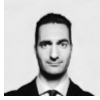
The Story of the DAO — Its History and Consequences

medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

Samuel Falkon

August 12, 2018



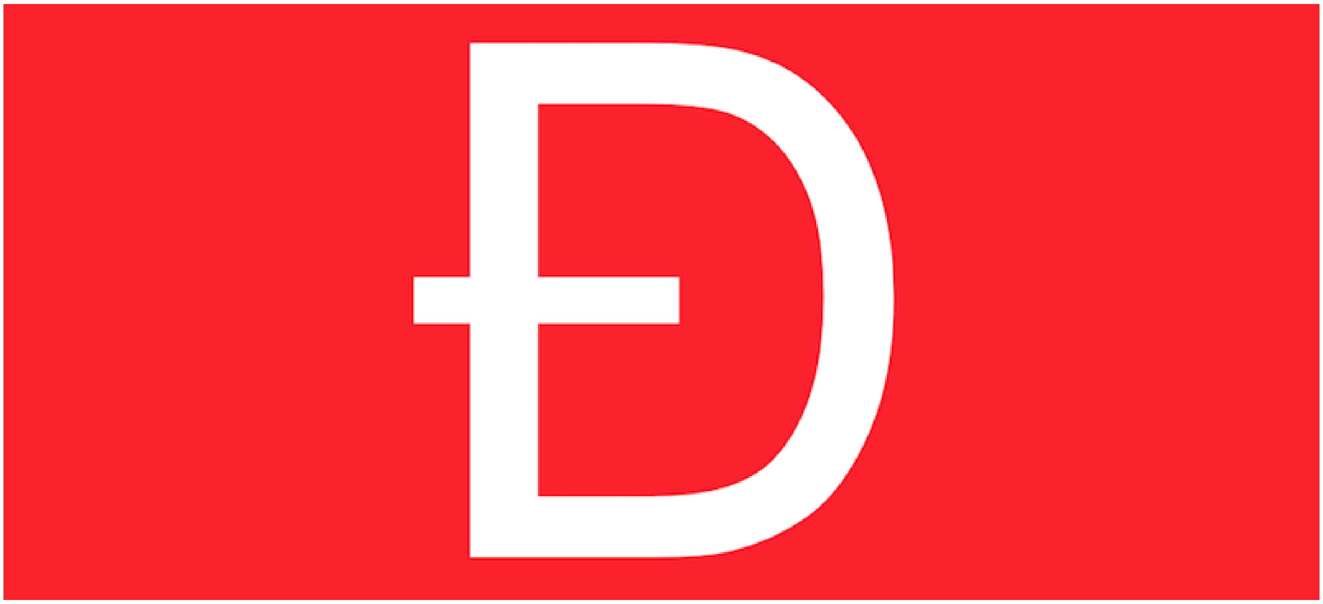
Samuel Falkon

Dec 24, 2017

·

5 min read

·



One of the most incredible concepts to be successfully implemented through blockchain technology is the DAO, a decentralized autonomous organization. Decentralized autonomous organizations are entities that operate through smart contracts. Its financial transactions and rules are encoded on a blockchain, effectively removing the need for a central governing authority — hence the descriptors “decentralized” and “autonomous.”

The Decentralized Autonomous Organization (known as The DAO) was meant to operate like a venture capital fund for the crypto and decentralized space. The lack of a centralized authority reduced costs and in theory provides more control and access to the investors.

At the beginning of May 2016, a few members of the Ethereum community announced the inception of The DAO, which was also known as Genesis DAO. It was built as a smart contract on the Ethereum blockchain. The coding framework was developed open source by the Slock.It team but it was deployed under “The DAO” name by members of the Ethereum community. The DAO had a creation period during which anyone was allowed to send Ether to a unique wallet address in exchange for DAO tokens on a 1–100 scale. The creation period was an unexpected success as it managed to gather 12.7M Ether (worth around $150M at the time), making it the biggest crowdfund ever. At some point, when Ether was trading at $20, the total Ether from The DAO was worth over $250 million.

In essence, the platform would allow anyone with a project to pitch their idea to the community and potentially receive funding from The DAO. Anyone with DAO tokens could vote on plans, and would then receive rewards if the projects turned a profit. With the financing in place, things were looking up.

The DAO’s Great Start Gone Wrong

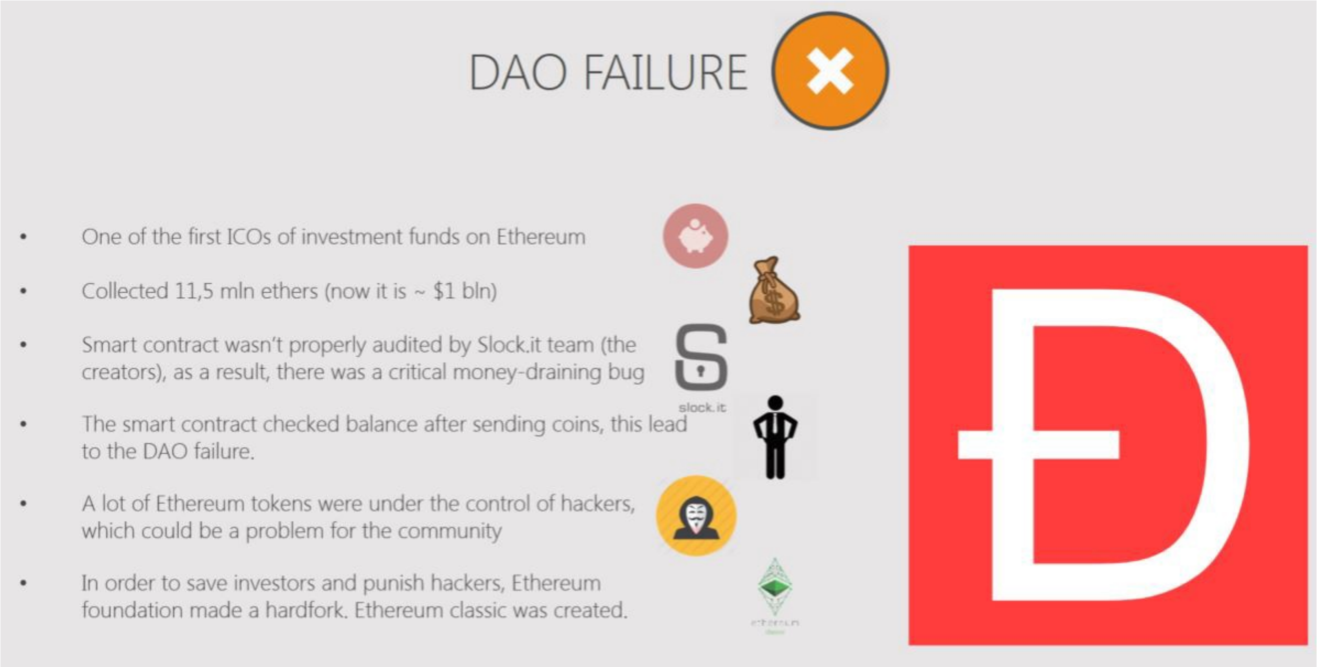
However, on June 17, 2016, a hacker found a loophole in the coding that allowed him to drain funds from The DAO. In the first few hours of the attack, 3.6 million ETH were stolen, the equivalent of $70 million at the time. Once the hacker had done the damage he intended, he withdrew the attack.

In this exploit, the attacker was able to “ask” the smart contract (DAO) to give the Ether back multiple times before the smart contract could update its balance. Two main issues made this possible: the fact that when the DAO smart contract was created the coders did not take into account the possibility of a recursive call and the fact that the smart contract first sent the ETH funds and then updated the internal token balance.

It’s important to understand that this bug did not come from Ethereum itself, but from this one application that was built on Ethereum. The code written for The DAO had multiple flaws, and the recursive call exploit was one of them. Another way to look at this situation is to compare

Ethereum to the Internet and any application based on Ethereum to a website — If a site is not working, it doesn’t mean that the Internet is not working, it merely says that one website has a problem. The hacker stopped draining The DAO for unknown reasons, even though he could have continued to do so. The Ethereum community and team quickly took control of the situation and presented multiple proposals to deal with the exploit.

However, the funds were placed into an account subject to a 28 day holding period so the hacker couldn’t complete his getaway. To refund the lost money, Ethereum hard forked to send the hacked funds to an account available to the original owners. The token owners were given an exchange rate of 1 ETH to 100 DAO tokens, the same rate as the initial offering.



DAO FAILURE

- One of the first ICOs of investment funds on Ethereum
- Collected 11,5 mln ethers (now it is ~ $1 bln)
- Smart contract wasn’t properly audited by Slock.it team (the creators), as a result, there was a critical money-draining bug
- The smart contract checked balance after sending coins, this lead to the DAO failure.
- A lot of Ethereum tokens were under the control of hackers, which could be a problem for the community
- In order to save investors and punish hackers, Ethereum foundation made a hardfork. Ethereum classic was created.

Unsurprisingly, the hack was the beginning of the end for the DAO. The hack itself was contested by many Ethereum users, who argued that the hard fork violated the basic tenets of blockchain technology. To make matters worse, on September 5, 2016, the cryptocurrency exchange Poloniex delisted DAO tokens, with Kraken doing the same in December 2016.

All of these issues pale in comparison to the United States Securities and Exchange Commision (SEC) ruling that was released on July 25, 2017. This report stated:

“Tokens offered and sold by a “virtual” organization known as “The DAO” were securities and therefore subject to the federal securities laws. The Report confirms that issuers of the distributed ledger or blockchain technology-based securities must register offers and sales of such securities unless a valid exemption applies. Those participating in unregistered offerings also may be liable for violations of the securities laws."

In other words, The DAO's offering was subject to the same regulatory principles of companies undergoing the initial public offering process. According to the SEC, The DAO violated federal securities laws, along with all of its investors.

The Ongoing Impact of The DAO's Rise and Fall

Though The DAO project has since folded, its impact is ongoing. Current blockchain development teams continually looked to The DAO's example for guidance — for what not to do.

First, The DAO teaches a valuable lesson about the importance of establishing secure blockchain platforms. The DAO's hack was not due to a problem inherent on the Ethereum blockchain; it came from a coding loophole exploited by an intelligent hacker. Had the code been written correctly, the hack could have been avoided.

Second, the SEC's ruling on The DAO has encouraged blockchain startups to come up with ways of avoiding security registration and federal regulation. One of the ways companies do this is by using the SAFT method. If tokens have legitimate utilitarian value on a blockchain platform, they violate a component of the Howey case, and therefore cannot be listed as securities or regulated by the SEC.

Without the DAO, who knows what lessons would still need to be taught.

This story is published in The Startup, Medium’s largest entrepreneurship publication followed by 298,432+ people.

Subscribe to receive our top stories here.
