5 reasons Web3 is less secure than Web 2.0

Web3 is the blockchain-based version of the Internet. It's the evolution of Web 2.0, focused on making data decentralized.

Besides decentralization, Web3 also boasts improved security compared to Web 2.0. Blockchains are virtually invulnerable, as those blocks are immutable, distributing data across multiple computers.

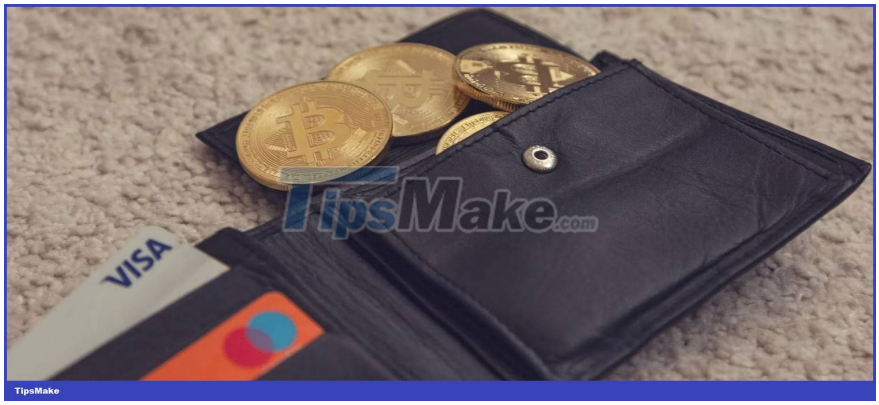
But everything has an exploitable loophole somewhere. Although major database breaches are not common in Web3, threat actors are as active on Web3 as they are on Web 2.0. Except the consequences of a Web3 data breach are even more modest.

So is Web3 as secure as it claims to be? Check it out and see how it is less secure than Web 2.0!

1. Web3 is tokenized with money

Since Web3 relies heavily on cryptocurrencies for transactions, funds are often exchanged for cryptographic tokens to access specific premium services or utilities on Web3. Some of these add-ons cost a lot of money and may or may not be replaceable (NFT). Although Web3 is decentralized in peer-to-peer transactions, the fact that the cryptocurrency is its native currency makes it a target for scammers.

2. You are responsible for managing your property

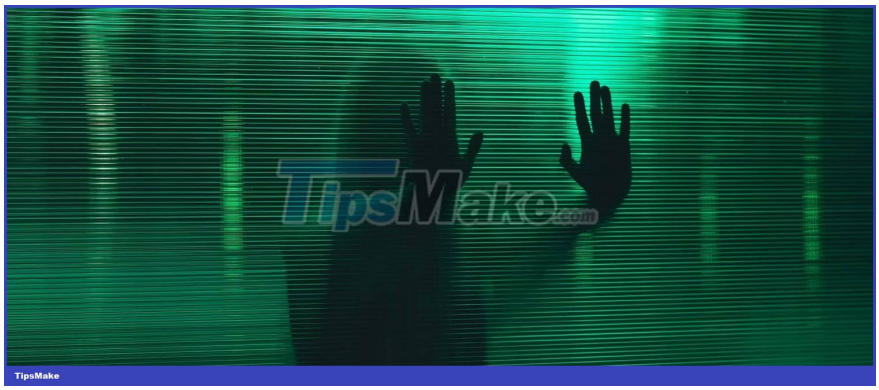


The Web3 decentralization concept implies that you will fully manage your data instead of storing it in a central database. Although this is a more transparent version of Web 2.0, scammers take advantage of it to target users and exploit their vulnerabilities to steal assets from them.

For example, banks have the technical resources to keep your money safe. Even if they lose your money, you can still get a refund. Don't expect an ordinary Internet user to meticulously manage the funds in their digital wallet. Besides, most users don't know which link to click or avoid despite the obvious sign.

Web3 relies on crypto wallets to enable trustless transactions, help users connect to DApps, and exchange assets with other users. You can think of a cryptocurrency wallet as a personal wallet. You are responsible for keeping this account secure - not the bank or any third party. When you lose your wallet or any property stored in it, you will bear the loss alone. Thus, when Web3 tried to close the transparency gap, it opened a loophole that could be exploited through smart contracts.

3. Poor transparency



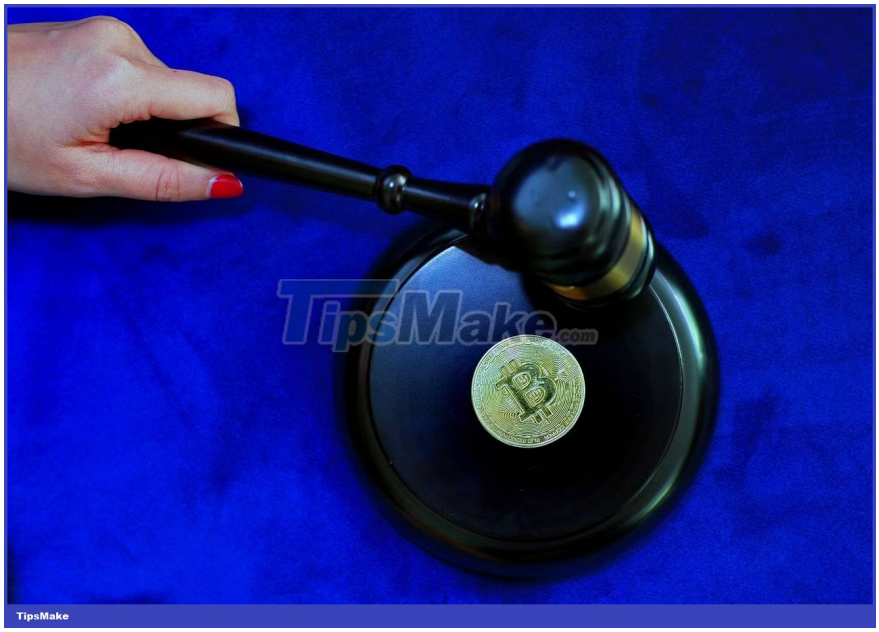
Cryptocurrency transactions have a binding contract that you must sign to agree to. Once signed, you agree that a service may take part of your tokens or assets in the transaction. The transparent contract tells you what you are about to offer. Unfortunately, many ambiguous contracts and algorithms have infected the cryptocurrency, directly affecting Web3.

It's hard to believe that just clicking on a malicious link can wipe your wallet. But it happens a lot in Web3. While hackers may not be able to attack the blockchain that powers Web3, they do leverage Social Engineering to trick gullible users into connecting their wallets to a fake website and signing a fraudulent contract. Bad guys

do this through targeted emails, Discord hacks, or crypto scams on Twitter.

A vivid example of such scams is when hackers visit Bored Ape Yacht Club and OtherSide Discord channels and trick members into clicking on a fake website. More than 145 ETH and 32 NFTs, including blue chips, were stolen in this case.

4. Poor regulation and financial provision



Recently there have been growing concerns about regulations with cryptocurrencies. For instance, the US SEC asserts that cryptocurrencies are not digital assets but financial instruments. The agency has embarked on a crackdown on crypto companies that fail to comply with regulatory frameworks that bind other financial securities.

The action of the SEC may be seen by many as a bit serious. But cryptocurrencies, really, need proper regulation. While condemning the outright bans by regulators, even Changpeng Zhao, CEO of Binance, agrees that cryptocurrencies need risk-based regulation.

Some decentralized exchanges (DeXes) that facilitate cryptocurrency transactions on Web3 also lack adequate redundancy to cover customer withdrawals; this is why cryptocurrency exchange platforms are offering proof of reserve (PoR). In 2022 alone, we have seen many crypto crashes, causing customers to lose money. The Terra/Luna crash and the bankruptcy of FTX are some of the consequences of poor crypto management.

5. Transactions can't be tracked and identity management is poor

Many Web3 transactions are anonymous and untraceable. Unfortunately, threat actors and cybercriminals take advantage of this attribute to commit crimes.

International terrorist financing, ransomware payments, cross-border drug transactions, and many other terrifying financial activities are funded with cryptocurrencies. We have seen many cases of cybercriminals selling ransomware solutions in exchange for cryptocurrency through the dark web.

While this is not the purpose of Web3 or cryptocurrency, it is of international concern as long as criminals use it as a shield to transact money.