WeirFoulds LLP

Canadian Medjedovic Indicted for DeFi Fraud in the Eastern District of New York: Rule of Law '2', Code is Law '0'?

February 4, 2025

By Benjamin M. Bathgate, Jessica Stansfield

The ongoing saga of decentralized finance (DeFi) protocol fraud,[1] and in particular the exploitation of smart contract code[2] to enrich a bad actor at the expense of other users, has now leapt forward with a new chapter – the Indexed Finance and KyberSwap's criminal cases. Yesterday, the U.S. Attorney's Office in the Eastern District of New York announced the unsealing of an indictment charging Andean Medjedovic with extortion, wire fraud and computer hacking in relation to a highly sophisticated scheme to exploit two DeFi protocols, steal tens of millions in crypto from investors and launder the proceeds. The charges arise from exploitations he allegedly carried out on the Indexed Finance and KyberSwap pools, in October 2021 and November 2023, respectively.[3]

Medjedovic is accused of exploiting vulnerabilities in KyberSwap's smart contract to allow him to drain liquidity pools, which were funded by KyberSwap's users and intended to facilitate trading on the platform. It is alleged that Medjedovic borrowed millions in cryptocurrency that he used to artificially inflate the prices in the liquidity pools, while executing dozens of trades that caused KyberSwap's automated market maker to miscalculate the available liquidity in the pools and consequently allowed Medjedovic to steal $48.8 million from the pools. The indictment alleges that Medjedovic called the exploit a "glitch" with "fake" liquidity and labelled his code for the exploit as "rape", in addition to describing himself as a "pirate" and considering the possibility that he "may or may not be a criminal".[4]

After the exploit, it is alleged that Medjedovic attempted to extort KyberSwap's developers, investors, and members of its de-centralized autonomous organization (DAO), initiating "negotiations" that he said would "start in a few hours when I am fully rested." Medjedovic was reportedly offered a 10% 'bug bounty' in exchange for return of the digital assets, but instead, Medjedovic is alleged to have demanded control of both KyberSwap's protocol and DAO in exchange for returning only 50% of the stolen cryptocurrency.[5] Such post-exploit negotiations and attempted 'settlements' between bad actors and DAO token holders will sound familiar to many readers, as similar such conduct came under heavy scrutiny and prosecution in the Mango Markets civil, criminal and CFTC cases including in the Southern District of New York, as covered by these authors.[6] The negotiations in this case, between KyberDAO and Medjedovic, allegedly took an even stranger turn in this case, with Medjedovic supposedly warning KyberSwap's support channel that he would "alert authorities" if his gains were not unfrozen and if he was not allowed to remove them from the protocol. Medjedovic apparently suggested that "committing a crime against someone who may or may not be a criminal is still a crime".[7] A bold move, to be sure.

The indictment also covers the Indexed Finance DeFi smart contract exploit, which Medjedovic is alleged to have perpetrated in October 2021.[8] In this part of the indictment, Medjedovic is alleged to have committed a similar exploit against the Indexed Finance DeFi protocol, using a flurry of trades to 'borrow' millions in crypto in order to manipulate the "re-indexing" function in Indexed Finance smart contracts, which normally is used to add new tokens to liquidity pools. He then traded to set artificial prices during re-indexing, stealing $16.5 million from liquidity pools.[9]

Medjedovic allegedly attempted to launder the proceeds of both exploits, collectively $65 million between Indexed Finance and KyberSwap, through bridge protocols and use of a cryptocurrency mixer.[10] It is also alleged that Medjedovic agreed to pay $80,000 in an attempt to have $500,000 of the stolen crypto released from the protocol, which had been frozen from one of his bridge transactions, but the software developer that Medjedovic approached to circumvent the protocol's rules turned out to be an undercover law enforcement agent.[11] Medjedovic apparently went as far as creating a "step-by-step playbook for moving large amounts of cryptocurrency through mixers" and also considered how to use "false KYC information for 'hacks and cashing out'".[12] What appears to be a literal 'how to guide' on carrying out end-to-end smart contract fraud and circumventing defences put into place to frustrate anonymous offboarding of illicitly obtained funds.

Medjedovic has reportedly claimed that his exploit of Indexed Finance was legal and that he was merely taking advantage of what the smart contract allowed him to do.[13] It remains to be seen whether Medjedovic will remain silent or defend the KyberSwap exploit on the same basis, and whether he will respond to the charges in the Eastern District of New York with the beleaguered 'Code is Law' defence. One assumes that, unless he is brought back to face justice in the U.S. criminal courts, he will once again proclaim 'Code is Law' from the sidelines.

We saw from the recent U.S. criminal conviction of Avi Eisenberg, where he was arrested in Puerto Rico and defended charges in relation to a similar exploit of the Mango Markets protocol with a defence of 'Code is Law': however, just because it is *technically possible* to do something within a smart contract, does not make such exploits a *lawful use* of the smart contract (particularly when one takes into consideration the intention of the investors in those liquidity pools).[14] Time will tell whether Medjedovic will be brought before the court system in this next installment of the 'Code is Law' vs. 'Rule of Law' saga.

If this new indictment in the Eastern District of New York proceeds against Medjedovic, it does raise intriguing questions about what trends we expect to see going forward with DeFi fraud cases and attacks perpetrated against DAOs, including:

- How will the criminal and civil courts assess negotiations and even purported settlements (as in the case of Mango Markets) between DAO token holders and bad actors, given repeated instances of attempted post-exploit deals and black hat bounties, with promises 'not to prosecute'? Which settlements will and will not be enforceable and who will be bound by them?
- When one bad actor defrauds multiple protocols, and ill-gotten gains are co-mingled or possibly pooled with or invested in other sources of crypto, how will respective claims on that wallet or account be assessed by criminal and civil courts facing competing claimants? What about when the bad actor claims they *too* were hacked and the funds are 'gone'? Who else, at a DAO for example, might hold the bag for potential loss holders?
- Will we continue to see an upward trajectory of money laundering prosecutions against crypto 'mixers' for their facilitation of DeFi frauds and other cyber crimes, and other efforts to frustrate attempts to hide the transfer of illicit funds obtained from exploited protocols?
- And, of course, will the new U.S. administration effect a change of course in the existing message being sent by U.S. law enforcement to fraudsters in the unregulated DeFi marketplaces, and will we see an end to the active prosecution of protocol frauds and resulting money laundering cases, and an early sunset on regulation by enforcement?

[1] This is the third in a series of articles by these authors on DeFi protocol frauds and how these proclaimed smart contract 'trades' (or 'arbitrages') are being tested in the criminal and civil courts in the U.S. and Canada, putting the 'Code is Law' theory to the legal test. Benjamin Bathgate, Jessica Stansfield and Priya Dube together authored the first two in the series of articles, "Postponement of

Long-Awaited Mango Markets Criminal Trial on the Heels of SBF Guilty Verdict: What's to Come?", on November 27, 2023: online and "Rule of Law '1', Code is Law '0': Eisenberg Convicted in Mango Markets Criminal Trial after He Shies Away from Testifying", on April 19, 2024: online.

[2] A smart contract is computer code – a program – that works on predetermined conditions to automatically carry out specified functions, and in the case of DeFi, is the basis on which trades or other financial transactions are carried out among protocol users.

[3] Press Release: Canadian National Charged With Stealing Approximately $65 Million in Cryptocurrency From Two DeFi Protocols, United States Attorney's Office Eastern District of New York, February 3, 2025: online.

[4] Indictment, *United States of America v. Andean Medjedovic*, 24-CR-529 (Brooklyn Office), filed under seal December 30, 2024: online.

[5] Indictment, *United States of America v. Andean Medjedovic*, 24-CR-529 (Brooklyn Office), filed under seal December 30, 2024: online.

[6] Benjamin Bathgate, Jessica Stansfield and Priya Dube, "Postponement of Long-Awaited Mango Markets Criminal Trial on the Heels of SBF Guilty Verdict: What's to Come?", on November 27, 2023: online and "Rule of Law '1', Code is Law '0': Eisenberg Convicted in Mango Markets Criminal Trial after He Shies Away from Testifying", on April 19, 2024: online.

[7] Indictment, *United States of America v. Andean Medjedovic*, 24-CR-529 (Brooklyn Office), filed under seal December 30, 2024: online.

[8] These authors represent Cicada 137 LLC in the civil fraud case against Andean Medjedovic in the Ontario Superior Court.

[9] Indictment, *United States of America v. Andean Medjedovic*, 24-CR-529 (Brooklyn Office), filed under seal December 30, 2024: online.

[10] Cryptocurrency 'mixers' or 'tumblers' are self-proclaimed privacy services whereby potentially identifiable data on crypto funds are mixed together and rendered unidentifiable, with the effect of obscuring the trail back to the funds original source. Some crypto 'mixers' have been prosecuted for money laundering, including in the case of Bitcoin Fog (Sabrina Willmer, "Crypto 'Mixer' Gets 12 ½ Years for Money Laundering", on November 8, 2024: online.

[11] Press Release: Canadian National Charged With Stealing Approximately $65 Million in Cryptocurrency From Two DeFi Protocols, United States Attorney's Office Eastern District of New York, February 3, 2025: online.

[12] Press Release: Canadian National Charged With Stealing Approximately $65 Million in Cryptocurrency From Two DeFi Protocols, United States Attorney's Office Eastern District of New York, February 3, 2025: online.

[13] Aleks Gilbert, "Indexed Finance hacker charged in US for alleged $65m theft", February 3, 2025: online.

[14] Benjamin Bathgate, Jessica Stansfield and Priya Dube together authored the first in the series of articles, "Rule of Law '1', Code is Law '0': Eisenberg Convicted in Mango Markets Criminal Trial after He Shies Away from Testifying", on April 19, 2024: online; David Voreacos, Chris Dolmetsch, "Crypto Trader Convicted in $110 Million Mango Markets Fraud", April 18, 2024: online.

For more information or inquiries:

Benjamin M. Bathgate

Toronto
647.715.3544

Email:
bbathgate@weirfoulds.com

Benjamin M. Bathgate is the Chair of the Commercial Litigation Practice Group and Co-Chair of the Blockchain and Digital Assets Practice Group at WeirFoulds LLP. His practice focuses on complex, high stakes fraud, digital asset recovery and cross-border litigation and investigations. Ben is widely recognized in the crypto industry as the go-to digital asset investigations and recovery lawyer in Canada. Ben is top ranked (Band 1) in the Chambers FinTech Guide "Crypto-Asset Disputes – Canada" category.

Jessica Stansfield

Toronto
416.947.5095

Email:
jstansfield@weirfoulds.com

Jessica Stansfield is a Partner in the Commercial Litigation Practice Group and the Blockchain and Digital Assets Practice Group at WeirFoulds LLP. Jessica is top ranked (Band 1) in the Chambers FinTech Guide "Crypto-Asset Disputes – Canada" category.

WeirFoulds LLP

www.weirfoulds.com

Toronto Office
4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110
Fax: 416.365.1876

Oakville Office
1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110
Fax: 905.829.2035