

OAT CHAIN

Whitepaper

V1.0 Feb 2024

Abstract

This whitepaper proposes a full overview of the OAT network and gives an overview of its capabilities as a Layer 2 solution for the Bittensor network. It will give an overview of Bittensor and explain how OAT Network can support their ecosystem.

Introduction

Bittensor has been established as a groundbreaking solution for decentralized computing, bringing together the idea of trustlessness between various independent actors to solve challenges in the booming Al industry.

The Bittensor ecosystem uses an incentive-based mechanism where each incentivebased competition market is a subnet on the network. These subnets are fundamental to the functioning network.

The subnets are run on a blockchain, to ensure decentralization and permission-less for all actors involved. All essential elements are connected with a Bittensor API, which also connected the subnets with the blockchain.

Bittensor uses the TAO token as an incentivization mechanism for individual actors. TAO tokens can be earned by miners by performing useful tasks, eg by solving computational problems which in turn secure the network.

Subnet validators independently evaluate these computational tasks by the subnet miners. The opinion of these validators regarding the state of security of the network, based on the mining mechanism, is then expressed as a collective input to the Yuma Consensus mechanism on the blockchain. The output of the Yuma Consensus will then determine the allocation of rewards of the validators and miners. Allocation of TAO tokens are used as an incentivization mechanism for these individual actors.

Participation in the Bittensor ecosystem occurs primarily on subnets, as either subnet owner, validator or miner.

Bittensor Challenges

With the AI industry projected to create trillions of dollars in the next years in value, demand for AI, data and computing will soar rapidly.

Bittensor thus faces the issue of scalability, having to prepare their network for an influx of thousands of data engineers and scientists.

For this environment Bittensor requires low latency and low transaction costs. Given the sensitivity of data, which may include medical or insurance data, enhanced privacy options are paramount.

As well, an easy onboarding of new users is essential. These users may not want to deal with the hassle of complicated tokenomics and low speed and prefer a system which offers a great user experience from day one.

Solutions brought by OAT Network

To alleviate these challenges and issues Bittensor faces, we propose an EVMcompatible based Layer 2 on Bittensor. This allows users high transaction speed and onboarding,

OAT Network uses a simple design philosophy where interfaces for every actor are created, which provide data off- and on-chain. No sensitive information is shared.

Nodes can collaborate to train machine learning models and transfer learned knowledge or pre-trained models to improve performance on related tasks.

Bittensor is the heart of the system, with OAT interacting with Cross-Chain messages on the Layer 2, with Bittensor being the verifier of OAT, while OAT remains the layer on which applications are being built and run on.

Key Features of OAT Network

OAT Network will be the ideal place for engineers to provide storage for their data training in AI. OAT creates interfaces for everyone to run nodes, profiting data off- and on-chain without sharing sensitive information.

Resources for computing are shared between nodes, so they can collaborate to train machine learning models or transfer learned knowledge or pre-trained models to improve performance on related tasks.

Smart contract Audit: Data which is shared on-chain from OAT nodes and other EVM blockchains can be verified and audited, in order to find weak spots which may be abused or attacked.

However, OAT always remains within the Bittensor ecosystem and its Cross-Chain capabilities mean that OAT constantly interacts with Bittensor. Every task within the OAT network is verified internally by Bittensor validators.

Thus OAT is a flexible solution for developers within the Bittensor ecosystem.

Technical background

Cryptographic Hash Functions

In the realm of blockchain technology, cryptographic functions serve as vital tools ensuring the integrity and immutability of transactions. A hash function, a fundamental mathematical algorithm, generates a fixed-size numerical output, often referred to as a fingerprint or digest, based on input data. Formally, a hash function can be represented as: A hash function takes on the input of any size and produces a fixed k length output. In addition, it must satisfy the following properties:

• It is easy to compute H regardless of input data size.

• Given any h, it is computationally infeasible to find an input x such that H(x) = h.

• Given any x, it is also computationally infeasible to find y such that H(y) = H(x) and $x \neq y$.

• It is computationally infeasible to find any (x, y) such that H(x) = H(y) and $x \neq y$.

SHA-256 and Keccak-256 are widely used in several blockchains, and they produce a hash (output) of 256 bits in size.

Digital Signatures

Secp256k1 Curve

Note that all elliptic curves are equations defined as $y^2 = x^3 + ax + b$. The code Secp256k1 is an elliptic curve used by several blockchains to implement public and private key pairs. For instance, we can define Secp256k1 as a = 0 and b = 7 (i.e., secp256k1 lives on the equation $y^2 = x^3 + 7$).

Before a user generates a public and private key pair (pk, sk), he/she must first generate a sufficiently large random number (which is going to be sk) and use it to multiply with the private key by the generator point G as sk.G (which is going to be the pk).

We use this number to define a point on the secp256k1 curve. Due to the underlying discrete log problem (DLP), no one can derive the private key from the given public key and the generator point (as long as the key size is sufficiently large).

Note that for each value of x, the y component is squared in this equation leading to having two symmetric points across the x-axis. Hence, there are two values of y called odd and even numbers. Therefore, public keys can be identified by the x-coordinate and the parity of the y-coordinate. In the blockchain space, this feature is crucial, as it saves significant data storage.

ECDSA Signature Algorithm

Elliptic Curve Digital Signature Algorithm (ECDSA) is a cryptographic algorithm for creating digital signatures. More concretely,

<u>Setup</u>

• <u>Public Parameters</u>: Let F_q be a finite field, two parameters and define an elliptic a and b curve C over F_q , a seed which validates C, a prime integer $n > 2^{255}$, and a point $G \in C$ of order n where q is either prime or a power of 2.

- <u>Private Key:</u> An integer d in [1, n 1].
- Public Key: Q = dG.

Signature generation for a given message M:

- Generate $k \in [1, n 1]$
- Compute

$$(x_1, y_1) = kG$$

$$r = x_1 modn$$

$$s = \frac{H(M) + dr}{k} modn$$

- If r = 0 or s = 0, try again. The signature is (r, s).
- Signature: (M, r, s).

Verification:

- Given (*M*, *r*', *s*').
- Verify if r' and s' are in [1, n 1] and that $r' = x_1 modn$ for

$$(x_1, y_1) = u_1 G + u_2 Q, u_1 = \frac{H(M)}{s'} modn, \text{ and } u_2 = \frac{r'}{s'} modn \cdot s').$$

Ethereum Virtual Machine (EVM)

A virtual machine is a layer of abstraction between the executable code and the executing machine. This layer is necessary to improve the portability of software and to ensure that applications are separated from each other and from their hosts.

The Ethereum Virtual Machine (EVM) is a software platform that developers can use to build decentralized applications (dApps) on Ethereum. All Ethereum accounts and smart contracts live in this virtual machine.

The Ethereum virtual machine and EVM codes are designed using memory, bytes, along with blockchain concepts such as Proof-of-Work (PoW) or Proof-of-Stake (PoS), Merkle tree, and hash functions. The purpose of the EVM is to determine what the total Ethereum state will be for each block in the blockchain.



OAT Network architecture



Data layer

Transactions

Normal transaction: Similar to every transaction in EVM: sending the token and interacting with the smart contract. It will be executed and confirmed by the validator node.

Cross-chain message: The transaction sends proof of the task to the Bittensor. It will be processed by the validator and sent to the sequencer, then submitted to TAO and await the result.

Components

Sequencer: Responsible for ordering and processing transactions within the OAT network. The sequencer plays a critical role in the OAT network's scalability solution by efficiently processing and ordering transactions off-chain before committing them to the TAO main net, enabling significant improvements in throughput and cost-effectiveness compared to executing transactions directly on the Ethereum main net.

OAT network: The OAT network consists of several types of nodes: storage nodes, computing nodes, and validator nodes. They operate independently like separate blockchains. It uses the dPoS consensus mechanism with the native token being TAO, bridged from the Bittensor network through LayerZero.

Validator node: Validates transactions within the network, distributes rewards to storage nodes and computing nodes, and sends cross-chain messages and tasks to the sequencer for submission to the Bittensor network.

Computing node: Provides resources to perform tasks related to machine learning and AI. Before providing resources, the computing node must register with the OAT network through the Task Contract.

Storage Node: Connects to off-chain data service providers through the OAT adapter. Additionally, the storage node links to nodes of other blockchains to retrieve on-chain data via the OAT adapter. Similar to computing nodes, storage nodes must register with the OAT network through the Node Contract.

OAT smart contract: The OAT network features several smart contracts for management, including:

• Governance contract (consensus): Manages the governance of the network, including consensus mechanisms.

• Node contract: Manages nodes within the network and distributes rewards to nodes.

• Task contract: Manages tasks and rewards users upon task completion.

Bridge: The OAT network utilizes LayerZero as a bridge from the Bittensor network. TAO is the native token of the OAT network, used to pay fees for transactions within the OAT network.

OAT adapter: The OAT adapter is a protocol that enables storage nodes to access data from other blockchains and provide that data for activities within the OAT network. The OAT adapter is currently undergoing development and refinement.

Possible use cases for OAT Network

Given OAT will be the first EVM-compatible based Layer 2 on Bittensor, a wide range of applications can be built on top to support the Bittensor ecosystem:

- dApps with the assistance of artificial intelligence technology, improve efficiency and capabilities, creating more application scenarios and empowering the entire AI ecosystem, thus advancing progress towards Artificial General Intelligence

- NFTs for encrypting high quality datasets, which upon acquisition can be used by actors to train their own models in Al

- DeFI applications such as borrowing or lending, including a trading market for high quality data sets

- Decentralized social networks, where users can earn rewards for participating. The data of the many interactions could be stored and sold to LLM researchers, which would let users benefit from actually being paid for their own content, while also benefiting the state of AI industry

\$OAT TOKEN

\$OAT serves as the primary governance token for the OAT Network, with a strong focus on community engagement. It offers a wide range of use cases to holders.

Governance & Voting

\$OAT holders will join in the collective construction of the OAT Network, with the right to participate in governance proposals and voting, aiding in building a robust community for the OAT Network.

Staking

\$OAT holders can earn \$TAO through staking system, receiving continuous rewards. The staking system contributes to the more stable development of the OAT Network.

Contributor Rewards

Another important role of \$OAT is for incentive programs, including rewards for liquidity providers, early participants, and ecosystem builders. These incentive programs help promote the continuous growth of the OAT Network ecosystem.

References

• Ameer Rosic: Bittensor: Decentralized Machine Learning in 2023 https://blockgeeks.com/guides/bittensor/ , Nov 2023.

• Bittensor. <u>heeps://bittensor.org</u> 2023.

• Ethereum Virtual Machine. <u>https://ethereum.org/en/developers/docs/evm/</u>.

• Ethereum Wire Protocol.

https://github.com/ethereum/devp2p/blob/master/caps/eth.md, Feb 2019.

• Paxos, Raft, EPaxos: How Has Distributed Consensus Technology Evolved? <u>https://www.alibabacloud.com/blog/paxos-raft-epaxos-how-has-distributed-</u> <u>consensus-te chnology-evolved_597127</u>, Jan 2021.

 An Introduction to Binance Smart Chain (BSC), <u>https://academy.binance.com/en/articles/an-introduction-to-binance-smart-chain-bsc</u>, Sep 2021.

• The Raft Consensus Algorithm, <u>https://raft.github.io/</u>, 2021.

• Paxos consensus for beginners, <u>https://medium.com/distributed-knowledge/paxos-</u> consensus-for-beginners-1b8519d3360f, May 2020.

Ongaro, J. Ousterhout, In search of an understandable consensus algorithm
 Proceedings of the 2014 USENIX Conference; 19–20; Philadelphia, PA, USA, USENIX
 Association, pp. 305-320, June 2014.