The biggest smart contract hacks in history or how to endanger up to US $2.2 billion

In this post we will give you a short overview of the biggest smart contract hacks and failures of the last few years.

Morisander

> ***Not so smart contracts constitute a huge problem for the crypto community***

Smart contracts like the ERC-20 token standard held digital assets worth over US $3.8 billion in 2017, and US $4.7 billion up until march in 2018 (during the three days of editing this piece another US $1.4 billlion hit the market). Unfortunately, these assets are not always as secure as we wish, as a multitude of hacks and bugs prove. This puts a significant burden on the crypto community. **Hacks discourage institutional investors and make regulators more wary of blockchain technology in general.**

A recent study with the poetic name, "Finding The Greedy, Prodigal and Suicidal Contracts at Scale" found around 3.4% of smart contracts to be faulty by only checking via an algorithm for the most common exploit possibilities. If you apply this to the total amount raised by ICO's from 2016 to now (US $8.5 billion), **US $289 million** may be at risk of being stolen or being frozen.

Top Ten ICOs of 2017

Position	Project	Total Raised
1	Hdac	$258,000,000
2	Filecoin	$257,000,000
3	EOS Stage 1	$185,000,000
4	Paragon	$183,157,275
5	Bancor	$153,000,000
6	Status	$90,000,000
7	BANKEX	$70,600,000
8	TenX	$64,000,000
9	Nebulas	$60,000,000
10	MobileGO	$53,069,235

Monthly Number of ICOs

Month	Number of ICO
Jan	7
Feb	6
Mar	5
Apr	15
May	26
Jun	21
Jul	21
Aug	21
Sep	14
Oct	19
Nov	10
Dec	45

US $3.8 billion were invested in 2017 alone

US $289 million? If this number already seems high to you, watch out for the actual amount of ether that have already been frozen or hacked in the following bugs.

1. The mother of all smart contract hacks — The DAO

Date: June 17, 2016

Price then: 3.6 million ether, US $79.6 million

Price now (March 23, 2018, only ETH): US $1.89 billion

The DAO was a decentralised venture capital fund where investments were based on votings by the community. On June 17, 2016 the DAO was attacked by unknown hackers, exploiting a combination of vulnerabilities in the DAO smart contract. The heart of the problem was that an external “call” present in a codepath that should have been possible to execute only once per stakeholder (address), was positioned before the part of the code that revoked the stakeholder’s right to trigger the codepath after first execution. This allowed the hacker to use the external call to execute the codepath recursively multiple times, thereby draining much more funds from the contract than should’ve been possible.

The exploited functionality was built in to allow users to create their own Child-DAO's in case they were unhappy with the collectives decision, even though several researchers pointed out that this functionality bears great security risks.

The hacker was able to obtain **3.6 million ether** which was valued around $50 million USD at the time of the attack. However, due to the nature of the Child-DAO's, the funds were locked for 28 days, giving the community the chance to hard fork the ethereum chain to refund the investors. This move sparked a highly controversial debate in the community. After this ideological earthquake, a lot of investors argued that the immutability of the blockchain as sacrosanct and decided to still mine on the old chain resulting in the continuation of the legacy chain as Ethereum Classic. Afterwards, the DAO was liquidated and investors were refunded on the Ethereum chain.

2. Parity - The beginning

Date: July 19, 2017

Price then: 150,000 ETH, US $30 million

Price now (March 23, 2018): US $79 million

Led by Ethereum founder Gavin Wood, the crypto startup Parity provides a range of crypto infrastructure solutions including an ETH wallet. On July 19, 2017, a bug in a multi-signature contract called wallet.sol was attacked and hackers were able to obtain **150.000 ETH**. Interestingly enough, the draining of funds was noted by a "White Hat Group" of hackers, who were able to save more than 377.000 ETH from the clutches of the attackers. This was later returned to their respective owners.

Most notably, this incident happened in spite of the fact that the code

was reviewed by a Solidity expert, as well as extensive auditing and peer review.

Apparently a restructuring of the original code, which was pushed by the team together with a UI change(written in HTML, CSS and JS), leading the Parity team to lower their review practices before merging. This shows that it is not just the code itself which needs to undergo severe auditing, but also highlights the **importance of proper deployment and review practices**.

3. Shutting down the Par(i)ty; or how to accidentally freeze US $153 Million

Screenshot from the Parity github thread

Date: November 6, 2017

Price then: 513.774 ether frozen + other currencies , US $153 million

Price now (March 23, 2018): US $269 million

> *"I accidentally killed it".*
>
> *Devops199 in the parity github*

This now infamous statement, written by a user under the pseudonym Devops199 on November 6th 2017, began the cold drama of how over US $300 million in assets were frozen. The victim: Parity's Multi-Sig smart-contract library on github.

We have already explored the details of this hack in this blog, so we will not dive into it much further here: https://medium.com/@cdurr

However, it is notable that up until now there is still no solution for the rescue or resurrection of the frozen money. Parity was initially pushing for a hard fork but now seems to back away from this solution after loud protests from the community.

4. POWH Coin — Self-destruction at its best

Developer from POWH Coin — Credits to this great article

Date: January 28th 2018

Price then: 2,000 ETH, US $2.3 million

Price now (March 23, 2018): US $1,1 million

> *"The team also repeatedly warned (and continues to warn) anyone against investing in the project."*
>
> *functionZer0 — Developer of POWH Coin*

This sketchy remark of functionZer0, one of the developers of POWH Coin, was not enough to deter people from investing into a self-sustaining pyramid scheme that paid its early users a dividend of 10%. Talking about sketchy, the developers added an even more spicy version of their contract (PoWH Coin Shadow) with a 20% dividend which broke shortly after its inauguration and caused several hundred ether to be lost. Even worse, immediately after this, a White Hat hacker found another severe bug in the original POWH Coin smart contract and posted it in the discord resulting in the total loss of **2000 Ether**. Apparently, they exploited an unsigned integer underflow, thereby enabling the hackers to withdraw an infinite number of POWH's tokens.

Conclusions

Of course there are bazillions of other hacks and bugs of cryptocurrencies, including the infamous and particularly damaging hacks of exchanges and ICOs like Mt. Gox, Bitfinex, Etherdelta, Coindash, Bitgrail etc. In these cases, however, attackers found vulnerabilities other than smart contracts, ranging from capturing domains and poor code, to blatant management errors and organizational problems. Unfortunately this situation is far more serious than POWH Coin would have you believe. Smart contract hacks and bugs significantly shape the picture of the crypto space as being immature and sketchy for investors, users, regulators and in the eyes of the general public.

If you just look at the four highlighted cases above, more than **4.2 Million ether** were already subject to hacks or bugs, making up a substantial portion of the total supply of Ethereum. The playing field continues to become more complicated. At the moment, **99% of ICOs are still happening on the Ethereum chain**. However, challenging new protocols and token standards will come to the market in 2018 (EOS, Cardano), enhancing the need for a proper auditing process of smart contracts across different chains.

The problem of faulty smart contracts is only going to expand, given the exponential growth of digital assets and their application in almost every imaginable business area. Especially in highly critical areas ranging from aviation to banking **smart contract safety is crucial**. Here, smart contracts may endanger not only investors but also have implications for whole economies.

Considering that up to 5% of all smart contracts are potentially in danger, the demand for a decentralised auditing platform, like **Solidified**, grows.