AO-Bridge

Connection between Ethereum and AO

Team

Kevin Lin
Team Leader
Github: tokenlin
lkw040535@gmail.com

oxfu
dev
Twitter: @smallfu666
github: smallfu6

capi
dev
Github: Hzzy2O

Aurora Lu
operation
twitter:@Aurora_Lu_sihan
sihanlu78@gmail.com

Motivation

- Ethereum, the largest ecosystem, as knowns, there are still many shortcomings, especially the computations due to system limitations. And AO currently is the top leader in this decentralized calculations.

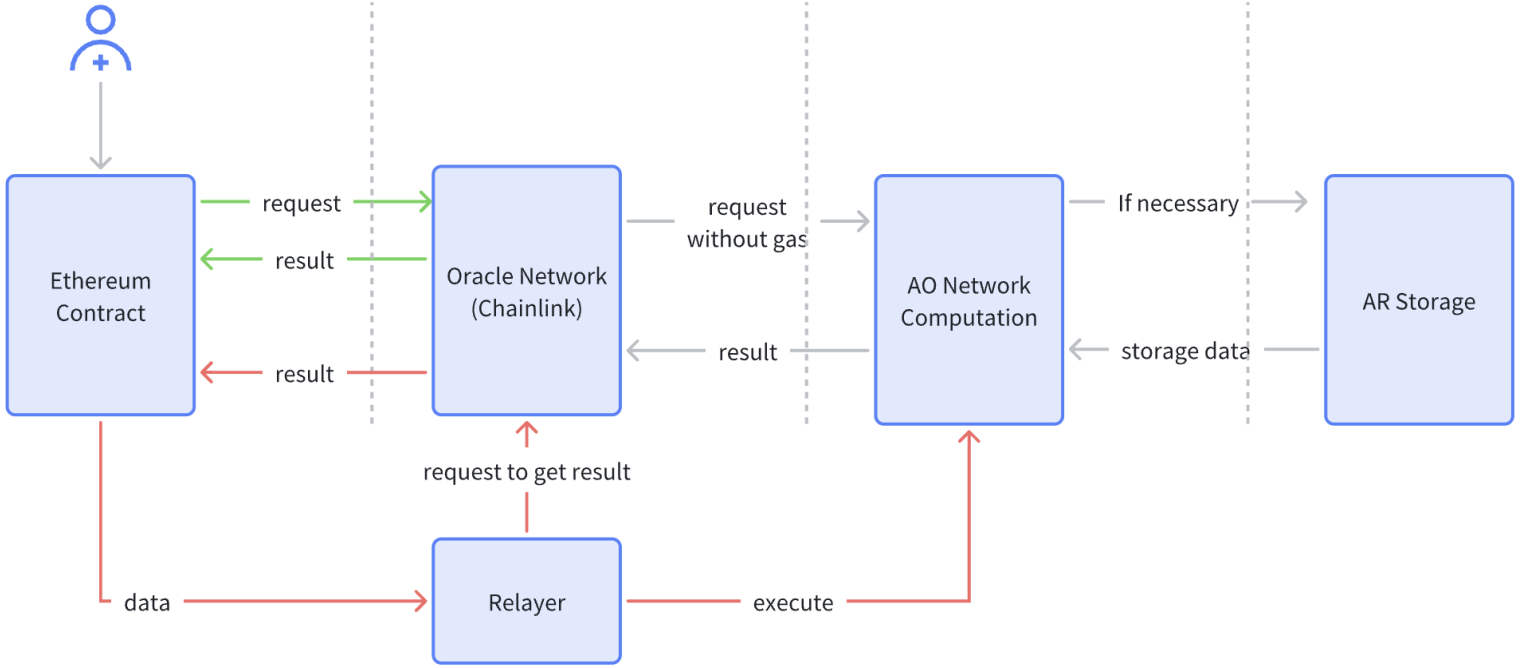
- So, we combine the advantages of both, establish a connection. For the heavy tasks that require a lot of calculations on Ethereum, we complete them on AO, and return the calculation results to Ethereum

- And the connection bridge is our AO-Bridge.

Principles and Feasibility

- Use Chainlink as decentralized Oracle network to connect the Ethereum and AO system for security.
- For the request without gas consumption on AO, user can send data directly from Ethereum to Chainlink, then Chainlink will get data from AO and write back to the Ethereum.
- If the request with gas consumption, firstly, user initiates an on-chain request on Ethereum, and here, a trustless Relayer will get data from Ethereum, and send to AO for calculation including storing the calculation results on AO in advance. Then send the request to Chainlink to obtain and write the results back to the Ethereum.

Flowchart


Ethereum Contract
request
result
result
Oracle Network (Chainlink)
request without gas
result
AO Network Computation
If necessary
storage data
AR Storage
request to get result
data
Relayer
execute

Another Infrastructure

- Another infrastructure is that AO needs to have functions related to Ethereum, especially the elliptic curve calculations.
  So that it can seamlessly undertake the computing tasks of Ethereum.

- These infrastructures will be carried out along with the AO-Bridge protocol.

Functions Comparison

We summarize the main functions:

Functions Comparison between Ethereum and AO

SN	Name	Ethereum	AO	Description	Remark
1	keccak256(string)	yes	yes	AO built-in	
2	keccak256(bytes)	yes	yes		by AO-Bridge team
3	Elliptic curve add()	yes	yes	Add two points in elliptic curve cryptography	by AO-Bridge team
4	Elliptic curve scalarMul()	yes	yes	Point multiplication in elliptic curve cryptography	by AO-Bridge team
5	solidity.abi.encode(arg1, arg2, ...)	yes	no	Parameters can be of different types	TBD
6	solidity.abi.encodePacked(arg1, arg2, ...)	yes	no	Parameters can be of different types	TBD
7	Elliptic curve sign()	yes	no	Sign message	TBD
8	Elliptic curve ecrecover()	yes	no	Recover the signer of signature	TBD
9	Elliptic curve encrypt()	yes	no	Encrypt the message	TBD
10	Elliptic curve decrypt()	yes	no	Decrypt the message	TBD
...	...	...	...	...	

Conclusion

- In addition to undertaking the calculations of Ethereum, the AO-Bridge can also perform regular cross-chain bridge functions, such as cross-chain tokens, etc.

- So, the AO-Bridge protocol, will have a very large influence not only for Ethereum, but also for AO ecosystem.

Thanks !