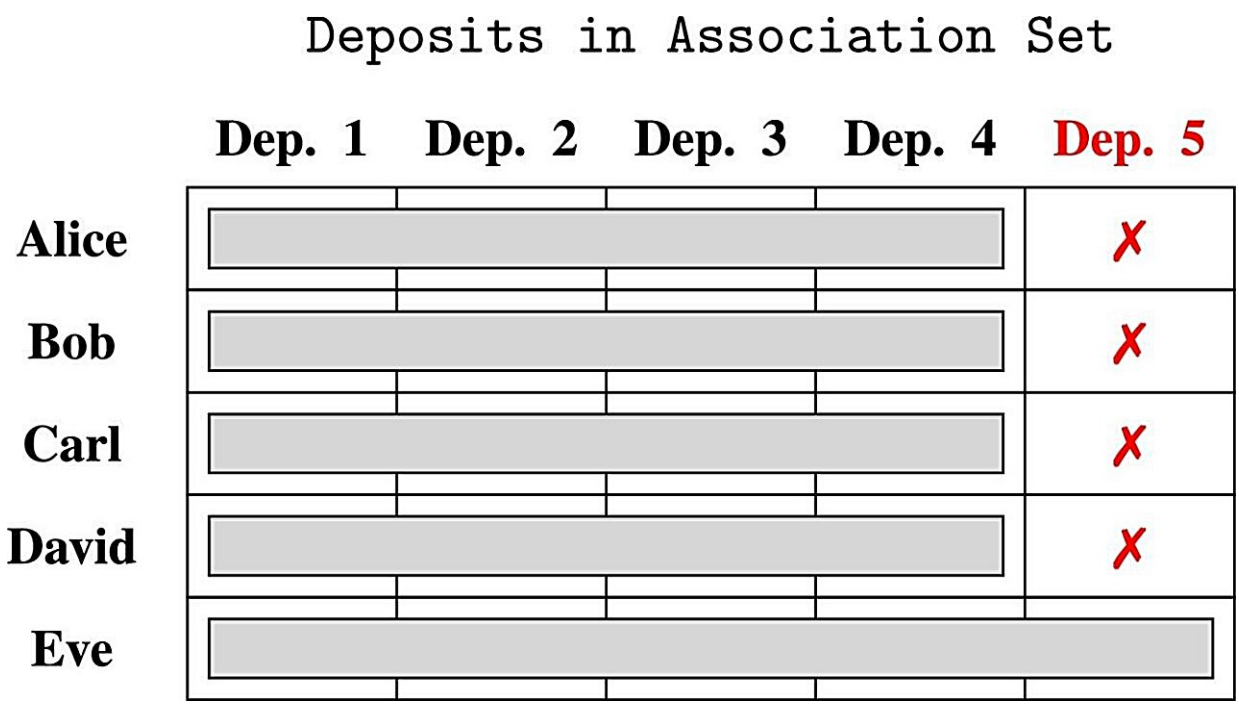
Innovative blockchain technology balances privacy with regulatory compliance

February 27 2024



In our simplified example, we assume that Alice, Bob, Carl and David include all other "good" deposits in their respective association sets and exclude deposit 5, that originates from a known illicit source. Eve, on the other hand, cannot create a proof that disassociates her withdrawal from her own deposit. Credit: TranSpread

In a recent study published in *Blockchain: Research and Applications*, researchers have developed a protocol called Privacy Pools that enhances

privacy on blockchain transactions while complying with regulatory standards.

This new smart contract-based protocol enables users to prove specific attributes of their transactions without exposing their entire history, maintaining both privacy and transparency.

The Privacy Pools protocol introduces a novel approach by allowing users to publish zero-knowledge proofs. These proofs confirm whether their funds are associated with lawful or unlawful sources without revealing their entire transaction history. This method involves proving membership in pre-defined association sets, aligned with regulatory frameworks, thus separating compliant from non-compliant transactions.

"This study offers a promising approach to reconciling the seemingly conflicting goals of blockchain privacy and regulatory compliance," said Dr. Fabian Schär, the corresponding author of this article. "By enabling users to prove compliance without revealing their entire transaction history, Privacy Pools could pave the way for a more privacy-preserving and inclusive blockchain ecosystem."

The Privacy Pools protocol offers a pragmatic solution to the long-standing challenge of maintaining privacy in blockchain transactions while meeting regulatory requirements. This innovation not only enhances user privacy but also strengthens the integrity and trustworthiness of blockchain technology. It demonstrates that privacy and regulatory compliance can coexist, paving the way for more secure and private financial transactions in the digital age.

More information: Vitalik Buterin et al, Blockchain privacy and regulatory compliance: Towards a practical equilibrium, *Blockchain: Research and Applications* (2023). DOI: 10.1016/j.bcra.2023.100176

Provided by TranSpread