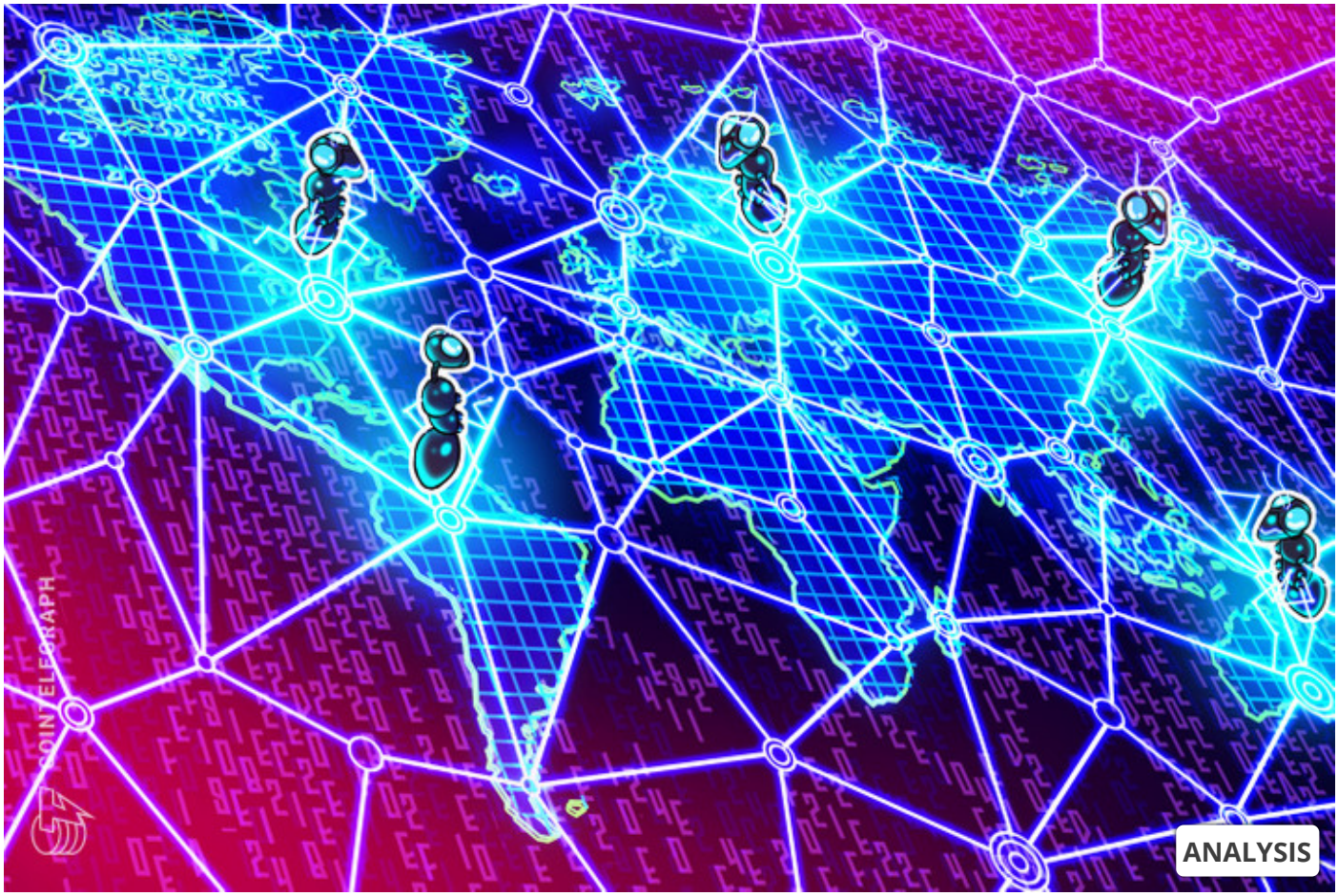
JULIA MAGAS AUG 13, 2020

Figuring Out Who's to Blame for DeFi's Persistent Security Issues

Is Ethereum's architecture to blame for the growth of decentralized finance hacks, and will the network upgrade make the sector more secure?

9339 35 9:47



The decentralized finance sector continues to gain unprecedented popularity as the total value of assets locked in DeFi products doubled to over $4 billion in July and is now approaching the $5 billion mark.

At the same time, an increased demand for such applications among users and developers makes it a target for bad actors, given the lure of direct access to funds. Over the past few months, hackers have stolen over $27 million from DeFi projects, and more attacks are expected to come in the near future. If this is the case, does the DeFi sector rely strongly on

2020, it's the decentralized finance market that's on the radar. This is largely made possible by vulnerabilities in platforms' smart contracts and technically imperfect security mechanisms. At the same time, as the history of hacks shows, the attackers use not only vulnerabilities but also various legitimate capabilities of blockchain to carry out attacks.

This is how hackers attacked Opyn at the start of August, a protocol that ironically claims to deal with DeFi protection. About $371,000 was stolen due to an exploit of the project's native token, whereby a double-spend attack on Ethereum put options was implemented, granting access to users' funds.

Previously, a vulnerability in the smart contract code led to another DeFi project hack where $25 million was stolen from the Lendf.me decentralized lending protocol and decentralized crypto exchange Uniswap. Both sets of developers built their own add-ons on top of the ERC-777 protocol, making the smart contracts vulnerable to reentrancy attacks. During such an attack, hackers withdraw funds repeatedly until their original transaction is approved or rejected.

Another hack occurred on June 28, again because of a code vulnerability. Hackers stole over $500,000 in ETH and other altcoins from the Balancer platform via an exploit of its token deflation mechanism that destroys 1% of the transaction amount upon each funds transfer.

Is Ethereum to blame?

Evidently, the Achilles heel of DeFi projects is bugs and vulnerabilities in the smart contract codes, but what or who exactly to blame for this? Is it the DeFi developers who don't properly test or audit code before launching their apps, or does the fault lie with Ethereum's architecture, meaning that little depends on platforms?

On one hand, as Brian Kerr, CEO of DeFi lending platform Kava Labs, previously told Cointelegraph, the Ethereum blockchain's architecture is not capable of responding to the security demands of the DeFi sector because testing possible bugs is almost impossible in the Solidity programming language.

However, most DeFi platforms are built on the Ethereum blockchain framework and, therefore, are experimenting with the original source code, especially if the result of these experiments is not thoroughly audited before the launch of the product's final version, potentially opening doors for hackers.

Shayan Eskandari, a security engineer and auditor at ConsenSys Diligence, told Cointelegraph that most of DeFi hacks were preceded by changes made by developers shortly prior to

platform launch. For instance, ERC-20 was not implemented in a standard way, or some new token designs added functionalities that changed the behavior of the ERC-20 token, causing unforeseeable issues. According to Eskandari, such changes led to Balancer pool attacks and the Lendf.me hack.

This suggests that in some instances, the teams working on particular platforms are to blame. In a conversation with Cointelegraph, Arnie Hill, CEO of Plutus DeFi — a full-stack DeFi aggregator — noted that most DeFi developers do not pay enough attention to security, as they are at the early stage of product development: "Today developers are paying more attention to the technical side and capitalization, focusing on how to build lending services on blockchain, rather than the security of smart contracts."

Additionally, the complexity of DeFi products plays a cruel joke with them, according to Larry Sukernik, Digital Currency Group investor: "You get people with a big brains that need to be put to work. And when they're put to work, the result is often a complex, brilliant, but massively unusable product."

Charlie Lee, the creator of Litecoin (LTC), previously claimed that decentralization is to blame for everything. Decentralization actually was the reason for the hacking of the Opyn options protocol, as the team could not control or temporarily disable it in the event of an attack.

However, the presence of hackers is a natural occurrence, given that the industry is young. Nevertheless, as the DeFi sector evolves, its developers should become exceedingly aware of the growing security risks and work to reduce them, according to Hill:

> "Scaling the market requires the use of more serious protection mechanisms and cooperation with regulators and auditors. At the end of the day, this is no longer just a network of DApps, but a multi-billion dollar financial market that is at the early stage of its development and, hence, hacks are inevitable, the same as it was with the digital banking industry some years ago."

According to the latest report published by research company Dgen in collaboration with an open-source DeFi protocol Aave, ever since DeFi projects have become hacking targets, the developers began working on sandboxes and clear frameworks for dispute resolution. The analysts also noted that as long as scaling is of highest priority for DeFi developers right now, major hacks similar to the DAO incident of 2016 will likely happen again.

Another possible issue behind decentralized finance projects is that they rely on data oracles

to deliver critical data like asset prices. The accelerating growth of DeFi platforms and products with their unique composability creates interdependencies and requires a solid source of asset pricing data, as explained by Paul Claudius, co-founder of DIA — a Swiss open-source DeFi oracle platform — who told Cointelegraph:

> "Currently, most DeFi projects lack a pricing data solution that is transparent, open-source, and reliable. Many do not even share the methodologies used by oracles for pricing data. This creates substantial risks as bad actors can exploit both the technological and methodological vulnerabilities with unreliable data sources."

Audit, due diligence and insurance

So, is there anything DeFi teams can do to mitigate security risks, given that there are many products that successfully maintain a high level of security for their own and user funds?

Marc Zeller, integration lead at Aave, stressed the importance of conducting due diligence procedures before adding a new token to a DeFi platform to help avoid major hacks within the protocols. He also noted that projects dealing with decentralized finance may use the services of insurance companies to further protect user funds, although this is not always enough.

Speaking about the role of insurance in combating hacks, Kain Warwick, founder of synthetic asset platform Synthetix, said that DeFi insurance is very limited, adding: "DeFi still has significant tail risk, so insurance is likely to remain very costly in the short term, but as protocols mature, costs should come down [...] allowing for simpler and more useful insurance to emerge."

Insurance is good to have if the attack has already happened, but if the task is to prevent it, auditing and tracking suspicious transactions is what DeFi projects need in order to detect and fix vulnerabilities in the network before code flaws are exploited by hackers. Analysts point out that crypto exchanges play a significant role in tracking and locking down cryptocurrencies that may have come from hacked platforms.

Related: The DeFi Hack: What Decentralized Finance Should and Shouldn't Be?

As the industry scales, it's getting increasingly important for DeFi developers to cooperate with regulators and work on both sandboxes and clear frameworks that allow for dispute resolution and arbitration if a hack occurs. According to Hill:

> "Scaling the market requires the use of more serious protection mechanisms and cooperation with regulators and auditors. At the end of the day, this is no longer just a network of DApps, but a multi-billion dollar financial market that is at the early stage of its development."

Will ETH 2.0 bring more security?

Some believe that along with scalability, network upgrades will bring security to DeFi, while others say that Ethereum's 2.0 transition to the proof-of-stake algorithm will put the DeFi sector in even greater danger. Based on research by analyst Tarun Chitra, Dragonfly Capital investor Haseeb Qureshi came to the conclusion that DeFi protocols run counter to the network security mechanism based on the PoS algorithm. The problem is that funds locked in DeFi lending do not participate in staking and, therefore, are a security.

MolochDao analysts confirmed that the move to ETH 2.0 could open up new attack vectors for DeFi applications. However, there is a positive side of it — attacks on ETH 2.0 are easier to scale than attacks on ETH 1.0.

Related: Put to Good Use: Ethereum Racks Up Serious Numbers to Set Benchmarks

Before the rollout, the DeFi industry will face many new attacks, according to Consensys analysts Tanner Hoban and Tom Borgers, especially during the first phases of the transition to Ethereum 2.0. The reason is that at the beginning of the transition, validators must block their ETH until the proof-of-work chain is fully merged with the proof-of-stake chain. This will reduce liquidity and, according to the study authors, can lead to centralization.

So it's likely that DeFi products will face major hacks again, but with the development of insurance and auditing tools, as well as market entry by global regulators, it will eventually become safer. Ethereum 2.0 may add its own fly in the ointment, but with a slow and gradual roll-out of the new model and sufficient testing, the risks are likely to be minimized.

#Blockchain #Ethereum #Hacks #DeFi #Decentralized Finance

RELATED NEWS

Ousting the Greenback: USD Still King as BTC and CBDCs Mount Challenge

TIDAL backs VR universe aiming to change the way we experience culture

Copycats and Copyright: Empowering Content Creators in the Digital Age

Virtual Economies Gear Up the Gravy Train in Blockchain-Based Gaming

MakerDao Brings Bitcoin to the Ethereum Blockchain

Total Value Locked in DeFi Hits New ATH of $4B

Loading