Opinion **Decentralised finance**

DeFi is a reminder of the risks of unfettered financial engineering

While they rely on libertarian ideals of self-governance, nascent blockchain systems are vulnerable

ESWAR PRASAD

Sophisticated hackers have been able to take advantage of vulnerabilities in decentralised finance products © Photonphoton/Dreamstime

Eswar Prasad 13 HOURS AGO

The writer is author of 'The Future of Money: How the Digital Revolution is Transforming Currencies and Finance'

Decentralised finance, or DeFi, is the next frontier in finance. New forms of financial intermediation are using blockchain technology to open up access to finance and bypass inefficient and lumbering traditional institutions like commercial banks. DeFi even makes it possible to sidestep government oversight and regulation. In China, for instance, a national ban on investing in cryptocurrency is pushing traders towards DeFi.

While there is no doubt that the technology opens up exciting opportunities, this kind of unfettered financial engineering also opens the door to new risks.

At face value, DeFi might seem a more secure way to conduct transactions. The system is characterised by transparent digital ledgers maintained on multiple computers, so there is no centralised point of failure. Its governance is also decentralised — control rests with the members of a network rather than a central authority. Trust is achieved through public consensus: community members must themselves agree about the validity of transactions, rather than relying on third parties.

In principle, these features make DeFi invulnerable to hacks of particular computer nodes or malfeasance by individuals or institutions. DeFi also enables "permissionless composability". That means a developer can easily connect together multiple DeFi applications built on open-source technology to create new financial products and services, without having to seek permissions.

Several innovative DeFi products are already available. Flash loans, for example, enable borrowing without collateral, using that money for a transaction and then returning the borrowed amount, all for a small fee. A flash loan is initiated, executed, and completed in the blink of an eye, using just computer code. They have many uses, from helping to arbitrage price differences across markets, to increasing market efficiency. Since they are instantaneous, default and liquidity risks are reduced.

Then there are smart contracts, which allow financial and other assets to be exchanged using computer code with no attorney or escrow agent involved. Computer tools can perform rigorous economic risk assessments of smart contracts and specific DeFi products. The open source nature of the applications helps uncover and eliminate security and other weaknesses.

Still, sophisticated hackers have been able to take advantage of vulnerabilities in DeFi products. Malevolent agents can exploit the larger "attack surface" that is created when combining multiple applications. They are also more vulnerable to software bugs and users who do not fully understand the risks.

The absence of a central authority to police bad behaviour also has risks. Researchers at Cornell University found that automated bots could front-run certain trades — for instance, executing open orders at an unfavourable price before they can be cancelled when prices change. With no one to report this flaw to, the researchers published a blog post detailing the risk, assuming the community would protect itself. Instead, a cottage industry of bots emerged to exploit the idea before the loophole could be closed.

It is worth remembering that while DeFi may rely on libertarian ideals such as its own rule of law, with the community creating and enforcing rules in the broad interests of stakeholders, in reality nascent blockchain systems are vulnerable to governance capture by small groups of stakeholders, who could twist rules in their favour.

Moreover, while blockchains are self-contained, they still need information about prices and ownership of assets to execute certain transactions. For instance, on-chain hog futures contracts need access to hog prices from commodity exchanges. Computer programs called oracles obtain such off-chain information and pass on-chain information back to the real world. These oracles are vulnerable to technical risks including hacks and even problems with external data providers.

Given all this, regulators are in a quandary — even open-minded ones who see potential in DeFi but worry about financial stability risks. They can now intercede only at the point where these products

intersect with institutions they oversee. As decentralised finance grows in size and scope, regulators will have to pay attention to risks building up in these markets and their spillovers into traditional financial markets.

Updated regulatory frameworks that encompass DeFi will eventually be needed, although they should strike a reasonable balance in the innovation-risk trade-off. At a minimum, naive retail investors swept up by the technological razzle-dazzle must be protected from taking on outsized risks.