World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:18, No:03, 2024

Zero-Knowledge Proof-of-Reserve: A Confidential Approach to Cryptocurrency Asset Verification

Authors : Sam Ng, Lewis Leighton, Sam Atkinson, Carson Yan, Landan Hu, Leslie Cheung, Brian Yap, Kent Lung, Ketat Sarakune

Abstract : This paper introduces a method for verifying cryptocurrency reserves that balances the need for both transparency and data confidentiality. Our methodology employs cryptographic techniques, including Merkle Trees, Bulletproof, and zkSnark, to verify that total assets equal or exceed total liabilities, represented by customer funds. Importantly, this verification is achieved without disclosing sensitive information such as the total asset value, customer count, or cold wallet addresses. We delve into the construction and implementation of this methodology. While the system is robust and scalable, we also identify areas for potential enhancements to improve its efficiency and versatility. As the digital asset landscape continues to evolve, our approach provides a solid foundation for ensuring continued trust and security in digital asset platforms.

Keywords : cryptocurrency, crypto-currency, proof-of-reserve, por, zero-knowledge, ZKP
Conference Title : ICAC 2024 : International Conference on Applied Cryptography
Conference Location : Taipei, Taiwan
Conference Dates : March 04-05, 2024