Stworzono pierwszy na świecie kwantowy blockchain

28 maja 2017

Fizycy z Rosyjskiego Centrum Kwantowego stworzyli i przetestowali pierwszy na świecie „kwantowy blockchain" – nierozerwalny system rozproszonego przechowywania danych, chroniony przy pomocy metod kryptografii kwantowej i opublikowali instrukcję jego montażu w bazie elektronicznej arXiv.org

Pomysł stworzenia blockchainów – chronionych baz danych, w których każdy blok jest połączony ze wszystkimi innymi częściami bazy i nie może być zmieniony ani naruszony, pojawił się już dość dawno, około 30 lat temu. Mimo perspektyw tego pomysłu pierwsze swoje zastosowanie znalazł stosunkowo niedawno, w 2008 roku, kiedy została stworzona pierwsza na jego podstawie kryptowaluta – bitcoin.

Takie systemy obecnie przyciągają uwagę finansistów i ekspertów w dziedzinie bezpieczeństwa danych, ponieważ blockchain pozwala bezpiecznie gromadzić rejestr wszystkich transakcji i operacji walutowych bez obaw o włamanie. To według ekspertów pozwala obniżyć koszty ochrony banków przed włamaniem i pozwoli rozwiązać spory prawne między graczami na rynku w „automatycznym" porządku.

Oprócz samej architektury blockchainów, gwarantem tego jest to, że blockchain jest rozproszonym systemem – stale aktualizujące się kopie bazy danych są dostępne na komputerach wszystkich użytkowników i „nielegalne" zmiany w jednej z nich zostaną szybko wykryte i tłumione.

Komputery kwantowe, jak mówią Aleksiej Fiodorow i jego współpracownicy z Rosyjskiego Centrum Kwantowego, będą mogły obejść obie te przeszkody w przyszłości – ich niemal nieograniczone moce obliczeniowe pozwolą przestępcom podrabiać

podpisy elektroniczne, którymi podpisane są transakcje w blockchainie i niepostrzeżenie dokonywać w nim zmian lub nie pozwalać innym członkom sieci na jego używanie.

Aby rozwiązać ten problem Fiodorow i jego współpracownicy stworzyli własną wersję blockchainu, która umożliwia wykorzystanie kryptografii kwantowej i systemu kwantowego przekazu danych w celu ochrony tych baz danych przed włamaniem.

W jej ramach kwantowe kanały łączności, zabezpieczone przed włamaniem, są wykorzystywane do przesyłania danych o tych transakcjach, które są właśnie dokonywane. Kiedy wszyscy uczestnicy blockchainu otrzymają informacje o przygotowywanych transferach informacji lub przekazów pieniężnych, oni sprawdzają wiarygodność ich uczestników i wspólnie decydują, czy warto wprowadzić je do bazy, parami porównując otrzymane wartości między sobą.

Takie podejście, jak zauważają autorzy artykuły, chroni blockchain tylko przed pewnymi „nieuczciwymi" uczestnikami transakcji, którzy wysyłają sprzeczne dane do różnych członków sieci, ale nie gwarantują też pełnej ochrony przed pełnym przejęciem sieci i podrobieniem całej bazy. Z drugiej strony, według fizyków, takie włamanie do blockchainu jest niezwykle trudnym i praktycznie nierozwiązywalnym zadaniem, ponieważ wymagałoby to przechwycenia znacznej części uczestników sieci.

Jak mówią naukowcy, dany blockchain został przetestowany na niedawno stworzonej trójwęzłowej sieci kwantowej pomiędzy oddziałami „Gazprombanku" w Moskwie. Wszystkie próby „intruza", którego rolę odgrywał jeden z uczestników sieci, wprowadzenia fałszywych transakcji do bazy danych nie powiodły się, co potwierdziło działanie blockchainu.

„Według prognoz ekspertów na podstawie blockchainów w połowie lat 2020. powstawać będzie około 62 bilionów dolarów usług. Przy tym efekt naszego opracowania może wielokrotnie

powiększyć objętość rynku. Ważne jest również to, że ta technologia została opracowana i po raz pierwszy przetestowana w Rosji w warunkach rzeczywistych" – podsumowują Fiodorow i jego współpracownicy.

Źródło: pl.SputnikNews.com