Find 3 examples where a blockchain network was attacked or hacked. Note: attacks on exchanges does not count

For each example, find and read 3 related articles and write a summary (250 words max) on how the attack happened and what was done to resolve it.

According to Lex Sokolin, the global director of fintech strategy at Autonomous Research LLP, hackers have comprised more than 14% of the Bitcoin and Ether supply[1] in less than a decade. Many of these disastrous hacks have happened due to vulnerabilities in smart contracts. Smart contracts allow the performance of credible transactions without third parties and are commonly used to facilitate transactions on the blockchain. In this assignment, I will look at 3 famous smart contract hacked examples.

1. The DAO Hack
2. Parity's Multi-signature Wallet Hack
3. Parity's User-Triggered Wallet Freeze

Hacks Example 1 – The DAO Hack
(225 words)

Brief:

A DAO is a Decentralized Autonomous Organization or an organization that is run through rules encoded as computer programs called smart contracts. Decisions are made electronically by a written computer code or through the voting of organization's members eliminating the need for documents and people governing and consequently, a system of decentralized control. The DAO was crowd-funded through token sales and raised $152 million funds.

How did the attack happen?

In this case, the DAO comprised a series of smart contracts intended to democratize how Ethereum projects were funded. A hacker, realizing a vulnerability, stole $50 million by exploiting the fallback function[2] in the code that was exposed to re-entrancy. The code was written to recursively call the split function and retrieved funds multiple times before going to the subsequent lines of code that check and confirm the updated balance.

What was done to resolve?

To recover the funds, the Ethereum founder, Vitalik Buterin and his entire Ethereum team decided that the Ethereum's codebase had to be reset through a hard fork leading to the creation of Ethereum Classic and Ethereum as 2 separate chains. Those that were not in favour of the fork argued that the core value of blockchain should be completely decentralized and immutable. Ethereum as a platform provider should not really get involved in the problems of a single developer.

Hacks Example 2 – Parity's Multi-signature Wallet Hack
(244 words)

Brief:

Parity Technologies made multi-signature (multi-sign) software "wallets" for the management of Ether cryptocurrency. An unknown hacker stole 150,000 Ethers, around $30 million at the time, by exploiting the delegatecall function[3] in the smart contract library for the multi-sig wallets. To reduce the size of each wallet and save gas, the Multi-sig wallet was split into a library contract called "WalletLibrary" and the actual "Wallet" contract consuming the library.

How did the attack happen? The attacker sent 2 transactions to each of the affected contracts. The first to InitWallet function to obtain exclusive ownership of the Multi-Sig and the second to forward all unmatched function calls using the delegatecall function to move all its funds. Unfortunately, initWallet has no checks to prevent attackers from calling it after the contract was initialized. The attacker exploited this by simply changing the contract's owners state variable to a list containing only his address. After that, it was just a matter of invoking the execute function to send all funds to an account controlled by the attacker since the attacker was then the only owner of the multi-sig account.

What was done to resolve?

Following the hack, the White Hat Group hacker quickly began to drain as many multi-sig wallets as possible to prevent the hackers from making off with any more funds while Parity Technologies worked on a fix. The group held approximately 337,000 ether in a secure wallet. A fix was released on 20 July 2017.

Hacks Example 3 – Parity User-Triggered Wallet Freeze
(252 words)

Brief:

In Nov 2017, just a few months after Parity Technologies released a fix for its multi-sig wallet issue, another issue was uncovered. It was possible to turn the Parity Wallet library contract into a regular multi-sig wallet and become the owner of it but what made the matter worst was the "new owner" subsequently wiped the account. Since "code is law" in Smart Contracts, no funds can be moved out of the multi-sig wallets making recovery of the stolen funds impossible.

How did the attack happen?

Parity disclosed that a self-proclaimed newbie by the name of devops199 become the owner of the multi-sig wallets by calling the initWallet function of the smart contract library code. The initialization function[5] affected 587 wallets and turned devops199 into the new owner of more than 513, 774.16 ETH[4]. Being a newbie and unknown to him, devops199 subsequently called the Kill function which was a self-destruct function of the code, wiping out the library code which in turn rendered all multi-sig contracts unusable since their logic was inside the library. This means that there were no funds that can be moved out of the multi-sig wallets.

What was done to resolve?

There was a discussion of whether a fork should be implemented to recover the losses. Nevertheless, it was not implemented as the community felt that what was lost should remain lost. There should not be another similar DAO-attack on Ethereum fork resulting in Ethereum and Ethereum Classic. The core value of blockchain should be preserved.

References:

[1.] Olga Kharif, “Hackers have walked off with about 14% of big digital currencies”, “https://www.bloomberg.com/news/articles/2018-01-18/hackers-have-walked-off-with-about-14-of-big-digital-currencies”, 18 Jan, 2018.

[2.] Phil Daian, “Analysis of the DAO exploit”, “https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/”, 18 Jun, 2016.

[3.] Lorenz Breidenback, Phil Daian, Ari Juels, Emin Gun Sirer, “An in-depth look at the Parity Multi-sig bug”, https://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/, 22 July, 2017.

[4.] Alyssa Hertig, “Ethereum client bug freezes user funds as fallout remains uncertain”, https://www.coindesk.com/ethereum-client-bug-freezes-user-funds-fallout-remains-uncertain, 8 Nov, 2017.

[5.] Parity Technologies, “A Postmortem on the Parity Multi-Sig library self-destruct”, https://www.parity.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/, 15 Nov, 2017.