Emily Lemmerman*

08・23・2016

Lessons Learned from theDAO Project: The Future of Regulating Blockchain

1. Timeline

TheDAO is a DAO (Decentralized Autonomous Organization) set up by German IoT + blockchain company Slock.it with ties to the Ethereum Foundation. TheDAO is code that runs on the Ethereum blockchain, the largest among other decentralized apps (dapps) and transactions that run on the Ethereum blockchain, a public blockchain. It began collecting funds in April 2016, and had US$100 million by May 15, 2016, and $150 million by June 2016. TheDAO is the largest crowdfunding in history, raising over $150 million from more than 11,000 members.[i] As one of the first decentralized autonomous organizations to date, the outcomes of the theDAO project hold significance for the future of DAOs, the decentralized web, and the much-hyped blockchain.

Even in its' early stages, security vulnerabilities of theDAO were raised, particularly because of its' enormous amount of funding. A temporary moratorium on the DAO was being considered as early as May 7, 2016, due to security issues, as advised by Cornell computer science professor Gun Emin Turer and Vlad Zamfir of the Ethereum Foundation.[ii] In response to these concerns, Slock.it and other developers revised the code of theDAO, and claimed by Jun 12, 2016, that they had resolved the vulnerabilities.[iii]

On June 17th, an unknown attacker took advantage of a security issue, related, but not identical to the one raised by Turer, putting 3.6 million ether, worth approximately US$50 million at the time, into 'child DAOs', inaccessible to the rest of the tokenholders of the DAO. The attacker, by means of the way that the DAO is set up, does not have access to the contents of the child DAO for 28 days after the creation of the child DAO, which falls on the 14th of July. The bug, or vulnerability, allowed the attacker to repeatedly call the split() function within the DAO, which moves funds to a childDAO, without updating the attacker's balance, meaning that more funds than the

* Emily Lemmerman
Intern, Nippon Institute for Research Advancement (NIRA)
/BA Candidate, Stanford University

attacker should have had the rights to were transferred into a childDAO controlled by the attacker.

2. Response to the heist

In response to the attack, Slock.it and the Ethereum community initially considered three options: to either do nothing, allowing the ether to go to the attacker, to “soft fork” the Ethereum blockchain, thus blacklisting the wallet address of the attacker, or to “hard fork” the blockchain, returning the ether to those from whom it had been taken, by returning to a place in the blockchain before the attack, and continuing the Ethereum blockchain from that point. Hard forking the Ethereum blockchain affects not only token holders of the DAO, but also the users of ether, the Ethereum currency, and users of other decentralized apps that run on Ethereum. However, in part because the community of Ethereum users is small, and because many of these users hold DAO tokens, in this particular case, members of theDAO as an entity that exists on the Ethereum blockchain was taken to approximately represent the community of Ethereum users.

Professor Gun Emin Turer, among others, revealed a security vulnerability that the soft fork would pose on June 28th, thus making the decision one of simply to hard fork, or to do nothing.

The decision whether to hard fork, or to do nothing at all, was extremely contentious, and revealed the differences within the community of Lawrence Lessig’s famous phrase, “code is law.” Essentially, the debate is whether the “intention of the code” should prevail over the “wording of the code,” as it does in our current legal system, governed by interpretation.[iv] Those against the hard fork take the phrase “code is law” at face value- taking it to mean that code should be followed as law, while on the other hand, those in favor of the hard fork take the phrase to mean that computer code is subject to the same interpretation as law, and is affected by other regulators identified by Lessig as “Norms, Market and Architecture.”

The fundamental argument against a hard fork is that allowing changes to the blockchain, even by consensus, would go against the fundamental purpose of the

blockchain, to exist as an immutable, decentralized entity. Some prominent voices, including Cornell professor Gun Turer, Ethereum Foundation lead designer Alex van de Sande, and Bitcoin Core developer Peter Todd, are of this opinion.

On the other hand, the Slock.it team, was very pro- hard fork, as was the result of a vote taken of theDAO token holders. Martin Koppelman, Ethereum developer, wrote that "forks are part of the ecosystem," going further even to say that MtGox could have been prevented with one simple hard fork, or rolling back of the blockchain.[v] Vitalik Buterin, founder of Ethereum, has also made similar remarks justifying the hard fork, saying that the decision would have "no consequences for decentralization" because it arose from the community. Furthermore, he has stated that it is an exception that the cryptocurrency community will learn from because Ethereum and DAOs are in their infancy. [vi] Either way, the theDAO hard fork does raise a question: who decides what is a crime, and what is not a crime, and when the community is allowed to go against the purpose of blockchain to "undo" a crime?

The Ethereum Foundation and Slock.it developers' support for the hard fork was seen as selfish, as many thought that they owned a large amount of ether, and thus the hard fork would be advantageous to them. However, Alex van de Sande of the Ethereum Foundation debunked this myth in response to criticism, writing that Foundation members were not among the greatest tokenholders of theDAO by any means—Vitalik Buterin, founder of Ethereum, had 1500 ETH in theDAO, less than .3% of his ETH holdings, and most Ethereum developers had no ETH in theDAO.

On July 20th, at UTC 14:30 (approximately 11:30pm Tokyo time), the hard fork, implemented by Slock.it developers, as well as many in the Ethereum community, was completed.

3. Responses to the hard fork

After the hard fork, there are 2 versions of the Ethereum blockchain, allowing users to update and "adopt the fork," or move to the new blockchain, or not. Eventually, the idea is that the updated blockchain will take over, because users will stop using the old blockchain.[vii] The code of theDAO has been changed, so that token holders are now only able to withdraw funds, and the fundraising and investing aspects of theDAO are on hold.

A movement sprung up on July 21st to maintain the old blockchain, and to not adopt the hard fork, called “Ethereum Classic.” The idea to stay on the old blockchain began on Russian language forums, but has taken off. Even though the developers at Slock.it claim that there was a clear majority vote for the hard fork by theDAO token holders, those at Ethereum Classic are claiming that there are up to 40% of Ethereum users who disagree with the hard fork. (Note that the hard fork affects all Ethereum users, not only those who own theDAO tokens- it is unclear how much of the Ethereum community at large agrees with the hard fork.)[viii] Vitalik Buterin, inventor of Ethereum, points to the fact that 85% of miners have switched to mining on the new Ethereum blockchain as proof that the community agrees. On the other hand, some Ethereum users do not think that miners are a good representation of the Ethereum community, because the 3 largest Ethereum mining pools, similarly to Bitcoin, control more than 60% of Ethereum mining.

Those at Ethereum Classic have identified as being “radical Crypto-decentralists.” They ask why the community cannot simply block addresses that they arbitrarily select as being “criminal,” if they are willing to hard fork in this situation. (ie. Should the Silk Road and similar services be blacklisted? Should the Bitcoin blockchain have been hard forked after MtGox?).

On a broader level, responses to both Ethereum and Ethereum Classic can be gauged by their market value. Previous to the incident, the ETH to USD exchange was $18.28. Immediately after the incident, ETH’s value dropped to US$11.50. Following the success of the hard fork, it rose to $12.50. While the currency was up to $13.70 by the 29th, it has since then weakened, dropping to $8.30 following the August 2nd US$65 million Bitfinex hack. Ethereum classic (the non-forked blockchain) is now at $2.70. Many, including Vitalik Buterin stressed that the main reason that the hard fork was carried out was in order to protect Ethereum, and Ether, given that theDAO was such a large part of the Ethereum blockchain. It remains to be seen whether ether will make a full recovery.

4. Outside opinions on theDAO incident

The Securities Exchange Commission (SEC) on theDAO

According to Gary Goldsholle, deputy director of the SEC’s trading and markets division, theDAO incident “highlights a number of concerns that are really core to the

SEC's role, which is not only issues of disclosure, investor protection," but also includes "the technology and the systems that underpin the markets." However, he also says that he "[doesn't] have concerns at this point. I think it's a little premature to really start to identify shortcomings or other issues," he said. "We are very broadly supportive of innovation in technology and are eagerly engaging partners."[ix]

KPMG on theDAO incident

US blockchain lead for international accounting firm KPMG, Eamonn Maguire, claims that clients are not seeing the incident as an impediment to the progress of blockchain as a whole, describing the incident as a 'hiccup'.[x]

Australian Corporate Law Firm Gilbert + Tobin

2 partners at Australian corporate law firm Gilbert + Tobin responded to the DAO heist by insisting that "decentralized networks need governance like every state needs a government." However, they offer no solution, and it remains to be seen whether a better solution to blockchain governance than the voting and collaboration seen in theDAO incident has emerged.

Primavera de Filippi (Blockchain legal expert at Berkman Klein Center at Harvard Law School)

According to de Filippi, there is no such thing as a "trustless network": in fact, the functioning of Ethereum and other blockchains depends on the trust that users of the network have in each other (including miners, developers, and other users) to actively participate in the maintenance and upkeep of the blockchain. De Filippi identifies the opposition to the hard fork as a blind, rigid commitment to the vision of blockchain as "immutable." She emphasizes that while decentralization is important, and can be carried out by the blockchain, "*social organizations cannot be ruled only and exclusively by code.*"[xi] Thus, she is calling on regulators and the cryptocurrency community to develop alternate methods of thinking about social and legal contracts surrounding uses of blockchain.

5. In Conclusion

Should blockchains be hard forked, for reasons besides routine updates or fixing security vulnerabilities? Who decides for which reasons blockchains can be hard

forked? What are the other factors (Architecture, Norms, Market) as identified by Lawrence Lessig that shape how regulation works, if we consider computer code as legal code (law)? The development of democratic and legal structures for blockchain becomes more critical the less that centralized entities are able to prosecute bad actors, but perhaps also opens the door to a more malleable social contract. However, it is important to note that this hard fork of the Ethereum blockchain was only possible under the very specific circumstances seen here, and that similar responses would not always be possible given a bad actor, which begs the question of what would happen in such a situation.

Taking from both Lessig and de Filippi, if code is not our only basis upon which to make decisions, what fair, decentralized ways can we innovate to regulate smart contracts and the blockchain? In the case of theDAO and Slock.it, users' "votes" were taken both through many users contributing open-source development, miners and users deciding to switch to the new blockchain, and a vote for DAO token holders, based on the amount of tokens they held. It is clearly under heavy scrutiny whether these methods of gauging Ethereum users' opinions was sufficient. However, regardless of whether the system accurately gauged majority opinion, the results of the hard fork and the emergence of Ethereum Classic point to a classic problem of democracy: tyranny of the majority. Christopher Jentzsch of Slock.it celebrated the community in the case of theDAO incident by saying that it acted as the "Supreme Court": what exactly does this mean?

One central problem seems to be that consensus, or unanimous agreement, is not fully achieved by the way blockchains exist now (ie. because of the centralization of mining pools, because of electricity costs, as well as the reality being that not all users of a system will want, or be able to contribute code, but would instead prefer to contribute their opinion in other ways.) It is critical to work to improve both computer, legal, and social codes among users of decentralized technologies to solve this issue. Perhaps Ethereum's switch from proof-of-work to proof-of-stake will help resolve mining centralization—but the other issues remain, of developing systems which can develop consensus without tyranny of the majority. If the means of dissent is not to accept a mainstream fork (a la Ethereum Classic), can this be considered a decision that is free from "mob mentality", or is this an inherent part of group decision-making?

---

[i] https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e993#.t25yu9hb7

[ii] https://dao.consider.it/temporary-moratorium-on-the-dao-security-issues?results=true

[iii]https://blog.slock.it/no-dao-funds-at-risk-following-the-ethereum-smart-contract-recursive-call-bug-discovery-29f482d348b#.z0ozu15di

[iv] http://motherboard.vice.com/read/thedao

[v] https://twitter.com/koeppelmann/status/750151861471092736

[vi] http://www.ibtimes.co.uk/ethereums-vitalik-buterin-democratic-hard-fork-proves-mining-oligopoly-cannot-engage-censorship-1569079

[vii]http://blogs.wsj.com/moneybeat/2016/07/20/ethereum-gets-its-hard-fork-and-the-truth-gets-tested/

[viii] http://ethereumclassic.github.io

[ix] http://www.wsj.com/articles/sec-official-says-ethereum-hack-illustrates-blockchain-concerns-1466459986

[x] http://www.coindesk.com/kpmg-dao-failure-private-blockchain-progress/

[xi] http://motherboard.vice.com/read/thedao