

DECENTRALISED FINANCE SERVICES USED FOR ILLICIT TRANSFERS, U.S. REGULATOR SAYS

Relevant for: Indian Economy | Topic: Issues relating to Growth & Development - Foreign Capital, Foreign Trade & BOP

To enjoy additional benefits

CONNECT WITH US

April 07, 2023 07:54 am | Updated 07:54 am IST - WASHINGTON

COMMENTS

SHARE

READ LATER

File photo of tokens representing Bitcoin | Photo Credit: REUTERS

North Korea, cybercriminals, ransomware attackers, thieves, and scammers [are using decentralised finance \(DeFi\) services](#) to transfer and launder their illicit proceeds, the U.S. Treasury Department warned on Thursday.

So-called DeFi platforms allow users to lend, borrow, and save, usually in cryptoassets and stablecoins, without using banks.

In a new illicit finance risk assessment on decentralised finance, the Treasury found that illicit actors are exploiting vulnerabilities in U.S. and foreign anti-money laundering and combating the financing of terrorism (AML/CFT) regulation and enforcement as well as the technology underpinning the services.

DeFi services that fail to comply with these obligations to prevent money laundering and terrorism financing pose the most significant illicit finance risk in this domain, the assessment found.

(For top technology news of the day, [subscribe](#) to our tech newsletter Today's Cache)

"Our assessment finds that illicit actors, including criminals, scammers, and North Korean cyber actors are using DeFi services in the process of laundering illicit funds," the Treasury's Under Secretary for Terrorism and Financial Intelligence, Brian Nelson, said in the statement.

Nelson added that the private sector should use the findings of the assessment to inform their risk mitigation strategies and to take steps to prevent illicit actors from using decentralised finance services.

Other vulnerabilities found in the assessment included the potential for DeFi services to be out of scope for existing AML/CFT obligations, the lack of implementation of international AML/CFT standards and poor cybersecurity practices.

The assessment recommended strengthening U.S. AML/CFT supervision, considering additional

guidance for the private sector on DeFi obligations and addressing any regulatory gaps related to the services.

COMMENTS

SHARE

[technology \(general\)](#) / [cyber crime](#) / [cryptocurrency](#)

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our [community guidelines](#) for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com

CrackIAS