INPUT | OUTPUT

IOHK | BLOG

SOME HISTORY, SOME MUSINGS AND MY TAKE ON THE DAO

JANUARY 12, 2016 CHARLES HOSKINSON 12 MIN READ

I recall the mid-summer Virginia afternoon back in 2013 being filled with copious conversations ranging from how to achieve value stability for a cryptocurrency to this strange idea Stan Larimer had called a DAC - a decentralized autonomous company. His drafts contained terms like Steely Eyed Geeks and a nice list of rules definitely inspired by Arthur C Clarke and Isaac Asimov, but with the boyish enthusiasm only Stan could muster. The article (Bitcoin and the Three Laws of Robotics) eventually found its way to Bitcoin Magazine and the Let's Talk Bitcoin's blog as well as Vitalik's September series (1).

I'd like to believe that we were all after the same goal in those more innocent and lower stakes days. All cryptocurrencies, and protocols for that matter, suffer from a fundamental meta problem of governance. Eventually changes will need to be made to accommodate some unforeseen complication, the burning march of ever changing technology and social pressures, or even a black swan event. Furthermore, how do you pay the selfless (sometimes not so much) people who are maintaining the protocol? How do you balance the different interests of various stakeholders from regulators to service providers such as exchanges and miners.

The foundational premise of Bitcoin can be encapsulated succinctly as people suck so just trust a protocol. This line of thought has lead to numerous problems from a lack of recourse for theft (see MtGox and the dozen other exchanges) to dark market operators such as silk road using Bitcoin as their payment network. Furthermore, the rewards to miners are not connected to any external reality- just hard locked and unresponsive to the needs of the network. The protocol marches on like a silent, yet diligent sentinel uncaring in judgement, but utterly fair.

We were interested in DACs because the sentinel needs some method of getting an update and if one appointed a centralized body or even a federated one, then one has completely defeated the ultimate purpose of these systems. With more time given for clarity, when one abstracts the idea, one can notice that most businesses are a collection of systems that decompose into protocols. Thus, it stands to reason they too can be transformed into sentinels and if only we had a DAC, then they too could be fair, yet dynamic. Hence, DAOs were born.

Back in 2013, we didn't have Ethereum. Sergio Lerner had created a wonderful turing complete system

intended for gaming called Qixcoin, but it wasn't well known or funded. Thus, DAOs didn't have the requisite technology nor a clear commercial path forward. Yet with the dawn of the crowdsale and Ethereum as a platform, this reality has changed.

Now up to this point, it is reasonable to assess what progress has been made. The existence of the crowdsale our space has been using for the last few years has created a funding mechanism for all kinds of interesting projects ranging from Maidsafe to Swarm. Whether these produce utility or are attractive places to store value is yet mostly unproven; however, it's truly amazing to see the amount of passion and enthusiasm. Of course, never forget that people suck so yes a lot of fraud seems to be seeping in (See Hoskinson Doctrine).

Ethereum has created a way of deploying distributed protocols with a host network that has known and probably strong security guarantees about the execution of the code. Whether this system can be made secure under some reasonable formal model and associated proofs and also made efficient is another story. Yet we should at least concede that it's a pretty fun sandbox to run experiments.

The DAO is one such experiment, which brings us to the ultimate point of this article. Slock.it and their affiliates apparently wanted to create a large pool of capital that could be used to fund interesting projects (sound like any type of structure you could think of?), but make the pool a sentinel without a master. Just some helpful curators and the Ethereum network's guarantees behind it.

Ideally, a Surowiecki utopian wisdom would envelope the DAO making it the smartest way to allocate capital or something along those lines. To be honest, I mostly ignored the original proposal thinking that people wouldn't invest much time or money into it.

Common sense seems to yield a litany of concerns from the fidelity of the code controlling this concept to the creator's utter unwillingness to stand behind the DAO from a legal sense. If something goes wrong, then no one is responsible? Do we have sufficient faith in our ability to do things perfectly right the first time that we are willing to invest in a blameless system? Imagine if planes worked this way. Would you fly?

Furthermore, there was a reckless desire to maximize the size of the fundraiser without any concern to factors everyone should be wary of in some capacity. Why wasn't the DAO milestoned with the majority of the funds stored in a large multi-signature feeder contract that gradually released money into the main fund given progress and investment success? Who was responsible for maintaining, upgrading and auditing the code long term? What metrics should the DAO be held accountable for over the long term? Apparently, having a dream team means that we should abandon basic due diligence and the ability to imagine bad events happening. Does anyone recall a certain other company called Theranos?

So now we are faced with the predictable nightmare scenario only yielded from grand hubristic endeavors such as the unsinkable titanic. The DAO has been looted by a hacker who potentially has enough pithy gall to claim that the theft actually conforms to the DAO's terms and conditions. Lawyers, please bookmark everything you find on Tual and his friends. This class action lawsuit is writing itself.

So why should Ethereum care? The point of the system is to be a sandbox for ideas to succeed or fail. It's a lab for experiments. That's why Ethereum is worth so much money as a system. Following this line of thought, Ethereum SHOULDN'T CARE.

You don't change the lab when someone performs a poorly formed experiment. You blame the chemist and move on. We can make a fair argument for better safety equipment (which has already been proposed), but you don't change the nature of a facility to accommodate someone who screwed up.

Yet Vitalik and others close to the Ethereum Foundation are advocating to do just that. They want to fork the protocol in order to prevent the theft. Bruce Fenton and others have already done a good job explaining why this proposal is an extremely bad idea. It's pointless to add another argument to the pile. Rather I'd like to take this opportunity to explain what has really failed in the Ethereum ecosystem. It has a governance problem.

Several of the Founders have scattered across the seven seas and created new commercial ventures ranging from Consensys to Ethcore. Each has its own blend of fiduciary obligations depending upon their investors

and stakeholders, yet these are not directly aligned to the needs of the Ethereum ecosystem. The closest thing Ethereum should have to a neutral body ought to be the Foundation.

You know those bodies that don't pick winners and losers and try to just protect the protocol itself? Except for the time when its leaders join multiple ventures, plaster their name everywhere and seem to have a very comfortable relationship with companies like Deloitte and Microsoft for "Projects".

Yes helping the DAO investors get their money back is a noble knee jerk reaction. But what about Gatecoin and the theft that occurred there? What about the ether purchasers who experienced an event that prevented them from redeeming their ether they fairly purchased? What about all the ether lost to defective smart contracts? DAO gets precedence, yet the others don't? Is this because its failure would invite regulatory scrutiny to the Foundation members as they have too close a relationship to it?

Returning to the core thesis of bitcoin and its children - people suck; trust the protocol - applied to the bailout of the DAO, we have people who are trusted to be neutral who cannot be due to whatever obligations that have encumbered upon themselves. As we should expect given human nature. They now want to change the protocol to prevent in part personal harm to themselves given the damage the DAO has done.

The argument of wanting to help cannot be sensibly made given their lack of interest in the other thefts and bad events in the system. I honestly can't fault them for this behavior, but I have to point out how dangerous this act is for sentinel that is the Ethereum protocol.

Stan Larimer had the foresight to imagine events like this occurring, which is why he wrote his article. The ethereum community needs to embrace this tragedy and accept it as a failure we can learn from. We need a DAO, but not one to store money to make some investors rich. We need one to help us make these kinds of hard decisions in a responsible way.

Ethereum is the first platform in human history that can transcend this predictable cycle of betrayal of integrity for person preservation and emerge into something far better. It won't be nice. It won't be kind. But It will be fair. That ultimately is why I signed up for this wild space. To build something beyond our nature, yet always accepting- sometimes painfully so- it won't always work out for me.