Majority is not Enough: Bitcoin Mining is Vulnerable

INTRO

Keamanannya bitcoin sangat bergantung pada distribusiprotokol yang memelihara blockchain, protokol tersebut dijalankan oleh pekerja yang disebut penambang. Kebijakan konvensional menegaskan bahwa protokol tersebut kompatibel dengan insentif dan aman dari kelompok minoritas yang berkolusi, yaitu dengan cara memberi insentif kepada penambang untuk mengikuti protokol yang telah ditentukan.

PERMASALAHAN

Pada paper ini menunjukkan bahwa protokol Bitcoin tidak kompatibel dengan insentif. paper menghadirkan serangan penambang yang berkolusi memperoleh pendapatan yang lebih besar daripada bagian mereka yang adil/jujur. Ide kunci di balik strategi serangan ini disebut Selfish Mining, selfish mining adalah kolam untuk menjaga blok yang ditemukan tetap pribadi, sehingga dengan sengaja memotong rantai publik. Ketika cabang publik mendekati cabang kolam pribadi, para penambang egois mengungkapkan blok dari rantai pribadi mereka ke publik.

CARA SERANGAN

Strategi ini membuat penambang jujur yang mengikuti protokol Bitcoin menjadi sia-sia sumber daya untuk menambang cryptopuzzles yang akhirnya tidak berguna. Analisis paper ini menunjukkan bahwa, sementara pihak yang jujur dan egois menyianyiakan beberapa sumber daya, penambang yang jujur membuang lebih banyak secara proporsional dan hadiah kumpulan penambang egois melebihi bagiannya dari kekuatan penambangan jaringan, hal tersebut memberi penambang egois keuntungan kompetitif dan memberi insentif kepada penambang rasional untuk bergabung dengan kumpulan penambangan yang egois.

AKIBAT SERANGAN

Serangan ini dapat memiliki konsekuensi yang signifikan untuk Bitcoin:

1. Penambang rasional akan lebih suka bergabung dengan penambang egois, dan kelompok yang berkolusi akan bertambah besar sampai menjadi mayoritas.

2.Pada ini titik, sistem Bitcoin tidak lagi menjadi mata uang yang terdesentralisasi.

3. Penambangan yang egois dapat dilakukan untuk semua ukuran kelompok penambang yang berkolusi.

SOLUSI

Paper ini mengusulkan perubahan sederhana yang kompatibel dengan protokol Bitcoin untuk mengatasi masalah ini dan meningkatkan ambang batas ketika seorang penambang belajar cabang yang bersaing dengan panjang yang sama, itu harus menyebarkan semuanya, dan pilih yang mana untuk ditambang secara seragam secara acak.

Setiap penambang yang menerapkan perubahan akan mengurangi kemampuan kumpulan penambang egois untuk meningkatkan nilai Y melalui kontrol propagasi data, Peningkatan ini bersifat independen adopsi perubahan di penambang lain, oleh karena itu tidak memerlukan "hard fork", Perubahan kami secara eksplisit mengacak pilihan sewenang-wenang ini, dan karena itu tidak memperkenalkan kerentanan baru.