When Smart Contracts are Outsmarted: The Parity Wallet "Freeze" and Software Liability in the Internet of Value

The recent Parity wallet "freeze" provides yet another example of a coding vulnerability in a smart contract (rather than a flaw in the underlying blockchain or cryptography) resulting in an exploit that compromises cryptocurrency worth millions, according to Proskauer Rose LLP's **Blockchain and the Law**.

Wai Choy and **Pengtao Teng** write: "It again highlights some of the pitfalls of insecure code in the context of digital assets and raises questions regarding the extent to which software developers can be held liable to its users for losses suffered due to those oversights. As blockchain-related software that serve as storage vaults for digital assets continue to proliferate, it will be interesting to see how industry standards and the existing software liability regime in the U.S. and other jurisdictions evolve to reflect the critical role of secure software in the 'Internet of Value.'"

Read the article.