A Survey on Long-Range Attacks for Proof of Stake Protocols

Revolusioner Bitcoin yang membuatnya terkenal di seluruh dunia, ada jauh lebih banyak potensi dari teknologi yang mendasarinya. Nakamoto menggunakan primitif kriptografi yang kuat untuk memperkenalkan menghasilkan teknologi blockchain, peer-to-peer terdistribusi. Prevalensi teknologi blockchain, dalam hal keamanan, privasi, dan kekekalan, pada kenyataannya, beberapa serangan dapat diluncurkan terhadap mereka.

Literatur sistematis tentang serangan jarak jauh untuk bukti protokol pasak. Jika berhasil, serangan ini dapat mengambil alih rantai utama dan sebagian, atau bahkan seluruhnya, menulis ulang riwayat transaksi yang disimpan di blockchain. Untuk tujuan ini, kami menjelaskan cara kerja protokol bukti pasak, fundamentalnya properti, kekurangannya, dan permukaan serangannya. Setelah menghadirkan serangan jarak jauh, kami membahas kemungkinan penanggulangan dan penerapannya.

blockchain ini didasarkan pada concept of Proof of Work (PoW). Secara praktis, kami menganggap pengguna dapat dipercaya karena dia menghabiskan banyak uang upaya komputasi untuk memverifikasi beberapa transaksi. Sebaliknya protokol Proof of Stake (PoS), pengguna yang validasi transaksi yang dipilih berdasarkan kekayaan (stake).

Serangan Jarak Jauh yang berhasil tidak hanya akan mengubah beberapa blok tetapi akan memungkinkan musuh untuk sepenuhnya menulis ulang sejarah semua transaksi yang disimpan dalam blockchain. Seperti dimaklumi, serangan ini mungkin tidak berasal dari implementasi protokol tertentu, tetapi dari desainnya, membuatnya agak sulit untuk ditambal.

Tindakan pencegahan ini dapat memberikan perlindungan penuh dari semua ancaman tersebut. Bahkan lebih solusi yang diusulkan bersifat parsial untuk setiap ancaman secara individual. Terlepas dari timestamping dan mengintegrasikan rantai terpanjang aturan dan pos pemeriksaan bergerak yang tampaknya terintegrasi oleh semua protokol, ada keragaman dalam integrasi sisanyapenanggulangan dari protokol. Sedangkan penggunaan TEE sangat menjanjikan, mereka tidak diterapkan oleh salah satu dari protokol sebagai adopsi mereka menyiratkan kendala perangkat keras.