****

**Socio-political stakes in the digital era**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

“Decentralized autonomous organizations:

What are the important aspects of a DAO?

What are its use-cases?

*By Cyril van Schreven*

**I. Sources / ideas**

Intro elements:

-First mention by Dan Larimer: <https://letstalkbitcoin.com/is-bitcoin-overpaying-for-false-security#.Ui-p9WTFT7s>

Called it Decentralized Autonomous Organization at that point.

*Think of a crypto-currency as shares in a Decentralized Autonomous Corporation (DAC) where the source code defines the bylaws.    The goal of the DAC is to earn a profit for the shareholders by performing valuable services for the free market.  With this goal in mind set out to maximize shareholder value at every stage as you design the bylaws that govern operation of the DAC.*

He defines every crypto-currency to be a DAC. (09/2013)

-Vitalik “DAOs, DACs: terminology”: <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>

Also one of the first articles (04/2014). Laying the foundation

-Vitalik “Bootstrapping a DAO”: <https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274/>

Software structure:

-“the dao structure / implementation” (basic) : <https://www.ethereum.org/dao>

Socio-political thoughts: -“Tao of the dao” : <https://hackernoon.com/ethereum-the-tao-of-the-dao-fa561b2f6b54>

DAO == cooperative?

-“can’t code away social problems”: <https://www.coindesk.com/system-problems-social-issues-daos-structure/>

*While The DAO gets labeled revolutionary more often than not, this income-based reputation is how the current political system works, and many are finding it appalling as the income gap widens.*

How to measure votes? With financial power, with ID, with reputation (based on? Often a mix of financial power and participation)

*For instance, Steemit wants to create a social networking site where positive and accurate information is dispersed, but those adjectives are dependent on people voting. For sites that hope to gain momentum from cryptocurrency enthusiasts first, this could mean biased posts on the advantages of cryptocurrency get upvoted, while information about its flaws or weaknesses get downvoted or ignored, thus burying those stories for other users.*

Need for aligned interests, in turn can lead to misrepresentation / biased information.

-“Anti-DAO mysticism”: <https://ftalphaville.ft.com/2016/05/17/2162084/more-decentralised-autonomous-organisation-dao-mysticism/>

*We won’t go on about […] what happens when you remove the professional executive/management function from corporate identity[…]. Any cursory review of modern history (or a quick read of*[*Animal Farm*](https://en.wikipedia.org/wiki/Animal_Farm)*) will flag up the problems: indecision paralysis; wasted time and resources on voting and bureaucracy; entirely non-diplomatic means of grabbing power just to get things done; uninformed decision making; exploitation of the ignorant; tragedies of the commons scenarios and last but not least: a lack of skin-in-the-game accountability for poor decision making leading to post-facto due diligence processes with dire consequences for capital, human resources and environments.*

A bunch of counter arguments to “the DAO”. The author here is clearly against it (is against crypto since its birth). Raises interesting points though.

-“Dan Larimer criticizes DAOs’’ : <https://steemit.com/crypto-news/@dan/is-the-dao-going-to-be-doa>

Regulation / juristic status:

-“SEC DAO report (note)”: <https://cointelegraph.com/news/forewarned-is-forearmed-key-takeaways-from-sec-dao-report>

*The Securities and Exchange Commission (SEC) has*[*ruled*](https://cointelegraph.com/explained/sec-ruling-on-the-dao-and-ico-explained)*that the Decentralized Autonomous Organization (DAO) tokens were indeed securities and that their sale in 2016 should have been registered as a security with the SEC.* Ruling are developing atm. SEC regards investments and taxes. But who would be ‘responsible’ for the decisions of a well-developed DAO.

Human / non-human:

(the dao hack)

-“The DAO was all too human”: <https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/>

 “*Instead, the DAO led to a heist that raises philosophical questions about the viability of such systems. Code was supposed to eliminate the need to trust humans. But humans, it turns out, are tough to take out of the equation.”*

Was a human bug, can’t take human out of equation… but:

*“The Ethereum team is now debating how, and whether, to refund the stolen funds. Ethereum works much like Bitcoin does: the system records each transaction in a global ledger that resides on every Ethereum user's computer. The Ethereum team could release a new version of the software that tweaks this ledger to essentially reverse all of the DAO heist transactions.”*

Humans fixed it. All blockchain systems so far rely on consensus. A majority can always modify (theoretically) anything. Is what happened to The DAO. Dan Larimer is now promoting this human safety net.

-“dao-hack, more tech-savyy and in depth”: <https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce>

**II. Possible structure**

**A- Past / existing projects**

Bitshares / Steemit

“The DAO”

-first implementation reaching mainstream public.

-raised 150 million from more than 11,000 investors, making it the largest crowd sale ever. Biggest investor had 4% (nicely decentralized). Represented 14% of the circulating ether.

-was promoted by the lead developers of Ethereum.

-launched 30 April 2016. Hacked 17th of June 2016 (for about 30% of its values).

-considered as securities by the SEC

-to interface with real world legal structures, was established in Switzerland

-20 July, hard-fork of the Ethereum network to restore all the ‘stolen’ money

-raised important debate about: governance, legality and authority of smart contracts vs ‘common good’. Consensus ruled. Also, critics about the central role of Ethereum devs in the process.

-about 10% of the users refused the hard ford. This blockchain (history of transactions) is still active as Ethereum classic. Main arguments is that this hard ford would put a precedent.

-opposed two philosophies: 0 governance and code is law, vs decentralized governance and human consensus is law.

-lessons learnt: no code is fail proof (even more under such economical incentive; multi-million); there are always unknown unknowns; ability for the community to reverse anything by consensus increases security

Eos / Cardano

**B- The technical architecture (tools) and its effect on the system**

1. Blockchain, smart contracts (general overview)

From bitcoin to Ethereum to smart contracts to alternative systems (Larimers)

2. The burden of quantification and anonymity.

Quantification is a must in such a digital environment. It clarifies what the organization is for as well.

Financial transfers are the best tool for organizing in this environment: yields power and is quantifiable. What are the alternatives? Power per person, or power per reputation. Power per person as in a western democracy requires to avoid anonymity. It is a complex problem for internet, though it is being considered. Sites such as gambling sites already correctly identify their users.

Power by reputation or power by account (vs by person) is also viable. It has been explored, as a mix of financial investment and time (participation) investment.

3. Game theory

Incentive is of major importance for DAOs. The interests of all involved actors should align as much as possible with that of the DAO (financial investments serves this purpose well..). If as scenario can create where the incentive of some actors is against that of the DAO, it will perish on the long term. Note that the ‘rules of the game’

**C- Its place amongst competing organizational architectures**

**TEXT START**

Let’s start by defining what a Decentralized Autonomous Organization (DAO) is.

In the current literature the definition is not very strict, and its use-cases are often debated. Here we will try to grasp what its various definitions share, and perhaps explain why the definition cannot be absolute. At the very least, it will avoid any misunderstanding by setting the scope of this paper.

As a first point let’s note that the term was born in the Blockchain movement, and for good reasons. However, we will try to explore which pre-existing organization models could best fit the description. As such, we will keep the definition as broad as possible. This will allow us to best distinguish which characteristics of the Blockchain technology made the development of such organizations possible.

Let’s proceed word by word.

**Organization**: An organization is an organized group of people with a particular purpose. A group of people is said to be organized if it functions in a structure within which it obeys a set of rules. The collective goal it follows is the very reason of its existence. Note that this word can apply to a wide-range of cases. It does not hold any legal, nor financial requirements such as the word ‘company’.

We will now define the two other terms, solely on their application to an organization.

**Decentralized**: Without delving into the different network topologies (comparing decentralized to distributed network), an obvious point for a decentralized system is that it is not fully centralized. As such, its most important mechanisms do not all pass through a single entity. Note how in practice organization describe a continuous distribution on the axis of centralization. They cannot be categorically (binarily) defined by this adjective.

Decentralization can be defined through multiple axes of analysis. The two most dominant for organizations are: political and architectural.

Political decentralization defines how many different human entities are in control of the system. It applies to decision making. We use the word human entity to describe: individuals or organized groups of people that have a single voice. Notice how the group of people is an organization itself and whether it is decentralized or not will have an impact on the decentralization of the organization it is active in.

Architectural decentralization defines to which extend the logistical part of the organization is decentralized. This relates to the more physical aspect. How inter-connected are the decision makers of an enterprise? Under which conditions do they interact? Is the data center of an enterprise in one place, or smartly split amongst many? How independent is each (human or electronic) entity, i.e. can the fall of one cause the fall of the others?

Discussion

As an example of entity that architecturally exercises a lot of power, though it does not have any politically, consider the diplomat. In practice, a diplomat has the power to speak in name of its country. However, politically he is not allowed to make any decisions, he should only work as a transmitter.

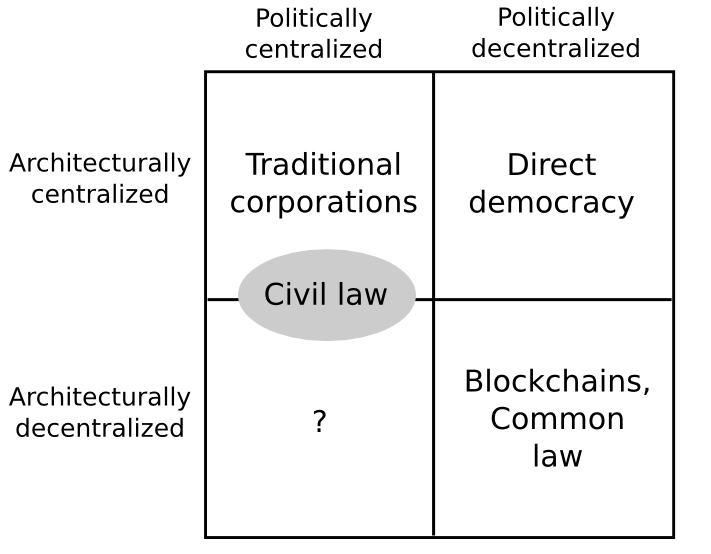
This does raise a question: On the long term, does decentralization on one axis, affect the decentralization of the other one?

-Politics can obviously influence the architecture. In fact, they can set the objective towards which it will tend. Nevertheless, they will be limited by physical and technological constraints. They don’t have unlimited influence for that matter.

-In the reverse direction, the architectural placement of power can also strongly influence the political placement of power.

As an enlightening example consider the case that *Timothy Mitchell* makes in Carbon Democracy: political power in the age of oil[[1]](#footnote-1). This book explores the inter-connected history of fossil fuels and modern democracy. The point that is interesting for the discussion at hand is: the materiality of our primal source of energy has had a huge impact on the localization of power. Amongst other factors, the extraction and transport of coal gave birth to a working class with a strategical asset, which ‘provided the means for assembling effective democratic claims’ (p8). With the switch to oil, the extraction went from miners to oil rigs, the transport from crewed trains and ships to pipelines. This took away the strategical asset of the working class and undermined its political power in the long term.

Now let’s look at what different organization could exist from these two axes of analysis. Vitalik Buterin provides an interesting table[[2]](#footnote-2) for this very purpose:



We would argue that Blockchains are indeed architecturally decentralized but not per definition politically decentralized. Strong and popular examples of politically centralized blockchain applications are Ripple[[3]](#footnote-3), and Tether[[4]](#footnote-4). We will develop on the case of Ripple later.

Vitalik Buterin also point to a third important axis of decentralization.

-Logical decentralization: “Does the interface and data structures that the system presents and maintain look more like a single monolithic object, or an anmorphous swarm?”. Does it act, in all its interactions, as a single entity? A regular peer-to-peer platform such as BitTorrent does not follow this rule. However, a blockchain based platform such as Bitcoin does. In fact, this relies on the revolutionary aspect of blockchain technology: the ability to keep a unique ledger on a decentralized platform.

**Autonomous:** An organization is considered autonomous if it is self-governing / independent. Let’s consider autonomy in all its possible dimensions.

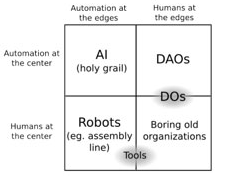
Governance autonomy: In geopolitics this applies to the right of countries to govern themselves, without any input from external powers. It refers to sovereignty. For a legislator, having institutional autonomy means “to be able to implant and pursue official goals”. It is in fact a delegated form of governance. A lower level of delegated governance is the use of legally binding contracts. Many, if not all institutions rely on such contracts. This permits governance within the institution. Though this will be developed later, it is interesting to briefly mention smart contracts. Smart contracts, as first developed on Ethereum, have no legal weight. They can be signed without the involved parties revealing their identities. Nevertheless, they are ‘binding’ contracts. Once signed, there is no canceling them except with the pre-established modalities. Instead of the regular jurisdictional system enforcing it, it is the agreed upon code and the Blockchain it relies on that does.

Physical autonomy: The ability to be physically autonomous is equivalent to the ability to perdure independently. Living organisms naturally possess this ability. Dead organisms rarely posses this ability, and if they do it is in a more restricted environment. Typically, let’s consider autonomous robots. To be considered physically autonomous, the robot would at the very least need to be unmanned and disconnected from outside commands. Important aspects for such robots are: environment sensing, autonomous navigation, self-maintenance and, if aimed for long term, energy foraging.

Mind autonomy Autonomy as the capacity to make decision through one’s own independence of mind. How to define and measure this type of autonomy has often been debated amongst philosophers. It is generally accepted that all human beings possess this autonomy. Applying this to a non-human being is more contentious. If we consider a physically autonomous robot, whether the decisions it takes are pre-programmed and thus delayed commands, or actual autonomous decisions, is up for debate. Programs, such as chatbots, are able to fool human beings into believing they are interacting with another human being. Recent advances in artificial intelligence gave birth to programs that are fundamentally more capable than chatbots. Nevertheless, these systems do not go beyond the scope of what they were programmed to do, because of this they cannot easily qualify for mind autonomy.

Discussion

Once again, Vitalik Buterin provides a very interesting table distinguishing organizational models on two of the above defines axes.



What Vitalik Buterin defined as automation at the center is what we have defined as governance autonomy. And what he has defined as automation at the edges is what we have defined as physical autonomy.

-A regular organization fully relies on humans for its operations and governance.

-A DAO uses smart contracts to enforce laws within its organization. It is able to have its own legislation and enforce it. This makes it a self-governing entity. Note that is easier to be self-governing when confined within the space of the digital world. Even more so when done in an automated manner. Indeed, DAOs enforce their law automatically. In regular jurisdictions, if a contract is breached, the offended party can rely on higher institutions such as the state to handle the case. For smart contracts, which can be signed anonymously, this is not possible. Instead the smart contract imposes the condition the agreed upon code states. If not careful a priori, an offended party cannot rely on the common sense of a human jury. A priori, there is room for flexibility though. In fact, a new jurisdiction can be defined for every smart contract. For example, a hand-picked jury can be predefined in the contract in case a litigation arises. Nevertheless, the code will (almost) always be enforced in a sovereign manner. The biggest smart-contract abuse to date is The-DAO hack[[5]](#footnote-5). Though called a hack, this is does not correspond to a hack in the traditional way. The smart-contract in question has not been hacked, but common sense says it has been abused. This raised an interesting debate as to whether a smart-contract could stay sovereign even if opposing the view of a clear majority of involved individuals. This lead to a division in the community and finally in the affected blockchain: To cancel the ‘hack’ a hard-fork was performed in July 2016. Since not the whole community agreed on this hard-fork, the blockchain split into two different chains. Here[[6]](#footnote-6) are more details on hard-forking and chain-splitting. Though this was the first chain-split on a major blockchain, there has since been two chain-splits on the Bitcoin Blockchain.

Physically it is far from autonomous. As any web-based platform it relies on a physical support and is unable to sustain it independently. However, its decentralized architecture makes it more resilient, it has no single point of failure.

-A certain category of robots is able to autonomously interact with the outside world. As mentioned previously, this will usually be restricted to the scope of their intended application. For example, an automated lawn mower will be able to explore its flat field, avoid obstacles, perform its duty, and navigate to its charging station when needed. An example corresponding more to an organization is that of autonomous power plants. Its implications were first discussed in The Human Use of Human Beings[[7]](#footnote-7) by *Nobert Wiener*, along with the implications of self-regulated mechanisms as whole. Norbert Wiener has given the name ‘cybernetics’ to this field of study. Indeed, power plants are an interesting case because they are easily energetically independent. Such power plants are physically independent to the point that they could continue functioning even if abandoned by human beings.

However, they are not self-governed: they are not politically independent and are unable to enforce rules. It is just a tool used within a bigger institution.

-Lastly Buterin, defines the artificial intelligence holy grail as a combination of governance autonomy and physical autonomy.

Internet-based systems exist in a dimension that is so distinct from geographical sovereignties, that many applications are not affected by any pre-existing regulation and may act as if independent.

DAOs have barely or no official recognition[[8]](#footnote-8). Nevertheless, law is applied within the organization in a sovereign manner. Every example of DAO has a method to make binding contracts. Though these contracts are more than often not legally applicable, they do share many characteristics with their legal counterparts. Indeed, they are contracts in the sense that once signed, there is no canceling them except with the pre-established modalities. This aspect will be developed in detail later.

1. https://nycstandswithstandingrock.files.wordpress.com/2016/10/mitchell-2013.pdf [↑](#footnote-ref-1)
2. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 [↑](#footnote-ref-2)
3. https://ripple.com/files/ripple\_consensus\_whitepaper.pdf [↑](#footnote-ref-3)
4. https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf [↑](#footnote-ref-4)
5. https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ [↑](#footnote-ref-5)
6. https://lightco.in/2017/07/30/bitcoin-fork-split/ [↑](#footnote-ref-6)
7. https://monoskop.org/images/5/51/Wiener\_Norbert\_The\_Human\_Use\_of\_Human\_Beings.pdf [↑](#footnote-ref-7)
8. <https://cointelegraph.com/news/forewarned-is-forearmed-key-takeaways-from-sec-dao-report> [↑](#footnote-ref-8)