PART 1 OF MCMILLAN SERIES - DEFI PLATFORM MANGO LOSES $117 MILLION IN SMART CONTRACT EXPLOIT: ARE DAOS RESPONSIBLE FOR BAD SMART CONTRACTS?

Posted on October 14, 2022

Categories: Insights, Publications

On October 12, 2022, CoinDesk reported that a rogue crypto trader drained over $116 million in liquidity from the Solana-based DeFi platform, Mango Markets ("**Mango**").[1]

Mango allows users to trade spot and perpetual futures using its on-chain trading interface at low fees. Like other decentralized exchanges, Mango uses smart contracts to match trades between DeFi users. Smart contracts are self-executing contracts – programs – that run when predetermined conditions are satisfied. Far too often, they are recycled and reused. With enough resources, rogue traders can exploit loopholes in smart contract code before anyone can step in to stop the attack.

The Mango exploit is described in detail here. According to CoinDesk, the rogue trader used over 10 million USD Coins to take out over $116 million from Mango, paying minimal fees for conducting the attack and "doing everything within the parameters of how the platform was designed".[2] According to CoinDesk, Mango was not hacked. Rather, "[the exchange] worked exactly as intended, and a savvy trade, albeit with nefarious intentions, managed to wring token liquidity out".[3]

The hack comes less than a week after Binance (the world's largest DeFi exchange) suffered a $570 million loss.

After the attack, Mango's developers were quick to defend their exchange, noting that their pricing oracle providers were not at fault. But if smart contract code is deficient or insufficient for its purpose, and therefore vulnerable to exploitation by bad actors, who is at fault?

As attacks on DeFi cryptocurrency platforms become more frequent and the losses become more substantial, there is increasing pressure on the decentralized autonomous organizations ("**DAOs**"), within which users interact, to protect them from vulnerabilities in their smart contracts. Are DAOs and their principals doing enough to weed out substandard smart contracts and avoid vulnerabilities in the code? Can DAOs be liable for 'allowing' attacks to happen through the use of recycled and weak smart contract code? What is the standard of care in drafting smart contract code?

There is also more pressure on DAOs to reimburse affected users. In this case, Mango has promised to "reimburse as much as [they] can using the DAO treasury (subject to vote) and whatever tokens [they are] able to recover".[4] Mango has asked the attacker to contact them at blockworks@protonmail.com to collect a bug bounty in exchange for returning the funds. What happens if the attacker rejects the bounty? What recourse might DAOs have against attackers? What recourse might users have against DAOs? These scenarios are playing out with regularity in the DAO space and they raise serious legal questions, some of which the courts are starting to consider.

In Canada, some of these questions have already been raised in a case prosecuted by these McMillan authors. In *Cicada 137 LLC v. Medjedovic* ("***Cicada 137***"), an anonymous attacker stole over USD$15,000,000 worth of digital assets from Indexed Finance, another DeFi exchange.[5] In *Cicada 137*, the attacker used a similar series of exploit transactions to devalue several of Indexed Finance's index pools and artificially overvalue the cryptocurrency he immediately acquired. The question of whether exploitation of bad code in smart contracts is actionable in the civil courts, or defensible as 'arbitrage', will form the next chapter of this ongoing legal battle.

If you have any questions related to the above exploits, or the 'Code is Law' debate now moving into the Canadian courts, please do not hesitate to contact the authors.

[1] Shaurya Malwa, "How Market Manipulation Led to a $100M Exploit on Solana DeFi Exchange Mango", October 12, 2022: online.
[2] Shaurya Malwa, "How Market Manipulation Led to a $100M Exploit on Solana DeFi Exchange Mango", October 12, 2022: online.
[3] Shaurya Malwa, "How Market Manipulation Led to a $100M Exploit on Solana DeFi Exchange Mango", October 12, 2022: online.
[4] Shaurya Malwa, "How Market Manipulation Led to a $100M Exploit on Solana DeFi Exchange Mango", October 12, 2022: online.
[5] Christopher Beam, "The Math Prodigy Whose Hack Upended DeFi Won't Give Back His Millions", May 19, 2022: online.

by Benjamin Bathgate, Reuben Rothstein, and Madeline Klimek

A Cautionary Note


mcmillan