

The Ethereum DAO (Distributed Autonomous Organization) was supposed to be an innovative and exciting new organization. The first corporation with NO legal paperwork, where all shareholders have say equal to their share of the company decided by how many DAO tokens they held (think stocks). When the DAO was first released and offered their DAO tokens for sale, they raised 150 million dollars, making it the largest crowdfunding project EVER. Optimism was high, and they promised to make smart investments to grow the organization ever faster. But like all things in the world, when something seems too good to be true, it probably is.

On June 17th, 2016 it all came crashing down to the ground, with a hack of the DAO. Ever since the start, there were warnings of a weak code to protect the funds of the DAO and it was finally exploited by a hacker who stole 3.6 million Ethereum (valued at 60 million dollars at that time), funneling it into a series of smart contracts dubbed a "child DAO". People were shocked as the news slowly made its way through Reddit. The good thing for the community was that the funds were not withdrawable for a certain amount, giving them time to act. However, the minute the hack was reported, ETH crashed all the way to an abysmal 13 dollars from a previous 20 dollar price (Many people suspect that the hacker pulled a large short on Ethereum and made his money that way).

After the event, the community split into 3 factions. The no action community wanted to leave the blockchain and not mess with the funds that were hacked. The soft fork community wanted to reverse the transaction through a "soft fork". A blockchain is built off of many nodes who organize all transactions into blocks, which are sequenced into a chain. (Hence the term blockchain). When 2 conflicting transactions happen, the blockchain automatically rejects one. The soft fork would write a transaction that would make any transactions out of the DAO invalid. No other blocks would be affected and life would go on as normal. However, all cryptocurrencies are based off the fact that something like this could NOT happen! If the miners could reverse a transaction, the public's trust in the blockchain would reduce dramatically. As one person put it: "I made a bad contract in the first days ETH was online and lost 2K ETH with it, can I also get it back? Thanks!" On top of this, after the soft fork was proposed, the hacker said this with a signed message from the address to which the stolen funds were sent to: "Soon we will have a smart contract to reward miners who oppose the soft fork and mines the transaction. 1m ETH + 100 BTC will be shared with miners." While many were surprised by this blatant statement, it showed how serious the situation was, with millions of dollars at stake.

There was one last group. This group wanted something called a "hard fork". This would basically unwind the theft and put all DAO funds with only 1 purpose. To withdraw. This proposal would put an end to the DAO and let DAO token holders withdraw their Ethereum with no loss except wasted time. After heated debate, it was decided that this was the only viable way to keep the public's trust in Ethereum.

The community prepared for the hard fork with nervous anticipation. There was always the chance that something could go wrong. Then finally, on July 20th, the hard fork happened. Block

number 1,920,000 reversed the hackers withdrawal of funds from the DAO and put those funds into a smart contract that DAO token holders could withdraw from.

The aftermath of this hack was huge! More than 40 percent of funds in DAO's around the world were withdrawn. The hard fork implemented by Ethereum was also the first ever in the crypto world. Community trust in Ethereum went way down, with many cashing out ASAP leading to the price crash as I mentioned earlier. This event truly changed the system of DAO, showing how weak it really is. However, While the DAO is dead, Ethereum is recovering nicely, currently at 14.34 as of now