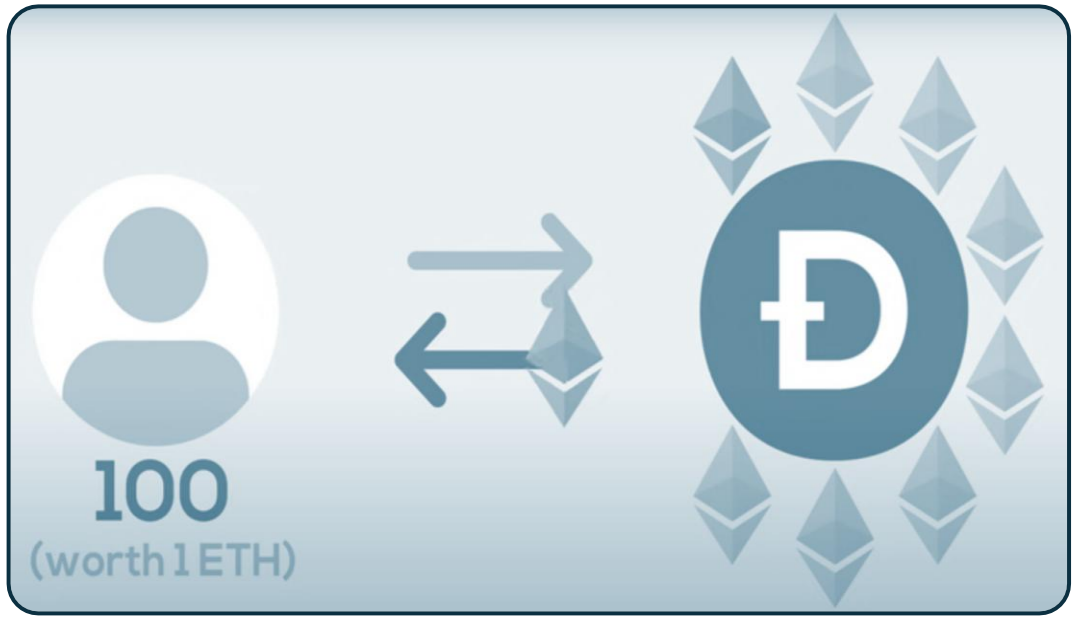
Smart Contracts Security

Jahad Jafarov
Duy Tung Tran

Smart Contract Security – DAO Hack

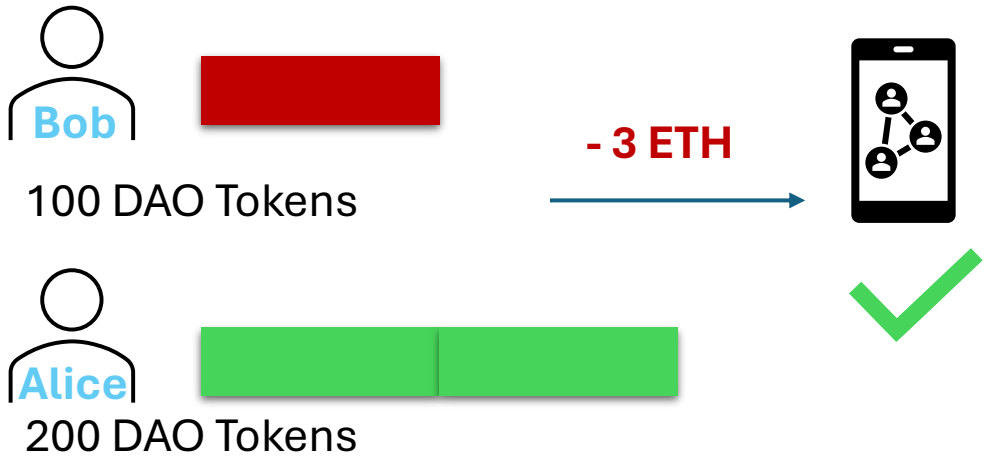
- Ethereum was the first blockchain platform to introduce smart contracts—that run on its network. These contracts are primarily written in Solidity.
- Ethereum's Turing completeness allows it to execute any computable function. This enables complex financial applications like decentralized finance (DeFi) and tokenized assets. However, this flexibility also introduces security risks, as complex logic increases the likelihood of coding errors and unforeseen vulnerabilities.
- In this presentation we will focus on a well-known example of a smart contract attack – DAO Hack.

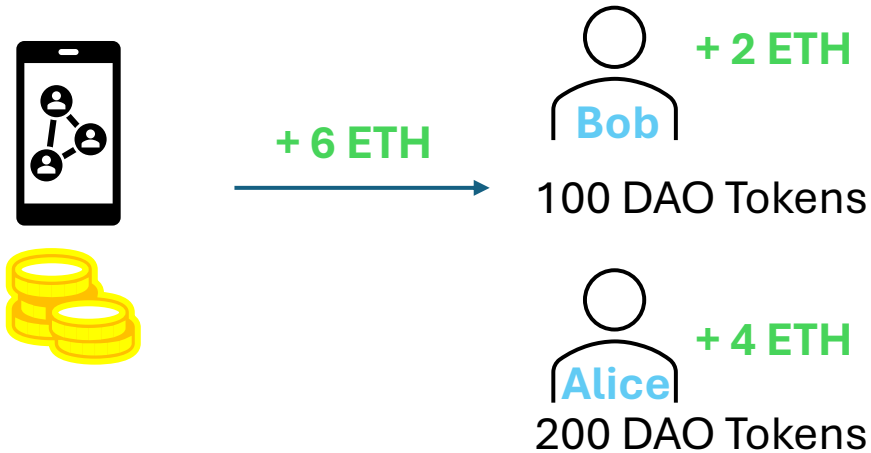
DAO



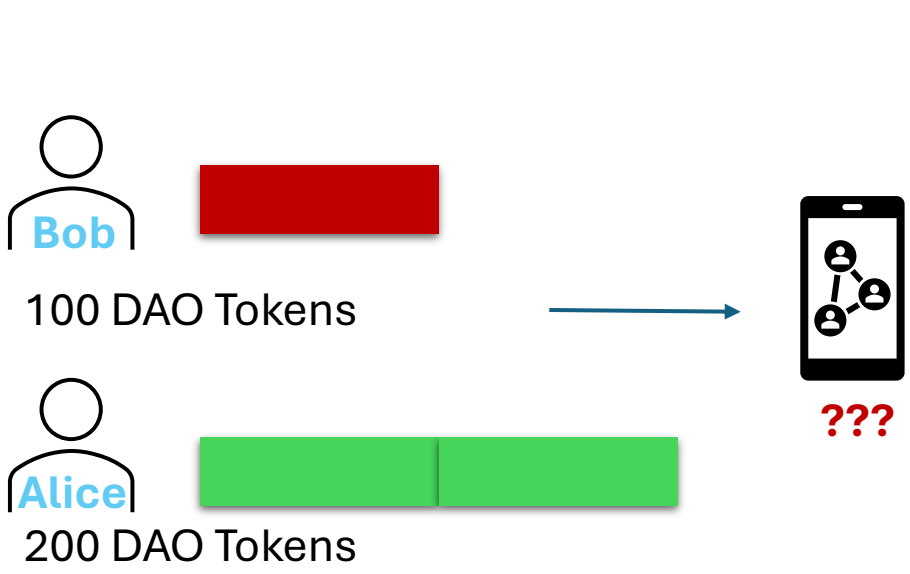
How DAO worked

- Users bough DAO Tokens that conferred them voting rights on projects within DAO.
- 1 ETH was being sold for 100 DAOs.
- Majority vote ultimately decided whether the project was to be executed
- If users voted for the project, then their money (ETH) was invested in the project
- If the project made money the investors received their return further pushing the DAO Token price upwards





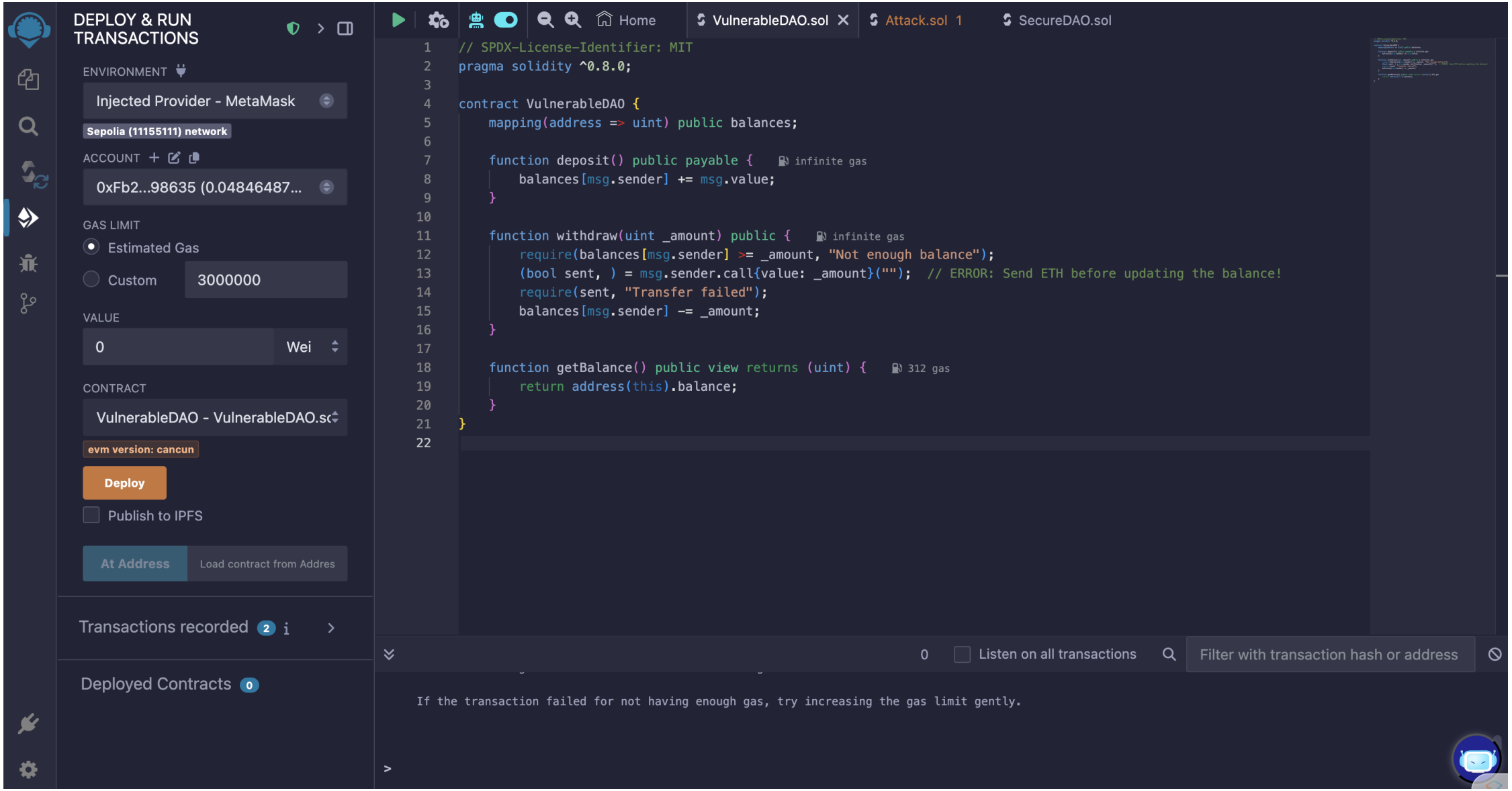
DAO Split



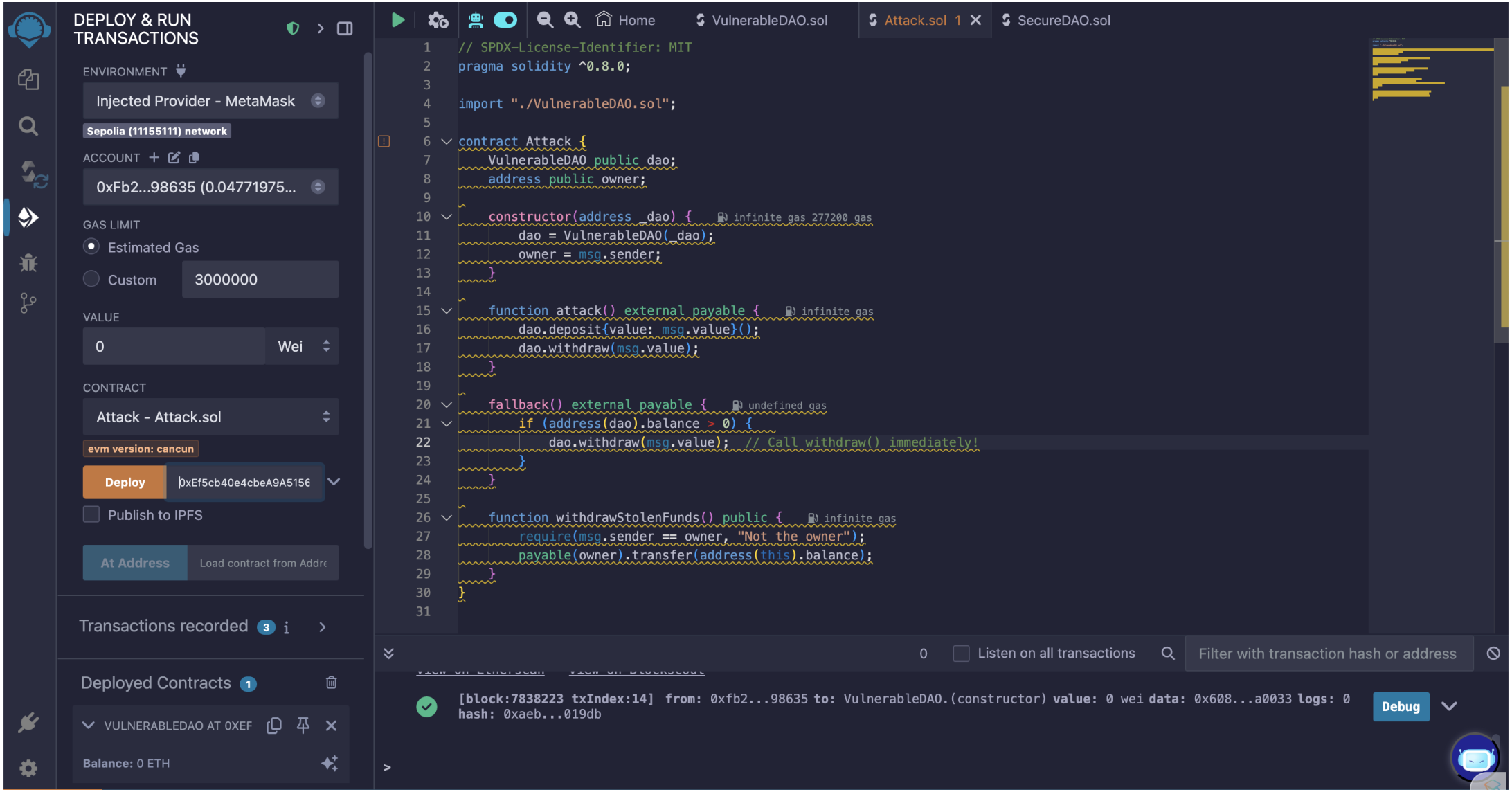
DAO Split

- Why was split() needed? It allowed investors to exit The DAO by creating a child DAO if they disagreed with funding decisions.
- How did it work? Users called split() to move their share of Ether to a new child DAO, triggering a 7-day joining period and 14-day curator approval delay before withdrawal.
- They aimed to prevent quick withdrawals and allowed time for curators to verify and approve legitimate exits.

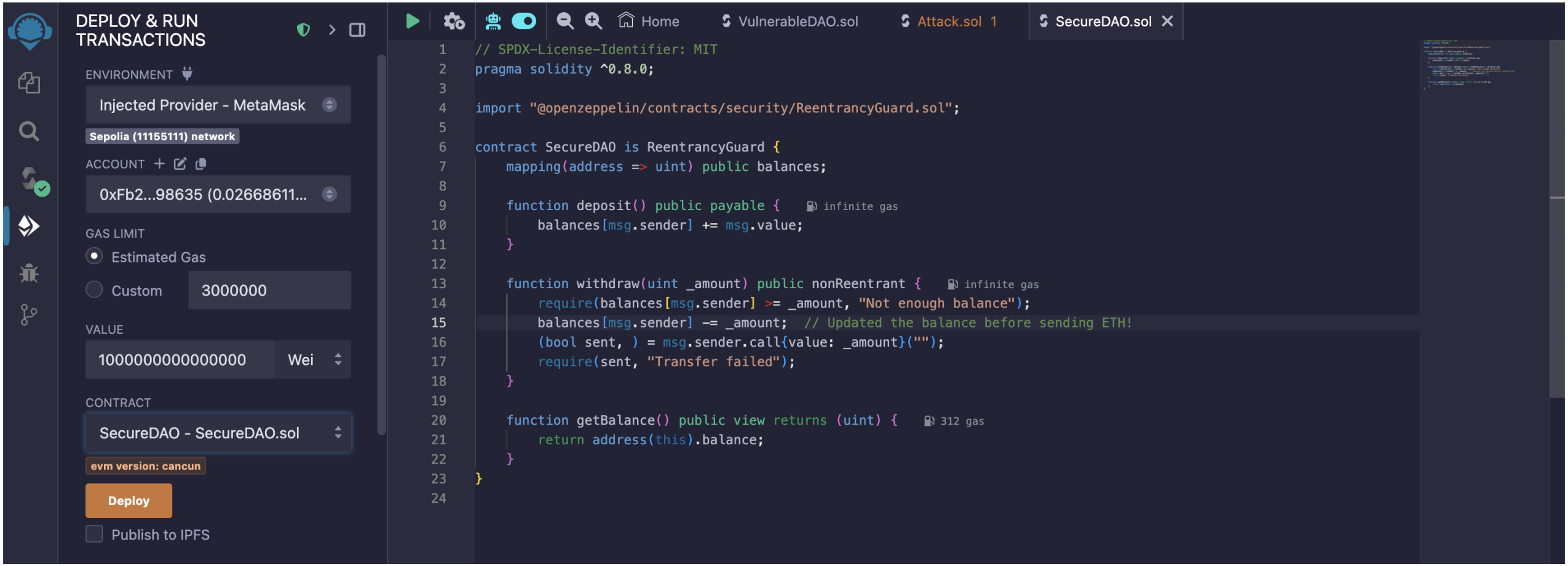
The Smart Contract that is targeted by Hacker



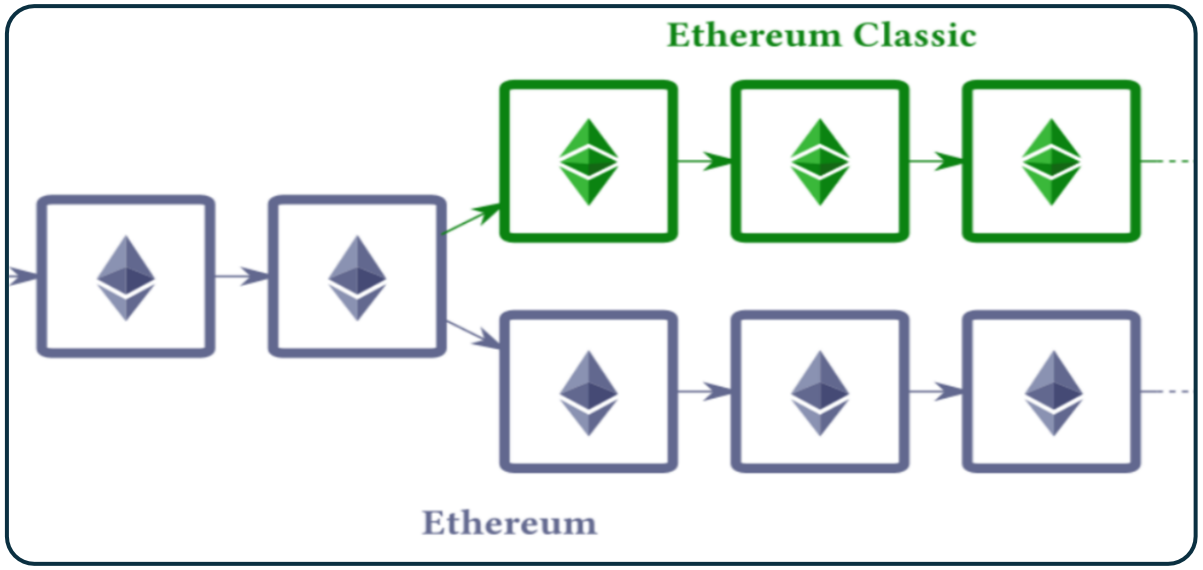
How Hacker Makes Use Of The Vulnerable Contract



The Optimized Contract That Corrects the Vulnerable Point



DAO Hack Aftermath



- Eventually a group of white hackers called Robin Hood Group launched a white hack attack, and drained the remaining DAOs
- The community had 41 days (27 + 14) to decide what to do with the all the DAOs
- The Ethereum community had a choice between doing nothing and hard forking the chain
- Code is Law vs Hard-Fork
- Vitalik Buterin advocated for the hard fork
- Eventually the more than 80% of the community voted for the hard fork

Conclusion

- ETH Classic started trading at about 2$ per coin. The attacker would thus have made around USD 7 Million in today's money.
- The hacker eventually walked away with 3.6M ETH Classic worth 150 Million dollars today
- Without the fork that 3.6M ETH would be worth over 7 Bn dollars today
- Today, many DeFi protocols and smart contracts are being audited, and in some way the original DAO paved the way to numerous other, more secure projects