ORACLE ETHEREUM

1. What is an Oracle?

According to 'ethereum.org', they define: "*An oracle is a bridge between the blockchain and the real world. They act as on-chain APIs you can query to get information into your smart contracts. This could be anything from price information to weather reports. Oracles can also be bi-directional, used to 'send' data out to the real world".*

On Ethereum blockchain, smart contracts are deployed to the network to allow users to interact with by submitting transactions that execute a function defined on the smart contracts. Smart contracts are public so it can be thought of as open APIs which means that they can be called from other smart contracts.

The Ethereum blockchain network is a cluster of nodes that execute smart contracts. All the nodes in network must access to the same set of inputs to obtain the consistent outcome, which is called ***determinism*** property.

The Ethereum will rely on this property to validate the smart contract's output – all the validators must have the same output while running the code.

To maintain this property, Ethereum has to restrict all the access from smart contracts to the off-chain information. The reason is that if smart contracts are allowed to collect information from the external sources, any tiny time difference may cause the different set of inputs which will result in different smart contracts' output – violating the ***determinism*** property. Therefore, Oracle appears as a solution for this problem. Oracle itself is a type of smart contracts which grabs the off-chain data and push it onto the blockchain for the other smart contracts to access it. Any node replaying the transaction will use the same immutable data.

2. How to allow a smart contract to retrieve off-chain data automatically?

The Oracle will comprise two components: the on-chain oracle (a smart contract) and the off-chain oracle service.

The on-chain oracle is a smart contract that has some public functions to emit events to trigger the oracle service outside of the blockchain.

The off-chain oracle is composed of several services that will query the API and return to the contract the response.

When smart contracts access to the on-chain oracle and call a function of the oracle, the on-change oracle will emit an event to trigger a service on the off-chain oracle. Here it will query API and retrieve the valid data which the blockchain requests. Then, it updates the data to the on-chain oracle by calling a function of the oracle smart contract and returns the data to smart contracts accessing to the on-chain oracle.

By this protocol, a smart contract can automatically retrieve off-chain data. It can be described by the below figure.