JAN 21
Sherry Fairchok

The dark side of DeFi: Why the SEC wants to level the playing field

Article

What we've noticed: The **decentralized finance (DeFi)** sector of the crypto ecosystem offers exciting opportunities for early adopters. But the newness of the space and relative inexperience of the investors has provided bad actors with a new playground for widespread scamming and theft, according to a report on 2021 crypto crime trends by **Chainalysis**. And regulators are taking notice of DeFi's inherent problems.

What's DeFi? A thriving segment of the crypto sector, DeFi seeks to revolutionize financial services using blockchain-based software instead of centralized intermediaries. This enables crypto-denominated lending outside of traditional banks.

Investors facing historically low or sub-zero interest rates have been drawn to DeFi by the promise of high returns on savings and the hype over successful decentralized tokens like Shiba Inu. Consequently, **DeFi transaction volume grew 912% in 2021**, per Chainalysis.

Today, the DeFi market has **more than $96 billion in total value** locked, DeFi pulse data showed—expanding more than 600% since October 2020.

Data dive: As DeFi grows, so too does its issues with stolen funds, according to Chainalysis and the blockchain forensics company **CipherTrace** (now owned by Mastercard)—which both hold some of the **largest datasets on crypto-crime and blockchain metadata in the world.**

- **Since 2020, users have lost over $12 billion through crime within DeFi apps**, lending platforms, and exchanges, with the vast majority, $10.5 billion, lost coming in 2021 alone, according to a report from London-based blockchain analytics firm **Elliptic**.
- In 2020, just under $162 million worth of crypto was stolen from DeFi platforms, **which was 31% of the year's total amount stolen**. That was a 335% increase from DeFi theft in 2019. **In 2021, that figure rose another 1,330%**, per Chainanalysis.
- **DeFi scams are increasing in number and they have shorter lives.** The average scam ran for 70 days in 2021, Chainalysis found, versus 192 days in 2020.
- Acting US Comptroller of the Currency Michael Hsu told The Blockchain Association in late September that the crypto and DeFi "fool's gold rush" reminded him of the prelude to the 2008 financial crisis. Hsu warned: "**Crypto and DeFi today are on a path that looks similar to [credit default swaps] in the early 2000s**."

What are the risks? DeFi's greatest strength is also its greatest weakness: The ethos of decentralization that makes it so dynamic also allows for scamming and theft. As David Carlisle, director of policy and regulatory affairs at Elliptic, told CNBC: "How do you apply regulatory standards designed for centralized intermediaries to marketplaces where there's no clear centralization?"

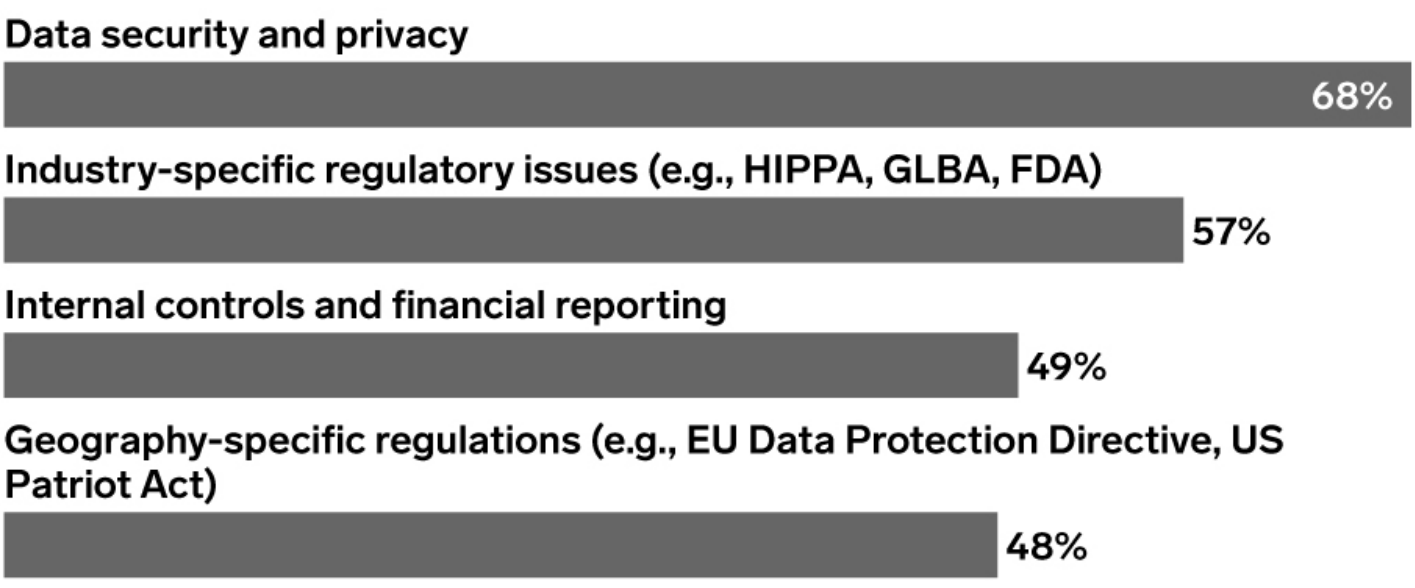
Major DeFi platforms say they bolster security by doing things like hiring external firms to audit code for vulnerabilities and maintaining keys and passwords needed to access user wallets in secure environments. But critics' main concern is that the DeFi market eliminates

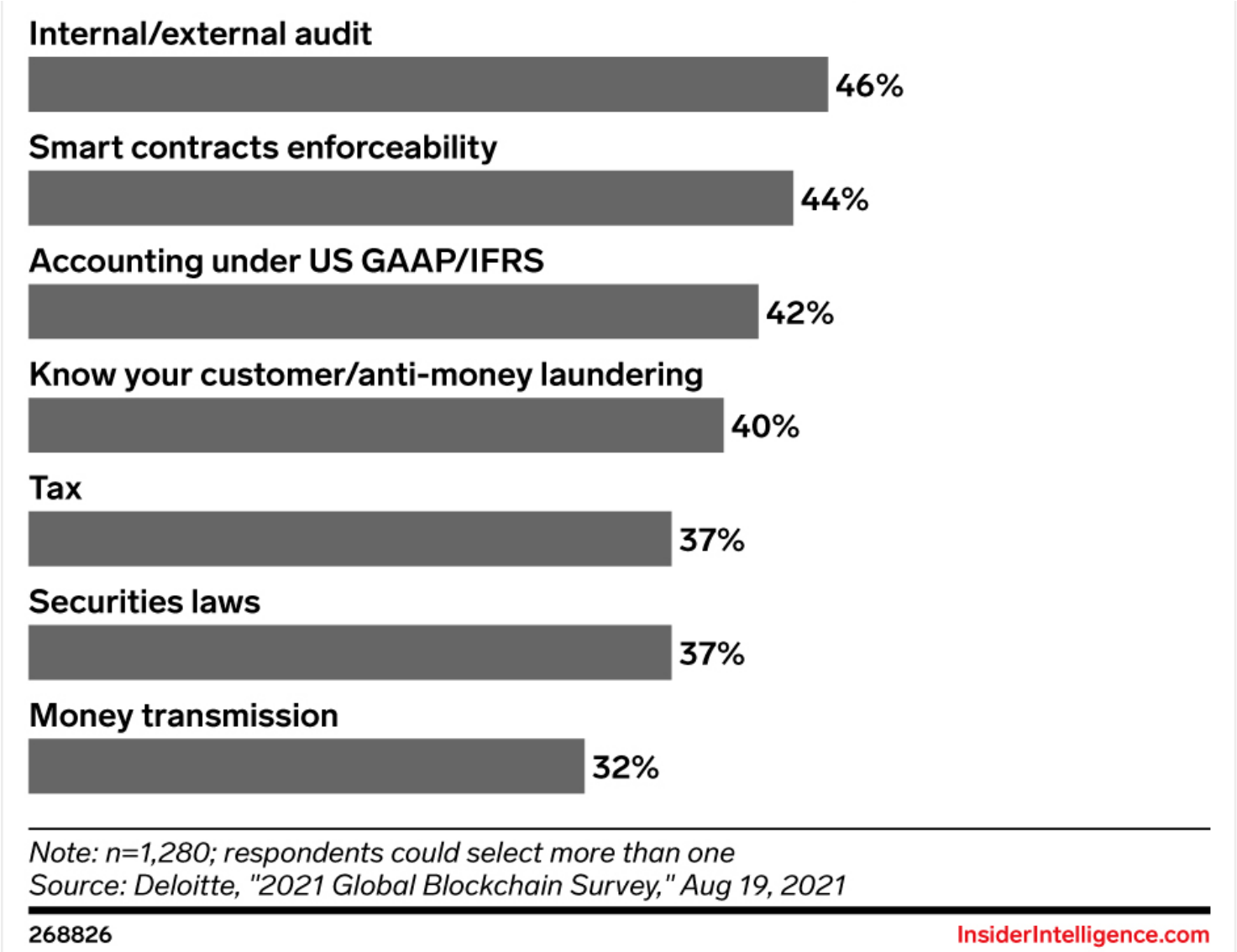
third-party control of users' assets—the same third parties that, in traditional finance, help spot and stop scams.

- Instead of a service provider taking custody of your funds to provide financial services, they're held by a **smart contract**.
- Cryptocurrency transactions and DeFi platforms are "**trustless**"—meaning the two parties in a trade don't have to know or trust each other or rely on a trusted third party like a bank or broker. Insead, they rely on the "immutable, permanent, and unchangeable" blockchain.
- Many DeFi exchanges are governed by protocols that require a majority vote by unknown token holders—which means it can take a week or more to update the protocol. This is a problem when an exploit is letting hackers drain funds and nobody can fix the bug fix until it's over. It also means **there's no personal accountability**—and often no way to block even known scammers, per PYMNTS.

Areas of Regulation Most in Need of Change to Facilitate Adoption of Blockchain and Digital Assets According to Financial Services Executives Worldwide, April 2021

% of respondents





What do regulators want to see fixed? According to the US Securities and Exchange Commission, the DeFi community needs to address two structural problems—indicating the direction its regulatory work will take:

Lack of transparency: DeFi investing is not transparent—creating "a two-tier market" in which professional investors and insiders have a huge advantage over retail investors.

- A relatively small group of people can actually read and understand the publicly available code—and even highly qualified experts miss flaws or hazards.
- Professional investors can afford to hire people like technical experts, engineers, economists and run tests before making an investment decision.

- Retail investors, on the other hand, must get information from marketing, advertising, word of mouth, and social media.
- Decentralization removes the intermediaries that would help screen potential investments, perform risk assessments, and reduce fraud.

Pseudonymity: DeFi markets are vulnerable to difficult-to-detect manipulation.

- Blockchains assign users alphanumeric addresses that obscure their real-world identity when sending or receiving assets.
- And if investors can't determine traders' actual identities, they also can't tell whether asset prices and trading volumes are real or the product of bots operating multiple wallets—or a group of people trading collusively.
- In DeFi, because markets often turn on asset prices, trading volumes, and momentum, investors are vulnerable to losses due to manipulative trading that makes those signals unreliable.

The SEC's objections to opacity and pseudonymity suggest that in the future, it could require DeFi projects to provide information on originators and beneficiaries in the transfer of funds.

What's the solution? DeFi's adoption and growth face an uphill battle if potential users don't feel they can trust new projects. They need to be educated on how to spot and avoid the dubious ones. But "buyer beware" and an ethos of personal responsibility won't be enough to bring DeFi and crypto safely into the mainstream.

The industry needs to self-police until regulations arrive:

- Hsu, speaking to the The Blockchain Association in September, concluded his speech with: "Fortunately, this group has the power to change paths and avoid a crisis."
- And as SEC Commissioner Caroline A. Crenshaw wrote in the International Journal of Blockchain Law: "Developers have an obligation to optimize for more than profitability, speed of deployment, and innovation." She added that they also need to create a fair and equitable "system in which all investors have access to actionable, material data," to reduce the potential for manipulation and other criminal activity.
- In the longer term, DeFi exchanges may also need to figure out how to prevent tokens associated with potentially fraudulent or unsafe projects from being listed on major exchanges.

- Regtechs will play a critical role in this: More than 20 firms offer blockchain analysis and surveillance to identify and thwart bad actors. Aside from Chainalysis, CipherTrace , and Elliptic, notable platforms include **AnChain**, **CertiK**, **Coinfirm**, **TRM Labs**, and others.