F F E R R T T R S

Proof-of-Work (PoW) is one of the fundamental and widely used consensus algorithms in blockchains. In PoW, nodes compete to receive the mining reward by trying to be the first to solve a puzzle. Despite its fairness and wide availability, traditional PoW incurs extreme computational and energy waste over the blockchain. This waste is considered to be one of the biggest problems in PoW-based blockchains and cryptocurrencies. In this work, we propose a new useful PoW that mitigates the energy waste by incorporating-pre computed (disclosable) randomness into the PoW. The key idea is to inject special randomness into puzzles via (way) algebraic commitments that can be stored and later publicly disclosed. Unlike the traditional PoW which is wasteful, our apach enables pre-computed commitments to be utilized by a vast array of public key cryptography methods that require offline-online processing (e.g., digital signature, key exchange, zero knowledge protocol). Moreover, our PoW preserves the desirable properties of the traditional PoW and therefore does not require a substantial alteration in the underlying protocol. We formally proved the security of our PoW and then fully implemen (tion)3.3 J.4 (l)3.3 (m)3.4 7.3 (o)-3.say b)0 capabilities.We will also talk about our performance analysis of the Traee protocol which leverages accumulator schemes used in Blockchain settings.

Friday, November 20, 2020
4:00pm
Online, Microsoft Teams
Please email efe3@usf.edu for more information

THE PUBLIC IS INVITED

Examining Committee
Attila A. Yavuz, Ph.D., Major Professor
Nasir Ghani, Ph.D.
Mehran Mozaffari Kerman, Ph.D.
Jay Ligatti, Ph.D.
Kaiqi Xiong Ph.D.

Sudeep Sarkar, Ph.D.
Department Chair
Computer Science and Engineering
College of Engineering

Computer Science and Engineering
College of Engineering

R S TT R