


# Proposing solutions to overcome security flaws of **Decentralized Cryptocurrency Exchanges (DEX)**



The background features a complex network diagram with white lines forming a grid-like pattern of squares and diamonds. Small blue hexagons are placed at various intersections, and tiny blue dots are scattered along the lines. Several small grey speech bubbles containing binary code (011, 001, 010, 100) are also visible.

“ ... think of it like  
**Airbnb for cloud storage,**  
where anybody with  
extra hard drive space  
can sell it on the network

Market capitalization of cryptocurrencies

**~\$2,230,000,000,000**

Market capitalization of cryptocurrencies

~\$2,230,000,000,000

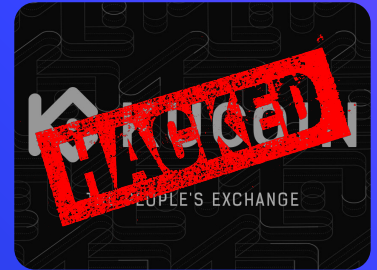
Centralized Cryptocurrency Exchanges



Market capitalization of cryptocurrencies

~\$2,230,000,000,000

Centralized Cryptocurrency Exchanges



# But DEXs aren't completely safe



# But DEXs aren't completely safe

## False Decentralization

Deliberate permissioned  
backdoor built in

Over 25,000 ETH from  
 **Bancor hack** Moved to  
Exchange

# But DEXs aren't completely safe

## False Decentralization

Deliberate permissioned backdoor built in

Over 25,000 ETH from  
 **Bancor hack** Moved to  
Exchange

## Programming Bugs

Smart contracts running  
these exchanges exploited

```
118 if (validator == 0) {  
119     require(factory.isLighthouse(msg.sender));  
120     require(token.transfer(promisor, cost));  
121 } else {  
122     require(msg.sender == validator);  
123  
124     isConfirmed = _agree;  
125     if (isConfirmed)  
126         require(token.transfer(promisor, cost));  
127     else  
128         require(token.transfer(promisee, cost));  
129  
130     if (validatorFee > 0)  
131         require(factory.xrt().transfer(validator, validatorFee));  
132 }
```

Entry point





# Goal: Asset Loss Prevention in DEXs



## Analyze vulnerabilities

By deep diving into the open-source code of the smart contracts

## Propose solutions

To address these vulnerabilities from different levels  
E.g. Protocol, Application, Architecture, Network



**Improve trust in DEXs by  
safeguarding cryptocurrencies  
more securely**

# Thanks!

Any questions?



# References

- [1] “Mt. Gox”, Wikipedia, n.d. Accessed on: Nov. 24, 2020. [Online]. Available: [https://en.wikipedia.org/wiki/Mt.\\_Gox](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-exchange-giant-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\\_\(organization\)](https://en.wikipedia.org/wiki/The_DAO_(organization))