World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:19, No:08, 2025

A Contribution to Blockchain Privacy

Authors : Malika Yaici, Feriel Lalaoui, Lydia Belhoul

Abstract : As a new distributed point-to-point (P2P) technology, blockchain has become a very broad field of research, addressing various challenges including privacy preserving as is the case in all other technologies. In this work, a study of the existing solutions to the problems related to private life in general and in blockchains in particular is performed. User anonymity and transaction confidentiality are the two main challenges for the protection of privacy in blockchains. Mixing mechanisms and cryptographic solutions respond to this problem but remain subject to attacks and suffer from shortcomings. Taking into account these imperfections and the synthesis of our study, we present a mixing model without trusted third parties, based on group signatures allowing reinforcing the anonymity of the users, the confidentiality of the transactions, with minimal turnaround time and without mixing costs.

Keywords : anonymity, blockchain, mixing coins, privacy
Conference Title : ICCSPS 2025 : International Conference on Computer Science, Programming and Security
Conference Location : Vancouver, Canada
Conference Dates : August 05-06, 2025