# A design and implementation of a deep learning oriented blockchain oracle

Guoqiang Chen ( Software Engineering )

Directed by Xiang Jing

## ABSTRACT

After years of development, blockchain technology has been widely used in many fields. Although the current blockchain smart contract has Turing completeness, it must be calculated based on the data on the ledger, which has much limitations. Therefore, with the help of Oracle concept, blockchain developers propose a blockchain Oracle, which is designed to give blockchain smart contract the ability to obtain off-chain data.

In recent years, deep learning technology has developed rapidly. By combining deep learning technology. By combining with deep learning, blockchain can make the results of deep learning transparent, durable and traceable. However, due to the mismatch of the computing resources, it is difficult to combine blockchain technology with deep learning. The Oracle is an effective way to solve this problem. However, the current blockchain Oracle is a model to "push" the data from off-chain to on-chain. This "push" model is only suitable for smart contracts to passively obtain data from the Oracle. While Contracts cannot actively push the required data and algorithms to the oracle and pull the results.

Aiming at the problem of "push" mode Oracle, this paper designs a "pull" mode blockchain Oracle, that is, the deep learning algorithm is not stored in the oracle in advance, but when the contract nodes have computing needs, the data and algorithm to be calculated are pushed to the Oracle for execution, and the calculation results are pulled back. The main challenges of the pull mode Oracle are how to write deep learning algorithm in the smart contract and how to realize the verifiability of the calculation results. Aiming at these challenges, this paper defines an extension mechanism of how to use deep learning library in contract, and guarantees the verifiability of calculation results through TLS-Notary protocol. Specifically, the main work of this paper includes:

(1) This paper designs a new Oracle mechanism, and designs a deep learning oriented blockchain Oracle through this mechanism. In order to solve the problem of computing resources mismatch, this paper proposes a solution to place the complex computing scene of deep learning in the Oracle machine off-chain. This Oracle has more computing resources than

the nodes on-chain, and it is suitable for complex computing. In view of the lack of deep learning library support for blockchain smart contract language, this paper defines an extension mechanism of how to use deep learning library in the contract, so that the smart contract can easily expand the support for other language libraries and frameworks. To solve the problem of verifiable calculation results, this paper uses TLS-Notary protocol to prove the authenticity of the calculation process, so that the blockchain nodes can check the authenticity of the pull results by checking the evidence.

(2) It is implemented on the blockchain of Beida Shurui. To solve the problem of lack of deep learning library support, this paper defines a way for smart contract to call other languages by taking Python language as an example; for the interaction between smart contract and Oracle, this paper defines a type of interface for smart contract to interact with Oracle based on RPC.

(3) Finally, the experiment and verification are carried out in the scene of Beida Shurui to prove the rationality and feasibility of this design. Combined with the specific experimental environment, the experimental design and example verification of this experiment are shown in final. The experimental results show that this new mechanism is more practical in the scene of alliance chain, and can achieve millisecond level fast response in most deep learning algorithms.

Keywords: blockchain, Oracle, smart contract language, deep learning framework, TLS-Notary protocol