive characteristics (speed, modularity, trustlessness) is due to the way consensus is reached, and how it's assessed on a transactional basis.

With Muon, any type of computation can be performed on a set of data and subsequently transmitted to a target chain destination. The key understanding of layers built on top of blockchains is the way they reliably transmit said data, and this is where Muon stands out. The common way to pass oracle data to a chain would be as follows:

1. The node performs or relays computational tasks.
2. The result is complemented with signature and submitted to node cluster
3. The Node cluster verifies the validity of all the provided signatures (and data fields) If valid: pass data to blockchain/contract. If invalid: punish/slash node (broadly speaking), and retry.

In our solution, the verification process (as described in step 3) is executed *after* the transaction has been submitted to the blockchain. By this logic, Muon nodes (or clusters) are vastly more efficient in interacting with blockchains than traditional methods. The mechanics to protect this logic from faulty actors are described below.

Collateral

Nodes are required to provide collateral as insurance for the data that they are signing off. When a node provides its signature for data that it is verifying, its collateral is locked into a dedicated Muon smart contract for a brief amount of time until all other nodes agree on the data. If there are no disputes then the collateral is released back to the node. This is something we named Subsequential Consensus - the collateral is locked upfront with the consensus coming later.

How much is the collateral worth?

The collateral can never be less than the transactional value of the payload, as it acts as insurance against attacks. Nodes are not required to match the collateral at all times, they can easily opt-out if they can't afford it but they will also miss out on rewards. In the event of a high transactional value where the minimum required number of signatures (nodes) can't afford the collateral, the transaction is rejected.

It is recommended to perform such checks client-side, in order to not waste gas on reverted transactions. Depending on the payload, one method to bypass rejection is to batch and submit the transaction into smaller affordable chunks.

***Disclaimer**: The ownership of Muon tokens does not represent any participation in Muon Labs AG capital nor any rights of payment, remuneration, profit distribution or money reward of any kind. This Litepaper has been prepared in good faith to provide a comprehensive overview of the Muon project and Muon token crowdsale and is for information purposes only.*

With the development of Muon platform and/or any Muon mobile applications, it may be amended in the following. Please also note that the Muon Project itself may be redesigned or otherwise revised in future, if that would be required for any material reasons (including, but not limited to: commercial considerations, technical possibilities, or the need to ensure compliance with any (existing or future) applicable laws and regulations, or any other material reasons). Muon tokens are not intended to constitute securities in any jurisdiction.

This Muon Litepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investments in securities in any jurisdiction. The contents of this document are not a financial promotion. Therefore, none of the contents of Muon Litepaper serves as an invitation or inducement to engage in any sort of investment activity.

U.S. Persons, as defined in Regulation S under the U.S. Securities Act of 1933, as amended (the "U.S. Securities Act"), are prohibited from accessing this Litepaper and Muon website. Nothing in this Litepaper or Muon website shall be deemed to constitute an offer, offer to sell, or the solicitation of an offer to buy, any securities in any U.S. jurisdiction. Each person accessing this Litepaper or Muon website will be deemed to have understood and agreed that: (1) he is not a U.S. citizen and he is located outside of the U.S.; (2) any securities described herein have not been and will not be registered under the U.S. Securities Act or with any securities regulatory authority of any state or other jurisdiction of the United States, and may not be offered, sold or delivered within the United States or to, or for the account or benefit of, U.S. persons except pursuant to an exemption from, or in a transaction not subject to, the registration requirements of the U.S. Securities Act and applicable state securities laws.

Do not contribute any money that you can't afford to lose in the Muon Token Sale. Make sure you read and understand this Litepaper and TERMS AND CONDITIONS FOR PARTICIPATING IN THE Muon TOKEN SALE (including all warnings regarding possible token value, technical, regulatory and any other risks; as well as all disclaimers contained therein), as will be published on our website https://www.muon.net/ (as they may be amended from time to time).

Should you have any questions regarding the Muon project, Muon token, the contents of this Litepaper or the sale of Muon tokens, please, do not hesitate to contact contact@muon.net or https://t.me/muon_net