SESSION 16

Decentralized Autonomous Organization (DAO)

Learning Objectives

- Explain DAO and its working
- Discuss the latest trends related to DAO
- Describe The DAO hack
- Distinguish between the security of smart contracts and the blockchain protocol

SESSION 16

Introduction

Currently, organizations across the world use a slow and private process to make strategic decisions. Most of these decisions are made by very few persons in management while their consequences affect most of the stakeholders. This led to the development of decentralized autonomous organizations (DAOs) so that the decision-making process can be more efficient, transparent and stakeholder driven.

Suppose there is a driverless car which picks and drops passengers, collects fares and uses the cash for fuel and server maintenance. The car can work and perform its tasks without a driver or a person controlling it. This is how a DAO works. DAO does not need any bureaucratic governance.

In this session, you will learn about DAOs, how they work and their advantages and disadvantages. You will also learn about some of the latest trends related to DAO. After this, you will be familiarized with The DAO hack. Towards the end of this session, you will learn about the distinction between the security of smart contracts and the blockchain protocol.

Introduction to DAO

[LO - Explain DAO and its working]

A DAO is an organization which can function properly without any conventional management structure having deep hierarchies. It manages and sustains itself using smart contracts in which users decide the direction for future using elections. Imagine a washing machine that operates and maintains itself. A person only has to bring dirty clothes and take out clean clothes. The machine operates on its own by selecting the detergent amount, water, time and routine maintenance. This washing machine is analogous to a DAO.

Bitcoin network was considered as the first autonomous corporation which was managed through a distributed consensus protocol. Now, DAOs are implemented using smart contracts. These smart contracts are executed on top of blockchains.

Decentralized Organizations (DO)

A decentralized organization is an organization where there is no central authority which can take decisions. Instead, it provides power to all the members irrespective of hierarchical structure to take part in the decision-making process. On the other hand,

in a centralized organization, all the major decisions are made by those sitting at the top of the hierarchy.

In a decentralized organization, a set of people interact with each other according to a protocol specified in the code and applied on the blockchain. It may or may not use the legal system to protect its physical property. An example of a decentralized organization can be a shareholder-owned corporation and implemented completely on the blockchain. A smart contract running on a blockchain maintains a record of every person's holdings of their shares and voting on blockchain allow the shareholders to select the positions of the board of directors.

Figure 1 shows the differences between a traditional organization and a DAO.

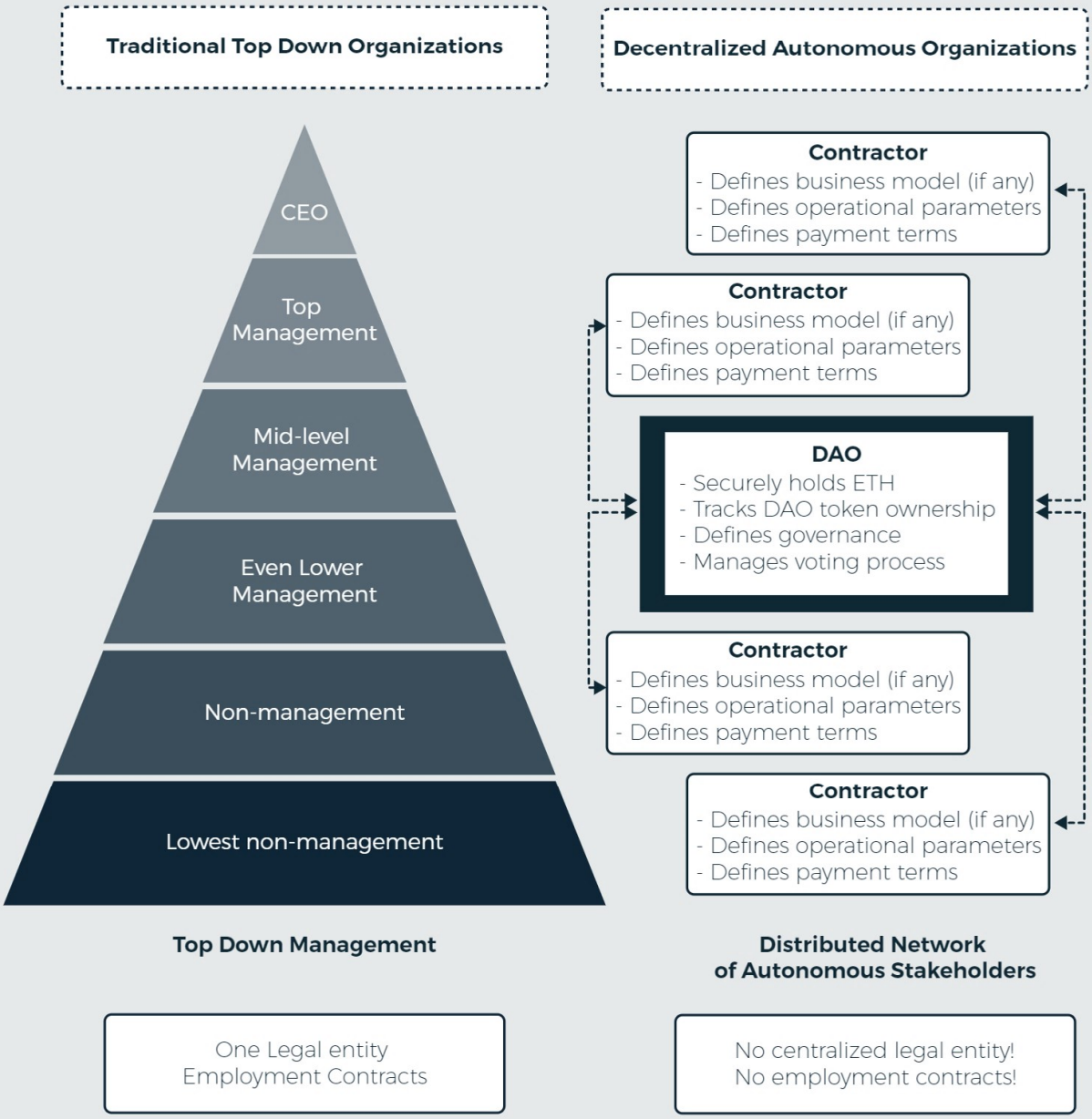

Figure 1: **Traditional Organization Vs DAO**

How DAOs Work

DAOs operate with the help of smart contracts that play a major role in the governance of the platform. It is an autonomous entity that exists on the Internet. However, it depends on hiring people with the right skill sets to carry out certain tasks which cannot be accomplished with the automation.

Earlier, Bitcoin was considered as the first fully functional DAO because it has a pre-programmed set of rules, functions autonomously and uses a distributed consensus protocol. After this, smart contracts came on the Ethereum which brought the concept of DAOs closer to the general audience and shaped their current form.

In order to be a full-fledged decentralized organization, there are certain essential factors that need to be taken care of. These factors include the rules of governance, funding, consensus, autonomy, proposals from the participants and the voting mechanisms. The factors and their importance in establishing a completely decentralized autonomous organization are as follows:

- **Smart contracts**: Smart contracts are the piece of code that contains rule and helps in governing autonomous organizations. These rules allow DAO to run without any central authority.
- **DAO Tokens (funding):** A DAO does not have a hierarchical organizational structure. In order to reward developers, DAOs need a token to ensure that people keep working on the entity. A DAO is funded by crowdsale or an ICO. The tokens provide the ability to influence the decisions of DAO by voting.
- **Autonomous**: When a DAO is deployed, it becomes independent of its founders and developers. The system becomes open source as anyone can view the code behind the DAO. All the financial transactions and program rules are recorded on the blockchain which makes it transparent and incorruptible.
- **Consensus**: When a DAO is completely operational, the decisions on where and how to spend the funds are taken via consensus. While the consensus mechanism provides complete decentralization; however, if a security loophole exists in an initial code, it cannot be rectified until the majority votes in favor of rectifying it. This makes the DAO vulnerable to attacks.
- **Proposals**: Proposals provide a mechanism to bring changes and make decisions in DAO. To prevent spamming through proposals, a fixed amount of money (cryptocurrency) needs to be spent to make a proposal and vote for it.
- **Contractors**: A DAO cannot develop a product by itself. It needs to appoint contractors to achieve its goals. They get appointed by voting of token holders.
- **Voting**: When a proposal is submitted in DAO, voting takes place.

The working of DAO can be explained in the following four phases comprising the aforementioned factors:

1. **Proposal**: First, a proposal is submitted by the DAO token holders for the development of products/services. It also defines the amount of cryptocurrency to be paid to a service provider.

2. **Vote:** DAO token holders conduct discussions/debates and subsequently vote on the proposal.
3. **Development**: After the proposal has been accepted, the development of products/ services is started.
4. **Deployment:** Anyone other than the DAO token holders can be charged for using the products and services created as a result of the proposal.

Figure 2 shows the working of DAO:

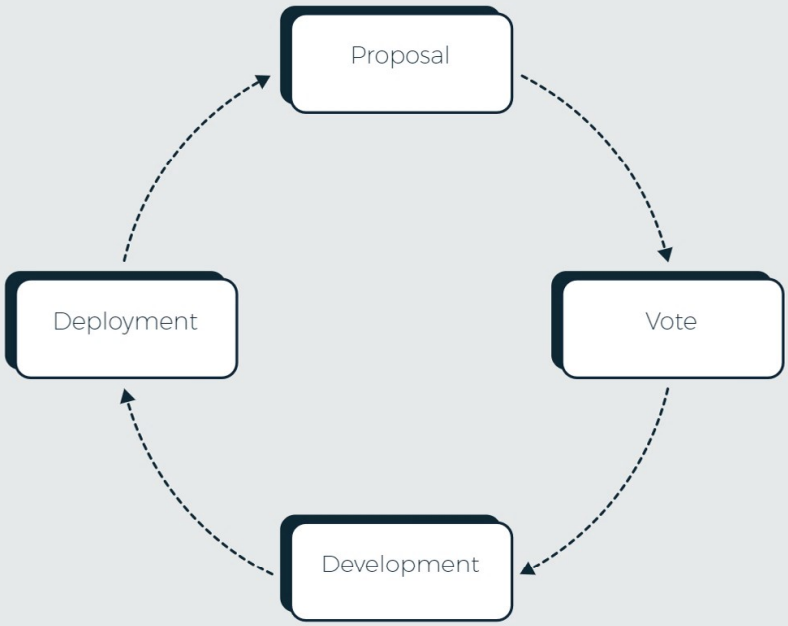

Figure 2: **Working of DAO**

Advantages and Disadvantages of DAO

A DAO provides many benefits similar to the blockchain in which the main aim is decentralization. Various blockchain-based startups have adopted DAO due to decentralization and a strictly regulated contractual relationship between the founders and investors. It seeks to solve various problems associated with the functioning of modern-day organizations which are essentially centralized. Most of these problems arise due to the management of such organizations and DAO removes them by applying decentralization.

DAO provides equal opportunity to every investor for shaping the future of an organization. They have a say in the decision-making process. Stakeholders can submit proposals and those proposals can be considered by the whole organization.

Another advantage of a DAO is its autonomous structure which leaves very little room for conflict. It works on a set of preplanned rules and policies. Stakeholders can access those rules and policies before making any investment. Once those rules are established, DAO implements them without any need for a central management authority.

In DAO, the transaction time is faster and more efficient. As placing proposals and voting requires some specified number of tokens, stakeholders tend to not waste them on ineffective solutions.

Another important advantage of DAO is transparency. As DAO is built on blockchain, every transaction, rules and decisions are recorded on the public ledger. Stakeholders can decide how to spend and manage the funds with the help of consensus. They can track how the funds have been utilized at any point of time, thereby leading to transparency.

DAO structure seems ideal; however, it is far from perfect. Its first project known as The DAO, launched in 2016, failed which exposed many issues in the code. A DAO is only as good as its code. A major disadvantage of DAO is that when the rules of a contract are coded, it is difficult to alter them. Since the code is visible to everyone and hard to fix, the known security issues are open for exploitation. Another disadvantage is its legal status. While most countries have legalized cryptocurrencies, the legal status of DAO is still unclear. Businesses who have adopted DAO still need a legal framework in order to conduct business.

Latest trends Related to DAO

[LO - Discuss the latest trends related to DAO]

Any autonomous organization with decentralized budgeting and governance is a DAO. This makes almost every decentralized cryptocurrency network a DAO. Some of the successful and well-known DAOs are:

- **Dash DAO**: It is an open-source, peer-to-peer cryptocurrency which provides instant payments and private transactions. It works on a Proof-of-Work consensus. The DAO structure comprises miners, masternodes, and treasury. The miners execute software in order to run complex algorithms to create coins. They run the network by processing transactions in exchange for nominal fees. The masternodes deal with instant transactions and private transactions. The treasury constitutes a portion of new funds that can be spent on anything subject to a masternode vote.
- **DigixDAO (DGD)**: It is a cryptocurrency which tokenizes gold. It is a decentralized group which has purchased the DGD coins in a crowdsale. The DGD holders receive awards in the form of Digix Gold token which represents 1 gram of LMBA standard gold. They use Proof-of-Asset consensus.
- **BitShares DAO**: BitShares is a decentralized cryptocurrency exchange which is hosted on Microsoft Azure blockchain. It uses Delegated Proof-of-Stake consensus algorithm. It uses a system of delegates and witnesses to run the network. Delegates make changes by making proposals on which stakeholders vote. Witnesses validate signatures and timestamp transactions.

Describing The DAO Hack

[LO - Discuss The DAO hack]

The very first DAO was Bitcoin itself which is governed by the consensus. Other than Bitcoin, all the DAOs have been launched on the Ethereum platform. The DAO is the name of a company programmed by the team behind German startup Slock.it. It is a company similar to a decentralized version of Airbnb that allows people to share things such as cars, boats, and apartments.

The DAO was launched on 30th April 2016 and had a 28-day funding window. It raised over 100 million dollars by 15th May and by the end of the funding period, it raised over 150 million dollars from more than 11,000 enthusiastic members. However, during funding, various people expressed concerns saying that the code was vulnerable to attack.

When the funding was over, the company announced before funding proposals that there was a recursive call bug in the software, but it did not affect any DAO funds. It is important to mention that the Ethereum network has no bugs and has been working perfectly during that entire time. While programmers were working on fixing the issue in the code of DAO, an unknown attacker started exploiting this issue and draining Ether collected from the sale. By 18th June, the attacker was able to drain more than 3.6 million Ether into a "child DAO" that had the same structure as The DAO. It caused a price drop in Ether from 20 dollars to under 13 dollars.

The DAO tried to resolve this issue with a soft fork. However, it had a bug, therefore, it was not approved. After this, the team went for a hard fork. The hard fork would return the Ether taken from The DAO and refund into a smart contract. This raised debate in the Ethereum community. This debate resulted in the creation of Ethereum and Ethereum Classic through a hard fork.

Security of Smart Contracts Vs. Security of Blockchain Protocol

[LO - Distinguish between the security of smart contracts and the blockchain protocol]

Today, due to lack of proper information, most people get confused when it is said that blockchains are extremely secure. With all the news of hacks worth millions of dollars, the perception that maybe blockchain solutions aren't that secure has become common.

However, it is important to understand the difference between the security of the underlying blockchain network and the security of the smart contracts deployed on it.

In November 2017, a user accidentally froze Ether worth around 155 million dollars in Parity, which is a popular Ethereum wallet. It was due to a bug in the wallet's software which was accidentally triggered. Parity is not the only organization which has suffered from the smart contract vulnerabilities.

When The DAO smart contracts got hacked, it divided the Ethereum community and resulted in two versions of the famous cryptocurrency platform. The DAO was hacked due to vulnerabilities in its smart contract, which is a code that runs on the Ethereum blockchain and enables the creation of decentralized applications (DApps).

Smart contracts are a crucial component of the blockchain industry. A smart contract is a code which is similar to any other software running on computers. After deploying it once on the blockchain, it cannot be changed which acts as an advantage as they cannot be tampered with. However, the disadvantage is that any bug will be permanent too. There are methods to fix bugs in smart contracts, but they are tough to adopt.

Smart contracts are directly tied to the payments and they can contain millions of dollars' worth of cryptocurrencies. If any bug is open to attackers, then they can steal the cryptocurrencies.

Smart contracts are relatively new and best coding practices for them are still being developed. This makes auditing of the smart contract very necessary because when a traditional software is being developed, it involves multiple write-release-fix cycles, but with smart contracts, it is necessary to get everything right the first time. Else, the stakes are very high, and you can lose millions of dollars in one go.

Now, various firms provide auditing services for smart contracts, review the code and provide feedback on their quality and security. However, these services cost a lot, much more than blockchain startups can afford. Another problem is that the investors and users cannot verify the auditing procedure of smart contracts.

One more security aspect that is neglected is the end-user security measures. One of the most common approaches to stealing huge amounts of cryptocurrencies is to attack an individual and steal his/her private key. Once the private key is known, no security measures can prevent the hacker from stealing the funds.

In some cases, hackers attack one of the less secure systems attached to a crypto-exchange, and thus gain access to the privileged information over time. Then they steal the private key of the exchange wallet and thus steal huge funds in a matter of minutes.

When such an event occurs, misinformed media publishes this as an attack on the blockchain network itself, without understanding that this is nowhere related to the blockchain network.

In summary, the underlying blockchain network is usually extremely secure, but users must be alert and keep the private keys of their wallets safe and secure. Similarly, smart contract code must be audited and kept updated and bug-free (preferably using upgradable logic contracts approach, which will be discussed in the upcoming module on Ethereum).

SUMMARY

- A DAO is an organization which can function properly without any conventional management structure having hierarchies.
- DAOs are implemented using smart contracts. These smart contracts are executed on top of blockchains.
- A smart contract running on a blockchain maintains a record of every person's holdings of their shares.
- Proposals provide a mechanism to bring changes and take decisions in DAO
- DAO provides equal opportunity to every investor for shaping the future of an organization.
- A disadvantage in DAO is that when the rules of a contract are coded, it is difficult to alter them.
- The DAO got hacked due to vulnerabilities in its smart contract, which is a code that runs on the Ethereum blockchain.