Best Practices for Limiting Liability Arising from Smart Contract Vulnerabilities

Jared Butcher, writing in the **Steptoe Blockchain Blog**, says it is no secret that smart contracts have vulnerabilities, but he suggests a mix of best practices to limit potential liabilities that may arise when vulnerabilities interfere with smart contract performance.

“There is potential for manipulation by insiders, which is of particular concern for smart contracts that operate based on ‘proof of stake’ protocols, given the ongoing concerns that those protocols will not be effective in ensuring that the parties play by the rules,” Butcher writes. “Even without intentional interference by hackers or insiders, smart contracts may have software bugs that disrupt performance, and there is the possibility of unintended outcomes if the smart contract’s code fails to anticipate an unusual situation.”

In the post, he offers six best practices to consider when implementing a smart contract.

Read the article.

Join Our LinkedIn Group