DAO (Decentralized Autonomous Organization) | DAO Hack

A Decentralized Autonomous Organization (DAO) is an organization operating through a set of smart contracts that establish and provide governance rules for an organization. These rules are transparent and immutable because they are embedded in a blockchain network, a technology for storing and transmitting information that is transparent, secure and operates without a central control body.

In this study, I will talk about DAO Decentralized Autonomous Organization in the blockchain. The aim of this DAO Ethereum article is to discuss the meaning of Decentralized Autonomous Organization in the first section. In this second section, I will see the working of the DAO with DAO. In third section, I will learn about the DAO Hack and smart contract on Ethereum finally a tutorial of DAO contract code reorganized into a Truffle project is given.

I.   DAO in Ethereum

The functioning of the Ethereum is similar to that of a computer network, which justifies the existence of a "supercomputer". Ethereum is regulated by the blockchain. This technology allows to manage the payments. This means that merchants must adopt it as a method of payment to purchase goods and services.
   In addition, the ETH protocol makes it possible to carry out intelligent contracts. The special feature here is that intelligent contracts are neither censored nor controlled by third parties.
The purpose of this software is to automate the transactions of the blockchain.

A DAO means a localized decentralized autonomous organization. Its objective is to systematize the decision-making principles and equipment of a company, eliminating the need for documents and other people in governance, creating a structure with localized management.

II.   How DAO Works?

The aim of this section is to discuss the working of DAO. A program call smart contract write by a group of individuals, which will run the organization. An Associate in Nursing initial funding amount, during which individuals add funds to the DAO by buying tokens that represent possession – this often known as a crowd sale, or Associate in Nursing Initial Coin Offering (ICO) – to allow it the resources it wants. When the funding amount is over, the Decentralized Autonomous Organization begins to work. People then will build proposals to the Decentralized Autonomous Organization on a

way to pay the money, and the members United Nations agency have bought it will vote to approve these proposals.
When the funding amount is over, the Decentralized Autonomous Organization begins to work. People then will build proposals to the Decentralized Autonomous Organization on a way to pay the money, and also the members United Nations agency have bought it will vote to approve these proposals.

III.   DAO Hack on Ethereum

While programmers were performing on fixing this and different issues, associate degree unknown assailant began victimization this approach to start out exhausting the DAO (Decentralized Autonomous

Organization) of ether collected from the sale of its tokens. By Saturday, 18th June, the assailant managed to empty quite three. 6m ether into a "child DAO" that has an equivalent structure because of the DAO. The worth of ether born from over $20 to beneath $13.

Several individuals created tries to separate the DAO to forestall a lot of ether from being taken, however, they could not get the votes necessary in such a brief time. As a result of the designers did not expect this abundant cash, all the ether was in a very single address (bad idea), and that we believe the assailant stopped voluntarily once hearing concerning the fork proposal. In fact, that attack, or another similar one, may continue at any time.

IV.   Smart Contract with DAO

Smart contracts mean entering into agreements - not subject to interpretation by outside entities or jurisdictions. The code itself is supposed to be the final arbiter of the "agreement" it represents. However, in fact, it is an associated (crypto-anarchist) dreamer's perspective. Prior to the attack, many lawyers insisted that the DAO had exceeded its equity financing mandate and was in violation of securities laws in many countries or jurisdictions. The code itself is supposed to be the final arbiter of the "agreement" it represents. However, in fact, it is an associated (crypto-anarchist) dreamer's perspective. Prior to the attack, many lawyers insisted that the DAO had exceeded its equity financing mandate and was in violation of securities laws in many countries.

Lawyers also pointed out that its creators were undoubtedly responsible for any problems that might arise, and several others expressed concern that DAO token holders accepted a responsibility that they apparently did not know about. The DAO exists in a very grey area of law and regulation.

Because the DAO child has equivalent structure, limitations and vulnerabilities. Because the parent DAO, the ether of this newly created child DAO cannot access for twenty-eight days.

Everyone will see the ether during this kid DAO – any tries to money in it can trigger alarms and investigations. It may be that the assailant can ne'er get to money or pay one ether of it. It's entirely attainable that the assailant had an outsized short position on ether at the time of the attack that he or she then paid out once ether had been cut roughly in 0.5. The assailant might already create his cash, notwithstanding the ether sitting within the kid Decentralized Autonomous Organization. There are things the Ethereum Foundation may do this could also be ready to nullify the ether during this DAO. That is wherever things get difficult.

Therefore, this was all about DAO (Decentralized Autonomous Organization) in Ethereum.

V.   DAO contract code reorganized into a Truffle project

In this section, I will provide a tutorial to developer with a quick start for interacting with the DAO. The used project in this tutorial you can find it in the link below:

https://github.com/tcoulter/dao-truffle

1. Installation

As mentioned, this project uses the latest Truffle on the develop branch. To get started, first uninstall Truffle if you have it installed already:

```
$ npm uninstall -g truffle
```

The second step is to download and install the develop branch with the following command:

```
$ git clone https://github.com/ConsenSys/truffle.git
$ cd truffle
$ git checkout develop
$ npm install -g .
```

The Third step after Truffle is installed, we can now checkout The DAO code with the following commend:

```
$ git clone https://github.com/tcoulter/dao-truffle.git
$ cd dao-truffle
```

2. Usage Example: Interacting with the DarkDAO

You can now use this project as if it were any other Truffle project. However, there's one use case I'd like to highlight, which is interacting with the DarkDAO.

The DarkDAO exists at address: 0x304a554a310c7e546dfe434669c62820b7d83490

To interact directly with it, ensure you have a live geth client running on port 8545, then open the console:

```
$ cd dao-truffle

$ truffle console

truffle(default)> var DarkDAO = DAO.at("0x304a554a310c7e546dfe434669c62820b7d83490");

truffle(default)>DarkDAO.totalSupply.call().then(function(total){console.log(web3.fromWei(total).toNumber())})

3641694.241898507
```

VI.   Conclusion

In this tutorial, we learned about the term DOA i.e. Decentralized Autonomous Organization. Moreover, we discussed the DAO hack & smart contracts and I give tutorial of DAO contract code reorganized into a Truffle project.