Análisis de Estabilidad y Seguridad de protocolos de consenso descentralizados para criptomonedas basadas en blockchain (Proof of Stake): el Ejemplo de Algorand

Nombre: Esteban Mocskos

Filiación: Departamento de Computación, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires y Centro de Simulación Computacional p/Aplic Tecnológicas (CSC-CONICET).

Resumen:

En los últimos años, con el auge del mundo de las criptomonedas, entró en debate el derroche energético de las redes de Proof of Work como Bitcoin, y ganaron importancia aquellas que implementan protocolos de consenso basados en Proof of Stake. En ellas, la participación en las decisiones de la red está determinada por la cantidad de stake que tiene cada cuenta. De esta manera, se puede resolver el problema de lograr el consenso de manera descentralizada sin tener que usar grandes cantidades de recursos computacionales. En esta charla vamos a mostrar algunos resultados obtenidos al analizar la plataforma Algorand, una de las plataformas más populares que utilizan Proof of Stake. El objetivo fue experimentar con su estabilidad y adaptación a cambios en la topología física de la red, creando potenciales vectores de ataque. También nos enfocamos en intentar reconstruir la topología lógica de la red para intentar exponer aquellos nodos con mayor cantidad de stake, los cuales serían los objetivos más interesantes para un ataque. Para esto impusimos como restricción solo utilizar los mensajes que circulan por la red sin inyección de tráfico adicional.