$100 Million Blockchain Hack

By: www.ProfitableInvestingTips.com

The strongest argument for using blockchain technology is that the system is redundant. It never erases information but rather adds or modifies information. The argument goes that this feature makes it difficult if not impossible to hack a blockchain. Wrong! *Fortune* reports a $100 million **blockchain hack** of a blockchain transfer protocol. This brings the total lost from blockchains by hacking in 2022 to more than $1 billion. How did this happen and does the $100 million blockchain hack invalidate arguments about blockchain safety?

Cross-chain Blockchain Vehicle Hacked

The most recent victim of blockchain hacking was Harmony's Horizon bridge. According to Harmony, the hackers got away with DeFi tokens (SUSHISUSHI and AAVEAAVE), stablecoins (USDCUSDC dau, and UDST), and blockchain tokens (BNBBNB and ether). The hack took nearly 70% of Harmony's total capital. The Horizon bridge facilitates transfers between Binance Smart Chain and Ethereum blockchains. According to Harmony they still have more than $50 million in ETH and BNB after the theft. The Horizon bridge has been shut down and other exchanges have been notified as the team attempts to track and recover their losses.

How Do These Recurring Blockchain Hacks Happen?

Fortune writes that there have been five major hacks in 2022. These include the Ronin Network, and Wormhole which amount to $600 million and $325 million respectively. Ronin hosts the Axie Infinity gaming network and Wormhole bridges between Ethereum and SolanaSol. The weakness in the system that allowed a hack at Horizon was a security structure that allowed transactions to proceed with only two of the four possible signers. Thus only two accounts needed to be compromised in order to steal money from the entire system. All of the blockchain redundancy in the world did not stop a hack that took advantage of a design error in the system. The small number of owners needed for a consensus was pointed out before this hack by the founder of Chainstride Capital who predicted a "nine figure hack." The theft took place over a series of fourteen transactions between Binance Smart according to a report by Elliptic. It turns out that Harmony has a good idea who the hacker is and is negotiating to get back at least part of the stolen goods.

Meanwhile they are working, after the fact, with the FBI and cyber security firms. The effect on Harmony's ONE token has been a decline of eight percent with a current price of 2.4 cents. The company's market cap stands at just over $300 million.

51% Rule Allows Blockchain Hacks

Cipher explains **how the blockchain can be hacked** starting with the 51% rule. Blockchain hackers, like all hackers, exploit weaknesses in the systems that they attack. The distributed records of a blockchain are validated, recorded and announced by network members. These are not paid employees but independent entities who are “incentivized” to do this work. Basically the validator gets a tiny fraction of the cryptocurrency involved when they do their work. A problem in the system lies with having a majority of the validators on the hacker’s side. This is called a 51% attack. When the hackers control more than half of the computing or hashing power of the system, they create fraudulent records which they then validate. A common trick is to create double payments. These systems have protocols that give authority to the “longest transactional history” which belongs to the hackers when they control 51% or more of the system. As a general rule, smaller systems are more vulnerable to attacks because it takes fewer entities to reach the 51% barrier.

Smart Contracts Depend on Smart Code

Smart contracts would seem to be safe from hacking in that they are designed to execute only when specific criteria are satisfied. But even these are vulnerable if they have glitches in their programming. (GIGO = garbage in garbage out is an old computer programming adage.) As of today there is no specific tool for detecting and testing these flaws except for the “old fashioned way” of sitting down and step by step testing and retesting the programs. As the crypto world comes under increasing pressure from the collapse of Bitcoin and others companies will lay off some of their staff and, unfortunately, this will probably include exactly the people needed to test and validate programming code!

For more insights and useful information about investments and investing, visit www.ProfitableInvestingTips.com.

Disclaimer: Trading and investing involves significant financial risk and is not suitable for everyone. No content on this document should be considered as financial, trading, or investing advice. All information is intended for educational purposes only.