IS4302
Blockchain and Distributed Ledger Technology

Lecture 9

17 Mar, 2023

NUS
National University
of Singapore

Overview

- **Decentralized Autonomous Organization (DAO)**
  - Definition
  - The DAO
  - Examples
  - Discussions

Definition

- **No consensus on how to define a DAO**
- **A DAO is an internet-native entity with no central management which is regulated by a set of automatically enforceable rules on a public blockchain, and whose goal is to take a life of its own and incentives people to achieve a shared common mission.**
- **A DAO is an organization whose essential operations are automated agreeing to rules and principles assigned in code without human involvement. A DAO is a novel scalable, self-organizing coordination on the blockchain, controlled by smart contracts.**

Features

- **DAOs enable people to coordinate and self-govern themselves online.**
  - people acting towards a common goal, rather than a legally registered organisation
- **source code is deployed in a blockchain with smart contract capabilities like Ethereum—arguably always a public blockchain**
- **smart contract code specifies the rules for interaction among people**
  - unclear to which extent there may be other governance mechanisms that can affect or overrule such code

Features

- **Since these rules are defined using smart contracts, they are self-executed independently of the will of the parties.**
- **The DAO governance should remain independent from central control.**
- **Since they rely on a blockchain, DAOs inherit some of its properties, such as transparency, cryptographic security, and decentralisation**

Overview

- **Decentralized Autonomous Organization (DAO)**
  - Definition
  - The DAO
  - Examples
  - Discussions

The DAO

- **In June 2015, Slock.it begun development of a decentralized autonomous organization framework, accepting contributions from the open source software community.**
- **By March 2016, a large community had begun to form around the open source framework, and Christoph Jentzsch of Slock.it published the corresponding whitepaper on March 15, 2016**
- **The community formed through the Slack messaging service initially, and then launched an online forum independent of Slock.it, calling themselves DAOhub.**

The DAO

- **Slock.it was sympathetic and encouraging of the DAOhub, and wanted their design to become a "standard" for future decentralized autonomous organizations to build on.**
- **The DAO was intended to allow cryptocurrency "investors" to directly fund and manage new enterprises—all to be run on the Ethereum blockchain.**
  - ensure that all business transactions and organizational changes would be immutably recorded on a public ledger
  - each organization would be, in-effect, directly managed by its investors, as per the investment stake of the individual

The DAO

- **The DAO was launched on April 30, 2016, at 10:00am GMT/UTC**
  - by several “anonymous” submissions associated with DAOhub, who executed the open source bytecode on the Ethereum blockchain
- **A funding or “creation” period of 28 days**
- **As the funding period came to a close (concluding May 28, 2016), The DAO went live with the equivalent of about $250m USD in funding, breaking all existing crowdfunding records.**
  - Some 10,000 to 20,000 (estimated) people invested in The DAO
  - amounted to about 14% of the total ETH supply

The DAO

- **Shortly after the minimum two week "debating" period, on June 17, 2016, The DAO's code was "exploited" by an unknown individual.**
  - Re-entrancy attack
- **Immediately, Slock.it, the leaders of the Ethereum platform, numerous cryptocurrency exchanges, and other informal technical leaders stepped in to stem the bleeding—shutting down "exits" through the exchanges, and launching counter-attacks.**
- **In the end, the whole project was disbanded, with an inglorious "hard fork" rolling back the ostensibly "immutable" ledger.**

The DAO system

- **The DAO was an attempt to build a funding platform, similar to Kickstarter**
  - Kickstarter raises funds from many individuals through their centralized administration
  - The DAO sought to raise funds direct from peers

- **This "funding" mechanism remains poorly-understood**

The DAO system

- **The first stage of The DAO was a funding period or "creation phase" of 28 days**
  - anyone could exchange ETH for DAO tokens in return
  - During the initial funding period the price of DAO tokens rose programmatically (from an initial value of 1:100)—encouraging early buy-in
  - After the initial funding period, no more tokens would be created
  - it would be possible to trade existing tokens on public cryptocurrency exchanges

The DAO system

- **Tokens would be used to directly fund and control "proposals" on The DAO platform.**
- **Anyone with a (refundable) minimum token deposit could create a proposal to be voted on by token holders.**
- **Investors voted/invested by allocating DAO tokens for specific proposals.**
  - Unlike Kickstarter, however, DAO voting members would have significant control over projects.

The exploit

- **In the months leading up to the post-funding, launch date of The DAO, numerous community members expressed worry about the security and governance of The DAO.**
  - an “experiment in responsibility”
  - it was becoming clear that Slock.it might not be the safe shepherd the community had hoped for
- **Cryptocurrency researchers Dino Mark, Vlad Zamfir, and Emin Gün Sirer released a whitepaper on May 26, 2016 (when The DAO was launched but in the static “funding” period), outlining eight possible security risks**
  - based on game theory issues, rather than actual code bugs
  - they call for a temporary “moratorium” , well supported in the community

The exploit

- **Stephen Tual, founder and COO of Slock.it (who had taken on a de facto corporate messaging role), assured the community that such concerns would be addressed, and that there was no need for panic.**
- **Between June 5th and June 9th, 2016, another issue was discovered—a technical bug this time, called a "race to empty" attack—just days before the first activities of The DAO were to begin.**
- **The attack had been tested by a similar (but much smaller) DAO project called "MakerDAO," which confirmed that it was executable, and had alerted The DAO developers about the security risk.**

The exploit

- **To address the rising tide of security issues, and to reassure an increasingly worried public, on June 13, Tual issued a statement about a 1.1 software update to The DAO framework, which had been in the works for "over a month" .**
- **However, during this time, Tual was also increasingly vocal that Slock.it did not "own" or "run" The DAO.**
- **On June 12, just prior to his prepared statement about the launch of the version 1.1 update, Tual issued a statement about this security risk, insisting that "no funds were at risk", and that the forthcoming 1.1 software update would address this exploit**

The exploit

- **On June 17, 2016, an unknown "attacker" launched a "race to empty" exploit that was similar to the one that had been previously identified, and began draining The DAO of funds (in the end, 3,689,577 ETH, or about 30% of the total).**
- **The first warning came from a Reddit community member**
- **Within hours, Ethereum Foundation member George Hallam roused key Ethereum developers and other pertinent members of the community to an internal Slack communication channel**

The exploit

- **Knowing that the attacker would want to convert the "stolen" funds into "traditional" currency, the assembled group contacted several individuals in charge at the major exchanges responsible for trading ETH, and strongly requested that these exchanges halt trading.**
- **Worried that shutting down trading would cause panic and reputational damage, some exchanges resisted such a drastic action, but with $250m USD and an existential crisis for the entire Ethereum platform on the line, the major exchanges eventually relented.**
  - the funds were effectively "frozen" for the time being

After the exploit

- **The value of ETH plummeted, and the community speculated that an unknown individual had shorted the price of ETH prior to the exploit and made millions in the aftermath, fuelling the belief that the true purpose of the attack was to devalue ETH and make money by short selling**
  - some of the evidence for this short sale, however, is circumspect, as it may have been a mere coincidence

After the exploit

- **Debates over solutions raged online**
  - Driven by ideologies that saw any kind of “hard fork” as tantamount to an existential deceit
- **A letter purportedly written by the attacker circulated, arguing that since The DAO was defined by its code, the “exploit” was nothing more than a clever (and legal) loophole.**
- **The letter writer and a vocal minority in the community argued that “code is law”**

After the exploit

- **Within the next few weeks, with the political clout of Buterin and the Ethereum Foundation behind the decision, a "hard fork" version of the Ethereum software was developed and released to miners.**
  - A majority of miners implemented this software, and the blockchain ledger was updated to effectively erase The DAO.
- **"Moderates" saw the hard fork as evidence of the flexibility and practicality of Ethereum and its leaders**
- **The more ideological saw the hard fork as censorship by a powerful cabal, or proof that blockchain technology was unable to live up to its idealistic promises.**
  - Ethereum Classic (ETC)

Overview

- **Decentralized Autonomous Organization (DAO)**
  - Definition
  - The DAO
  - Examples
  - Discussions

Protocol DAOs

- **Offer an ownership and governance mechanism to support lending platforms.**

- **The most common variant among DAOs**

Uniswap

- **Decentralized exchange runs on Ethereum**
  - enables peer-to-peer (P2P) crypto (ERC20 tokens) trades

- **Challenges**
  - segmented liquidity
  - disjointed user experience
  - network scalability

Uniswap

- **Liquidity pool**
  - provides tokens that are used for facilitating trades

- **Automated Market Maker (AMM)**
  - a smart contract used for managing the liquidity pools
  - defines the effective price of a token according to the interplay between the supply and demand of tokens in the liquidity pools.

Uniswap

- **Uniswap's AMM**
  - provides incentives for people on the exchange to take on the role of liquidity providers
  - Liquidity providers receive a token representing their stake in the liquidity pool, which they can redeem later for a specific share in the trading fees
  - each listed token has its respective liquidity pool where users can contribute
  - The AMM protocol helps in determining the price of the tokens for trading according to a mathematical equation

Uniswap

- **A liquidity pool is with respect to a pair of ERC-20 tokens.**
  - E.g., a ETH/DAI pool
- **In a pool, the price is determined by constant product formula.**
  - E.g., a ETH/DAI pool in which there are 60 ETH and 60 DAI, the product of the two volumes is 60*60 = 3600
  - If you want to buy 10 ETH with DAI, you need to give enough DAI such that the product is a constant, i.e., DAI needed in the pool = 3600/(60-10) = 72, so you need to give 72-60 = 12 DAI.
  - Similarly, for the next 10 ETH, the price will be 3600/(50-10)-72 = 18 DAI

Uniswap

- **Governance of Uniswap DEX**
- **Uniswap token, UNI, introduced in September 2020.**
- **UNI token holders have the privilege of voting on developments in the Uniswap project, which will determine the platform's future. Furthermore, the UNI token could also serve other functionalities such as funding liquidity mining pools, partnerships, and grants.**
- **UNI is tradable.**

DAOs

- **Another example of protocol DAO: MakerDAO**
- **Other kinds of DAOs**
  - Investment and grant DAOs
    - **E.g., LAO, Uniswap Grants**
  - Social DAOs
    - **exclusive clubs where you can gain membership by purchasing a specific amount of DAO tokens**
    - **E.g., Bored Ape Yacht Club NFTs**

Aragon

- **Extends the use of DAOs as a free and open-source technology.**
- **Allows the creation and management of decentralised organizations.**
- **Provides a static template to make your own DAO, but it also allows you to create a customized one.**
- **Customization is enabled through "apps" (sets of smart contracts) which can be installed or removed from DAOs.**
  - a vault in which to store DAO's funds
  - decision-making systems, including an app which introduces the DAOstack's decision system
  - …

Aragon

- **Those apps can be used to create a template which enables the creation of DAOs with a more specific purpose.**
  - E.g., the Committee template sets a special token which is used by a small group of members to take decisions, like accepting new members.
- **The other key feature that Aragon introduces are permissions.**
  - an access control system intended to safely connect apps and entities (users or other apps) together.
  - Initially, the DAO creator has the permissions to manage it, but usually, the creator transfers those permissions to the voting app.

DAOstack

- **The DAOstack platform does not offer many customizations.**
- **a single decision-making system for all their DAOs**
- **Holographic Consensus**
  - aims to solve the problems of scaling a DAO
  - Increasing the scale of a DAO (in terms of either members or decisions) makes it susceptible to attacks, or to require many users to make it work.

DAOstack

- **Holographic Consensus**
  - The quorum required to approve a proposal can be reduced from absolute majority to relative majority if some conditions are met.
  - The most significant condition concerns to the predictors or stakers, who are not necessarily members from any DAO.
  - Those predictors can stake a special token to predict the result of a proposal. If stakers are right, they are rewarded, while if they fail, they lose their stake.

DAOstack

- **Holographic Consensus**

  - Regarding the proposal, if the staked amount reaches a specific limit, then the quorum of that proposal will be reduced to a relative majority.

  - Stakers help DAOs to highlight meaningful proposals and make profit if their service is useful.

DAOhaus

- **A fork of Moloch DAO's smart contracts**
  - Moloch, named as an ancient God of sacrifice
  - seeks to promote an infrastructure where the collective benefit is always greater than the individualised benefit of any particular entity
- **A voting system that tries to minimize attacks and abuses**
- **For each new decision, the proposer has to pay a tribute in tokens, and some amount of influence, which any Moloch's member has.**

DAOhaus

- **Before the decision is finally taken, if any participant does not agree with the result, they will able to make rage quitting, exiting with their portion of resources.**
  - To avoid majority bullying minority
- **Moloch simplifies the voting system as no minimum quorum is needed to approve proposals.**
  - They just count cast votes, and if there are more than 50% up-votes, the proposal passes

Colony

- **Colony's DAOs are shared by people with common goals, and resources to accomplish them**
- **These DAOs can be split into domains or even sub-domains with more specific purposes.**
- **Those purposes are translated into tasks that DAO members can accomplish to gain more influence.**
  - E.g., a web company could split its organisation into a 'front-end' domain, or a 'back-end' domain, and finally, assign tasks to those domains.
- **DAO members have a reputation token and the only way to gain more is by performing tasks.**

Colony

- **The only way to increase the member's influence is working for the organisation (i.e. work-driven)**
  - Not mainly voting-based
- **Tackles scalability**
  - splitting DAOs into domains which are potentially independent
  - all decisions are approved by default unless someone has an objection, in which case it is discussed and solved with voting

The case of Genesis Alpha

- **Genesis Alpha, a.k.a. Genesis DAO: the DAOstack DAO**
- **To promote the use of DAOs through DAOstack and to boost the use of the GEN token as a specific tool for decentralised governance.**
- **They state that Genesis Alpha receives monthly funding of 40k USD dollars (in cryptocurrencies) from DAOstack**
- **Due to a vulnerability in its code, it was hacked, and approximately 15k USD were drained from Genesis DAO on the 6th of February 2019.**
- **This delayed its launch until the vulnerability was fixed.**
- **The final launch of Genesis Alpha was in April 2019.**

The case of Genesis Alpha

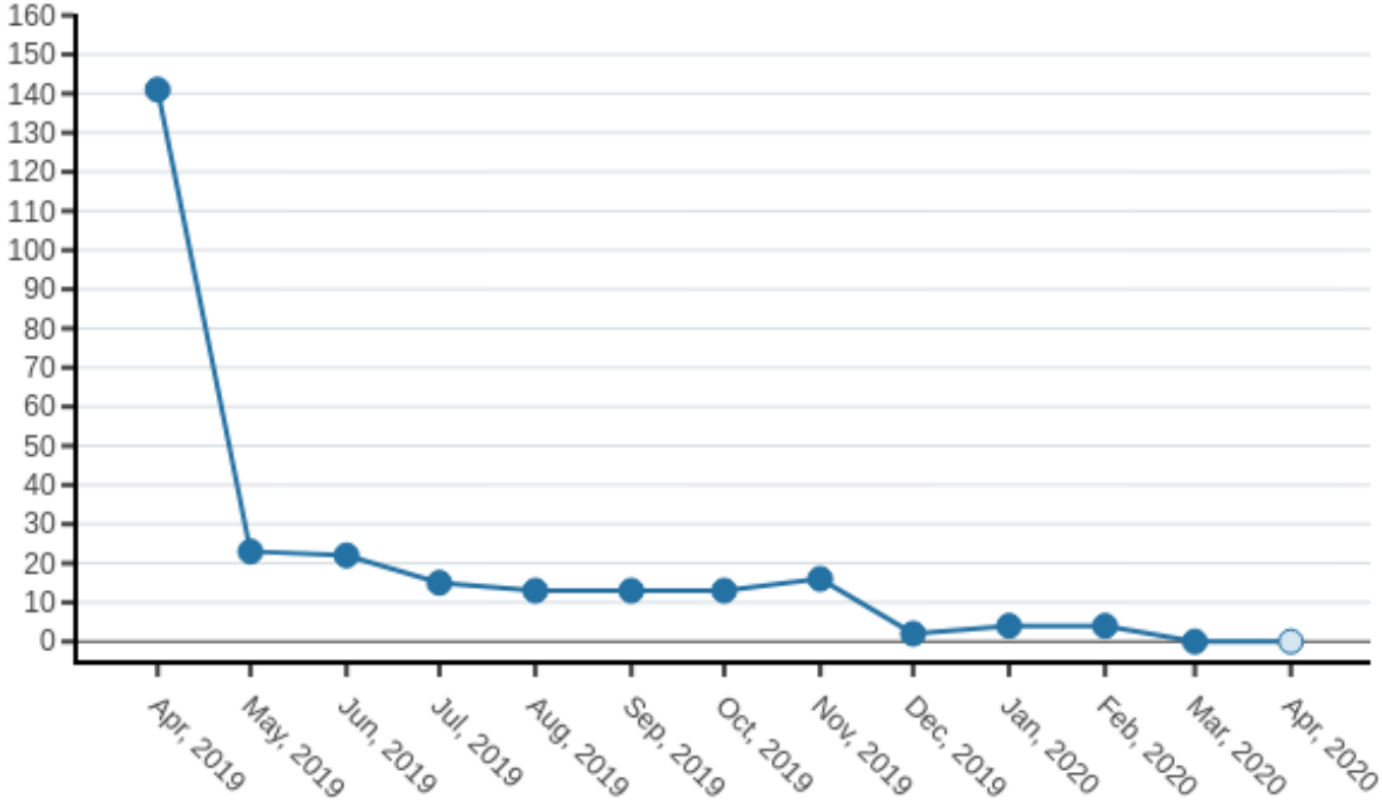

Figure 2: Genesis Alpha new members time series

The case of Genesis Alpha

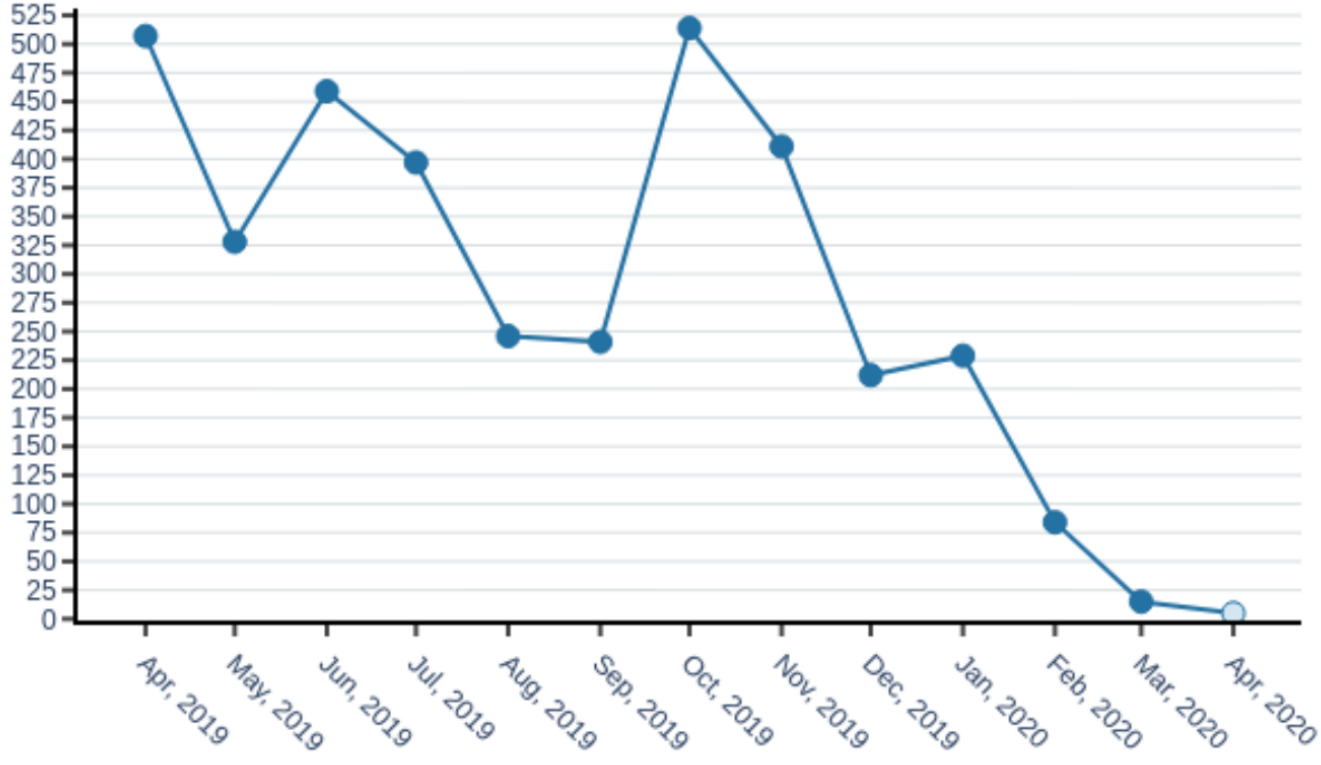

Figure 3: Genesis Alpha activity (new proposals + votes + stakes) time series

The case of Genesis Alpha

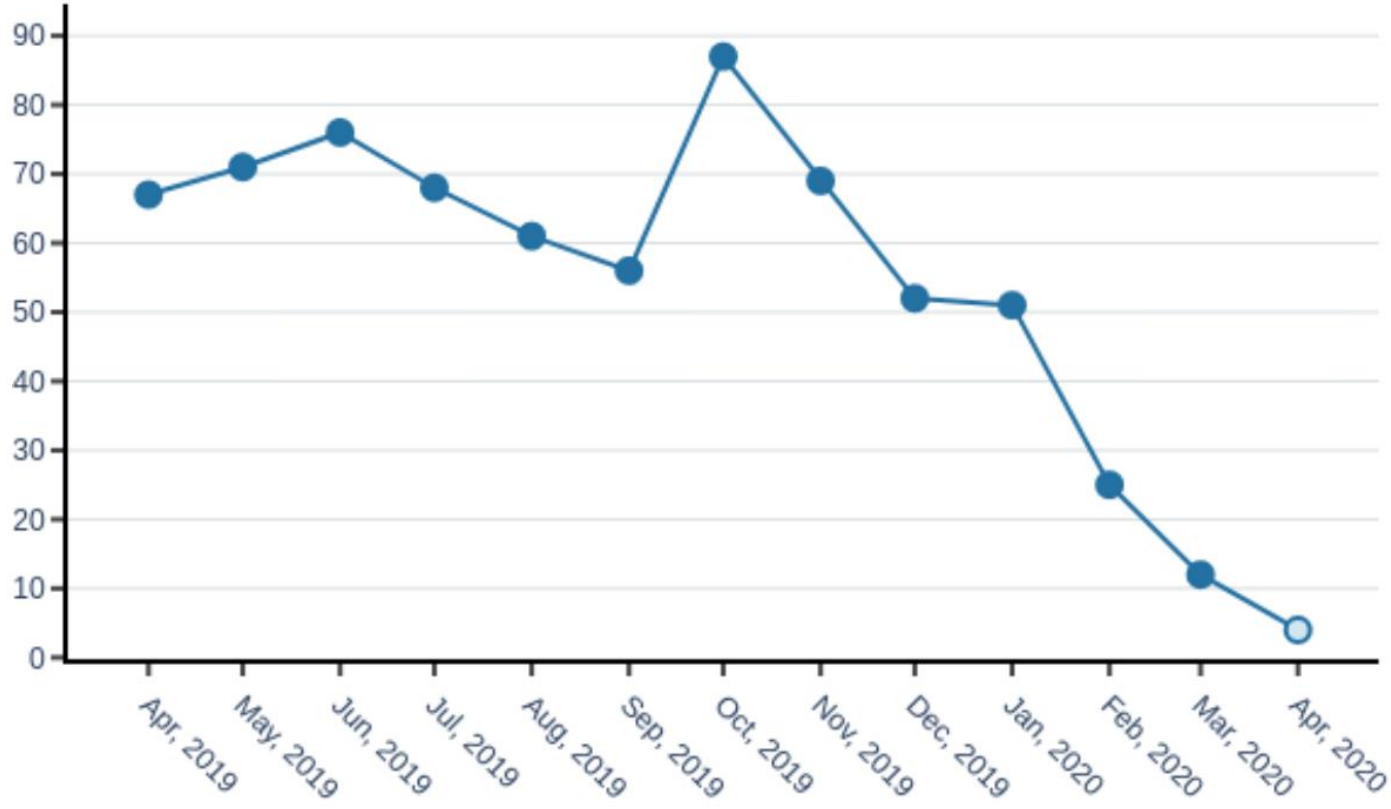

Figure 4: Genesis Alpha active members time series

The case of Genesis Alpha

- **Genesis Alpha is the most active DAO in DAOstack**
- **From November 2019, Genesis has abruptly started a downfall on activity, having its peak just a month before.**
  - it is said that DAOstack cut the funds to Genesis Alpha
  - since November 2019 its total balance of Ether has been strongly reduced
- **“the lack of accountability measures turns passed proposals into ‘promises’ and requires the community to become vigilant of one another”**

Overview

- **Decentralized Autonomous Organization (DAO)**
  - Definition
  - The DAO
  - Platforms
  - Discussions

Open discussions

- **Legal authority**
  - Code is law?

- **Practical governance**
  - Off-chain interactions
  - A small group of people
  - Social ties
  - …

Thank you!

References:

DuPont, Quinn. "Experiments in algorithmic governance: A history and ethnography of “The DAO,” a failed decentralized autonomous organization." Bitcoin and beyond (2017): 157-177.

Hassan, Samer, and Primavera De Filippi. "Decentralized Autonomous Organization." Internet Policy Review 10.2 (2021): 1-10.

El Faqir, Youssef, Javier Arroyo, and Samer Hassan. "An overview of decentralized autonomous organizations on the blockchain." Proceedings of the 16th international symposium on open collaboration. 2020.