Kontrowersyjna propozycja zamrożenia bitcoinów

13 grudnia 2024

Świat kryptowalut został wstrząśnięty niedawną propozycją Emina Güna Sirera, założyciela i dyrektora generalnego Ava Labs, który zasugerował radykalne rozwiązanie dotyczące bitcoinów należących do tajemniczego twórcy tej kryptowaluty. Sirer przedstawił pomysł zamrożenia około 1,1 miliona BTC przypisywanych Satoshiemu Nakamoto, argumentując to potencjalnym zagrożeniem ze strony rozwoju komputerów kwantowych.

U podstaw tej kontrowersyjnej propozycji leży techniczny aspekt wczesnych transakcji bitcoinowych. Pierwsze wydobyte bitcoiny wykorzystywały system Pay-to-Public-Key (P2PK), który według ekspertów może być podatny na ataki z wykorzystaniem komputerów kwantowych. Ta przestarzała metoda, stosowana przez Satoshiego Nakamoto w początkowych latach istnienia bitcoina, bezpośrednio ujawnia klucz publiczny, co teoretycznie mogłoby zostać wykorzystane przez zaawansowane systemy obliczeniowe przyszłości.

Rozwój technologii kwantowej stanowi coraz bardziej realne wyzwanie dla obecnych systemów kryptograficznych. Komputery kwantowe wykazują szczególną skuteczność w rozwiązywaniu określonych problemów matematycznych, w tym w faktoryzacji dużych liczb, co może stanowić zagrożenie dla tradycyjnych metod szyfrowania, takich jak RSA czy kryptografia krzywych eliptycznych. Jednak eksperci podkreślają, że nie wszystkie aspekty bezpieczeństwa kryptowalut są jednakowo zagrożone.

Społeczność kryptowalutowa zareagowała na propozycję Sirera z mieszanymi uczuciami. Podczas gdy niektórzy dostrzegają w niej próbę zabezpieczenia przyszłości bitcoina, inni uważają ją za sprzeczną z fundamentalnymi zasadami cryptocurrency. Krytycy

wskazują, że sama idea zamrażania środków podważa podstawową koncepcję zdecentralizowanych walut cyfrowych, która opiera się na nienaruszalności własności prywatnej.

Znaczące jest to, że nowoczesne portfele bitcoin już nie korzystają z podatnego systemu P2PK, co oznacza, że problem dotyczy głównie najstarszych transakcji w sieci. Sam Sirer zauważył, że współczesne rozwiązania, w tym te wykorzystywane przez platformę Avalanche, są znacznie lepiej zabezpieczone przed potencjalnymi zagrożeniami kwantowymi.

Eksperci w dziedzinie kryptografii zwracają uwagę, że mimo imponujących postępów w rozwoju komputerów kwantowych, obecne zagrożenie dla kryptowalut pozostaje stosunkowo niewielkie. Wskazują oni na dwa kluczowe czynniki: po pierwsze, komputery kwantowe mają ograniczone możliwości w zakresie odwracania funkcji skrótu, które są fundamentalne dla protokołów kryptowalutowych. Po drugie, potencjalny atakujący miałby bardzo wąskie okno czasowe na przeprowadzenie skutecznego ataku.

Propozycja zamrożenia bitcoinów Satoshiego wywołała również dyskusję na temat przyszłości kryptowalut w erze komputerów kwantowych. Vitalik Buterin, współzałożyciel Ethereum, również włączył się do debaty, podkreślając znaczenie rozwoju odpornych na kwantowe ataki rozwiązań kryptograficznych.

Źródło: ZmianyNaZiemi.pl