Tree-Proof-of-Position: Enhancing security, privacy and decentralisation in Web3 applications

Aida Manzano Kharman (Imperial College)

Abstract: We present a novel class of proof-of-position algorithms: Tree-Proof-of-Position (T-PoP). This algorithm is decentralised, collaborative and can be computed in a privacy preserving manner, such that agents do not need to reveal their position publicly. We make no assumptions of honest behaviour in the system, and consider varying ways in which agents may misbehave. Our algorithm is therefore resilient to highly adversarial scenarios. This makes it suitable for a wide class of applications, namely those where trust in a centralised infrastructure may not be assumed, Web3 applications, or high security risk scenarios. It serves as a future alternative in Distributed Ledger Technologies to replace proof-of-work or proof-of-stake access with proof-of-position instead. We also provide a mathematical model that summarises T-PoP's performance for varying operating conditions. We then simulate T-PoP's behaviour with a large number of agent-based simulations, which are in complete agreement with our mathematical model, thus demonstrating its validity. T-PoP can achieve high levels of reliability and security by tuning its operating conditions, both in high and low density environments. Finally, we also present a mathematical model to probabilistically detect platooning attacks.