Safety experts say bridge cyberattacks will still be a significant concern for DeFi in 2023. The development of decentralised finance (DeFi) has faced significant security challenges. According to statistics from Token Terminal, hackers stole more than $2.5 billion between 2020 and 2022 through flaws in cross-chain bridges. Comparatively speaking, this volume of security breaches is significant. Theo Gauthier, CEO and founder of Toposware, said that all bridge problems stem from an "inherent weakness" that each one of them possesses. No matter how safe a bridge is on its own, based on Gauthier, it is "completely dependant on the safety of the chains it links," which means any flaw or vulnerability inside one of the two chains it links renders the whole bridge susceptible. Bridges try to alleviate the absence of standards amongst protocols by establishing connections between various blockchains. It is thought that achieving interoperability between blockchains will significantly improve user experience and encourage wider use of cryptocurrencies. Even with the bear market, ideas for interoperability and safety in the cryptocurrency sector are gaining ground. For example, zero-knowledge proofs (ZKPs), one of the most important existing technologies, take information to be validated and certified as true without disclosing further data, in contrast to usual interoperability ideas that demand networks to expose their states.

Disclaimer

The information on this website is provided for educational and informational purposes only. Any action taken by readers based on the information contained on our website is entirely at their own risk.

- **Source: www.pipsafe.com – cyberattacks**
- www.bitcoin.org
- **What is Bitcoin?**
- **What is Ethereum?**