Lecture 9 - Dao

Rylan Schaeffer and Vincent Yang

May 25, 2016

Note: This lecture is based on Princeton University's BTC-Tech: Bitcoin and Cryptocurrency Technologies Spring 2015 course.

ZKP Continued

- Billard Balls: Alice is blind and has two billard balls. Bob claims that these two billard balls are of different color, but Alice doesn't believe him. What is a ZKP that Alice can use in order to distinguish if the two billard balls are really of different color?
- Other:

  Bridge 1, 2, 5, 10, 17

  1000 wine

  Light switches

DAO

- People crowdfunded $150 million into the DAO, also called the Decentralized Autonomous Organization

  This can be compared to the Pebble Watch, which had $20 million raised

  $30 million in the first 10 days
- In a normal company, any decision is made by whoever has the authority - CEO, Board of Directors, etc.

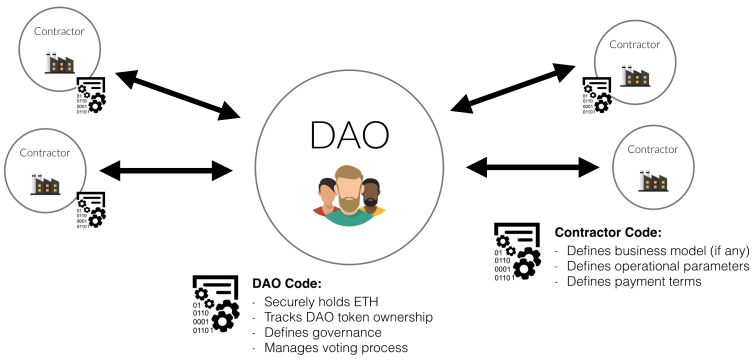
  Instead, the DAO functions similarly to shareholder rights in a company. Through DAO tokens, you can

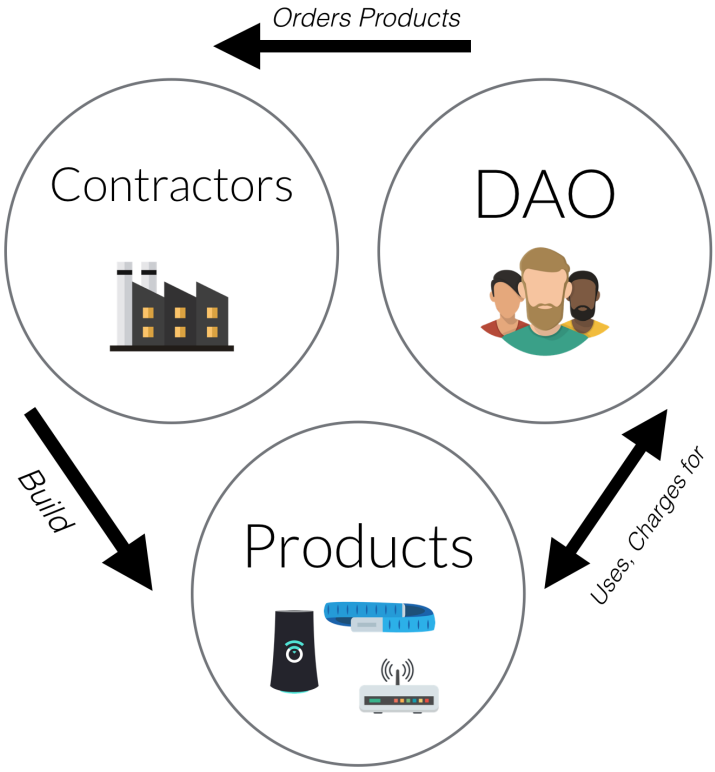
  1. Submit proposals for funding
  2. Vote on which proposals are funded
  3. Receive profits from funded projects
- Big promise: new way to manage and allocate capital

  Capital Allocation without a fund manager
- Backed up by 11,000 anonymous stakeholders who can vote on any major decision to spend funds
- Any company or individual who would like to use funds have to submit a proposal, which is then published online
- After these are published online, stakeholders vote on adoption - aka whether or not to allocate some of the $150 million or not

- Contractors submit Proposals for the development of products or services - these are written in English, then code

  DAO Token Holders can pull the plug on funding anytime, subject to the Proposal

- 

- 

- The only centralized aspect is the Curators who play an escrow role

  Escrow: financial aspect held by 3rd party on behalf of the other 2 for a transaction

  - This is a failsafe to prevent a 51% attack. Rather than adding centralization to the DAO, they're nominated by token holders and can be fired any time for any reason.
  - Curators curate the whitelist, which is the list of Contractors authorized to receive ether from the DAO.
  - Serve two functions:
    1. When a DAO Token Holder submits a Proposal in the form of a smart contract, the Curator checks that the published contract on the Ethereum blockchain matches the source that the Contractor says they've deployed (compare bytecode)

2. Second, a Curator confirms the origin of a Proposal, This is done by having the submitting entity send a signed transaction with a set of data known only to the Curator and the author of the proposal.

- Now, the following are functions of the DAO as a whole, not the Curator.

  Evaluate how good a Proposal is

  Audit smart contract code

  Provide legal advice

  Take responsibility for the proposal

- This is done by a multisig involving Vitalik Buterin (Inventor and Founder), Alex Van de Sande (Chief Designer), and other highly involved individuals
- Changing the Curator:
  * Changing the Curator takes the form of a Proposal with a special flag
  * Votes take place in two steps: First, a non binding vote on whether or not DAO Token Holders would like to switch Curators, then second, a confirmation vote to give a chance to DAO Token Holders a chance to confirm or deny the result of the first vote. If the minority chooses to split, they may do so, similar to how a company might split in two
- The huge advantage of having Curators is that even with a 51% attack, someone can't make a proposal sending themself 100% of the DAO's ETH.

- This is so big such that it now accounts for 14% of all Ether for Ethereum.
- Stakeholders are incentivized since they can potentially gain from their slice of the profits
- Proposals:
  - Stephan Tual is the chief executive of Slockit, which is a company with a proposal for funding from DAO that's played a large role in getting DAO going

    Slockit's CTO wrote a good portion of the code for DAO. This combines IOT with Blockchain

    Basically if you can lock it, you can rent, sell, or share it.

    IOT opening and closing locks based on smart contracts

    For instance, they could control access to cars, bikes, and storage units.

    Cars could be parked in roads waiting for the customer, then opened with an app

  - Mobotiq
    * Problem: Fossil fuel addiction is a large cause for pollution, global warming, geopolitical tensions, and terrorism

      Old product: polluted the Earth, inefficient, high cost per km, planned obsolescence
      Old organization: closed, innovation aversive
      Old manufacturing system: centralized mass production with high barriers to entry
      Old business model based on ownership
    * Solution: Create a new supply and demand ecosystem

      New product: clean, efficient, affordable, designed to last, software intensive, modular, simple

      New organization: open, innovation friendly networked meritocracy
      New manufacturing system: distributed without barriers to entry
      New business model: demand centric, based on p2p rentership
    * Modular parts for transportation that doesn't rely on gas
    * DIY mindset - people can assemble modular components with different configurations
    * Current prototype: tested to be safer than a conventional car
    * 1 m width, so it can lane split
    * Designed to lean in curves

* Swap and carry battery with wall charger
* Connected with IOT - everything is monitored by sensors and cameras, so you can record and understand how each part works with every other part
* P2P Rental by design, so this is actually designed to be coupled with slock.it so you can rent it to others
* Designed to be driverless as well while being modular - it has parts for traction, steering, suspension, brakes, and tilting