Proposing solutions to overcome security flaws of decentralized cryptocurrency exchanges

The rise of blockchains has enabled individuals to own and transfer assets across a decentralised network without needing to trust any external parties, leading to the rapid adoption of the ownership of cryptocurrencies that exist on the blockchain, such as Bitcoin and Ethereum.

Many centralized cryptocurrency exchanges, similar to the traditional financial stock exchanges, were launched to facilitate the efficient exchange of these cryptocurrencies. However, these exchanges suffered multiple hacks throughout history. In 2014, Mt. Gox, the largest Bitcoin exchange handling 70% of transactions at that time, lost USD450 million of Bitcoins [1]. Security did not improve over the years, as seen from the increase in the occurrence of hacks. In 2018 alone, over $1 billion were stolen from these exchanges. [2]. Binance and Kucoin, some of the world's largest cryptocurrency exchanges, were also hacked in 2019 and 2020 respectively [3], [4].

Due to the security flaws that centralized exchanges have demonstrated, a new wave of blockchain projects that aimed to solve this problem has emerged: decentralized exchanges. They aim to remove the vulnerabilities of centralized exchanges being the single point of failure by facilitating the storing and trading of assets through smart contracts to enable safer trading. This is of utmost importance since the theft of funds from exchanges is a huge risk-factor for customers.

While entrusting funds to smart contracts does reduce the risk, it is still not a completely risk-free solution. After all, smart contracts are computer programs written by humans, and thus, will only be as secure as the program itself.

Firstly, decentralized exchanges could be hacked because of false decentralization. In 2018, Bancor, a decentralized exchange, lost $23.5M in a hack. Hackers were able to exploit a deliberately permissioned backdoor in the smart contracts by the Bancor team. As such, the hackers were able to steal funds out of the contracts [5].

Secondly, the smart contracts that the decentralized exchanges operate on could have programming bugs. In 2017, The decentralized autonomous organization (DAO) was hacked and 3.6M Ether (~$50M) were stolen using the first reentrancy attack. It was one of the highest-profile reentrancy attacks in Ethereum's history. [6] Also, in 2018, many BeautyChain (BEC) tokens were hacked when a BatchOverflow bug in its smart contracts was exploited.

This research aimed to analyze existing and potential security vulnerabilities in decentralized cryptocurrency exchanges and smart contracts that may result in users losing their assets, and propose solutions to address these vulnerabilities. This is because security is the minimal expectation that users have of a cryptocurrency exchange, and failure to provide it will hinder the mass adoption of decentralized applications. While partial centralization of exchanges by hosting order books outside the blockchain can result in frontrunning and denial-of-service that might result in less than ideal trading positions for end-users, we will not be discussing them as they do not increase the risk of users losing their funds and assets. Solutions from this research will help entities to build more secure decentralized exchanges to better safeguard users' cryptocurrencies and improve their trust in these platforms.

Citations:

[1] "Mt. Gox", Wikipedia, n.d. Accessed on: Nov. 24, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Mt._Gox

[2] Y. Khatri, Nearly $1 Billion Stolen In Crypto Hacks So Far This Year: Research, CoinDesk, Oct. 18, 2018. Accessed on: Nov. 24, 2020. [Online]. Available: https://www.coindesk.com/nearly-1-billion-stolen-in-crypto-hacks-so-far -this-year-research

[3] E. Lam, Hackers Steal $40 Million Worth of Bitcoin From Binance Exchange, Bloomberg, May 8, 2019. Accessed on: Nov. 24, 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2019-05-08/crypto-exchangegiant-binance-reports-a-hack-of-7-000-bitcoin

[4] A. Hui, W. Zhao, Over $280M Drained in KuCoin Crypto Exchange Hack, CoinDesk, Oct. 09, 2020. Accessed on: Nov. 24, 2020. [Online]. Available: https://www.coindesk.com/hackers-drain-kucoin-crypto-exchanges-funds

[5] J. Russel, The crypto world's latest hack sees Bancor lose $23.5M, TechCrunch, Jul. 10, 2018. Accessed on: Nov. 24, 2020. [Online]. Available: https://techcrunch.com/2018/07/10/bancor-loses-23-5m/

[6] "The DAO (organization)", Wikipedia, n.d. Accessed on: Nov. 24, 2020. [Online]. Available: https://en.wikipedia.org/wiki/The_DAO_(organization)