PART 2 OF MCMILLAN SERIES – DEFI PLATFORM MANGO LOSES $117 MILLION IN SMART CONTRACT EXPLOIT: IS MANGO'S SETTLEMENT WITH THE EXPLOITER ENFORCEABLE AND WHAT DOES IT MEAN FOR DAOS?

Posted on November 16, 2022

Categories: Insights, Publications

In Part 1 of this series, we described a recent crypto exploit in which a rogue trader drained over $116 million in liquidity from the Solana-based DeFi platform, Mango Markets ("**Mango**"). We noted that decentralized autonomous organizations ("**DAO**") are facing increasing pressure to protect community members from smart contract vulnerabilities. Shortly after we published Part 1, Mango's principals began to negotiate a settlement with the exploiter, believed to be Avraham Eisenberg.

The negotiation and outcome raise pressing questions about the validity of settlements in the DAO/DeFi space.

Eisenberg's Proposal

Shortly after the exploit, Eisenberg submitted a governance proposal to Mango's DAO governance forum proposing terms of settlement. Eisenberg offered to return $46 million worth of stolen tokens (MNGO, SOL, and Marinade Staked SOL) to Mango in exchange for: (a) a bounty of $70 million worth of tokens; and (b) Mango promising not to file criminal charges against him or freeze his assets.[1]

Eisenberg's proposal required approximately 100 million votes to reach quorum. He immediately voted for his own proposal with the tokens he acquired in the exploit, worth over 33 million votes.[2] Despite voting with the stolen tokens, Eisenberg's proposal failed to achieve quorum. He needed an additional 66.7 million votes.[3] The fact that Eisenberg used the fruits of his exploit, the stolen tokens, to vote in favour of his own settlement proposal – especially one that purported to deter criminal prosecution – was not only audacious but raises serious questions about what a DAO proposal can and cannot do to bind its token holders and their losses.

While some of Mango's principals appeared willing to engage with Eisenberg (commenting that they would "clear him of any wrongdoing" and ensure he made a "healthy profit"), many Mango token holders were outraged by his proposal. These token holders called for swift and aggressive legal action.[4] This dissention raises even more questions, including:

- Who speaks for a DAO?
- Who gets to decide what proposals should be put to a vote?
- What binding consequences can such votes hold?
- Who ultimately bears responsibility and risk in decentralized platforms?

Mango's Principals' New Proposal: Mango Settles with Eisenberg

On the heels of Eisenberg's failed proposal, Mango's principals submitted a new governance proposal setting out a counter-offer to Eisenberg. The proposal read:

To [Avraham Eisenberg]...

> We are seeking to make users whole to the extent possible. This is the amount you have agreed to return:
>
> ...
>
> Most of these funds are currently in the control of the solana wallet yUJw and should be sent to the wallet owned by Mango Upgrade Council: 9mM6NfXauEFviFY1S1thbo7HXYNiSWSvwZEhguJw26wY
>
> The 10,000,000 USDC can be sent either to the Upgrade Council solana wallet or the ethereum wallet setup by the developers: 0xa8e8729A6AAb10178FBac1E9D55A0c536ce3DCa8
>
> Within 12 hours of the proposal opening, you shall send back the assets other than USDC, MSOL, MNGO, and SOL as a show of good faith. The remaining assets shall be sent within 12 hours once the vote is complete and passes.
>
> The funds sent by you and the mango DAO treasury will be used to cover any remaining bad debt in the protocol. All mango depositors will be made whole. ***By voting for this proposal, mango token holders agree to pay off the bad debt with the treasury, and waive any potential claims against accounts with bad debt, and will not pursue any criminal investigations or freezing of funds once the tokens are sent back as described*** **above.**[5] [emphasis added]

Within a few days of the proposal opening, Mango's principals' counter-proposal passed. Once again, Eisenberg voted in favour of the proposal with the tokens he acquired in the exploit.[6] In accordance with the settlement, Eisenberg returned $67 million worth of stolen tokens to Mango. In exchange, Mango "allowed" Eisenberg to keep a 'bug bounty' of $47 million worth of stolen tokens and "promised" not to pursue any criminal investigations or freezing of funds against him.[7]

According to industry observers, the $47 million bounty is by far the biggest crypto bounty ever recorded. It far

exceeds the going bounty rate of approximately 10% of the total exploited funds.[8]

As predicted, many Mango token holders expressed frustration about the settlement. Token holders were particularly upset about the size of Eisenberg's bounty. One voter tweeted: "... a $50m 'bug bounty' is ridiculous. At most the exploiter should get their costs back ($15m?) plus $10m. $10m whitehat bounty is what was offered to the $600m wormhole hacker. Mango can negotiate better than this, especially given the exploiter is essentially doxed."[9] Token holders were also concerned about Mango's "promise" to waive any potential claim against Eisenberg.[10]

Eisenberg Asserts "Code is Law" Defence

On October 29, 2022, Eisenberg spoke with Laura Shin on her well-known podcast, Unchained.

During the interview, Eisenberg insisted that his actions were "legal, open market actions" that used Mango's protocol as designed, even if Mango's development team "did not fully anticipate all the consequences of setting parameters the way they are".[11]

Of course, Eisenberg's defense closely resembles those raised in other large DAO/DeFi smart contract exploits. The most prominent example presently before the courts arises from the Indexed Finance exploit allegedly carried out by Andean Medjedovic, as reported by Bloomberg Businessweek.[12] *The Cicada 137 LLC v. Medjedovic* case is being prosecuted by these McMillan authors and has already resulted in an Order for the seizure of the exploiter's cold storage wallet and a warrant for the exploiter's arrest.

Eisenberg also rejected the notion that keeping a significant portion of the funds was somehow a "bounty." He noted that profitable traders frequently face heated criticism. He gave the example of crypto billionaire Sam Bankman-Fried, the founder of FTX, who notably made his fortune in crypto through arbitrage opportunities.[13]

Pressing Questions

Mango's settlement with Eisenberg is yet another case where an individual exploits a DAO's vulnerable smart contract code, seemingly without redress. These exploits raise a number of pressing questions about who bears the risk arising from crypto exploits and the responsibility for the settlement proposals that follow them, as well as how legal rights may be impacted. More specific questions include:

- What responsibilities do DAO principals and coders have for vulnerable smart contract code, and does that create a conflict of interest if they are involved in drafting settlement proposals to the attackers when it all goes wrong?
- Are settlement proposals to exploiters (and subsequent votes to validate them) valid offers of

settlement? Are they enforceable agreements? Do they bind token holders?
- Can these 'settlements' prohibit token loss holders from seeking remedies in civil courts, or from filing criminal complaints with law enforcement?
- How can a DAO proposal on settlement and a vote in favour of resolution (like the ones in Mango's case) be fair and binding when those suffering the losses purportedly lose their individual right to decide and when the exploiter itself can vote the proceeds of the attack in favour?
- Can anyone (DAO principals or token holders) "promise" not to file criminal charges or seek freezing orders when settlements containing such agreements are often held to be void and unenforceable by the courts (i.e., for concealing/stifling criminal prosecution)
- Can a DAO vote alone bind a collective of diverse token holders, with disparate interests, in a settlement agreement with an exploiter? Can it stop those investors from "going it alone?"

In hopes of resolving lingering risks and uncertainties in these unregulated, decentralized platforms, some DAOs are now considering restructuring into a more traditional corporate form, taking on the shape of limited liability companies, for example.

In our next bulletin in this Mango Markets DAO/DeFi series, these authors will discuss how DAOs are restructuring and whether that provides effective legal armour in the vulnerable-to-attack DAO/DeFi space and the risk bearing.

If you have any questions related to the exploits above, or available remedies arising from such attacks or their purported settlements, please do not hesitate to contact the authors.

[1] Jesse Coghlan, "Mango Markets exploiter said actions were 'legal', but were they?", October 18, 2022, *Cointelegraph*, online.
[2] Sun, "Mango Markets hacker proposes steep settlement"; "Mango Markets looted of $117M, hacker demands massive bug bounty settlement" October 13, 2022, online.
[3] "Mango Markets looted of $117M, hacker demands massive bug bounty settlement".
[4] Repay bad debt discussion.
[5] Michael Bellusci and Sam Reynolds, "Mango Markets Community Counters Exploiter's Settlement Offer", October 14, 2022, *CoinDesk*, online.
[6] Prajeet Nair, "Mango Markets Set to Pay $47M Bug Bounty to Hacker", October 15, 2022, Bank Info Security, online.
[7] Michael Bellusci and Sam Reynolds, "Mango Markets Community Counters Exploiter's Settlement Offer", October 14, 2022, *CoinDesk*, online.
[8] Martin Yong and Ali Martinez, "Mango Markets Community Conflicted Over Record $47M 'Bounty'", October

15, 2022, *BeInCrypto*, online.
[9] Pereira, "Mango Market's DAO forum set to approve $47M settlement with hacker".
[10] Sun, "Mango Markets hacker proposes steep settlement".
[11] Nicholas Pongratz and Ali Martinez, "Mango Market Hacker Affirms He Isn't Sorry for Actions", October 29, 2022, online.
[12] Christopher Beam, "The Math Prodigy Whose Hack Upended DeFi Won't Give Back His Millions", May 19, 2022: online.
[13] On an separate note, see Adam Chisholm's latest op-ed in the Globe and Mail entitled "Despite FTX implosion, overzealous crypto enforcement is not the answer".

by Ben Bathgate, Reuben Rothstein, Maddie Klimek

A Cautionary Note