La sicurezza della chiave privata

Esistono 2^256 diverse possibili combinazioni di chiavi private e 2^160 diverse combinazioni di possibili indirizzi. Questo significa che per ogni indirizzo esistono approssimativamente (2^256)/(2^160)= 2^96 chiavi private. Conoscendo un indirizzo o indovinandone uno fra i 2^160 possibili è possibile appropriarsi dei suoi bitcoin se si scopre una fra le approssimativamente 2^96=7.922816251×10^28 chiavi private associate a quell'indirizzo sulle 2^256 chiavi esistenti. Lavoro tutt'altro che semplice se si pensa che 2^96 è una minuscola frazione di 2^256, all'incirca è lo 0,000…(50 zeri)..001%.

Per cercare di avere un'idea molto approssimativa di queste grandezze, si pensi che tutti i granelli di sabbia su tutte le spiagge della terra sono 2^63 (secondo una stima molto grossolana), mentre gli atomi dell'universo fra i 10^72 e 10^87 (vedi **qui**), ovvero fra circa 2^240 e 2^280. Quindi possiamo vedere i granelli di sabbia come il numero di chiavi private esistenti per ciascun indirizzo e il totale degli atomi dell'universo come il numero di chiavi private possibili. Perciò, data una chiave pubblica, abbiamo la stessa probabilità di aprirla che avremmo di incontrare un granello di sabbia della terra vagando in modo del tutto casuale fra i miliardi di miliardi di galassie nell'universo e soffermandoci a controllare ogni atomo. Dovremmo inoltre sperare di trovare tale granello in tempo utile (nell'arco di una vita umana) per goderci i bitcoin rubati, e dobbiamo tenere in conto che vagare così per l'universo ci costa parecchia energia elettrica da utilizzare come potenza di calcolo della nostra astronave (la potenza computazionale del computer). Se avessimo un computer che riesce a controllare un miliardo di miliardi di atomi al secondo (10^18) e lavorasse nel tempo per

un miliardo di miliardi di secondi (10^18), ovvero molti milioni di miliardi di anni, non riuscirebbe comunque a controllare tutti gli atomi ma solo 10^36 atomi, che è una cifra minuscola rispetto a 10^72. Se venisse inventato un supercomputer di eccezionale potenza (che controlli ogni atomo a incredibile velocità) lo script OP_HASH256 previsto dal protocollo bitcoin può comunque aumentare il numero di indirizzi possibili, diminuendo il numero di possibili chiavi private associate a ciascun indirizzo e dunque la probabilità di individuarle. Se infatti gli indirizzi fossero, per esempio, 2^256, tanti quanti le chiavi private, si dovrebbe trovare quella singola chiave privata associata alla chiave pubblica che vogliamo aprire, senza avere la possibilità di indovinarne una a caso fra le 2^96 disponibili.